Microsoft Exchange Server 2010 Service Pack 3

Официальная документация компании Microsoft.
Дата выхода: март 2013г.

Подготовил Pavel Nagaev.
Последнюю версию документации в PDF вы найдете на сайте
http://www.exchangeFAQ.ru

Создано:12.04.2013, 15:44

* В данной версии отстутсвует подробная информация по командлетам PowerShell

Table of Contents

1 Exchange Server 2010

Exchange Server 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-12-11*

Welcome to Microsoft Exchange Server 2010 Service Pack 2 (SP2)! We know you're eager to get started, but there are a few things you should be aware of before you start working with Exchange 2010 and using this content.

- If you want a quick overview of what's new in Exchange 2010 SP2, check out What's New in Exchange 2010 SP2.
- If you want to learn more about Exchange 2010, check out the Exchange 2010 TechCenter.
- To get started with Exchange 2010, head for Planning and Deployment. It lays out the recommended sequence for preparing for and then installing Exchange 2010, and it includes the following important topics:
  - Exchange 2010 System Requirements
  - Exchange 2010 Prerequisites
  - Exchange 2003 - Planning Roadmap for Upgrade and Coexistence
  - Exchange 2007 - Planning Roadmap for Upgrade and Coexistence
  - Understanding a New Installation of Exchange 2010
  - Install Exchange 2010 Using the Custom Installation Type
  - Understanding Upgrade to Exchange 2010
  - Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3

Exchange 2010 Help

The Help content for Exchange 2010 consists of the following top-level categories:

- Getting Started With Exchange 2010
- Planning and Deployment
- Permissions
- Exchange Management Console
- Exchange Management Shell
- Client Access
- Transport
- Mailbox
- Unified Messaging
- High Availability and Site Resilience
- Messaging Policy and Compliance
- Federation
- Hybrid Deployments
- Multi-Tenant Support
- Performance and Scalability
- About Exchange Documentation

Download the Exchange 2010 SP2 Help File

Looking for an offline version of this Exchange 2010 SP2 Help content? Download the Help file from the Microsoft Download Center.

Note:

Haven't upgraded to Exchange 2010 SP2? You can also download the Help file for previous versions of Exchange.

- Exchange 2010 SP1 Help

- Exchange 2010 RTM Help

Tell us what you think

If you have comments or questions about our topics or about the overall Help experience, we'd love to hear from you. Your feedback will help us provide the most accurate and concise content. There are a couple ways to provide feedback:

- Use the **Click to Rate and Give Feedback** link at the top of any topic. Feedback generated here is sent directly to the Exchange team for review and follow up.
- Add comments or content to the **Community Content** section located at the bottom of any topic. Content here will be seen by anyone viewing the topic.

1.1 Getting Started With Exchange 2010

Getting Started With Exchange 2010

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-28*

Microsoft Exchange Server 2010 Service Pack (SP2) can help you achieve better business outcomes while controlling the costs of deployment, administration, and compliance. Exchange delivers a wide range of deployment options and advanced compliance capabilities.

For more information about Exchange 2010, see Exchange 2010 Overview.

Using Exchange 2010 Help

Exchange 2010 SP2 Help content is organized by feature set. Use the top-level nodes to find the most appropriate Help topics when you're planning, deploying, or managing your Exchange 2010 organization.

Looking for an offline version of this Exchange 2010 SP2 Help content? Download the Help file from the Microsoft Download Center.

Note:

Haven't upgraded to Exchange 2010 SP2? You can also download the Help file for previous versions of Exchange.

- Exchange 2010 SP1 Help
- Exchange 2010 RTM Help

For a discussion of the new features in Exchange 2010 SP2, see What's New in Exchange 2010 SP2.

For a detailed roadmap that helps you get acquainted with all the features in Exchange 2010, see Roadmap for Exchange Features.

New to Exchange?

Before deploying Exchange 2010, your existing infrastructure must meet certain prerequisites. To help you plan the deployment of Exchange 2010 into your production environment, read Planning for Exchange 2010.

Upgrading from Exchange 2007?

Before you go too far in your planning for Exchange 2010, make sure your current Exchange Server 2007 organization meets the requirements for upgrading. To learn about planning considerations and configuration steps for upgrading from Exchange 2007 to Exchange 2010, read Exchange 2007 - Planning Roadmap for Upgrade and Coexistence.

Upgrading from Exchange 2003?

You can deploy Exchange 2010 in an existing Exchange Server 2003 organization that's operating in native mode. Coexistence between these two versions is supported. To learn about planning considerations and configuration steps for deploying Exchange 2003 and Exchange 2010 in a coexistence scenario, read Exchange 2003 - Planning Roadmap for Upgrade and Coexistence.

Moving to the cloud?

Exchange 2010 SP2 offers organizations the ability to extend the feature-rich experience and administrative control they have with their existing on-premises Exchange 2003, Exchange 2007, or Exchange 2010 organization to the cloud via a hybrid deployment. Hybrid deployments provide the seamless look and feel of a single Exchange organization between an on-premises organization and a cloud-based organization. In addition, hybrid deployments can serve as an intermediate step to moving completely to a cloud-based Exchange organization. For more information, see Hybrid Deployments.

1.1.1 Exchange Server 2010 Documentation Updates

Exchange Server 2010 Documentation Updates

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-02-04*

In response to the feedback we get from you, our customers, the Exchange Server documentation team is pleased to announce the following additions and changes to our content.

January 2013

- **New Content**

  Determine the Exchange Schema Version
  Understanding the Impact of Named Property and Replica Identifier Limits on Exchange Databases

- **Updated Content**

Account Information
Configure the Availability Service for Cross-Forest Topologies
Create a Managed Custom Folder
Determine the Exchange Schema Version
Discontinued Features
Exchange Server Supportability Matrix
HTTP Connectivity with Autodiscover - Unexpected Exception
Implement a Single Sign-On Solution for Live@edu
Issues That Are Fixed in Exchange 2010 SP3
New-WebServicesVirtualDirectory
Number of items in retry table has been more than 30000 for 30 minutes
Overview of Administrator Audit Logging
Release Notes for Exchange Server 2010 SP3
Remote PowerShell connectivity (Internal) failures
Start the MRSProxy Service on a Remote Client Access Server
The Microsoft Exchange Mailbox Replication service isn't scanning MDB queues for jobs
The Test-OutlookConnectivity (Internal) cmdlet failed to run
Transport Rule Predicates
Understanding Address Book Policies
Understanding Proxying and Redirection
Understanding the Autodiscover Service
What's New in Exchange 2010 SP3
White Papers: Exchange 2010 Tested Solutions

November 2012

- **New Content**

Configure a Dedicated Send Connector for a Specific Domain
Event IDs 1121 and 5000 Are Logged When You Try to Start the Information Store Service
Reclaim Space When the .edb File Size Grows Too Large

- **Updated Content**

Add-MailboxPermission
Before You Import the Exchange 2010 Monitoring Management Pack
Change the Ownership of a Distribution Group
Client Language Support for Unified Messaging
Configure an Ethical Wall
Configure Autodiscover Redirection for the Multi-Tenant Organization
Configure Safelist Aggregation
Create a Mailbox Export Request
Creating a New Monitoring Management Pack for Customizations
Discontinued Features
Exchange Server 2010
Exchange Server Build Numbers and Release Dates
Export Messages from Queues
Fax Advisor for Exchange 2010
Filterable Properties for the -Filter Parameter
Get-MailboxAuditBypassAssociation
How Retention Age is Calculated
How to Import the Exchange 2010 Monitoring Management Pack
Install or Upgrade to Exchange 2010 SP2 Unified Messaging
Managing Connectors

MSExchange ADAccess 2915
MSExchange ADAccess 2916
New-MailContact
New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1
Optional Configurations
Protecting Journal Reports
Regular Expressions in Transport Rules
Release Notes for Exchange Server 2010 SP2
Set-ActiveSyncMailboxPolicy
Set-DynamicDistributionGroup
Set-ImapSettings
Set-Mailbox
Set-PopSettings
Set-RemoteDomain
Start-RetentionAutoTagLearning
Start the MRSProxy Service on a Remote Client Access Server
Transport Rule Predicates
Troubleshooting the Exchange Management Pack
Understanding Alert Correlation
Understanding Calendar Repair
Understanding Client Throttling Policies
Understanding Exchange 2010 Virtualization
Understanding Exchange ActiveSync Reporting Services
Understanding Federated Delegation
Understanding Management Role Scopes
Understanding Monitoring Management Pack Operations
Understanding POP3 and IMAP4
Understanding Recipient Filtering
Understanding Retention Tags and Retention Policies
Understanding Safelist Aggregation
Understanding the Availability Service
Understanding the Exchange Management Pack Health State Model
Understanding Transport Database Configuration Options
Understanding Unified Messaging Languages
Update-SafeList
Use Windows Server Backup to Restore a Backup of Exchange
Voice Mail Preview Advisor for Exchange 2010

September 2012

- **New Content**

Modify the Time Limit for Autodiscover Operations
Understanding Database Maintenance

- **Updated Content**

Antispam Update Errors and Events
Configure an Ethical Wall
Configure Autodiscover Redirection for the Multi-Tenant Organization
Configure Calendar Repair Assistant Settings
Configure SSL for Exchange ActiveSync
Configure SSL for Outlook Anywhere
Configure the Automated Booking Policies for a Resource Mailbox
Configure the Availability Service for Cross-Forest Topologies
Enable or Disable Calendar Repair for a Mailbox
Enable or Disable Mailbox Audit Logging for a Mailbox
Exchange Network Port Reference

Exchange Server Build Numbers and Release Dates
ExchangeStoreDB Errors and Events
File-Level Antivirus Scanning on Exchange 2010
New-MoveRequest
Obtain a Server Certificate from a Certification Authority
Optional Configurations
Restore-Mailbox
Scripts for Managing Public Folders in the Exchange Management Shell
Session Border Controllers Tested with Exchange Online UM
Set-ActiveSyncOrganizationSettings
Set-CalendarProcessing
Set-TransportServer
Set-CASMailbox
Set-Mailbox
Set-MailboxServer
Set-OwaMailboxPolicy
Set-OwaVirtualDirectory
Set-TransportServer
Troubleshooting Reference for Client Access Servers
Understanding Calendar Repair
Understanding Client Throttling Policies
Understanding Database and Log Performance Factors
Understanding Digital Certificates and SSL
Understanding Information Rights Management
Understanding Mailbox Audit Logging
Understanding Mobile Phone Connectivity
Understanding Outlook Anywhere
Understanding RPC Client Access
Understanding Storage Configuration

August 2012

- **Updated Content**

Client Access Server Counters
Configure Calendar Repair Log Settings
Configure Exchange Online Archiving
Configure Language Settings for Outlook Web App
Configure Shadow Redundancy
Configure the Availability Service for Cross-Forest Topologies
Disable a Mobile Phone for Exchange ActiveSync
Enable a Device for Exchange ActiveSync
Exchange Server Build Numbers and Release Dates
Managing Outlook Web App Security
New Transport Functionality in Exchange 2010 SP1
Overview of Administrator Audit Logging
Overview of Services Installed by Exchange Setup
Overview of Unified Messaging
Release Notes for Exchange Server 2010 SP2
Remove Public Folder Databases
Understanding Client Throttling Policies
Understanding Exchange 2010 Virtualization
Understanding Personal Archives
Understanding Shadow Redundancy

1.1.2 What's New in Exchange 2010 SP3

What's New in Exchange 2010 SP3

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-02-20*

This topic provides you with an overview of important new features and functionality in Service Pack 3 (SP3) for Microsoft Exchange Server 2010. This overview can be useful when you're planning, deploying, and administering your organization. The following sections include information about changes to features and functionality that have occurred since the release of Microsoft Exchange Server 2010 Service Pack 2 (SP2):

- Exchange 2013 Coexistence support
- Sent Items Management feature
- Windows Server 2012

In addition to the changes described in this topic, Exchange 2010 SP3 also includes fixes that address issues identified since the release of Exchange 2010 SP2. For a complete list of issues that are fixed in Exchange 2010 SP3, see Issues That Are Fixed in Exchange 2010 SP3. If you're also interested in the release notes for Exchange 2010 SP3, see Release Notes for Exchange Server 2010 SP3.

For more information about the features introduced in previous versions of Exchange 2010, see the following topics:

- What's New in Exchange 2010
- What's New in Exchange 2010 SP1
- What's New in Exchange 2010 SP2

Exchange 2013 Coexistence support

You must install Exchange 2010 SP3 if you want to run Microsoft Exchange Server 2013 in a coexistence mode. You can't perform an in-place upgrade from Exchange 2010 to Exchange 2013. However, you can install an Exchange 2013 CU1 server in the existing Exchange 2010 organization after you install Exchange 2010 SP 3. For more information about how to install an Exchange 2013 server in the existing organization, see Install Exchange 2013 in an Existing Exchange 2010 Organization.

After you perform this procedure, your organization will be running in a coexistence mode. You can maintain this mode indefinitely, or you can immediately complete the upgrade to Exchange 2013 by moving all resources from Exchange 2010 to Exchange 2013, and then decommissioning the Exchange 2010 servers. For more information about how to upgrade to Exchange 2013, see Upgrade from Exchange 2010 to Exchange 2013.

Sent Items Management feature

Exchange 2010 SP3 introduces the Sent Items Management feature to Office Outlook Web Access (OWA). The Sent Items Management feature provides control over whether an item that is "sent as" you, or "on behalf of" you, is copied to your **Sent Items** folder and to the sender's **Sent Items** folder. Before Exchange 2010 SP3, messages that are "sent as" you or "on behalf of" you are copied only to the sender's **Sent Items** folder.

You can configure the Sent Items Management feature in OWA on the **Options** page. After Exchange 2010 SP3 is installed, the **Sent Items Options** settings will be available on the **Options** page in OWA.

Windows Server 2012

Exchange 2010 SP3 can be used together with Windows Server 2012. For more information about operating system supportability, see Exchange Server Supportability Matrix.

1.1.2.1 Release Notes for Exchange Server 2010 SP3

Release Notes for Exchange Server 2010 SP3

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-02-26*

For important legal information, see "Legal Notice" later in this document.

Welcome to Service Pack 3 (SP3) for Microsoft Exchange Server 2010. This document contains the following sections:

- Installing Exchange 2010 SP3
- Database Schema Upgrades
- Legal Notice

Installing Exchange 2010 SP3

Consider the following when you deploy Exchange 2010 SP3:

- Exchange 2010 SP3 makes updates to the Active Directory schema. To learn more about these schema changes, see Exchange Server Changes to the Active Directory Schema.
- You can select an option that installs the required Windows operating system roles and features for each selected Exchange 2010 SP3 server role.
- You can install Exchange 2010 SP3 only on computers that are running Windows Server 2008 with Service Pack 2 (SP2), Windows Server 2008 R2, or Windows Server 2012.

For detailed information about the requirements and steps for installing Exchange 2010 SP3, see the following topics:

- Exchange 2010 Prerequisites
- Exchange 2010 System Requirements
- Understanding a New Installation of Exchange 2010
- Understanding Upgrade to Exchange 2010

Database Schema Upgrades

The database schema has been updated in Exchange 2010 SP3. As a result, when Mailbox servers are upgraded to Exchange 2010 SP3, the databases are upgraded to the Exchange 2010 SP3 version of the database schema. After a database has been updated to the Exchange 2010 SP3 schema, it can't be mounted on a pre-Exchange 2010 SP3 Mailbox server.

The database schema upgrade process adds time to the overall service pack upgrade process. During the upgrade, the database is dismounted, and all mailboxes in that database are taken offline. If you're upgrading the Mailbox server from the release to

manufacturing (RTM) version of Exchange 2010 to Exchange 2010 SP3, the database upgrade process could take an additional 30 minutes or longer per database. This is because the upgrade process converts each database from Microsoft Exchange Server 2010 RTM to Microsoft Exchange Server 2010 SP1, from Exchange 2010 SP1 to Exchange 2010 SP2, and then from Exchange 2010 SP2 to Exchange 2010 SP3. If you're upgrading from Exchange 2010 SP2 to Exchange 2010 SP3, the upgrade process takes less time. You can track the progress of the database upgrade process by examining event **1185** in the **Application** event log on the server you're upgrading.

A database availability group (DAG) member that’s running an older version of Exchange 2010 can move its active databases to a DAG member running a newer version of Exchange 2010, but can’t do the reverse. After a DAG member has been upgraded to a newer Exchange 2010 service pack, its active database copies can't be moved to another DAG member that’s running Exchange 2010 RTM or to a service pack that's older than the service pack installed on the DAG member.

Legal Notice

1.1.2.2 Issues That Are Fixed in Exchange 2010 SP3

Issues That Are Fixed in Exchange 2010 SP3

Exchange Server 2010 > Getting Started With Exchange 2010 > What's New in Exchange 2010 SP3 >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-01-25*

This topic lists the issues that are fixed in Microsoft Exchange Server 2010 Service Pack 3 (SP3). For more information about Exchange 2010 SP3, see the following topics:

- To learn more about the new features in Exchange 2010 SP3, see What's New in Exchange 2010 SP3.
- To learn more about known issues that affect Exchange 2010 SP3, see Release Notes for Exchange Server 2010 SP3.
- To obtain Exchange 2010 SP3, see Exchange Server 2010 Service Pack 3.

Issues that are fixed

Exchange 2010 SP3 includes the changes that were made in the following Exchange 2010 SP2 rollups:

- Description of Update Rollup 1 for Exchange Server 2010 Service Pack 2
- Description of Update Rollup 2 for Exchange Server 2010 Service Pack 2
- Description of Update Rollup 3 for Exchange Server 2010 Service Pack 2
- Description of Update Rollup 4 for Exchange Server 2010 Service Pack 2
- Description of Update Rollup 4 Version 2 for Exchange Server 2010 SP2
- Description of Update Rollup 5 version 2 for Exchange Server 2010 Service Pack 2

1.1.3 What's New in Exchange 2010 SP2

What's New in Exchange 2010 SP2

Exchange Server 2010 > Getting Started With Exchange 2010 >

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-11*

This topic provides you with an overview of important new features and functionality in Service Pack 2 (SP2) for Microsoft Exchange Server 2010, which can be useful when you're planning, deploying, and administering your organization. The following sections include information about changes to features and functionality that has occurred since Service Pack 1 (SP1) for Exchange 2010:

- Hybrid Configuration Wizard
- Federated Delegation
- Address Book Policies
- Cross-Site Silent Redirection for Outlook Web App
- Mini Version of Outlook Web App
- Mailbox Replication Service
- Mailbox Auto-Mapping
- Multi-Valued Custom Attributes
- Litigation Hold
- Multi-Tenant Support

In addition to the changes described in this topic, Exchange 2010 SP2 also includes fixes that address issues identified since the release of Exchange 2010 SP1. For a complete list of issues fixed in Exchange 2010 SP2, see Issues That Are Fixed in Exchange 2010 SP2. If

you're also interested in the release notes for Exchange 2010 SP2, see Release Notes for Exchange Server 2010 SP2.

For more information about the features introduced in previous versions of Exchange 2010, see the following topics:

- What's New in Exchange 2010
- What's New in Exchange 2010 SP1

Hybrid Configuration Wizard

Exchange 2010 SP2 introduces the Hybrid Configuration Wizard which provides you with a streamlined process to configure a hybrid deployment between on-premises and Office 365 Exchange organizations. Hybrid deployments provide the seamless look and feel of a single Exchange organization and offer administrators the ability to extend the feature-rich experience and administrative control of an on-premises organization to the cloud. For more information, see Understanding the Hybrid Configuration Wizard.

Federated Delegation

In Exchange 2010 SP1, we recommended that organizations create a sub-domain of "exchangedelegation" for the account namespace in their federation trust with the Microsoft Federation Gateway. Now, in Exchange 2010 SP2, we have updated our recommendation and also automated the configuration process. If you use the Manage Federation or Manage Hybrid Configuration wizards when configuring a new federation trust, a pre-defined string is now automatically combined with an accepted domain for your organization and assigned as the account namespace for the federation trust. The account namespace for an existing federation trust is not modified by these wizards. For more information, see Understanding Federation.

Address Book Policies

Exchange 2010 SP2 introduces the address book policy object which can be assigned to a mailbox user. The ABP determines the global address list (GAL), offline address book (OAB), room list, and address lists that are visible to the mailbox user that is assigned the policy. Address book policies provide a simpler mechanism to accomplish GAL separation for the on-premises organization that needs to run disparate GALs. For more information, see Understanding Address Book Policies.

Cross-Site Silent Redirection for Outlook Web App

With Exchange 2010 SP2, you can enable a silent redirection when a Client Access server receives a client request that is better serviced by a Client Access server located in another Active Directory site. This silent redirection can also provide a single sign-on experience when forms-based authentication is enabled on each Client Access server. For more information, see Understanding Proxying and Redirection.

Mini Version of Outlook Web App

The mini version of Outlook Web App is a lightweight browser-based client, similar to the Outlook Mobile Access client in Exchange 2003. It's designed to be used on a mobile operating system. The mini version of Outlook Web App provides users with the following basic functionality:

- Access to e-mail, calendar, contacts, tasks and the global address list.
- Access to e-mail subfolders.
- Compose, reply to, and forward e-mail messages.
- Create and edit calendar, contact, and task items.
- Handle meeting requests.
- Set the time zone and automatic reply messages.

For more information, see Understanding the Mini Version of Outlook Web App.

Mailbox Replication Service

In Exchange 2010 SP1, if you wanted to move mailboxes from on-premises to Outlook.com or to another forest, you had to enable MRSProxy on the remote Client Access server. To do this, you had to manually configure the web.config file on every Client Access server. In Exchange 2010 SP2, two parameters have been added to the **New-WebServicesVirtualDirectory** and **Set-WebServicesVirtualDirectory** cmdlets so that you don't have to perform the manual configuration: *MRSProxyEnabled* and *MaxMRSProxyConnections*. For more information, see Start the MRSProxy Service on a Remote Client Access Server.

Mailbox Auto-Mapping

In Exchange 2010 SP1, Office Outlook 2007 and Outlook 2010 clients can automatically map to any mailbox to which a user has Full Access permissions. If a user is granted Full Access permissions to another user's mailbox or to a shared mailbox, Outlook, through Autodiscover, automatically loads all mailboxes to which the user has full access. However, if the user has full access to a large number of mailboxes, performance issues may occur when starting Outlook. Therefore, in Exchange 2010 SP2, administrators can turn off the auto-mapping feature by setting the value of the new *Automapping* parameter to `$false` on the **Add-MailboxPermission** cmdlets. For more information, see Disable Outlook Auto-Mapping with Full Access Mailboxes.

Multi-Valued Custom Attributes

Exchange 2010 SP2 introduces five new multi-value custom attributes that you can use to store additional information for mail recipient objects. The *ExtensionCustomAttribute1* to *ExtensionCustomAttribute5* parameters can each hold up to 1,300 values. You can specify multiple values as a comma-delimited list.The following cmdlets support these new parameters:

- **Set-DistributionGroup**
- **Set-DynamicDistributionGroup**
- **Set-Mailbox**
- **Set-MailContact**
- **Set-MailPublicFolder**
- **Set-RemoteMailbox**

Litigation Hold

In Exchange 2010 SP2, you can’t disable or remove a mailbox that has been placed on litigation hold. To bypass this restriction, you must either remove litigation hold from the mailbox, or use the new *IgnoreLegalHold* switch parameter when removing or disabling the mailbox. The *IgnoreLegalHold* parameter has been added to the following cmdlets:

- **Disable-Mailbox**
- **Remove-Mailbox**
- **Disable-RemoteMailbox**

- **Remove-RemoteMailbox**
- **Disable-MailUser**
- **Remove-MailUser**

Multi-Tenant Support

Exchange 2010 SP1 introduced the ability to install in a hosting mode by using the /`hosting` switch when running the installation script. However, in Exchange 2010 SP2, we no longer recommend installing Exchange using the /`hosting` switch. To learn more, see Multi-Tenant Support.

1.1.3.1 Release Notes for Exchange Server 2010 SP2

Release Notes for Exchange Server 2010 SP2

Exchange Server 2010 > Getting Started With Exchange 2010 > What's New in Exchange 2010 SP2 >

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-12*

For important legal information, see Legal Notice later in this document.

Welcome to Service Pack 2 (SP2) for Microsoft Exchange Server 2010. This document contains the following sections:

Installing Exchange 2010 SP2

Consider the following when you deploy Exchange 2010 SP2:

- Exchange 2010 SP2 makes updates to the Active Directory schema. To learn more about these schema changes, see Exchange Server Changes to the Active Directory Schema.
- You can select an option that installs the required Windows operating system roles and features for each selected Exchange 2010 SP2 server role.
- You can only install Exchange 2010 SP2 on computers running the Windows Server 2008 operating system with Service Pack 2 (SP2) and the Windows Server 2008 R2 operating system.

For detailed information about the requirements and steps for installing Exchange 2010 SP2, see the following topics:

- Exchange 2010 Prerequisites
- Exchange 2010 System Requirements
- Understanding a New Installation of Exchange 2010
- Understanding Upgrade to Exchange 2010

Setup

When you upgrade from a previous version of Exchange 2010 to Exchange 2010 SP2 and you've previously defined the execution policy of Windows PowerShell scripts using group policies, Setup will fail. After Setup fails, Exchange 2010 will no longer work on the affected server and you won't be able to restart Setup.

This issue happens because a required service is stopped by Setup during installation. This service is needed to query Active Directory Domain Services to verify the execution policy of Windows PowerShell scripts that must run as part of Setup.

To avoid this issue, do the following:

1. Use the **Group Policy Management Console** to disable the group policy. The Windows PowerShell execution policy group policy objects must be set to **Undefined**.
2. Install Exchange 2010 SP2.
3. Re-enable the previously defined Windows PowerShell execution policy through the **Group Policy Management Console**.

For more information about this issue, or if you've already run Setup and have encountered an error, see Microsoft Knowledge Base article 2668686, Error message when you try to install Exchange Server 2010 SP2: "AuthorizationManager check failed".

Database Schema Upgrades

The database schema has been updated in Exchange 2010 SP2. As a result, when Mailbox servers are upgraded to Exchange 2010 SP2, the databases are upgraded to the Exchange 2010 SP2 version of the database schema. After a database has been updated to the Exchange 2010 SP2 schema, it can't be mounted on a pre-Exchange 2010 SP2 Mailbox server.

The database schema upgrade process adds time to the overall service pack upgrade process. During the upgrade, the database is dismounted and all mailboxes in that database are taken offline. If you're upgrading the Mailbox server from the release to manufacturing (RTM) version of Exchange 2010 to Exchange 2010 SP2, the database upgrade process could take an additional 30 minutes or longer per database. This is because the upgrade process converts each database from Microsoft Exchange Server 2010 RTM to Microsoft Exchange Server 2010 SP1, and then from Exchange 2010 SP1 to Exchange 2010 SP2. If you're upgrading from Exchange 2010 SP1 to Exchange 2010 SP2, the upgrade process takes less time. You can track the progress of the database upgrade process by examining event **1185** in the **Application** event log on the server you're upgrading.

A database availability group (DAG) member running an older version of Exchange 2010 can move its active databases to a DAG member running a newer version of Exchange 2010, but not the reverse. After a DAG member has been upgraded to a newer Exchange 2010 service pack, its active database copies can't be moved to another DAG member running Exchange 2010 RTM or a service pack that's older than the service pack installed on the DAG member.

Client Access Server Prerequisite Changes

Several new prerequisites have been added when installing the Client Access server role. Prior to installing Exchange 2010 SP2, you must install these new prerequisites on servers that have the Client Access server role installed. If the prerequisites aren't installed, Setup will fail.

To install the prerequisites on Client Access servers, do the following:

Windows Server 2008 SP2

1. Open **Server Manager**.
2. Select **Roles**.
3. Under **Web Server (IIS)**, select **Add Role Services**.
4. In the **Add Role Services** wizard, on the **Select Role Services** page, select the following Windows features:
   - **IIS 6 WMI Compatibility**
   - **ASP.NET**
   - **ISAPI Filters**
   - **Client Certificate Mapping Authentication**
   - **Directory Browsing**
   - **HTTP Errors**
   - **HTTP Logging**
   - **HTTP Redirection**
   - **Tracing**
   - **Request Monitor**
   - **Static Content**
5. Click **Next** and then **Install**.

Windows Server 2008 R2

1. On the **Start** menu, navigate to **All Programs** > **Accessories** > **Windows PowerShell**. Open an elevated Windows PowerShell console, and run the following command:

   ```
   Import-Module ServerManager
   ```

2. Add the prerequisites by running the following command:

   ```
   Add-WindowsFeature Web-WMI,Web-Asp-Net,Web-ISAPI-Filter,Web-Client-Aut
   ```

If you want Exchange to install the new prerequisites during Setup, you can use unattended mode. Run the following command:

```
Setup /Mode:Upgrade /InstallWindowsComponents
```

Role Based Access Control

When you first install Exchange 2010 SP2 on an Exchange 2010 server in your organization, some Role Based Access Control (RBAC) management role definitions are updated in Active Directory. If you have multiple Exchange 2010 servers and you attempt to manage these roles from an Exchange 2010 server that hasn't been upgraded to Exchange 2010 SP2, you might receive one of the following warnings:

- Exchange Management Shell
  WARNING: The object MyMailboxDelegation has been corrupted, and it's in an inconsistent state. The following validation errors happened:
  WARNING: The property value you specified, "15", isn't defined in the Enum type "ScopeType".
- Exchange 2010 Control Panel
  There are multiple warnings. Click here to see more
  The object MyMailboxDelegation has been corrupted, and it's in an inconsistent state. The following validation errors happened:
  The property value you specified, "15", isn't defined in the Enum type "ScopeType".

To resolve the warnings, upgrade the server to Exchange 2010 SP2. The cause of these warnings doesn't prevent Exchange 2010 from functioning correctly and can safely be ignored until the server is upgraded to Exchange 2010 SP2.

Outlook Web App

If you're using redirection for Outlook Web App and aren't requiring Secure Sockets Layer (SSL), redirection will fail after the Client Access server is upgraded to Exchange 2010 SP2. To avoid this problem, after you've completed the upgrade to Exchange 2010 SP2, modify the Outlook Web App web.config file. For directions, go to "Use IIS Manager and Notepad to simplify the Outlook Web App URL when SSL isn't required" in Simplify the Outlook Web App URL. You don't have to make any changes in IIS Manager to prevent redirection from failing. You just have to modify the web.config file.

Mailbox Replication Proxy

When you upgrade to Exchange 2010 SP2, the Mailbox Replication Proxy (MRSProxy) service is disabled by Exchange if it was previously enabled. This happens because the way MRSProxy is enabled has changed in Exchange 2010 SP2 and the settings in the <Exchange Installation Path>\V14\ClientAccess\ExchWeb\EWS\web.config file are not migrated during the upgrade. Until MRSProxy is re-enabled, cross-forest mailbox move requests will not be processed.

In Exchange 2010 SP2, MRSProxy is enabled by using the *MRSProxyEnabled* parameter on the **Set-WebServicesVirtualDirectory** cmdlet. You must manually enable MRSProxy after you upgrade to Exchange 2010 SP2. MRSProxy must be manually re-enabled on each server where it was previously enabled. For more information about how to enable MRSProxy in Exchange 2010 SP2, see Start the MRSProxy Service on a Remote Client Access Server.

Prior to Exchange 2010 SP2, MRSProxy configuration was stored in the *<Exchange Installation Path>*\V14\ClientAccess\ExchWeb\EWS\web.config file. The settings stored in this file are no longer used by MRSProxy in Exchange 2010 SP2 and should not be changed.

Shadow Redundancy Promotion Feature

When you install Service Pack 2 for Exchange 2010, the value of the Shadow Redundancy Promotion feature is reset to False, and the setting is disabled.

If you enabled Shadow Redundancy in your Exchange 2010 SP1 organization, you must re-enable Shadow Redundancy after you install Exchange 2010 SP2. Note that other settings in EdgeTransport.exe.config are not reset when you install Exchange 2010 SP2.

Legal Notice

Components – Version 8.0

Outside In ® HTML Export Version 8.0

Platforms Supported – Version 8.0:

Windows Intel (32 bit binaries)

Windows® 2000/XP/Server 2003

Windows Itanium (64 bit binaries)

Windows.NET ® Server 2003 Enterprise Edition for Itanium

Windows AMD (64 bit binaries)

Windows Server 2003, Enterprise Edition for AMD Opteron

1.1.3.2 Issues That Are Fixed in Exchange 2010 SP2

Issues That Are Fixed in Exchange 2010 SP2

Exchange Server 2010 > Getting Started With Exchange 2010 > What's New in Exchange 2010 SP2 >

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-29*

This topic provides the list of issues that are fixed in Microsoft Exchange Server 2010 Service Pack 2 (SP2). For additional information about Exchange Server 2010 SP2, see the following:

- To learn more about the new features in Exchange Server 2010 SP2, see What's New in Exchange 2010 SP2.
- To learn more about known issues with SP2, see Release Notes for Exchange Server 2010 SP2.
- To obtain Exchange Server 2010 SP2, see Exchange Server 2010 Service Pack 2.

Issues that are Fixed

Exchange 2010 SP2 includes the changes made in the following Exchange 2010 SP1 rollups:

- Update Rollup 6 for Exchange Server 2010 Service Pack 1
- Update Rollup 5 for Exchange Server 2010 Service Pack 1
- Update Rollup 4 for Exchange Server 2010 Service Pack 1
- Update Rollup 3 for Exchange Server 2010 Service Pack 1
- Update Rollup 2 for Exchange Server 2010 Service Pack 1
- Update Rollup 1 for Exchange Server 2010 Service Pack 1

1.1.3.3 Multi-Tenant Support

Multi-Tenant Support

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-01*

A multi-tenant Exchange deployment is defined in this topic as one where the system has been configured to host multiple and discrete organizations or business units (the tenants) that ordinarily don't share e-mail, data, users, global address lists (GALs), or any other commonly used Exchange objects.

In Exchange 2010 Service Pack 1 (SP1), Exchange introduced the ability to install in a hosting mode by using the `/hosting` switch when running the installation script. However, in Exchange 2010 SP2, we no longer recommend installing Exchange using the `/hosting` switch. To learn more, see the Exchange Team Blog article Future of /Hosting Mode.

In Exchange 2010 SP2, hosting is supported by using the on-premises Exchange installation. For guidance about configuring a multi-tenant organization with Exchange 2010 SP2, download the white paper Multi-Tenancy and Hosting Guidance for Exchange Server 2010 SP2. This paper doesn't provide step-by-step instructions about how to achieve multi-tenancy with Exchange 2010 SP2. Instead, it provides information about the challenges and problems that must be solved, and offers advice and direction to ensure the Exchange environment you build can be supported by Microsoft.

1.1.4 What's New in Exchange 2010 SP1

What's New in Exchange 2010 SP1

Applies to: *Exchange Server 2010 SP1*

Topic Last Modified: *2012-07-23*

This topic provides you with an overview of important new features and functionality in Exchange Server 2010 Service Pack 1 (SP1), which you can use when you're planning, deploying, and administering your organization. The following sections include information about changes to features and functionality that has occurred since Exchange Server 2010 RTM (release to manufacturing) and information about features and functionality first introduced in Exchange 2010 SP1. For more information about the features and functionality that was introduced at Exchange 2010 RTM, see What's New in Exchange 2010.

For information about known issues with Exchange 2010 SP1, see Release Notes for Exchange Server 2010 SP1.

In addition to the changes described in this topic, Exchange 2010 SP1 also includes fixes that address issues identified since the release of Exchange 2010 RTM. For a complete list, see Issues That Are Fixed in Exchange 2010 SP1.

New Deployment Functionality

During an Exchange 2010 SP1 installation, you can now select a new option to install the required Windows roles and features for each selected Exchange 2010 SP1 server role. For more information, see New Deployment Functionality in Exchange 2010 SP1.

Client Access Server Role Improvements

The improvements and new features in the Client Access server role fall under several key areas: Federation certificates, Exchange ActiveSync, SMS Sync, Integrated Rights Management, Microsoft Office Outlook Web App, and virtual directories. Each area is described in more detail in the following sections.

Federation Certificates

In Exchange 2010 SP1, you can use a self-signed certificate instead of a certificate issued by a Certificate Authority to establish a federation trust with the Microsoft Federation Gateway. A self-signed certificate is automatically created and installed on Exchange servers in your organization when you use the **New Federation Trust** wizard in the Exchange Management Console. For more information, see Understanding Federation.

Exchange ActiveSync

In Exchange 2010 SP1, you can manage Exchange ActiveSync devices using the Exchange Control Panel (ECP). Administrators can perform the following tasks:

- Manage the default access level for all mobile phones and devices.
- Set up e-mail alerts when a mobile phone or device is quarantined.
- Personalize the message that users receive when their mobile phone or device is either recognized or quarantined.
- Provide a list of quarantined mobile phones or devices.
- Create and manage Exchange ActiveSync device access rules.
- Allow or block a specific mobile phone or device for a specific user.

For every user, the administrator can perform the following tasks from the user's property pages:

- List the mobile phones or devices for a specific user.
- Initiate remote wipes on mobile phones or devices.
- Remove old mobile phone or device partnerships.
- Create a rule for all users of a specific mobile phone or device or mobile phone type.
- Allow or block a specific mobile phone or device for the specific user.

For more information, see Understanding Exchange ActiveSync.

SMS Sync

SMS Sync is a new feature in Exchange ActiveSync that works with Windows Mobile 6.1 with the Outlook Mobile Update and with Windows Mobile 6.5. SMS Sync is the ability to synchronize messages between a mobile phone or device and an Exchange 2010 Inbox. When synchronizing a Windows Mobile phone with an Exchange 2010 mailbox, users can choose to synchronize their text messages in addition to their Inbox, Calendar, Contacts, Tasks, and Notes. When synchronizing text messages, users will be able to send and receive text messages from their Inbox. This feature is dependent on the user's mobile phones or devices supporting this feature.

Server-Side Information Rights Management Support

Exchange ActiveSync mailbox policies now contain support for Information Rights Management (IRM) functionality. Information Rights Management is enabled when creating a new Exchange ActiveSync mailbox policy. This new functionality allows non-Windows Mobile devices to receive and view protected e-mails. When the *IRMEnabled* property is configured on the Exchange ActiveSync mailbox policy and IRM is enabled for Client Access Servers, the protected e-mail will be decrypted on the server before it is downloaded to the mobile phone or device. The downloaded e-mail will be downloaded

with additional properties that indicate the restrictions sent with the original e-mail. Protected messages will only be decrypted and downloaded if the mobile phone or device connects to the Client Access server using Secure Sockets Layer (SSL).

Outlook Web App Improvements

The following is a list of the new Outlook Web App functionality in Exchange 2010 SP1:

- Improved management of the relationship between Office Communications Server and Outlook Web App. Configuration is stored in Active Directory instead of a web.config file and can be managed via cmdlet.
- Twenty-seven themes are available, and they have new administrative options:
  - Set default theme with the *DefaultTheme* parameter by using either the Set-OwaMailboxPolicy or the Set-OwaVirtualDirectory cmdlet.
  - Create custom themes by modifying existing themes.
  - Control the order themes are listed in Outlook Web App.
- By default, attachment types that are marked as **Force Save** will be excluded from security checks for XML or HTML. You can change this behavior by setting the *ForceSaveAttachmentFilteringEnabled* parameter to `$true` by using either the Set-OwaMailboxPolicy or the Set-OwaVirtualDirectory cmdlet.
- Users can change unexpired passwords by default. In Exchange 2010 SP1, you can also enable users to reset expired passwords. See Configuring the Change Password Feature in Outlook Web App.

Reset Virtual Directory

In Exchange 2010 SP1, you can use the new Reset Client Access Virtual Directory wizard to reset one or more Client Access server virtual directories. The new wizard makes it easier to reset a Client Access server virtual directory. One reason that you might want to reset a Client Access server virtual directory is to resolve an issue related to a damaged file on a virtual directory. In addition to resetting virtual directories, the wizard creates a log file that includes the settings for each virtual directory that you choose to reset. For more information, see Reset Client Access Virtual Directories.

Client Throttling Policies

You can use client throttling policies to help you manage performance of your Client Access servers. Consider the following changes as you use client throttling policies to manage performance when running Exchange 2010 SP1.

- In Exchange 2010 RTM, only the policies to limit the number of concurrent client connections were enabled by default. In Exchange 2010 SP1, all client throttling policies are enabled by default.
- In Exchange 2010 RTM, when the thresholds defined on a latency-based client throttling policy parameter such as *EWSPercentTimeInCAS* were exceeded, Exchange would cause the transactions and connections to fail. In Exchange 2010 SP1, exceeding the thresholds defined on a latency-based throttling policy parameter will not cause a failure. Instead, Exchange will delay transactions and connections until the transaction rate is within the policy limits. Such transaction and connection delays will usually not be apparent to end users. Client throttling policy parameters with a hard quota limits such as *EWSMaxSubscriptions* will cause a failure when exceeded. As an administrator, you can monitor the impact of your performance policies and make adjustments as needed.
- Two new cmdlets, **Get-ThrottlingPolicyAssociation** and **Set-ThrottlingPolicyAssociation,** help you manage and apply client throttling polices to specific objects.

For more information, see Understanding Client Throttling Policies and Managing Performance with Client Throttling Policies.

Improvements in Transport Functionality

The following is a list of new Transport functionality in Exchange 2010 SP1:

- MailTips access control over organizational relationships
- Enhanced monitoring and troubleshooting features for MailTips
- Enhanced monitoring and troubleshooting features for message tracking
- Message throttling enhancements
- Shadow redundancy promotion
- SMTP failover and load balancing improvements
- Support for extended protection on SMTP connections
- Send connector changes to reduce NDRs over well-defined connections

For more information and details about these changes, see New Transport Functionality in Exchange 2010 SP1.

Permissions Functionality

The following is a brief description of new permissions features and enhancements in Exchange 2010 SP1:

- **Database scope support** With database scopes, you can control which databases mailboxes can be created for a given set of administrators and also control which databases they can manage. For more information about database scopes, see Understanding Management Role Scopes.
- **Active Directory split permissions** Active Directory split permissions enable you to completely separate the administrative capabilities of Exchange administrators from your Active Directory administrators. The ability to create and remove Active Directory users and groups and manage non-Exchange attributes of Active Directory objects by Exchange administrators and servers has been removed in Exchange 2010 SP1. For more information about Active Directory split permissions, see Understanding Split Permissions.
- **Improved user interface** You can now create and manage management role groups and management role assignment policies in the Exchange Control Panel (ECP). This includes adding and removing management roles to role groups and role assignment policies, adding and removing members to and from role groups, and assigning users to role assignment policies. For more information about how to manage role groups and role assignment policies, see the following topics:
  - Managing Administrator and Specialist Users
  - Managing End Users

Exchange Store and Mailbox Database Functionality

The following is a list of new store and mailbox database functionality in Exchange 2010 SP1:

- With the **New-MailboxRepairRequest** cmdlet, you can detect and repair mailbox and database corruption issues.
- Store limits were increased for administrative access.
- The Database Log Growth Troubleshooter (Troubleshoot-DatabaseSpace.ps1) is a new script that allows you to control excessive log growth of mailbox databases.
- Public Folders client permissions support was added to the Exchange Management Console (EMC).

For more information and details about each of these features, see New Exchange Core Store Functionality in Exchange 2010 SP1.

Mailbox and Recipients Functionality

The following is a list of new mailbox and recipient functionality included in Exchange 2010 SP1:

- In Outlook 2010 and Outlook 2007, Autodiscover automatically loads any mailbox for which a user has been granted full access permission. Users can't control or disable this behavior.
- Calendar Repair Assistant supports more scenarios than were available in Exchange 2010 RTM.
- Mailbox Assistants are now all throttle-based (changed from time-based in Exchange 2010 RTM).
- Internet calendar publishing allows users in your Exchange organization to share their Outlook calendars with a broad Internet audience.
- Importing and exporting .pst files now uses the Mailbox Replication service and doesn't require Outlook.
- Hierarchical address book support allows you to create and configure your address lists and offline address books in a hierarchical view.
- Distribution group naming policies allow you to configure string text that will be appended or prepended to a distribution group's name when it's created.
- Soft-delete of mailboxes after move completion.

For more information and details about these features, see New Mailbox and Recipient Functionality in Exchange 2010 SP1.

High Availability and Site Resilience Functionality

The following is a list of new high availability and site resilience functionality included in Exchange 2010 SP1:

- Continuous replication - block mode
- Active mailbox database redistribution
- Enhanced datacenter activation coordination mode support
- New and enhanced management and monitoring scripts
- Exchange Management Console user interface enhancements
- Improvements in failover performance

For more information about these features, see New High Availability and Site Resilience Functionality in Exchange 2010 SP1.

Messaging Policy and Compliance Functionality

The following is a list of new messaging policy and compliance functionality included in Exchange 2010 SP1:

- Provision personal archive on a different mailbox database
- Import historical mailbox data to personal archive
- Delegate access to personal archive
- New retention policy user interface
- Opt-in personal tags

- Multi-Mailbox Search preview
- Annotations in Multi-Mailbox Search
- Multi-Mailbox Search data de-duplication
- WebReady Document Viewing of IRM-protected messages in Outlook Web App
- IRM in Exchange ActiveSync for protocol-level IRM
- IRM logging
- Mailbox audit logging

For more information and details about each of these features, see New Messaging Policy and Compliance Functionality in Exchange 2010 SP1.

Unified Messaging Server Role Improvements

The Unified Messaging server role has been improved and has added new features in Exchange 2010 SP1. To use some of these features, you must correctly deploy Microsoft Lync Server 2010 in your environment. The following is an overview of all the new features in Exchange 2010 Unified Messaging:

- **UM reporting** The reports for **Call Statistics** and **User Call Logs** found in the Exchange Management Console are displayed in the Exchange Control Panel.
- **UM management in the Exchange Control Panel** You can usethe ECP to manage UM components in a cross-premises environment.
- **Cross-Forest UM-enabled mailbox migration** In Exchange 2010 SP1, you can use the **New-MoveRequest** cmdlet with the Mailbox Replication Service (MRS) to move a UM-enabled mailbox within a local forest and multiple forests in an enterprise.
- **Outlook Voice Access improvements** Outlook Voice Access users can log on to their Exchange 2010 mailbox and choose the order to listen to unread voice mail messages, from the oldest message first or the newest message first.
- **Caller Name Display support** Exchange 2010 SP1 includes support for enhanced caller ID resolution for displaying names for voice mails from unresolved numbers using Caller Name Display (CND).
- **Test-ExchangeUMCallFlow cmdlet** With this Exchange 2010 SP1 cmdlet, you can test UM connectivity and call flow.
- **New UM Dial Plan wizard** An additional page has been added to the **New UM Dial Plan** wizard that allows you to add a UM server to the dial plan.
- **Lync Server 2010 Support** Migrating SIP URI dial plans and Message Waiting Indicator (MWI) notifications in a cross-premises environment has been added.
- **Secondary UM dial plan support** You can add a secondary UM dial plan for a UM-enabled user.
- **UM language packs added** New UM language packs are now available in Exchange 2010 SP1. In addition, the Spanish (Spain) (es-ES) UM language pack available for Exchange 2010 SP1 now includes Voice Mail Preview, a feature that wasn't available in the Exchange 2010 RTM release of that language pack.
- **Call answering rules improvements** There are three updates to Call Answering Rules for UM-enabled users in SP1.
- **Unified Communications Managed API/speech platform improvements** Beginning with Exchange 2010 SP1, the UM server relies on Unified Communications Managed API v. 2.0 (UCMA) for its underlying SIP signaling and speech processing.
- **UM auto attendant update** In Exchange 2010 SP1, a UM auto attendant will play only the holiday greeting on a holiday.

For more information and details about each of these features, see New Unified

Messaging Functionality and Voice Mail Features in Exchange 2010 SP1.

Audit Logging Improvements

Exchange 2010 SP1 provides improvements in functionality related to administrator audit logging and new functionality for mailbox audit logging:

- **Improvements in administrator audit logging** Exchange 2010 enhances the administrator audit logging functionality by providing you with the ability to perform searches of the admin audit log using the Exchange Management Shell. You can search on cmdlet and parameter names, date, the user who ran the command, and more. The results generated by your search can be displayed on the screen or e-mailed to a recipient you specify and viewed as an XML file. And, because all the administrative interfaces run Shell cmdlets in the background, the actions that occur in all the interfaces can be logged. For more information, see Overview of Administrator Audit Logging.
- **New mailbox audit logging** Exchange 2010 SP1 introduces new mailbox audit logging functionality to allow you to track mailbox access by administrators, delegates, and mailbox owners, and actions taken on mailbox items such as moving or deleting a message, using SendAs or SendOnBehalf rights to send messages, and accessing a mailbox folder or a message. You can use the ECP to generate a report of non-owner mailbox access and use the Shell to search mailbox audit logs. For more information, see Understanding Mailbox Audit Logging.
- The Exchange Control Panel also provides several reports which are generated based on the audit logs in Exchange 2010 SP1.

Support for Hybrid Deployments with Exchange Online

Exchange 2010 SP1 includes the following functionality that supports hybrid deployments with Exchange Online:

- **Migration of UM-enabled mailboxes** The New-MoveRequest cmdlet can be used with the Microsoft Exchange Mailbox Replication service (MRS) to move a UM-enabled mailbox within a hybrid deployment.
- **IRM support for hybrid deployments** IRM is fully supported for hybrid deployments. The tenant administrator can export the trusted publishing domain from the on-premises Active Directory Rights Management Services (AD RMS) server and import it to the cloud-based service. This functionality allows IRM-protected messages to be decrypted in the cloud, and cloud mailbox users to send IRM-protected messages that on-premises mailbox users can decrypt and access.
- **Remote Mailboxes** A new set of SP1 cmdlets allow you to create and manage a mail-enabled user in the on-premises Active Directory site and at the same time create and manage the associated mailbox in the cloud-based service. The cmdlets are:
  - New-RemoteMailbox
  - Set-RemoteMailbox
  - Get-RemoteMailbox
  - Enable-RemoteMailbox
  - Disable-RemoteMailbox
  - Remove-RemoteMailbox
- **Transport** Updated features in Transport help ensure that message flow remains protected between users regardless of where their mailboxes are located. Enhanced Transport features such as MailTips, delivery reports, and message moderation also support this deployment scenario.

Support for Multi-Tenancy

With Exchange 2010 SP1 built-in multi-tenant support, service providers that use Microsoft Service Provider Licensing Agreement (SPLA) no longer need a solution such as Microsoft Hosted Messaging and Collaboration version 4.5 to host multiple organizations. Multi-tenant support in Exchange 2010 SP1 provides the core feature set of Microsoft Exchange that can be deployed to multiple customers in a single installation, and it also provides ease of management and flexibility of provided features to end-users.

In addition to including most of the features and functionality available in Exchange 2010 SP1 Enterprise deployments, the multi-tenant solution available for Exchange 2010 SP1 also includes features and functionality that allow you to create and manage tenant organizations. For more information, see Multi-Tenant Support.

1.1.4.1 New Deployment Functionality in Exchange 2010 SP1

New Deployment Functionality in Exchange 2010 SP1

Applies to: *Exchange Server 2010 SP1*

Topic Last Modified: *2010-07-21*

This topic provides a brief overview of the new functionality available for deploying Microsoft Exchange 2010 Service Pack 1 (SP1). During an Exchange 2010 SP1 installation, you can now select a new option to install the required Windows roles and features for each selected Exchange 2010 SP1 server role.

Exchange 2010 SP1 Install

Exchange 2010 SP1 Setup has been improved to allow you to install the required Windows roles and features. If you select the option to install Windows roles and features, progress is shown and the appropriate roles and features are installed. If a reboot is required, you will have to reboot the server and launch Setup again. When Setup is launched again, Setup will resume where it left off. If you don't select the option to install Windows roles and features, you can manually install the Windows roles and features and continue Setup after the prerequisites are met.

Unattended Install

You can now select the */InstallWindowsComponents* parameter during an unattended install of Exchange 2010 SP1. If you select the option to install Windows roles and features, progress is shown and the appropriate roles and features are installed. If a reboot is required, you will have to reboot the server and launch Setup.com again with the */InstallWindowsComponents* parameter. If the Windows roles and features were correctly installed, Setup.com will continue.

Exchange 2010 RTM to Exchange 2010 SP1 Upgrade

When you run Exchange 2010 unattended install to upgrade from the release to manufacturing (RTM) version of Exchange 2010 to Exchange 2010 SP1, you can use the **Setup.com /m:upgrade /installwindowscomponents** command. If a reboot is required,

you will have to reboot the server and again launch **Setup.com /m:upgrade** with the /*InstallWindowsComponents* parameter. If the Windows roles and features were correctly installed, Setup.com will continue.

1.1.4.2 New Mailbox and Recipient Functionality in Exchange 2010 SP1

New Mailbox and Recipient Functionality in Exchange 2010 SP1

Applies to: *Exchange Server 2010 SP1*

Topic Last Modified: *2011-04-28*

Microsoft Exchange Server 2010 Service Pack 1 (SP1) provides new functionality for Mailbox servers, mailboxes, and recipients. New functionality is available for the following:

- Mailbox full access permission and Outlook Automapping
- Group naming policies
- Mailbox data
- Move requests
- Archive mailboxes
- Hierarchical address books
- Mailbox folder permissions
- Internet calendar publishing
- Calendar Repair Assistant
- Mailbox Assistants service troubleshooter

Mailbox Full Access Permission and Outlook Automapping

In Microsoft Office Outlook 2010 and Outlook 2007, Autodiscover automatically maps to any mailbox for which a user has full access permissions. After an administrator grants full access permission for a user to access another user's mailbox or if the user has full access permission to a shared mailbox, Autodiscover automatically loads all mailboxes for which the user has full access permissions. This behavior may cause performance issues when Outlook starts if the user has a large number of mailboxes to which they have full access. For example, in some organizations, Exchange administrators have full access to all users' mailboxes in their organization. If that is the case, Outlook attempts to open all mailboxes in the organization.

Note:
Users can’t control or disable this behavior.

For more information, see Allow Mailbox Access and Manage Full Access Permissions.

Group Naming Policies

A *group naming policy* is a template that you can apply to the name of distribution groups created in the organization. You can enforce the application of a prefix, a suffix, or both to distribution groups. You can also block specific words from being used in distribution group names.

For more information, see Create a Distribution Group Naming Policy.

Mailbox Data

Importing and exporting mailbox data has been improved so that you can import or export .pst files in an asynchronous process using the Microsoft Exchange Mailbox Replication service. The following cmdlets have been added in Exchange 2010 SP1 to support this feature:

- Get-MailboxExportRequest
- Get-MailboxExportRequestStatistics
- New-MailboxExportRequest
- Remove-MailboxExportRequest
- Resume-MailboxExportRequest
- Set-MailboxExportRequest
- Suspend-MailboxExportRequest
- Get-MailboxImportRequest
- Get-MailboxImportRequestStatistics
- New-MailboxImportRequest
- Remove-MailboxImportRequest
- Resume-MailboxImportRequest
- Set-MailboxImportRequest
- Suspend-MailboxImportRequest

For more information, see Understanding Mailbox Import and Export Requests.

Move Requests

New functionality in Exchange 2010 SP1 for move requests includes the following:

- In the release to manufacturing (RTM) version of Exchange 2010, when a mailbox move completed, the mailbox on the source database was deleted and wasn't recoverable. If there was a Mailbox server failover on the target database, the mailbox move was interrupted, and data loss for the in-transit mailbox could occur.
  Exchange 2010 SP1 now soft-deletes the mailbox on the source database, so you can recover the mailbox in the event of a Mailbox server failover or data loss. You can restore a soft-deleted mailbox by using the **MailboxRestoreRequest** cmdlets set.
  These soft-deleted mailboxes are visible when running the Get-MailboxStatistics cmdlet against a database and are identifiable by the property **DisconnectReason** with a value of `SoftDeleted`. The soft-deleted mailboxes will be retained in the source database until either the deleted mailbox retention period expires or the mailbox is purged by using the Remove-StoreMailbox cmdlet. If you're performing mailbox moves to reduce the amount of space being used in a database, you must also perform the additional step of purging the soft-deleted mailboxes. Soft-deleted mailboxes can't be reconnected.

  Note:
  You can't view soft-deleted mailboxes by using the Get-MailboxStatistics cmdlet in Exchange versions earlier than Exchange 2010 SP1.

- The **MoveRequest** cmdlet set has been updated to support moving archives to a separate database. For more information, see Understanding Move Requests.

Archive Mailboxes

You can now have a user's primary mailbox and archive mailbox on separate databases. For more information, see Understanding Personal Archives.

Hierarchical Address Books

With hierarchical address book support, you can create and configure your address lists and offline address books (OABs) in a hierarchical view. For more information, see Understanding Hierarchical Address Books.

Mailbox Folder Permissions

A new cmdlet has been added that you can use to modify the mailbox folder permissions. The Set-MailboxFolderPermission cmdlet updates folder-level permissions for all folders within a user's mailbox. The cmdlet differs from the Add-MailboxFolderPermission cmdlet in that it edits an existing permission entry.

Internet Calendar Publishing

In Exchange 2010 RTM, sharing user calendar information required a federation trust and an organization relationship or sharing policy with another federated organization. Exchange 2010 SP1 introduces Internet calendar publishing so that users in your Exchange organization can share their calendars with anyone that has access to the Internet, and not just with other recipients in other federated Exchange organizations. Highlights of Internet calendar publishing include:

- Federation configuration isn't necessary for your Exchange organization.
- Internet users don't need any type of authentication credentials to access user calendars (for example, Exchange or Windows Live).
- Users can invite their friends, family members, or business partners to view their calendar information by providing a link to their published calendar.
- Exchange administrators can control which users can publish their calendars and what can be shared, both organization-wide and on a per-user basis.
- Internet users can access calendar information without having to use a specific mail client; only an Internet browser is necessary.

For more information about sharing policy and calendar publishing, see the following topics:

- Understanding Federated Delegation
- Configure Sharing Policy Properties
- Create a Sharing Policy

You can use the **Test-CalendarConnectivity** cmdlet to verify that Internet calendar sharing is enabled and working properly. The Calendar virtual directory is a subdirectory of the Exchange Outlook Web App virtual directory.

Calendar Repair Assistant

The Calendar Repair Assistant (CRA), which was introduced in Exchange 2010 RTM, is a mailbox assistant that runs within the Microsoft Exchange Mailbox Assistants service on servers running Exchange 2010 with the Mailbox server role installed. CRA automatically detects and corrects inconsistencies that occur for single and recurring meeting items for mailboxes homed on that Mailbox server so that recipients won't miss meeting announcements or have unreliable meeting information. In Exchange 2010 SP1, the Calendar Repair Assistant checks for and detects the following new scenarios:

- The attendee's calendar is missing an occurrence or an exception of a meeting.
- The attendee's start or end time doesn't match the organizer's start or end time, including time zone inconsistencies.
- The attendee's meeting location is different from the organizer's meeting

location.
- The meeting organizer's calendar is missing an item.
- The attendee's recurrence pattern of a meeting series is different from the organizer's recurrence pattern.

For more information, see Understanding Calendar Repair.

Mailbox Assistants Service Troubleshooter

The **Test-AssistantHealth** cmdlet is a new cmdlet that can help you troubleshoot the health of the Microsoft Exchange Mailbox Assistants service (MSExchangeMailboxAssistants). Use the Test-AssistantHealth cmdlet to verify that the Mailbox Assistants service is healthy, to recover from health issues, and to report the status of the diagnosis or recovery action.

1.1.4.3 New High Availability and Site Resilience Functionality in Exchange 2010 SP1

New High Availability and Site Resilience Functionality in Exchange 2010 SP1

Applies to: *Exchange Server 2010 SP1*

Topic Last Modified: *2012-04-25*

Microsoft Exchange Server 2010 Service Pack 1 (SP1) includes new features, as well as enhancements to features introduced in the release to manufacturing (RTM) version of Exchange 2010. The new and improved features extend the scenarios in which you can achieve data and service availability for your Exchange 2010 environment.

The following new features for high availability and improvements to existing high availability features are available in Exchange 2010 SP1:

- Continuous replication - block mode
- Active mailbox database redistribution
- Enhanced datacenter activation coordination mode support
- New and enhanced management and monitoring scripts
- Exchange Management Console user interface enhancements
- Improvements in failover performance
- Extensible Storage Engine recovery on hung I/O

These features are discussed in greater detail below.

Continuous Replication - Block Mode

In the RTM version of Exchange 2010 and in all versions of Exchange Server 2007, continuous replication operates by shipping copies of the log files generated by the active database copy to the passive database copies. Beginning with Exchange 2010 SP1, this form of continuous replication is known as *continuous replication - file mode*. Exchange 2010 SP1 also introduces a new form of continuous replication known as *continuous replication - block mode*. In block mode, as each update is written to the active database copy's active log buffer, it's also shipped to a log buffer on each of the passive mailbox copies. When the log buffer is full, each database copy builds, inspects, and creates the next log file in the generation sequence. If a failure affects the active copy, the passive copies will have been updated with most or all of the latest updates. The active copy

doesn't wait for replication to complete to preclude replication issues from affecting the client experience.

Continuous replication - block mode is only active when continuous replication is up-to-date in file mode. The transition into and out of block mode is performed automatically by the log copier. Block mode dramatically reduces the latency between the time a change is made on the active copy and when the change is replicated to passive copies. In addition to replicating individual log file writes, block mode also changes the activation process for a passive copy. If a copy is in block mode when a failure occurs, the system uses whatever partial log content is available during the activation process. This eliminates the current log file on the active copy from being a single point of failure.

Active Mailbox Database Redistribution

Exchange 2010 SP1 includes a script called RedistributeActiveDatabases.ps1 that can be periodically run by administrators to balance the distribution of active database copies across a database availability group (DAG) based on administrator-configured activation preference. In addition, copy distribution awareness has been added to the Active Manager best copy selection process. Specifically, the first pass of best copy selection for lossless switchovers now sorts the possible targets by preference instead of least loss.

Enhanced Datacenter Activation Coordination Mode Support

Exchange 2010 RTM includes a configuration mode for DAG site resilience support called Datacenter Activation Coordination (DAC) mode. In DAC mode, Exchange cmdlets can be used to perform a data center switchover. In the RTM version, DAC mode is limited to DAGs with at least three members that have at least two or more members in the primary data center.

In Exchange 2010 SP1, DAC mode has been extended to support two-member DAGs that have each member in a separate data center. DAC mode support for two-member DAGs uses the witness server to provide additional arbitration. In addition, DAC mode has been extended to support DAGs that have all members deployed in a single Active Directory site, including single Active Directory sites that have been extended to multiple locations.

New and Enhanced Management and Monitoring Scripts

Exchange 2010 SP1 includes several new and enhanced scripts that greatly improve the management and monitoring experience:

- **CheckDatabaseRedundancy.ps1** *(new)* You can use this script to check the redundancy of replicated databases, and it will generate events if database resiliency is found to be in a compromised state (for example, there's only one healthy copy of a replicated database). The script is accompanied by a Microsoft System Center Operations Manager 2007 management pack change that can be used to monitor databases without redundancy, which is particularly useful in environments without RAID.
- **StartDagServerMaintenance.ps1 and StopDagServerMaintenance.ps1** *(new)* You can use StartDagServerMaintenance.ps1 to take a DAG member out of service for maintenance. It will move active databases off of the server and block databases from moving to that server. It will also make sure all critical DAG support functionality (for example, the Primary Active Manager PAM role) that might be on the server is moved to another server, and blocked from moving back to the server. Another script, StopDagServerMaintenance.ps1, is

provided to complete the operation and remove the blocks.

- **CollectOverMetrics.ps1** *(enhanced)* You can use this script to collect switchover and failover data. This script has been enhanced in Exchange 2010 SP1 to include metrics for continuous replication - block mode, and more details from the replication and replay pipeline. In addition, it also features enhanced reporting.
- **CollectReplicationMetrics.ps1** *(enhanced)* This script is an active form of monitoring because it collects metrics related to continuous replication in real time while the script is running. The script supports parameters that enable you to customize the script's behavior and output.

Enhanced Exchange Management Console User Interface

Exchange 2010 SP1 includes Exchange Management Console (EMC) enhancements for managing DAGs. For example, the EMC now includes support for managing IP addresses and alternate witness server settings for DAGs. It's no longer necessary to use the Exchange Management Shell to configure these settings.

Improved Failover Performance

Exchange 2010 SP1 includes changes to improve failover and switchover performance and behavior. In the RTM version of Exchange 2010, when either a failover or a switchover occurs, the passive copy being activated immediately stops replaying log files that were copied to that passive copy. The active copy is then dismounted (if it's not already), and any remaining log files are copied to the passive copy being activated. Assuming that any missing data is within the automatic database mount dial setting, the passive copy is made the new active copy and the database is mounted in a dirty shutdown state. At this point, all log files that were copied to the previously passive (and now active) copy will be replayed to make the database consistent.

In Exchange 2010 SP1, when either a failover or a switchover occurs, the Microsoft Exchange Replication service on the passive copy being activated continues to replay log files that have been copied to the passive copy until the last log file generated by the active copy is copied to it. This enables a mount operation to be performed against a database that is in a nearly consistent state.

Other performance-enhancing changes involve time-outs and other algorithmic details to improve failover performance as well as I/O performance after failovers.

Extensible Storage Engine Recovery on Hung I/O

Exchange 2010 SP1 includes new recovery logic that makes use of the built-in Windows bugcheck behavior when certain conditions occur. Specifically, Extensible Storage Engine (ESE) has been updated to detect when I/O is hung and to take corrective action to automatically recover the server. ESE maintains an I/O monitoring thread that detects when an I/O has been outstanding for a specific period of time. By default, if an I/O for a database is outstanding for more than one minute, ESE logs an event. If a database has an I/O outstanding for greater than 4 minutes, ESE logs a specific failure event, if it’s possible to do so. ESE event 507, 508, 509, or 510 may or may not be logged, depending on the nature of the hung I/O. If the problem is such that the operating system volume is affected or the ability to write to the event log is affected, the events aren’t logged. If the events are logged, the Microsoft Exchange Replication service (MSExchangeRepl.exe) intentionally terminates the wininit.exe process to cause a bugcheck of Windows.

In some cases, the entire storage stack may be affected by the hang, making it impossible to write failure events to the crimson channel or any other area of the Windows Event Log. ESE also monitors the crimson channel by verifying that the event log can be written to. If writing to the event log fails for a long period of time, MSExchangeRepl intentionally causes a bugcheck of Windows by terminating wininit.exe. When the operating system I/O is hung, the system is obviously unable to write any ESE events to the event log.

Note:

Applications and Services logs are a new category of event logs in Windows Server 2008. These logs store events from a single application or component rather than events that might have system-wide impact. This new category of event logs is referred to as an application's *crimson channel*. For more information, see Monitoring High Availability and Site Resilience

This new bugcheck-based recovery feature in Exchange 2010 SP1 is designed to make recovery from hung I/O or a hung controller fast, rather than re-trying or waiting until the storage stack raises an error that causes failover. When the bugcheck occurs, the error code reads as follows:

```
CRITICAL_OBJECT_TERMINATION (f4)

A process or thread crucial to system operation has unexpectedly exited or been terminated.
```

Warning:

The presence of this bugcheck error code doesn't necessarily mean that Exchange was the cause of the error. Any termination of wininit.exe, including one performed by an administrator using Task Manager or some other task management tool, will cause the same bugcheck error code.

1.1.4.4 New Messaging Policy and Compliance Functionality in Exchange 2010 SP1

New Messaging Policy and Compliance Functionality in Exchange 2010 SP1

Exchange Server 2010 > Getting Started With Exchange 2010 > What's New in Exchange 2010 SP1 >

[This topic is in progress.]

Applies to: *Exchange Server 2010 SP1*

Topic Last Modified: *2011-01-26*

Microsoft Exchange Server 2010 Service Pack 1 (SP1) includes new features, as well as enhancements to features that were introduced in the release to manufacturing (RTM) version of Exchange 2010.

This topic provides a brief description of new functionality for existing features and information about new features related to messaging policy and compliance in Exchange 2010 SP1.

Personal Archive Functionality

Personal archive functionality in Exchange 2010 SP1 includes the following:

- **Provision personal archive on a different mailbox database** You can provision a user's personal archive on a different mailbox database than the

one where the user's primary mailbox resides. This capability allows you to implement a tiered storage topology.

- **Import historical mailbox data to archive** You can import historical mailbox data from .pst files directly to the user's personal archive using the **New-MailboxImportRequest** cmdlet in the Shell. Data from .pst files can also be imported to the user's primary mailbox, and both the personal archive and the primary mailbox can be exported to .pst files using the **New-MailboxExportRequest** cmdlet.
- **Delegate access to archive** Delegates can access the delegating user's archive mailbox using Microsoft Office Outlook 2010, in addition to the primary mailbox.

For more information, see Understanding Personal Archives.

Messaging Records Management Functionality

Messaging records management functionality in Exchange 2010 SP1 includes the following:

- **New retention policy management features in EMC** You can use the New Retention Policy Tag and New Retention Policy wizards in the Exchange Management Console (EMC) to manage retention tags and retention policies.
- **Support for Notes default folder** You can also create retention policy tags for the Notes default folder.
- **Default retention and archive policy** The default archive policy and retention policy contains retention tags that move messages to the archive and remove messages from the mailbox after a certain period. The policy is automatically applied to a mailbox user when you provision a personal archive for the user.
- **Opt-in personal tags** Users with a retention policy assigned can use the Exchange Control Panel (ECP) to select personal tags not included in their retention policy. Users can then apply these personal tags to mailbox items and custom folders.

For more information, see Understanding Retention Tags and Retention Policies.

Multi-Mailbox Search Functionality

Multi-Mailbox Search functionality in Exchange 2010 SP1 includes the following:

- **Multi-Mailbox Search preview** In Exchange 2010 SP1, discovery managers (that is, users who are members of the Discovery Management management role group) can get an estimate of the number of items returned by a discovery search before the items are copied to the selected discovery mailbox. This functionality allows discovery managers to view the number of hits the specified keywords return, and then modify the search query, if required, before messages returned by the search are copied to the discovery mailbox.
- **Annotations** Discovery managers can also add annotations to messages returned by the discovery search.
- **Data de-duplication** Multi-Mailbox Search includes the optional data de-duplication feature. When selected, Multi-Mailbox Search copies only a single instance of a message returned across multiple folders within the same mailbox, or across different mailboxes.

For more information, see Understanding Multi-Mailbox Search.

Information Rights Management

Functionality

Information Rights Management (IRM) functionality in Exchange 2010 SP1 includes the following:

- **WebReady Document Viewing of IRM-protected attachments** In Exchange 2010 SP1, IRM in Microsoft Office Outlook Web App supports WebReady Document Viewing of supported IRM-protected attachments, allowing users to view IRM-protected attachments without having to download them. Users can preview IRM-protected documents on computers that don't have Microsoft Office installed. Along with the cross-browser and cross-platform support in Outlook Web App, this functionality extends the reach of IRM to various browsers and operating systems. For more information, see Understanding Information Rights Management in Outlook Web App.
- **IRM in Exchange ActiveSync** IRM in Exchange ActiveSync allows users with supported devices to access IRM-protected messages without first having to activate the device for IRM by tethering the device to a computer. For more information, see Understanding Information Rights Management in Exchange ActiveSync.
- **Cross-organization support** Exchange 2010 SP1 IRM features are supported in cross-organization topologies for easier collaboration between two organizations via OWA.
- **IRM logging** In Exchange 2010 SP1, you can enable logging of IRM features on the Mailbox, Hub Transport, Client Access, and Unified Messaging server roles. IRM logs contain detailed transaction and error information, allowing administrators to easily monitor and troubleshoot IRM features. For more information, see Understanding Information Rights Management Logging.
- **Discovery Manager access to IRM-protected messages in a Discovery mailbox** In Exchange 2010 SP1, you can configure IRM to allow members of the Discovery Management role group to access IRM-protected messages returned by discovery search. For more information, see Understanding Information Rights Management.

Mailbox Audit Logging Functionality

Exchange 2010 SP1 includes new logging functionality that allows you to enable logging of mailbox access. Mailbox audit logging enables you to log access to a mailbox by administrators, delegates, and mailbox owners. Actions taken on mailbox items such as access to a message or a folder, copying, and deletion of a message can be logged. You can search mailbox audit logs for a mailbox, and also generate reports of non-owner access to a mailbox from the Exchange Control Panel.

For more information, see Understanding Mailbox Audit Logging.

1.1.4.5 New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1

New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1

Applies to: *Exchange Server 2010 SP1*

Topic Last Modified: *2012-10-30*

The Unified Messaging server role has been improved in Microsoft Exchange Server 2010 Service Pack 1 (SP1), and new features have been added. To use some of these new

features, you must correctly deploy Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010 (the next generation of Office Communications Server) in your environment. This topic discusses the new and improved features that are added when you install Exchange 2010 SP1.

UM Features Found in Exchange 2010 SP1

The following is a list of the new features in Exchange 2010 Unified Messaging (UM) and a description of the features:

- **UM management in the Exchange Control Panel** The UM management user interface in the Exchange Control Panel makes it possible to manage all components of Unified Messaging in a Web browser. You can create UM dial plans, UM mailbox policies, UM IP gateways, and UM auto attendants, and enable users for Unified Messaging. This feature is available to tenant administrators (also called specialists) and to administrators in cross-premises Exchange environments. For details, see Managing Administrator and Specialist Users.
  Administrators can also use the Exchange Control Panel to manage some on-premises and cross-premises tasks. The following is a list of some of the additional administrative features available in the Exchange Control Panel for all server roles, including:
  - Text messaging integration
  - Voice messaging integration
  - Multiple mailbox search
  - Additional proxy addresses for mailboxes
  - Moderation and approval for distribution list submission

  In addition, end users can perform common administrative tasks in the Exchange Control Panel without having to call their helpdesk. This helps them to be more productive and reduces support costs.
  Although the Exchange Control Panel is available to Exchange administrators for managing Unified Messaging in a cross-premises environment, as a best practice, the Exchange Management Console and the Exchange Management Shell are the preferred tools for creating and configuring UM components.
- **UM reporting** The UM reporting features added in Exchange 2010 SP1 include call summaries and statistics and call details for UM-enabled users. These reports are displayed in the Exchange Control Panel. You can access Unified Messaging statistic reports by using **Call Statistics** in EMC and access call logs by using **User Call Logs**, also in the EMC. Both tools are located under the Toolbox node. They provide aggregated statistical information about calls for UM servers and calls for UM-enabled users. To support the UM reporting tools in the EMC, the following cmdlets have been added for SP1:
  - **Get-UMCallSummaryReport**
  - **Get-UMCallDataRecord**

  In the EMC toolbox, **Call Statistics** provides aggregated statistical information about calls forwarded to or placed by UM servers and can be used by administrators interested in overall statistics for the Exchange 2010 Unified Messaging servers in their organization. The results of the call statistics reports you request in the EMC are displayed in the Exchange Control Panel user interface. They can be filtered to show call statistics by month or by day for the past 90 days or since UM was deployed in your organization. You can then filter these results by UM dial plan and UM IP gateway within your organization.
  Call statistics reports display:
  - The total number of calls organized by type of call (for example, missed calls, Outlook Voice Access calls, or fax calls).
  - Whether the call was accepted or rejected.
  - The average audio quality.
  - The day or the month covered in the report, or all calls.

You can export the call logs to a Microsoft Office Excel template, or copy the call statistics information to the Clipboard so that it can be pasted into another application. You can use the **Audio Quality Details** button to display more specific information about the call, including:

- Date
- UM dial plan
- UM IP gateway
- Type of audio codec
- NMOS
- NMOS degradation
- Jitter
- Pack loss
- Round trip time
- Burst Loss Duration
- Number of calls sampled

For more information about the specific information that's available for calls, see Using Unified Messaging Tools.

You can use **User Call Logs** in the EMC toolbox to view the call statistics for a selected UM-enabled user. The report is displayed in the Exchange Control Panel and is useful in helpdesk-type situations where you have to gather information about specific calls for a UM-enabled user to assist them in diagnosing and fixing issues. After you click **Select a user** and specify the user, the following information will be displayed for calls of the UM-enabled user you selected:

- Date and time
- Duration of the call
- Type of call
- The calling number
- The called number
- The UM IP gateway
- Audio quality

You can copy the user's call statistics to the Clipboard and then paste them into another application. You can use the **Audio Quality Details** button to display more specific information about the call including:

- Date
- UM dial plan
- UM IP gateway
- Type of audio codec
- NMOS
- NMOS degradation
- Jitter
- Pack loss
- Round trip time
- Burst Loss Duration

For more information about the specific information that's available for calls, see Using Unified Messaging Tools.

- **Cross-forest migration of UM-enabled mailboxes** Before Exchange 2010 SP1, there wasn't a way to efficiently move UM-enabled mailboxes from a source Exchange 2010 forest to a target Exchange 2010 forest when performing any kind of Enterprise cross-forest migration. The only way to do this was to first disable the mailbox for UM in the source forest, and then move the mailbox to the target forest. If you were moving an Exchange Server 2007 mailbox, you would use the **Move-Mailbox** cmdlet. If you were moving an Exchange 2010 mailbox, you would use the **New-MoveRequest** cmdlet. After you moved the mailbox to the target forest, you would then enable the mailbox for UM.

  Following this process created several issues. The process took a long time to complete, the user's voice mail was taken offline, and the UM-enabled user's

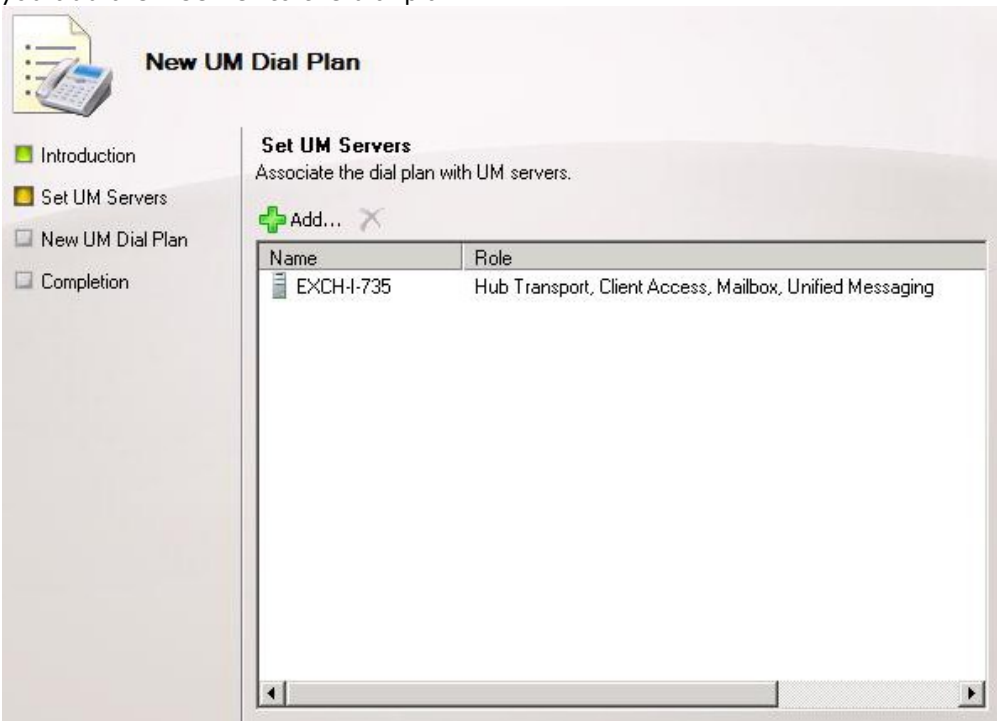
PIN would be reset, which forced the user to set up a new PIN for Outlook Voice Access.
In SP1, the **New-MoveRequest** cmdlet is used with the Mailbox Replication service (MRS) to move a UM-enabled mailbox within a forest, or between multiple forests in on-premises deployments. Using the **New-MoveRequest** cmdlet with the MRS to move the UM-enabled mailbox lets you speed up the process, leaves the user's voice mail online, and doesn't require an Outlook Voice Access user to reset their PIN.
The process for moving UM-enabled mailboxes works as follows in Exchange 2010 SP1:
In your source forest, you have UM-enabled mailboxes that are associated with a UM mailbox policy in the same source forest. You then:

- Identify the target UM mailbox policy that you want to associate with the UM-enabled mailboxes after you have moved them to the target forest.
- Use the **Set-UMMailboxPolicy** cmdlet and specify the name of the UM mailbox policy in the source forest using the *SourceForestPolicyNames* parameter on the UM mailbox policy in the target forest.
- Start moving the UM-enabled mailboxes to the target forest without disabling them. As you migrate the mailboxes, the mailboxes in the source forest will continue to receive voice mail messages and e-mail messages.
- Directly after the migration of the UM-enabled mailbox, the MRS will automatically disable the mailboxes in the source forest.
- In addition to the UM mailbox policy in the target forest, the MRS must have the extension numbers that are already assigned to the users whose mailboxes were moved. The MRS will use the extension numbers to locate the matching UM mailbox policy in the target forest by searching the *SourceForestPolicyNames* parameter on the UM mailbox policy. After the extension numbers and the name of the UM mailbox policy are found, MRS will UM-enable the mailboxes in the target forest.

Note:
The MRS uses RPC over HTTP for cross-forest migrations and RPC over TCP for intra-forest migrations.

- **Outlook Voice Access improvements** In Exchange 2007 and the RTM version of Exchange 2010, UM-enabled users can listen to their voice messages using Outlook Voice Access. By default, a Unified Messaging server retrieves and lists voice messages by date in descending order. For example, if two voice messages are sent, one at 10:00 a.m. and another at 1:00 p.m. the same day, UM will first play the voice message left at 1:00 p.m. and then play the voice message that was left earlier. Now, in SP1, when Outlook Voice Access users sign in to their Exchange 2010 mailbox, they can chose the play order for unread voice mail messages, either oldest first or newest first. Users can configure this order by using the **Voice Mail** tab in Outlook Web App, by managing their voice mail settings in Microsoft Outlook 2010, and by using the menu system in Outlook Voice Access.
- **Caller Name Display** Caller ID resolution has been enhanced in SP1. Names can now be displayed for voice messages from unresolved numbers using Caller Name Display. With Caller Name Display, IP gateways or IP PBXs pass caller name information as part of the SIP FROM header. In some countries, including the United States, the public telephone networks can supply the name of the registered subscriber for the calling phone number. This is administered by the telephone service provider that provides service to the caller. Phones with alphanumeric displays will show the registered name for the caller when the call offers it. With Caller Name Display, instead of displaying “Voice Mail from 4255551234”, the Unified Messaging server can send a voice message that displays “Voice Mail from Tony Smith”.
- **New UM Dial Plan Wizard and Set-UMServer** When you deployed Unified Messaging in Exchange 2010 RTM, you had to add or associate a UM server with a UM dial plan after you created the dial plan. In SP1, you can add or associate a UM server with a UM dial plan when you create a UM dial plan. An

additional page has been added to the **New UM Dial Plan** wizard that lets you add a UM server to the dial plan.



- **Microsoft Lync Server 2010 feature support (cross-premises)** You must deploy Lync Server 2010 if you're deploying UM in a cross-premises environment. UM is fully supported and functional with Lync Server 2010, including Message Waiting Indicator (MWI) notifications.
- **Office Communications Server migration (non-cross-premises)** If you're deploying or migrating from Exchange 2007 to Exchange 2010 and your Exchange deployment is integrated with Office Communications Server, Exchange 2010 SP1 includes support for migration of SIP URI dial plans that are used with Communications Server. Also, in Exchange 2010 SP1, it's no longer required that you have a Communications Server location profile that has the same name as the phone context property of the SIP URI dial plan. The following table summarizes the supported deployments for Microsoft Exchange, Office Communications Server, and Lync Server 2010.

Supported Deployments

	Exchange 2007 SP1, SP2, or SP3 Unified Messaging	Exchange 2010 RTM Unified Messaging	Exchange 2010 SP1 Unified Messaging
Office Communications Server 2007	Supported only in an Enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Supported only in an Enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Not supported
Office Communications Server 2007 R2	Supported only in an Enterprise deployment. Location profile names and UM dial plan phone	Supported only in an Enterprise deployment. Location profile names and UM dial plan phone	Supported only in an Enterprise deployment. Location profile names and UM dial plan phone

	contexts must match.	contexts must match.	contexts don’t have to match.
Lync Server 2010	Supported only in an Enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Supported only in an Enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Supported in a cross- premises or Enterprise deployment. Location profile names and UM dial plan phone contexts don’t have to match.

Note:
Exchange Server 2010 SP1 Unified Messaging no longer supports Office Communications Server 2007. You must use Office Communications Server 2007 R2 or Microsoft Lync Server 2010.

- **Secondary UM dial plan support** In SP1, you can add a secondary UM dial plan for a UM-enabled user. Secondary dial plans allow administrators to assign two extension numbers to a UM-enabled user. Or, you can assign a primary extension number in a UM-enabled user's primary dial plan on one PBX or IPX PBX and a secondary extension for that user within a secondary dial plan that exists on a different PBX or IP PBX.
  When an Exchange 2007 or Exchange 2010 user’s mailbox is enabled for UM, the administrator is required to specify an extension number and a UM mailbox policy. The extension number is needed by a UM server to identify the user when they call in to Outlook Voice Access to access their mailbox. The UM mailbox policy contains a collection of configuration properties, with values that UM uses to apply to a UM-enabled mailbox that's associated with that UM mailbox policy. One of the properties on the UM mailbox policy is the UM dial plan. The dial plan also contains a set of configurable properties that includes a numbering plan. The numbering plan defined on the UM dial plan doesn't allow for duplicate extension numbers. This ensures that the extension number is unique within the dial plan. By linking the extension number to a user in the UM dial plan, Unified Messaging uniquely identifies a UM-enabled user in an organization.
- **New UM language packs** Unified Messaging language packs make it possible for the Exchange 2010 UM server to speak additional languages to callers and recognize languages other than US English (en-US) when callers use Automatic Speech Recognition (ASR) or when voice messages are transcribed. The following is a list of additional UM language packs that are now available but don't contain support for Voice Mail Preview:
  - Catalan (ca-ES)
  - Chinese (Hong Kong) (zh-HK)
  - Danish (Denmark) (da-DK)
  - English (India) (en-IN)
  - Finnish (Finland) (fi-FI)
  - Norwegian (Bokmal) (nb-NO)
  - Russian (ru-RU)

  The following is a list of additional UM language packs that are now available that do contain support for Voice Mail Preview:
  - English (Canada) (en-CA)
  - Polish (pl-PL)
  - Portuguese (Portugal) (pt-PT)
  - Spanish (Spain) (es-ES)

Note:
The RTM version of the Spanish (Spain) (es-ES) UM language pack didn't include support for Voice Mail Preview. Voice Mail Preview

support was added in SP1. For more information about Voice Mail Preview, see Voice Mail Preview for End Users.

By default, when you install the Exchange 2010 Unified Messaging server role, the server will send voice mail previews to UM-enabled users if a supported UM language pack is installed.
There are Exchange 2010 Unified Messaging Voice Mail Preview partners that offer enhanced transcription support for the Voice Mail Preview feature. These partners employ people to correct voice mail transcriptions that were created using Automatic Speech Recognition (ASR). Each Voice Mail Preview partner must meet a set of requirements to be certified to interoperate with Exchange 2010 Unified Messaging.
If you determine that the voice mail previews sent to your users aren't accurate enough, you can contact one of the certified Voice Mail Preview partners listed on the Microsoft PinPoint web page and sign up with them at an additional cost. For more information, see Voice Mail Preview Advisor for Exchange 2010.
You can download the Exchange 2010 UM language packs for SP1 from the Microsoft Download Center. For details, see Install a Unified Messaging Language Pack on a UM Server.

Important:
To ensure that all Unified Messaging features are available in the UM language packs you install, you must install the Exchange 2010 Client and Server Language Pack on each UM server in the dial plan. If you don’t install the Client and Server Language Pack, some features may not work as expected. Some features, like Voice Mail Preview, will work in the language that is configured on the dial plan but when only the UM language pack is installed. However, features like Outlook Voice Access and user interface text won’t work in the language by the user without having both the UM language pack and the Client and Server Language Pack installed. To download and install additional client and server language packs on servers in your organization, see Microsoft Exchange Server 2010 SP1 Language Pack Bundle.

- **Call Answering Rules improvements** Using Call Answering Rules, end users can control how their incoming calls should be handled. Call Answering Rules are applied to incoming calls much as Inbox rules are applied to incoming e-mail messages. For details, see Understanding Call Answering Rules.
  There are two updates to Call Answering Rules in Exchange 2010 SP1:
  - In the RTM version, when a caller who's greeted by a call answering rule selects the voice mail option, a UM server first plays the called party's voice mail greeting before prompting the caller with the instruction to leave a voice message. This can be confusing if the user has created custom greetings. In Exchange 2010 SP1, the voice mail greeting is skipped if the caller has chosen to leave a voice message via a call answering rule that's configured.
  - In Exchange 2010 SP1, a missed call notification won't be left for a user if the inbound call reaches the called party using the Find Me feature, if a call transfer succeeds, or if a voice message is successfully left for the user.
- **Unified Communications Managed API/Speech Platform improvements** Beginning with Exchange 2010 SP1, the UM server relies on Unified Communications Managed API v. 2.0 (UCMA) for its underlying SIP signaling and speech processing. This dependency requires that the UCMA platform and prerequisites be installed on the UM server before Exchange 2010 UM SP1 installation or upgrade. For details, see Overview of Unified Messaging.
  As part of this integration with UCMA, you receive the following benefits when you've integrated UM and Lync Server 2010:
  - Unified Messaging reports Quality of Experience (QoE) data to Lync Server 2010 Quality of Experience Monitoring or QMS servers. This is available in both on-premises and cross-premises integrated environments.
  - UM doesn't drop the first incoming call if the first call to the UM server is

being made from an Enterprise Voice user who's connected the Internet.
- In earlier versions of Office Communications Server, the A/V Edge resources that were associated with the Office Communications Server pool didn't communicate with a specific UM server for a specific call. This led to less-than-optimal media quality in some scenarios. With SP1, you can set, on a per UM-server basis, the Office Communications Server pool and associated A/V Edge server resources that should be used for all calls to and from that specific UM server.

- **UM auto attendant update** In the RTM version of Exchange 2010, a UM auto attendant would play the after hours greeting and the holiday greeting on holidays. In SP1, UM auto attendant will play only the holiday greeting on a holiday.
- **Exchange 2010 UM Troubleshooting Tool** Use the **Test-ExchangeUMCallFlow** cmdlet to test call flow between UM servers, IP gateways, and SIP servers. With the **Test-ExchangeUMCallFlow** cmdlet, you can diagnose configuration errors found in telephony components, Exchange 2010 SP1 Unified Messaging settings, and connectivity issues between on-premises and cross-premises Unified Messaging deployments.
  The **Test-ExchangeUMCallFlow** cmdlet can be used to diagnose configuration errors specific to call answering scenarios and to test whether voice mail is functioning correctly in Office Communications Server 2007 R2 or Microsoft Lync Server 2010 and non-Office Communication Server 2007 R2 or Lync Server 2010 deployments for both on-premises and cross-premises UM deployments. This cmdlet emulates calls, runs a series of diagnostic tests, and outputs the cause and possible solutions for potential issues that are detected. It also outputs general audio quality metrics for diagnosing audio quality issues related to network connectivity such as jitter and average packet loss. The **Test-ExchangeUMCallFlow** cmdlet supports testing UM components in Secured, SIP Secured, and Unsecured calls and can be run either in `Gateway` or `SIPClient` modes.

  Important:
  The **Test-ExchangeUMCallFlow** cmdlet must be used to test only the voice mail functionality of a Microsoft Exchange Server 2010 Unified Messaging server that has Service Pack 1 (SP1) installed.

  The **Test-ExchangeUMCallFlow** cmdlet can be installed on a local Unified Messaging server or on another 64-bit computer running:
  - The Windows Vista or Windows 7 operating system
  - The Windows Server 2008 or Windows Server 2008 R2 operating system

  The **Test-ExchangeUMCallFlow** cmdlet requires the components below be installed on a Windows 7, Windows Vista, or Windows Server 2008 64-bit computer prior to installing the cmdlet:
  - Microsoft .NET Framework 3.5 Service Pack 1 (SP1) To download the service pack, see Microsoft .NET Framework 3.5 Service Pack 1.
  - Microsoft .NET Framework 3.5 Family Update for Windows Vista x64 and Windows Server 2008 x64 updates if the tool will be run on a Windows Vista or Windows Server 2008 computer To download the update, see Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64.
  - Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu) For more information, see Microsoft Knowledge Base article 968930, Windows Management Framework core package (Windows PowerShell 2.0 and WinRM 2.0).
  - Unified Communications Managed AP1 2.0, Core Runtime (64-bit) To download the UcmaRuntimeWebDownloadX64.msi program file, see Unified Communications Managed API 2.0, Core Runtime (64-bit).

The **Test-ExchangeUMCallFlow** cmdlet isn't included on the Exchange 2010 SP1 DVD or the Exchange 2010 SP1-only download. However, you can download the cmdlet from the

Microsoft Download Center.

1.1.4.6 New Exchange Core Store Functionality in Exchange 2010 SP1

New Exchange Core Store Functionality in Exchange 2010 SP1

Applies to: *Exchange Server 2010 SP1*

Topic Last Modified: *2010-07-13*

Microsoft Exchange Server 2010 Service Pack 1 (SP1) includes new features, as well as enhancements to features introduced in the release to manufacturing (RTM) version of Exchange Server 2010. This topic describes the new functionality in Exchange 2010 SP1 that's available for the following:

- Microsoft Exchange Information Store
- Mailbox databases
- Public folders and public folder databases

Exchange Information Store

Exchange 2010 RTM introduced store limits to prevent a single application or single user from using all the available connections to the Microsoft Exchange Information Store. In Exchange 2010 SP1, for any connections by users with administrative privileges, the session limits have been increased to 64,000 maximum sessions per server.

For more information, see Exchange Store Limits.

Mailbox Databases

The following describes new functionality related to mailbox databases in Exchange 2010 SP1:

- **Mailbox Database Repair Requests** In Exchange 2010 RTM and earlier, you could repair a mailbox with the Information Store Integrity Checker (Isinteg.exe) tool. To repair mailboxes, you needed to dismount the mailbox database on which that mailbox resided and run the fixes while the database was offline. Exchange 2010 SP1 introduces the **New-MailboxRepairRequest** cmdlet that allows you to detect and repair a corrupted mailbox while leaving the mailbox database online.
  For more information, see the following topics:
  - Managing Repair Requests
  - New-MailboxRepairRequest
- **Database Log Growth Troubleshooter** The Database Log Growth Troubleshooter script (Troubleshoot-DatabaseSpace.ps1) detects and takes action on excessive log growth that can cause the health of the Mailbox server to be at risk. By default, the configurable troubleshooter runs every 15 minutes to determine the amount of space available on the hard drive. If the hard drive space is less than 25 percent, the troubleshooter runs an algorithm to determine if the problem is caused by excessive log growth. If excessive log growth is the problem, the troubleshooter quarantines or throttles the mailboxes that are causing the excessive log growth. For more information, see Manage Database Log Growth by Using the Troubleshoot-DatabaseSpace.ps1 Script in the Shell.

- Database Latency Troubleshooter The Database Latency Troubleshooter script (Troubleshoot-DatabaseLatency.ps1) detects and takes action on high latencies on a database. For more information, see Manage Database Latencies by Using the Troubleshoot-DatabaseLatency.ps1 Script in the Shell.

Remove-StoreMailbox

The new Remove-StoreMailbox cmdlet allows you to permanently remove soft-deleted and disconnected mailboxes.

Public Folders and Public Folder Databases

The following changes were made to public folders and public folder databases in Exchange 2010 SP1:

- The AggregatePFData.ps1 script now aggregates statistics across all public folder replicas. For more information, see View Public Folder Item Statistics.
- You can now use the Exchange Management Console to configure client permissions for public folders. For more information, see Use the Public Folder Management Console to Manage Public Folder Settings.
- The New-PublicFolderDatabaseRepairRequest cmdlet has been added to allow you to detect and correct replication issues in the public folder database. This cmdlet replaces the Isinteg.exe tool. For more information, see Create a Public Folder Database Repair Request.

1.1.4.7 New Transport Functionality in Exchange 2010 SP1

New Transport Functionality in Exchange 2010 SP1

Applies to: *Exchange Server 2010 SP1*

Topic Last Modified: *2012-07-19*

Microsoft Exchange Server 2010 Service Pack 1 (SP1) includes new features, as well as enhancements to features introduced in the release to manufacturing (RTM) version of Exchange 2010.

This topic provides an overview of the following new features and improvements for Transport in Exchange 2010 SP1:

- MailTips functionality
- Message tracking functionality
- Throttling enhancements
- Shadow redundancy promotion
- SMTP failover and load balancing improvements
- Support for Extended Protection on SMTP communications
- Send connectors over reliable connections

MailTips Functionality

Here is a brief overview of MailTips features that were added in Exchange 2010 SP1:

- **MailTips access control over organizational relationships** You have granular control over the way MailTips are shared between your organization and other organizations with which you configured an organizational sharing relationship. You can control the types of MailTips that are shared and even designate a specific group of users for which to return MailTips.
- **MailTips monitoring and troubleshooting** Several new monitoring capabilities for MailTips were added in Exchange 2010 SP1. New capabilities include changes to event log entries, alerts, and performance monitor counters.

For more information, see Understanding MailTips.

Message Tracking Functionality

Here is a brief overview of message tracking features that were added in Exchange 2010 SP1:

- **Improved error messages for delivery reports** There may be situations where a user attempts to access delivery reports for a specific message but is unable to view the report. For example, a user may attempt to access delivery reports for a message immediately after sending it, but before the tracking information for that message is inserted into the logs. In these types of scenarios, the messages displayed to the users have been greatly improved, providing specific explanations as to why the information isn't available.
- **Message tracking monitoring and troubleshooting** Several new monitoring capabilities for message tracking were added in Exchange 2010 SP1. These include new event log entries, alerts, and performance monitor counters.
- **Message tracking trace levels** When you're troubleshooting message tracking, you can now request complete logs of every operation that was executed by a Client Access server processing a delivery report request.

For more information, see Understanding Message Tracking.

Throttling Enhancements

Transport servers in Exchange 2010 SP1 keep track of the current state of the overall Exchange organization and modify the way they handle messages accordingly. This allows the Transport servers to respond proactively to potentially problematic situations, improving the reliability of the overall message delivery.

In Exchange 2010 SP1, Transport servers maintain a running average delivery cost of messages sent by individual senders. If a user keeps sending costly messages, such as those addressed to large audiences or tha have large attachments, Transport servers start to give priority to other messages that have a lower cost before it processes messages from that sender. For example, if a user is sending multiple messages that have 10MB attachments, Transport starts to first process other messages that don’t have attachments before it handles additional messages from this particular sender.

Transport also keeps track of the RPC utilization of mailbox servers. A Hub Transport server makes RPC connections to a mailbox server for message delivery. If a Hub Transport server detects that a mailbox server is under RPC resource pressure, it scales back the RPC sessions that it opens to that mailbox server. This way, interactive client connections to the mailbox server take precedence over message delivery when it comes to utilizing RPC resources on a mailbox server.

Back pressure is a system resource monitoring feature of the Microsoft Exchange Transport service that exists on Hub Transport and Edge Transport servers In Exchange 2010. Exchange Transport can detect when vital resources, such as available hard disk

space and memory, are under pressure, and take action to try to prevent service unavailability. All configuration options for back pressure are available in the EdgeTransport.exe.config application configuration file.

In Exchange 2010 Service Pack 1, the default values in EdgeTransport.exe.config are revised for following parameters:

- *SmtpStartThrottlingDelayInterval*: decreased from 10 seconds to 1 second
- *SmtpStepThrottlingDelayInterval*: decreased from 5 seconds to 1 second

For more information about the EdgeTransport.exe.config file, see Understanding the EdgeTransport.exe.Config File.

For more information about back pressure configuration, see Understanding Back Pressure.

For more information about throttling, see Understanding Message Throttling.

Shadow Redundancy Promotion

Exchange 2010 introduced the shadow redundancy feature to minimize the loss of any message during delivery after it enters the Exchange organization. Exchange Transport servers achieve this by using the shadow redundancy SMTP protocol extension.

However, in any organization Exchange Transport servers need to communicate with other third-party SMTP servers that may not support the shadow redundancy protocol. This is especially true with Edge Transport servers that handle message traffic with various hosts on the Internet. When receiving messages from hosts that don't support shadow redundancy in Exchange 2010 RTM, Transport servers delay sending acknowledgement to incoming messages until they verify final delivery within the organization. However, when a specific threshold was reached, the Transport server issued an acknowledgement even if final delivery wasn't verified. This presented a scenario where messages received from hosts that don't support shadow redundancy can be lost in transit.

To address this issue, a new feature called *shadow redundancy promotion* is introduced in Exchange 2010 SP1. When faced with the scenario described above, instead of issuing an acknowledgment without delivery confirmation, a Transport server now routes the message to any other Transport server within the site so that the message is protected by shadow redundancy.

There are additional details about how this scenario works. To learn more, see Understanding Shadow Redundancy.

SMTP Failover and Load Balancing Improvements

Exchange 2010 SP1 improves the way Transport servers detect unhealthy servers and use enhanced DNS. Enhanced DNS distributes the load evenly when all servers are healthy, but in the case of an unavailable server, the load distribution among the remaining healthy servers may not be evenly balanced.

To address this issue, each Exchange 2010 SP1 Transport server maintains a list of unavailable servers. When routing a message, each server uses this information to filter out the known unavailable servers from the set of target servers. For example, assume that a Hub Transport server needs to route several messages to another Active Directory site which has three Hub Transport servers (Hub1, Hub2, and Hub3). If the server knows

that Hub2 is unavailable, it'll remove that server from the list of possible targets and only route to Hub1 and Hub3. It'll assume only two servers, Hub1 and Hub3, exist in the remote Active Directory site when load balancing messages.

As a result, Exchange 2010 SP1 Transport servers always distribute the load evenly between healthy servers and avoid any servers that are unavailable for any reason. For more information, see Understanding SMTP Failover and Load Balancing in Transport.

Support for Extended Protection on SMTP Communications

Windows offers channel binding to protect NTLM authentication over encrypted channels from authentication relay attacks. In Exchange 2010, all services provided by Exchange have been updated to support Extended Protection for Authentication. For more information, see Microsoft Knowledge Base article 968389, Extended Protection for Authentication.

To support this feature in Transport, the Receive connectors have been updated. You can allow, require, or disable Extended Protection for Authentication on your Receive connectors. For more information, see Understanding Receive Connectors.

Send Connectors over Reliable Connections

With Exchange 2010 SP1, several new features were added to the Send connectors. Most changes are to support coexistence with Exchange Online. In addition, the ability to downgrade connection failures was added to the Send connectors.

You may have dedicated Send connectors that are responsible for transmitting messages over well-defined communication channels that are expected to always be available, such as a Send connector dedicated to send messages to Exchange Online. On such connections, many of the typical errors that are possible on ordinary destinations on the Internet aren't expected. In this scenario, you may want to treat any communication errors as transient as opposed to issuing non-delivery reports (NDRs). With Exchange 2010 SP1, you can configure a Send connector to downgrade authentication and name resolution errors, which would normally result in an NDR, to transient errors. In these cases, Exchange will attempt delivery again instead of issuing an NDR.

For more information, see Understanding Send Connectors.

1.1.4.8 Release Notes for Exchange Server 2010 SP1

Release Notes for Exchange Server 2010 SP1

Exchange Server 2010 > Getting Started With Exchange 2010 > What's New in Exchange 2010 SP1 >

Applies to: *Exchange Server 2010 SP1*

Topic Last Modified: *2011-04-19*

For important legal information, see Legal Notice later in this document.

Welcome to Microsoft Exchange Server 2010. This document contains the following sections:

Functionality Available in Exchange 2010 SP1

Exchange 2010 Service Pack 1 (SP1) adds new and revised functionality. For more information, see What's New in Exchange 2010 SP1.

Installing Exchange 2010 SP1

Consider the following when you deploy Exchange 2010 SP1:

- You can now select a new option that installs the required Microsoft Windows operating system roles and features for each selected Exchange 2010 SP1 server role.
- You can only install Exchange 2010 SP1 on computers running Windows Server 2008 Service Pack 2 (SP2) and Windows Server 2008 R2.
- Although it isn't a recommended configuration, single-label Domain Name System (DNS) domain names are now supported for use with Exchange 2010 SP1.
- If you're running the beta release of Exchange 2010, you must uninstall the beta release before you install the SP1 version of Exchange 2010.
- If you upgrade an Edge Transport server that's running Forefront Threat Management Gateway (TMG) and has Forefront Protection for Exchange Server (FPE) enabled for SMTP protection, the Forefront TMG Managed Control service may fail to start.

For detailed information about the requirements and steps for installing Exchange 2010 SP1, see the following topics:

- Exchange 2010 Prerequisites
- Exchange 2010 System Requirements
- Understanding a New Installation of Exchange 2010
- Understanding Upgrade to Exchange 2010
- Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3

Mailbox Moves

The process for moving mailboxes has changed to help make sure that no data is unintentionally lost due to issues that may occur around the same time as a move, such as a lossy failover on the target database.

When mailboxes are moved from an Exchange 2010 SP1 database to any other database, Exchange no longer fully deletes the mailbox from the source database immediately upon completion of the move. Instead, the mailbox in the source mailbox database is switched to a *soft-deleted* state, which allows mailbox data to be accessed during a mailbox restore operation by using the new **MailboxRestoreRequest** set of cmdlets.

These soft-deleted mailboxes are visible when running the Get-MailboxStatistics cmdlet against a database and can be identified by having the property **DisconnectReason** with a value of `SoftDeleted`. The soft-deleted mailboxes will be retained in the source

database until either the deleted mailbox retention period expires or the mailbox is purged by using the Remove-StoreMailbox cmdlet. As a result of this change, if you're performing mailbox moves to reduce the amount of space being used in a database, you must also perform the additional step of purging the soft-deleted mailbox. Soft-deleted mailboxes can't be reconnected.

Note:

You won't be able to view soft-deleted mailboxes by using the Get-MailboxStatistics cmdlet in Exchange versions earlier than Exchange 2010 SP1.

If necessary, you can restore data from these soft-deleted mailboxes by using the **MailboxRestoreRequest** set of cmdlets, which is initiated with the New-MailboxRestoreRequest cmdlet. The **MailboxRestoreRequest** cmdlets replace the legacy **Restore-Mailbox** cmdlet. In addition to having the same capabilities as the **Restore-Mailbox** cmdlet, the **MailboxRestoreRequest** cmdlets perform additional tasks, including the ability to:

- Restore from rehomed or soft-deleted mailboxes that aren't in a recovery database.
- Be processed asynchronously (like a mailbox move in Exchange 2010).
- Restore data into an archive mailbox.

Known Issues with Mailbox Moves

The following are known issues associated with mailbox moves.

MRSProxy

An Exchange 2010 SP1 change to the Mailbox Replication Proxy (MRSProxy) service requires you to apply a Microsoft .NET Framework hotfix before you can move mailboxes across forests. If you don't apply the .NET Framework hotfix, you may receive transient exceptions on the remote forest due to MRSProxy failures, which leads to a series of "another administrator is moving the mailbox" error messages. Sometimes, the move request recovers and retries the move, but eventually the move will fail due to too many transient failures. In Event Viewer on the Client Access server, you will receive an error message similar to the following:

Log Name: Application

Source:.NET Runtime

Date:6/14/2010 3:56:55 PM

Event ID: 1023

Task Category: None

Level: Error

Keywords: Classic

User: N/A

Computer: CAS01.contoso.com

Description: .NET Runtime version 2.0.50727.4200 - Fatal Execution Engine Error (000007FEF884664E) (80131506)

You need to apply the hotfix to all Exchange 2010 SP1 Client Access servers in both forests. For more information about this hotfix and how to download it, see Microsoft Knowledge Base article 971030, FIX: An access violation occurs when you run a .NET

Framework 2.0-based application that has a virtual call the IList<T>, IEnumerable<T>, or ICollection<T> interface in an LCG method.

Move Request Versioning

When performing a cross-forest mailbox move, the Exchange 2010 RTM version of the Microsoft Exchange Mailbox Replication service (MRS) and the MRSProxy service can't log into an Exchange 2010 SP1 Mailbox server. This functionality is intentional. It prevents errors when moving mailboxes across Exchange versions to provide for new functionality such as soft-deletes. To prevent this issue from occurring, you can do one of the following:

- Make sure that all Client Access servers in the remote and local forests are running the same or a later version of Exchange than the Mailbox servers in the remote and local forests.
- In the remote forest, make sure you haven't mixed Exchange servers of different versions behind the same network load balancer (NLB) end point.
- Initiate cross-forest moves from the later version of Exchange.

Autodiscover

In the RTM version of Exchange 2010, when you move a mailbox across forests, the source mailbox is converted to a mail-enabled user. If the mailbox has a personal archive, after the move is complete, the **msExchArchiveDatabaseLink** attribute isn't cleared from the mail-enabled user in the source forest, and the new mailbox in the target forest also gets this attribute stamped with the database in which the archive now resides. If this attribute is present on the mail-enabled user, it will point to a database in the source forest.

As a result, when you upgrade to Exchange 2010 SP1, Autodiscover and Outlook can't determine where the mailbox resides because the mail-enabled user object and the mailbox object are pointing to different databases within different forests.

Therefore, before you upgrade to Exchange 2010 SP1, you must clear the **msExchArchiveDatabaseLink** attribute manually from Active Directory for each affected mail-enabled user. You can use a tool such as ADSIEdit to remove this property. For more information, see Microsoft Knowledge Base article 2387770, When using Autodiscover Outlook fails to connect to an Exchange 2010 SP1 mailbox with "Unable to open your default e-mail folders" if the user was moved cross forest.

Unified Messaging

Consider the following issues when you install and configure Exchange 2010 SP1 with Unified Messaging.

UM Language Packs

The Unified Messaging (UM) language packs for Exchange 2010 SP1 are intended to be used only on Unified Messaging servers running Exchange 2010 SP1. They must not be installed on 64-bit Unified Messaging servers running the release to manufacturing (RTM) version of Exchange 2010.

These new UM language packs allow a Unified Messaging server running Exchange 2010 SP1 to speak additional languages to callers and recognize other languages when callers use Automatic Speech Recognition (ASR) or when voice messages are transcribed. UM language packs contain:

- Prerecorded prompts, for example: "After the tone, please record your message. When you've finished recording, hang up, or press the # key for more options." These prompts are in the language of the UM language pack.
- Text-to-Speech (TTS) data and executable code so that text content (such as e-mail, calendar, and contact information) can be read to callers in the language of the UM language pack.

- ASR data and executable code, which allows callers to interact with Unified Messaging using the voice user interface (Outlook Voice Access) in the language of the UM language pack.
- Support for Voice Mail Preview, which adds a text version of voice mail messages that can be read from e-mail clients such as Microsoft Outlook or Microsoft Office Outlook Web App. The Voice Mail Preview feature isn't available in all UM language packs.

The following is a list of UM language packs in Exchange 2010 SP1 that contain support for Voice Mail Preview. The language packs marked with an asterisk (*) are new in SP1:

- English (United States) (en-US)
- English (Canada) (en-CA) *
- French (France) (fr-FR)
- Italian (Italy) (it-IT)
- Polish (pl-PL) *
- Portuguese (Portugal) (pt-PT) *
- Spanish (Spain) (es-ES) *

Known Issues

The following are known issues associated with UM language packs:

- **Installation issues**
  When you're installing a UM language pack, you may encounter the following error message: "This specified role, UmLanguagePack, isn't defined in the configuration file." To work around the problem, you can delete the C:\Program Files\Microsoft\Exchange Server\V14\Bin\en\ExBPA.Config.xml file, and then restart the language pack installation.
- **General recommendations and considerations when you're using UM language packs for name pronunciation**. The following issues are associated with name pronunciation:
  - The actual names should be recorded by UM-enabled users when they're setting up their voice mail (signing in to Outlook Voice Access for the first time).
  - If a recorded name is available, it will always be spoken to a caller by Unified Messaging.
  - If a recorded name isn't available, Unified Messaging will try to speak the user's display name phonetically. This requires the Unified Messaging server to use TTS synthesis to speak the user's name.
  - If a phonetic display name isn't available for the user, Unified Messaging will try to speak the user's display name. This also requires TTS synthesis.
  - The problems (described later in this document) with the pronunciation of names refer to the cases in which a recorded name or phonetic display name is used by a Unified Messaging server to speak the name of the user.
- **Language-specific issues**. Some language packs may have problems with the pronunciation of names. The following problems are listed by language pack:
  - **Japanese**
    In the case of some Romaji names (Japanese names spelled using Roman characters), instead of pronouncing the name in its entirety, Unified Messaging may read the name spelled out letter-by-letter, for example, instead of "Sugimoto," Unified Messaging may read "s-u-g-i-m-o-t-o."
    In addition, Unified Messaging may not read English names spelled out using Roman characters, remaining silent in place of a name.
  - **Russian**
    Some Romanized Russian names, as well as English names, might be pronounced in an unnatural manner.
  - **English (India)**
    While attempting to switch the language used to read e-mail messages in Outlook Voice Access, Unified Messaging may not

recognize the name of the requested culture. To work around this issue, try to use alternative names, for example, instead of "Chinese," use "Chinese P.R.C." or "Chinese Hong Kong."

Caution:

Deploying the Exchange 2010 SP1 English (India) (en-IN) Unified Messaging language pack in organizations that include Exchange Server 2007 servers running on Windows Server 2003 will cause the Exchange 2007 servers to fail.

- **English (US)**
  Unified Messaging may not pronounce names written with characters from non-Roman alphabets.
- **Chinese (Hong Kong)**
  Unified Messaging may not pronounce names written using characters from alphabets other than Chinese (H.K.).
- **Danish**
  When reporting hours, Unified Messaging may unnecessarily repeat the word "klokken," for example, "ankom I går klokken klokken 8:21."

Exchange 2010 UM Troubleshooting Tool

You can use the **Test-ExchangeUMCallFlow** cmdlet to test call flow between Unified Messaging servers, IP gateways, and Session Initiation Protocol (SIP) servers. This cmdlet can be used to diagnose configuration errors found in telephony components, Exchange 2010 SP1 Unified Messaging settings, and connectivity issues between on-premises and cross-premises Unified Messaging deployments.

The **Test-ExchangeUMCallFlow** cmdlet can also be used to diagnose configuration errors specific to call answering scenarios and to test whether voice mail is functioning correctly, both on-premises and cross-premises, for the following:

- Deployments that use Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010
- Deployments that aren't using Communications Server 2007 R2 or Lync Server 2010

This cmdlet emulates calls and runs a series of diagnostic tests that provide reasons, and possible solutions, for issues that are detected. It also provides metrics for diagnosing audio quality issues related to network connectivity, such as jitter and average packet loss. The **Test-ExchangeUMCallFlow** cmdlet supports testing Unified Messaging components Secured, SIP Secured, and Unsecured modes and can be run either in Gateway or SIPClient modes.

Important:

The **Test-ExchangeUMCallFlow** cmdlet must be used to test only the voice mail functionality of an Exchange 2010 Unified Messaging server that has Exchange 2010 SP1 installed.

The **Test-ExchangeUMCallFlow** cmdlet can be installed on a local Unified Messaging server or on another 64-bit computer that's running the:

- Windows Vista or Windows 7 operating system.
- Windows Server 2008 or Windows Server 2008 R2 operating system.

The **Test-ExchangeUMCallFlow** cmdlet requires that the components in the following list be installed on a computer running Windows Vista, Windows 7, or the 64-bit version of Windows Server 2008 before the cmdlet is installed:

- .NET Framework 3.5 SP1. For details, see Microsoft .NET Framework 3.5 Service Pack 1.
- .NET Framework 3.5 Family Update for the 64-bit version of Windows Vista, and the 64-bit version updates of Windows Server 2008 if the tool will be run

on a computer running Windows Vista or Windows Server 2008. For details, see Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64.

- Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu). For details, see Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0).
- Microsoft Unified Communications Managed API 2.0 Core Runtime (UcmaRuntimeWebDownloadX64.msi). For details, see Unified Communications Managed API 2.0, Core Runtime (64-bit).

The **Test-ExchangeUMCallFlow** cmdlet isn't included on the Exchange 2010 SP1 DVD or in the download for Exchange 2010 SP1 only. However, you can download the **Test-ExchangeUMCallFlow** cmdlet from the Microsoft Download Center. For details, see Unified Messaging Troubleshooting Tool.

Important:

The *Diversion* parameter in the UM troubleshooting tool doesn't currently accept multiple History-Info headers. When you're running the tool in `Gateway` mode, the *Diversion* parameter must be provided. This can be in the form of a Diversion or a History-Info header. When you specify diversion numbers using History-Info headers, Unified Communications Managed API 2.0 requires that at least two History-Info headers be provided. For example: "<sip:66242@10.197.22.149;user=phone >; index=1, \ < sip:66242@10.197.22.149?Reason=SIP; cause=480; \ text="Request Timeout">;index=1.1, \ ;index=1.2"

Office Communications Server 2007 and Lync Server 2010

Office Communications Server 2007 R2 or Microsoft Lync Server 2010 (the next generation of Office Communications Server) is required with Unified Messaging in Exchange 2010 SP1. The following table describes supported deployments.

Supported deployments

Office Communications Server or Lync Server version	Exchange Server 2007 SP1, SP2, or SP3 Unified Messaging.	Exchange 2010 RTM Unified Messaging.	Exchange 2010 SP1 Unified Messaging.
Office Communications Server 2007	Supported only in an enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Supported only in an enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Not supported.
Office Communications Server 2007 R2	Supported only in an enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Supported only in an enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Supported only in an enterprise deployment. Location profile names and UM dial plan phone contexts don't have to match.
Lync Server 2010	Supported only in an enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Supported only in an enterprise deployment. Location profile names and UM dial plan phone contexts must match.	Supported in a cross-premises or enterprise deployment. Location profile names and UM dial plan phone contexts don't have to match.

Note:

Exchange 2010 SP1 Unified Messaging no longer supports Office Communications Server 2007. You must use Office Communications Server 2007 R2 or Lync Server 2010.

Legal Notice

1.1.4.9 Issues That Are Fixed in Exchange 2010 SP1

Issues That Are Fixed in Exchange 2010 SP1

Exchange Server 2010 > Getting Started With Exchange 2010 > What's New in Exchange 2010 SP1 >

Topic Last Modified: *2012-03-07*

This topic provides the list of issues that are fixed in Microsoft Exchange Server 2010 Service Pack 1 (SP1). For more information about Exchange 2010 SP1, see the following topics:

- To learn more about the new features in Exchange 2010 SP1, see What's New in Exchange 2010 SP1.
- To learn more about known issues that affect SP1, see Release Notes for Exchange Server 2010 SP1.
- To obtain Exchange 2010 SP1, visit the following Microsoft Download Center website: Microsoft Exchange Server 2010 Service Pack 1 (SP1).

Issues that are Fixed

Exchange 2010 SP1 includes the changes made in the following Exchange 2010 RTM rollups:

- Description of Update Rollup 5 for Microsoft Exchange Server 2010 Release to Manufacturing
- Description of Update Rollup 4 for Microsoft Exchange Server 2010 Release To Manufacturing
- Description of Update Rollup 3 for Microsoft Exchange Server 2010 Release to Manufacturing
- Description of Update Rollup 2 for Exchange Server 2010: February 18, 2010
- Update Rollup 1 for Exchange Server 2010

1.1.5 What's New in Exchange 2010

What's New in Exchange 2010

Applies to: *Exchange Server 2010*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 brings a new and rich set of technologies, features, and services to the Exchange Server product line. New features and functionality in Exchange 2010 support several key concepts:

- Flexible and reliable
- Anywhere access
- Protection and compliance

The following sections provide you with an overview of some of the important new features and functionality, which you can use when you're planning, deploying, and administering your Exchange 2010 organization.

(For information about features that have been discontinued or de-emphasized from Microsoft Exchange Server 2003 or Exchange Server 2007 to Exchange 2010, see Discontinued Features.)

For information about the features and changes that have been added in Exchange 2010 SP1, see What's New in Exchange 2010 SP1.

Flexible and Reliable

The pressure to optimize your IT infrastructure to respond to changing business conditions demands agility and that means investing in solutions that provide you and your organization choice. Exchange 2010 gives you the flexibility to tailor your deployment based on your organization's unique needs and a simplified way to help keep e-mail continuously available for your users.

High Availability Functionality

Exchange 2010 integrates high availability into the core architecture of Exchange to enable customers of all sizes and in all segments to economically deploy a messaging continuity service in their organization.

Exchange 2010 includes many changes to its core architecture. In Exchange 2010, new features such as *incremental deployment*, *mailbox database copies*, and *database availability groups* work with other features such as shadow redundancy and transport dumpster to provide a new, unified platform for high availability and site resilience.

For more information about high availability features, see New High Availability and Site Resilience Functionality.

Exchange Store and Mailbox Database Functionality

The following is a list of core store functionality that's included or has been changed in Exchange 2010:

- Deprecated storage groups
- Mailbox databases no longer connected to the server object
- Improvements in Extensible Storage Engine (ESE) for high availability, performance, and database mobility
- Flattened Outlook store schema
- Enhanced reporting with public folders

For more information about Exchange store and mailbox database features, see New Exchange Core Store Functionality.

Permissions Functionality

In Exchange 2010, Role Based Access Control (RBAC) replaces the permissions model used in Exchange 2007. Using RBAC, you can define extremely broad or extremely precise permissions models based on the roles of your administrators and users.

For administrators and specialist users, management role groups define what these users can manage in the organization. Role groups associate role group members to a set of management roles that define what the members can do. By adding or removing users as members of role groups, and adding or removing role assignments to or from a role group, you can control what aspects of the organization the members can manage.

For end users, management role assignment policies define what users can configure on their own mailbox. Assignment policies are applied to every mailbox either by default or manually, and enable you to control whether users can change their personal information, contact information, distribution group membership, and so on.

Both role groups and role assignment policies are assigned management roles. Management roles control access to the cmdlets and parameters required to perform a task. For example, if a cmdlet exists on a management role, and that role is assigned to a role group, the members of that role group can then use that cmdlet.

For more information about RBAC features, see Understanding Permissions.

Transport and Routing Functionality

The following is a list of new transport and routing functionality included in Exchange 2010:

- Shadow redundancy
- MailTips
- Moderated transport
- Federated delivery
- Latency service level agreement (SLA) management
- End-to-end message tracking
- Incremental EdgeSync
- Transport rules integration with AD RMS
- Transport dumpster improvements
- Transport database improvements

For more information about transport features, see New Transport Functionality.

Exchange Server 2010 Deployment Assistant

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Administration Functionality in the Exchange Management Console

The following is a list of the new core Exchange Management Console (EMC) features included in Exchange 2010. The core EMC refers to new functionality that affects how you use the EMC, and not how you use specific features:

- Ability to add Exchange forests to the console tree
- Customer Feedback start tab
- Community and Resources
- EMC command logging
- Property dialog box command exposure
- RBAC permissions aware for the EMC
- Online Exchange Help

For more information about EMC features, see New Administrative Functionality in the Exchange Management Console.

Administration Functionality in the Exchange Management Shell

The following is a list of features available in the new Exchange Management Shell:

- **Remote administration** With the new Shell, you can connect to remote servers running Exchange 2010 across the network with only Windows Management Framework installed, which includes Windows PowerShell. For more information, see Overview of Exchange Management Shell.
- **RBAC integration** The Shell works with RBAC to give you and your users access only to the cmdlets and parameters you and they are allowed to use. If your permissions don't allow you to configure a certain feature, you aren't given access to the cmdlets, parameters, or both, that manage that feature. For more information, see Understanding Role Based Access Control.
- **Administrator audit logging** Actions that result in the modification of Exchange organization configuration and other object properties in the EMC, the Web management interface, and the Shell can now be logged for later review. For more information, see Overview of Administrator Audit Logging.
- **Improved multiple-valued property syntax** Instead of running multiple commands to add and remove values from a single property, you can now add and remove values with a single command. For more information, see Modifying Multivalued Properties.

Exchange Control Panel

Administrators can use the Exchange Control Panel for Outlook Web App to manage some on-premises tasks. The following is a list of the administrative features available:

- Text messaging integration
- Voice messaging integration
- Multiple mailbox search
- Additional proxy addresses for mailboxes
- Moderation and approval for distribution list submission

In addition, users have self-service capabilities in that they can perform administrative tasks via the Exchange Control Panel. The ECP enables users to perform common tasks without having to call the help desk. This allows your users to be more productive and

allows IT staff to deliver more, while reducing support costs.

For more information, see Configure ECP Virtual Directory Properties.

Mailbox and Recipient Functionality

The following is a list of the new mailbox and recipient functionality that's included or has been changed in Exchange 2010:

- Ability for users to share information, such as calendar free/busy information and contacts with users who reside in a different organization
- Improved scheduling and configuring for resource mailbox calendar processing
- Ability to move a mailbox while the end user is still accessing it
- Additional parameters added to distribution group cmdlets to allow users to create and manage their own distribution groups in Outlook Web App and Exchange 2010
- Ability to appoint a moderator to regulate the flow of messages sent to a distribution group
- Ability to manage folder-level permissions for all folders within a user's mailbox
- Expanded bulk recipient management to allow you to bulk manage recipient properties
- Ability to send mail to recipients from the EMC

For more information about mailbox and recipient features, see New Mailbox and Recipient Functionality.

Exchange Web Services Managed API 1.0

The Microsoft Exchange Web Services (EWS) Managed API 1.0 provides a managed interface for developing client applications that use Exchange Web Services. Beginning with Exchange 2007 Service Pack 1 (SP1), the EWS Managed API simplifies the implementation of applications that communicate with Exchange. Built on the Exchange Web Services SOAP protocol and Autodiscover, the EWS Managed API provides a .NET interface to Exchange Web Services that's designed to be easy to learn, use, and maintain.

For more information, see Introducing the Exchange Web Services Managed API 1.0 and Microsoft Exchange Web Services Managed API 1.0.

Client Throttling Functionality to Manage System Performance

Exchange 2010 uses client throttling policies to manage the performance of your Exchange organization. To do this, Exchange tracks the resources that each user consumes and enforces connection bandwidth limits as necessary.

Some of the benefits of client throttling include making sure that:

- Users aren't intentionally or unintentionally taxing the system.
- Users of various connectivity methods are proportionally sharing resources.

You manage client throttling policies with Shell cmdlets. For more information about client throttling policies, see Understanding Client Throttling Policies.

Anywhere Access

Enhancements in Exchange 2010 helps users get more done by helping them to access all of their communications—e-mail, voice mail, instant messaging—from virtually any platform, Web-browser, or device through industry standard protocols. Managing the flow of information into and out of an individual’s inbox daily can create overload and affect productivity and profitability. In response to this challenge, Exchange 2010 adds new productivity features that can help users more easily organize and effectively prioritize their communications.

Unified Messaging Features

The following is a list of new Unified Messaging features included in Exchange 2010:

- Call answering rules
- Additional language support included in Outlook Voice Access
- Enhancements to name lookup from caller ID
- Voice Mail Preview
- Message Waiting Indicator
- Missed call and voice mail notifications using text messaging
- Protected Voice Mail
- Incoming fax support
- Addressing to groups (personal distribution lists) support
- Built-in Unified Messaging administrative roles

For more information about Unified Messaging and voice mail features, see New Unified Messaging Functionality and Voice Mail Features.

Outlook Web App Features

The following is a list of new features in Outlook Web App included in Exchange 2010:

- Favorites in the navigation pane
- Search folders
- Message filtering
- Ability to set categories in the message list
- Options in the Web management interface for Outlook Web App
- Side-by-side view for calendars
- Multiple client language support
- Ability to attach messages to messages
- Expanded right-click capabilities
- Integration with Office Communicator, including presence, chat, and a contact list
- Conversation view
- Ability to send and receive text messages from Outlook Web App
- Outlook Web App mailbox policies

For more information about Outlook Web App features, see Understanding Outlook Web App.

Exchange ActiveSync Features

The following is a list of new Exchange ActiveSync features included in Exchange 2010:

- Conversation grouping of e-mail messages
- Ability to synchronize or not synchronize an entire conversation
- Synchronization of SMS messages with a user's Exchange mailbox
- Support for viewing of message reply status
- Support for availability information for contacts

Text Messaging Features

The following is a list of new text messaging features included in Exchange 2010:

- Missed call and voice mail notifications
- Calendar and agenda updates
- Text messages sent and received through Outlook Web App and Outlook 2010
- Text message synchronization with a mobile phone

POP3 and IMAP4 Cross-Site Connectivity Support

Cross-site POP3 and IMAP4 client connectivity is supported by default in Exchange 2010. For more information about POP3 and IMAP4 client connectivity features, see Understanding POP3 and IMAP4.

Protection and Compliance

Exchange 2010 delivers new, integrated e-mail archiving and retention functionality, including granular multi-mailbox search and immediate legal hold. Exchange 2010 also helps you to better protect your company's communications and e-mail through centrally managed information control capabilities. This includes the ability to more effectively intercept, moderate, encrypt, and block e-mail messages. Together, this functionality provides you with a flexible range of protection and control options, whether you want to automatically enforce controls or empower users to implement their own data protection.

Messaging Policy and Compliance Features

Exchange 2010 compliance features make retention independent of users' mailbox management and filing habits, and ensure retention policies are applied continuously. The following is a list of new messaging and compliance features included in Exchange 2010:

- Additional messaging records management (MRM) functionality to apply message retention policies
- Personal Archive feature to provide users with online archive mailboxes and help eliminate .pst files
- Mailbox search features for cross-mailbox search with Advanced Query Syntax (AQS) support
- Additional transport rules predicates and actions

For more information about messaging policy and compliance features, see New Messaging Policy and Compliance Functionality.

IRM-Protected E-Mail Functionality with Active Directory Rights Management Services

The following is a list of new Information Rights Management (IRM)-protected e-mail functionality with Active Directory Rights Management Services (AD RMS) included in Exchange 2010:

- Microsoft Outlook protection rules, to apply IRM-protection to messages in Outlook 2010
- Transport protection rules, to apply IRM protection to messages based on rule conditions
- Persistent protection of attachments in IRM-protected messages
- Support for AD RMS templates
- Support for IRM in Microsoft Office Outlook Web App
- Transport decryption, to decrypt IRM-protected messages to apply messaging policies
- Journal report decryption, to attach a decrypted copy of IRM-protected messages to journal reports
- AD RMS protection for Unified Messaging voice mail messages

For more information about IRM features, see Information Rights Management.

1.1.5.1 New Administrative Functionality in the Exchange Management Console

New Administrative Functionality in the Exchange Management Console

Exchange Server 2010 > Getting Started With Exchange 2010 > What's New in Exchange 2010 >

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic describes the changes to the Exchange Management Console (EMC) in Microsoft Exchange Server 2010.

Contents

Need help finding features in the EMC? Check out Roadmap for Exchange Features.

Feature Changes

This section briefly describes the new features that have been added to the EMC.

New Features in the Organization Configuration Node

Database management has moved from the **Server Configuration** node to the **Organization Configuration** node. In addition, the following wizards have been added to the node:

- **New Federation Trust wizard** Use this wizard to create a federation trust. A federation trust establishes a trust relationship between an Exchange organization and the Microsoft Federation Gateway. The trust is a prerequisite for enabling calendar free/busy sharing or federated delivery between two Exchange organizations, or allowing users to share their calendar and contacts with external recipients. For details, see Create a Federation Trust.
- **New Organization Relationship wizard** Use this wizard to create a relationship with an external Exchange 2010 organization for the purpose of sharing free/busy information, securing delivery of cross-premises e-mail using federated delivery, and moving mailboxes between on-premises Exchange servers and Microsoft Office Outlook Web App. For details, see Create an Organization Relationship.
- **New Sharing Policy wizard** Use this wizard to create a sharing policy to regulate how users inside your organization can share calendar and contact information with users outside the organization. For details, see Create a Sharing Policy.
- **New Outlook Web App Mailbox Policy wizard** Use this wizard to create an Outlook Web App mailbox policy to apply a common set of policy settings, such as attachment settings. Outlook Web App mailbox policies are useful for applying and standardizing settings for specific groups of users. For details, see Create Outlook Web App Mailbox Policy.

New Features in the Server Configuration Node

You can no longer manage mailbox or public folder databases from the **Server Configuration** node. Now, they're managed from the **Organization Configuration** node. However, you can view mailbox database properties (from the work pane of **Server Configuration** > **Mailbox**).

In addition, the following features have been added to the node:

- **Manage Diagnostic Logging Properties wizard** Use this wizard to modify the diagnostic logging level for processes used by Exchange 2010. Modifying these levels can help you troubleshoot issues that may occur in your organization. For details, see Manage Diagnostic Logging Levels.
- **Exchange Certificates tab** Use this tab to assign services to an Exchange certificate, remove or renew a certificate, or view the certificate's properties. For details, see the following topics:
  - Assign Services to a Certificate

  - Renew an Exchange Certificate
  - View Exchange Certificate Properties
- **New Exchange Certificate wizard** Use this wizard tohelp you determine what type of certificates you need for the features in your organization to function correctly. For details, see Create a New Exchange Certificate.
- **Import Exchange Certificate wizard** Use this wizard to help import a certificate with a valid private key to a specified Exchange server. For details, see Import an Exchange Certificate.

New Features in the Recipient Configuration Node

The following features have been added to the **Recipient Configuration** node:

- **Send Mail** Click this button to send mail to a recipient from the EMC. Before you can send mail, you need to set up an e-mail account on the computer from which you are sending mail.
- **Resource scheduling** The property pages for resource mailboxes now include tabs for configuring calendaring and scheduling. For details, see Configure User and Resource Mailbox Properties.
- **Archive mailboxes** You can enable or disable archive mailboxes directly from the EMC. In addition, you can manage the archive settings for users from the property page of their mailbox. For details, see Managing Archives.
- **Move requests** If you want to move mailboxes, you can use the New Local Move Request or New Remote Move Request wizards. You can also keep track of move requests that are in progress by using the **Move Requests** node. For details, see Managing Move Requests.

Core EMC Changes

The following new functionality affects how you use the EMC, but not how you use specific features. Expand each of these new feature sections to learn more.

Add Exchange Forests to the EMC Console Tree

You can now add Exchange forests to the EMC. The first forest will always be named **Microsoft Exchange On-Premises**. This is the default forest for your organization. You can add additional forests by using the Add Exchange Forest wizard. For details, see View Local Forest Properties.

Customer Experience Improvement Program

The Customer Experience Improvement Program (CEIP) collects anonymous information about how you use Exchange and the problems that you encounter. Microsoft uses this information to improve the products and features you use most often and to help solve problems. Participation in the program is voluntary, and the end results are software improvements to better meet your needs. For more information about the CEIP, see Microsoft Customer Experience Program FAQ. For details about how to opt-in or opt-out of the program, see Opt-in or Opt-out of the Customer Experience Improvement Program.

Organizational Health

The Organizational Health report lets you increase productivity by giving you a quick view of your organization and its operating characteristics. The report provides an organizational summary. This includes health and licensing information, and also a summary of Exchange servers and recipients.

Important:
This report is for information only. If errors occur while collecting the information, the report may not be accurate.

Exchange doesn't automatically gather the organizational information. You must use the Collect Organizational Health Data wizard to view a summary of your organization's health. For details, see Collect Organizational Health Data.

Customer Feedback

The **Customer Feedback** tab is located in the result pane of the **Microsoft Exchange On-Premises** node. The tab is divided into two sections:

- **Customer Feedback Options** This section allows you to run the Customer Experience Improvement Program wizard, which allows you to opt-in or out of the CEIP. For more information, see Opt-in or Opt-out of the Customer Experience Improvement Program.
- **Help and Feedback** This section provides a link to the Exchange Server TechCenter and allows you to submit feedback or to report bugs directly to the Exchange team.

Exchange Management Shell Command Log

The Exchange Management Shell Command Log records the commands that you execute in the EMC. For example, if you view the list of recipients from the **Mailbox** node, the **Get-Recipient** cmdlet is executed, and the Exchange Management Shell Command Log records that action.

Note:
The command log doesn't save the logging information. After you close the EMC, the log is erased. However, you can export the command log to tab-delimited or comma-delimited files.

To view the command log, from the EMC toolbar, click **View**, and then click **View Exchange Management Shell Command Log**.

For information about command logging, see Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC.

Property Dialog Command Exposure

Exposing the commands for actions executed in property pages allows you to see the Microsoft Windows PowerShell command and the parameters required to change object properties. To view the command, click the arrow icon located in the bottom left corner of the property page. To copy the command, select the command and press **CTRL+C**.

Note:
The command viewer is made available only after you make a property change.

Role Based Access Control in the EMC

When you open the EMC, Exchange checks to see what Role Based Access Control (RBAC) permissions you have. You can only view or configure features and items for which you have the correct permissions. If an administrator has permission to view an object but not edit it, the field text will appear dimmed and a caution icon will display. For more information about RBAC, see Understanding Role Based Access Control.

Exchange Help

The Exchange Help files are no longer downloaded to Exchange. Instead, they're hosted on Microsoft TechNet. This ensures that you're always viewing the most up-to-date Help topics.

Exchange 2010 contains two new cmdlets for managing Exchange Help:

- **Set-ExchangeAssistanceConfig** Using this cmdlet, you can modify the URLs that the Exchange Help client uses to connect to the source of the Exchange 2010 documentation. By default, TechNet is used as the source. For details, see Set-ExchangeAssistanceConfig.
- **Get-ExchangeAssistanceConfig** Using this cmdlet, you can view the configuration information for the URLs that the Exchange Help client uses to connect to the source of the Exchange 2010 documentation. For details, see Get-ExchangeAssistanceConfig.

1.1.5.2 New Exchange Core Store Functionality

New Exchange Core Store Functionality

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-28*

Microsoft Exchange Server 2010 includes many improvements to the Exchange database architecture:

- Public folder reporting has been enhanced.
- Databases are no longer associated with storage groups. Storage groups have been removed.
- Investments in store schema and Extensible Storage Engine (ESE) optimizations have reduced IOPS by 70 percent.

The following sections describe these improvements in more detail.

Contents

Enhanced Reporting for Public Folders

Public folder reporting has been enhanced to view user-initiated changes to any item in the public folder. You can view this information by using the **Get-PublicFolderStatistics** cmdlet in the Exchange Management Shell. For more information, see Exchange Management Shell.

Database Management

Databases are no longer associated with storage groups. In Exchange 2010, storage group functionality has been moved to the database.

In Exchange 2010, you can manage mailbox and public folder databases in the **Organization Configuration** node of the EMC. (In Exchange Server 2007, database management was performed in the **Server Configuration** node.)

Although public folder database management has been moved from the **Server Configuration** node to the **Organization Configuration** node with the mailbox databases, the functionality of public folder databases hasn't changed in Exchange 2010. Just like in Exchange 2007, you can't create database copies of public folder databases, and you can't add public folder databases to a database availability group (DAG). However, public folder databases can be hosted on Mailbox servers that are part of a DAG, although public

folder databases won't be subject to log shipping or any other DAG features.

Database Cmdlet Changes

With the removal of storage groups in Exchange 2010, the storage group cmdlets used in Exchange 2007 were deleted and the Exchange 2010 database cmdlets now provide the functionality, as shown in the following tables.

Database cmdlets in Exchange 2010 that replace Exchange 2007 storage group cmdlets

Exchange 2007 cmdlet	Description of functionality change in Exchange 2010
New-StorageGroup	This cmdlet has been deleted, and configuration parameters were moved to the **New-MailboxDatabase** and **New-PublicFolderDatabase** cmdlets.
Remove-StorageGroup	This cmdlet has been deleted, and configuration parameters were moved to the **Remove-MailboxDatabase** and **Remove-PublicFolderDatabase** cmdlets.
Set-StorageGroup	This cmdlet has been deleted, and configuration parameters were moved to the **Set-MailboxDatabase** and the **Set-PublicFolderDatabase** cmdlets.
Get-StorageGroup	This cmdlet has been deleted, and configuration parameters were moved to the **Get-MailboxDatabase** and **Get-PublicFolderDatabase** cmdlets.
Move-StorageGroupPath	This cmdlet has been deleted, and configuration parameters were moved to the **Move-DatabasePath** cmdlet.

Database cmdlets in Exchange 2010 that have extended functionality from Exchange 2007 cmdlets

Exchange 2010 cmdlet	Description of extended functionality in Exchange 2010
New-MailboxDatabase **New-PublicFolderDatabase**	These cmdlets have been extended with the parameters and functionality from the **New-StorageGroup** cmdlet. They also update the server object with a link to the new database and the database object with the hosting server name.
Remove-MailboxDatabase **Remove-PublicFolderDatabase**	These cmdlets have been extended with the parameters and functionality from the **Remove-StorageGroup** cmdlet. In addition, they also update the server object with the link to the new database and the database object with the hosting server name.
Set-MailboxDatabase **Set-PublicFolderDatabase**	These cmdlets have been extended with the parameters and functionality from the **Set-StorageGroup** cmdlet. When changing the host servers, they also update the server

	object with the link to the new database and the database object with the hosting server name.
Get-MailboxDatabase **Get-PublicFolderDatabase**	These cmdlets have been extended with the parameters and functionality from the **Get-StorageGroup** cmdlet. The *Status* parameter is extended to return the status information currently returned by the **Get-StorageGroupCopyStatus** cmdlet.
Move-DatabasePath	This cmdlet has been extended with the parameters and functionality from the **Move-StorageGroupPath** cmdlet.

In addition to the preceding cmdlet changes, the **StorageGroupCopy** cmdlets have been deleted. For more information, see Managing Mailbox Database Copies.

Store Changes

In Exchange 2010, the store schema has been changed to remove the dependency of mailbox databases on the server object. In addition, the new schema has been improved to help reduce database I/O per second (IOPS) by refactoring the tables used to store information. Refactoring the tables allows higher logical contiguity and locality of reference. These changes reduce the store's reliance on the secondary indexes maintained by ESE. As a result, the store is no longer sensitive to performance issues related to the secondary indexes.

Store resilience and health has also been improved by adding several features related to detecting and correcting errors and providing alerts, such as the following:

- Mailbox quarantine on rogue mailboxes
- Transport cutoff to databases with less than 1 GB of space
- Thread time-out detection and reporting

For more information about store resilience and health, see Understanding the Exchange 2010 Store.

Core store functionality has received many changes to improve high availability features. High availability has been integrated into the core architecture of Exchange 2010 to enable organizations of all sizes and in all industry segments to economically deploy a messaging continuity service. For more information about the high availability changes in Exchange 2010, see Understanding High Availability and Site Resilience.

New ESE Functionality

Extensible Storage Engine (ESE) has been improved in Exchange 2010 to achieve the following goals:

- Larger I/O and sequential I/O to reduce IOPS
- Optimization for commodity storage
- Database management reduction
- Online defragmentation
- Online database scanning

Larger and Sequential I/O

By increasing the size of the I/O and reducing the frequency of read/writes in Exchange 2010, ESE is able to increase performance. In addition, ESE can increase performance by

making the data in the database more sequential, which increases the likelihood that related data is in the same vicinity in the B-tree.

In Exchange, all data inside the database is stored in B-trees, and the B-trees are then divided into pages. In Exchange 2007 and earlier, the data stored in the B-trees isn't contiguous. In fact, previous versions of Exchange performed random read/writes to the database. This means that related data may not be in the same vicinity on the hard disk. Non-contiguous data requires more passes to read and write to the hard disk.

B-Tree Defragmentation

The B-tree defragmentation process has been improved to reduce I/O operations by maintaining contiguous data in the B-tree.

B-tree defragmentation is performed in-place (as opposed to creating a new B-tree and renaming the indexes and tables) with three new operations:

- **Page move** A page move consists of moving all data from one page to a newly allocated page.
- **Partial left merge** A partial left merge is the same as a right merge in Exchange 2007 or earlier, except that data is moved from the left page to the right page.
- **Full left merge** A full left merge is the same as a full right merge in Exchange 2007 or earlier.

Defragmentation has been changed from right merges to left merges to optimize performance. Data is read from or written to the hard disk from right to left. If the database is being defragmented in the same direction as the read/writes, defragmentation will conflict with the read/writes. In addition, space allocation allows the next page in an extent to be allocated, but not the previous page. Because a page move needs to allocate a new page, defragging the database from left to right is much more efficient.

The Defragmentation Manager is a new event in ESE that monitors which B-trees require defragmenting and which B-trees have already been defragmented. The Defragmentation Manager compiles a list of the B-trees in all mounted databases that should be defragmented. As fragmented B-trees are discovered, they're registered with the Defragmentation Manager, and the Defragmentation Manager will process them.

Page Size Increase to 32 KB

All data inside the database is stored in B-trees, and the B-trees are divided into pages. The page size is the minimum size for reading and writing to the database; it's also the unit size used for database caching. Reading from the disk is slower than performing operations in memory; therefore, by increasing the page size to 32 KB, ESE reduces IOPS, which increases performance by caching the larger page size in memory.

Optimize for Commodity Storage

Another of the goals of ESE in Exchange 2010 is to reduce the capital and operational costs of deploying Exchange. This can be done by reducing storage costs and optimizing for commodity storage using JBOD and SATA class hard disks.

Disk subsystems are more efficient at handling fewer but larger I/O. In Exchange 2010 or earlier, the page size is the minimum read/write size and the minimum size for database caching. Coalescing I/Os refers to the process of combining database page operations into a single I/O operation, thereby producing fewer and bigger I/O operations.

Increasing the average database I/O sizes via coalescing I/Os has the following benefits:

- **Increased disk use efficiency** Disks are more efficient at processing large I/Os. The more efficiently the disk is utilized, the more mailboxes can be hosted on that disk.
- **Increased cache warming rate** Cache warming is a process that helps reduce the execution times by preloading the initial queries that were

executed against a database the last time the database was started. After a server restart, failover, or switchover, the larger I/O allows ESE to increase the rate at which the cache is warmed.

Database Maintenance

One of the goals of ESE in Exchange 2010 is to reduce the cost of maintaining and managing a database. Database maintenance is comprised of several tasks that manage and keep the integrity of your mailbox database.

Database maintenance is divided into the following:

- Store mailbox maintenance
- ESE database maintenance

In Exchange 2007, ESE database maintenance was disk-intensive. In Exchange 2010, improvements have been made to increase performance. In Exchange 2010, on large or very heavy profile servers, the store mailbox maintenance task only lasts approximately 45 minutes, while ESE database maintenance usually took from six to eight hours per night to complete on large Exchange 2007 databases (2 GB quotas).

In Exchange 2010, improvements have been made to support both large mailboxes as well as to support JBOD storage and storage without the use of RAID.

Note:

All Exchange Store-focused online database maintenance functions such as recovery item cleanup are the same in Exchange 2010 as they are in Exchange 2007. Only ESE functions, online defragmentation, and database checksumming have changed.

Database Defragmentation

Defragmentation makes the internal pages of an Exchange database contiguous. Defragmentation can either be performed automatically by the system while the database is online (online defragmentation) or manually by an administrator when the database is offline (offline defragmentation).

Online Defragmentation

In Exchange 2010, the architecture for online defragmentation has changed. Online defragmentation was moved out of the Mailbox database maintenance process. Online defragmentation now runs in the background 24×7. Because online defragmentation runs all the time, Exchange no longer posts events to the event log indicating the amount of white space in the database. During background database maintenance, items marked for removal from the database are removed, which frees up database pages. The percentage of white space is constantly changing due to the efforts of the continuous online defragmentation process.

You can estimate the amount of white space in the database by knowing the amount of mail sent and received by the users with mailboxes in the database. For example, if you have 100 2-GB mailboxes (total of 200 GB) in a database where users send and receive an average of 10 MB of mail per day, the amount of white space is approximately 1 GB (100 mailboxes × 10 MB per mailbox). The amount of white space can exceed this estimate if background database maintenance isn't able to complete a full pass.

You don't need to configure any settings for this feature. Exchange monitors the database as it's being used, and small changes are made over time to keep it defragged for space and contiguity. If the database analyzes a range of pages and finds that they aren't as sequential as they should be, it starts an async thread to defragment that section of the B-tree/table. Online defragmentation is also throttled so it doesn't have a negative impact on client performance.

Use the ESE performance counter set MSExchange Database ==> Defragmentation Tasks to see the tasks that are performed. For more information, see How to Enable Extended ESE Performance Counters.

Offline Defragmentation

Offline defragmentation is a manual process that is performed by an administrator while the database is in a dismounted (offline) state. In this process, the ESEUTIL tool is used to read the database file and write a new database file using the contents in a contiguous fashion. The offline defragmentation process doesn't copy the white space from the original database; therefore, the size of the newly created database file is smaller than the original database on disk (potentially much smaller, depending on the amount of white space in the database). Historically, the typical reasons for performing an offline defragmentation of a database included the following:

- To shrink the size of the database file on disk
- To reclaim white space in a database
- To avoid low free disk space
- To repair a damaged database (the second step in the repair following ESEUTIL /p)

Offline defragmentation has never been part of regular maintenance for Exchange databases and, for some time now, Microsoft has recommended against regular, proactive offline defragmentation of databases. This recommendation was made for a variety of reasons, including the following:

- It results in downtime because you have to take the database offline.
- In a replicated mailbox database environment, it results in the need to re-seed all passive copies of an active copy that has been defragmented offline, and it results in the need to re-seed any passive copy that has been defragmented offline. (Thus, you should never perform an offline defragmentation of a passive database copy.)
- It results in the creation of a new database, with a new database signature, and that eliminates the ability to restore log files from a backup of the database that was taken prior to offline defragmentation.

As an alternative to offline defragmentation, we recommend that customers create a new database and move the mailboxes to the newly created database. In an Exchange 2010 environment, the mailboxes are moved online with no interruption in service to end users. In addition, when you move all mailboxes from an existing database to a new database, the end result is the same: A defragmented database with pages written contiguously and with no appreciable white space in the database file. After that process is complete, you simply delete the old (now empty) database. This guidance only covers proactive offline defragmentation to reclaim white space. You should still perform defragmentation if directed to do so by Microsoft Customer Support Services.

Online Database Scanning

Online database scanning (also known as database checksumming) has also changed. In Exchange 2007 Service Pack 1 (SP1), there was an option to use half of your online defragmentation time for this database scanning process (to ensure Exchange read every page from your database in a specific period of time to detect any corruptions).

In Exchange 2010, online database scanning checksums the database and performs post Exchange 2010 Store crash operations. Space can be leaked due to crashes, and online database scanning finds and recovers lost space. The system in Exchange 2010 is designed with the expectation that every database is fully scanned once every seven days. A warning event is fired if a database isn't completely scanned in this timeframe. In Exchange 2010, there are now two modes to run online database scanning on active database copies:

- Run as the last task in the scheduled Mailbox Database Maintenance process. You can configure how long it runs by changing the Mailbox Database Maintenance schedule. You can use this option for smaller databases that are less than 1 terabyte (TB) in size, which require less time to complete a full scan.
- Run in the background 24×7, the default behavior. This option works well for all database sizes, but it's recommended for large database sizes (1-2 TB in size). Exchange scans the database no more than once per day. This read I/O

is 100 percent sequential (which makes it easy on the disk) and equates to a scanning rate of about 5 megabytes (MB)/sec on most systems.

For more information about configuring database maintenance, see Maintain Mailbox Databases.

1.1.5.3 New High Availability and Site Resilience Functionality

New High Availability and Site Resilience Functionality

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2011-07-11*

Microsoft Exchange Server 2010 reduces the cost and complexity of deploying an e-mail solution that provides the highest levels of server availability and site resilience. Building on the native replication capabilities introduced in Exchange Server 2007, the new high availability architecture in Exchange 2010 provides a simplified, unified framework for both high availability and disaster recovery. Exchange 2010 integrates high availability into the core architecture of Exchange, enabling customers of all sizes and in all segments to be able to economically deploy a messaging continuity service in their organization.

Lessons Learned from Exchange Server 2007

Exchange 2007 decreased the costs of high availability and made site resilience much more economical by introducing new technologies such as local continuous replication (LCR), cluster continuous replication (CCR), and standby continuous replication (SCR). Still, some challenges remained:

- Some administrators were intimidated by the complexity of Windows failover clustering.
- Achieving a high level of uptime can require a high level of administrator intervention.
- Each type of continuous replication was managed differently and separately.
- Recovering from a failure of a single database on a large Mailbox server could result in a temporary disruption of service to all users on the Mailbox server.
- Site resilience solutions were not seamless.
- The transport dumpster feature of the Hub Transport server could only protect messages destined for mailboxes in an LCR or CCR environment. If a Hub Transport server fails while processing messages and can't be recovered, it could result in data loss.

Exchange 2010 includes significant core changes that integrate high availability deep in its architecture, making it even less costly and easier to deploy and maintain than Exchange 2007 for all customers. Organizations can now deploy a fully redundant Exchange organization with just two servers, and benefit from database-level failovers. Customers benefit from automatic, database-level failover capabilities without having to become experts in Windows failover clustering. Moreover, you can add site resilience to your existing high availability deployments with less complexity.

Exchange 2007 introduced many new architectural changes designed to make deploying high availability and site resilience solutions for Exchange faster and simpler. These improvements included an integrated Setup experience, optimized out-of-box configuration settings, and the ability to manage most aspects of the high availability

solution using native Exchange management tools.

Still, management of an Exchange 2007 high availability solution required administrators to master some clustering concepts, such as the concept of moving network identities and managing cluster resources. In addition, when troubleshooting issues related to a clustered Mailbox server, administrators had to use Exchange tools and cluster tools to review and correlate logs and events from two different sources: one from Exchange and one from the cluster.

Two other limiting aspects of the Exchange 2007 architecture have also been re-evaluated and re-engineered based on customer feedback:

- Clustered Exchange 2007 servers require dedicated hardware. Only the Mailbox server role could be installed on a node in the cluster. This meant that a minimum of four Exchange servers were required to achieve full redundancy of the primary components of a deployment, that is, the core server roles (Mailbox, Hub Transport, and Client Access).
- In Exchange 2007, failover of a clustered Mailbox server occurs at the server level. As a result, if a single database failure occurred, the administrator had to fail over the entire clustered Mailbox server to another node in the cluster (which resulted in brief downtime for all users on the server, and not just those users with a mailbox on the affected database), or leave the users on the failed database offline (potentially for hours) while restoring the database from backup.

Mailbox Resiliency

Exchange 2010 has been re-engineered around the concept of *mailbox resiliency*, in which the architecture has changed so that automatic failover protection is now provided at the individual mailbox database level instead of at the server level. In Exchange 2010, this is known as *database mobility*. As a result of this and other database cache architectural changes, failover actions now complete much faster than in previous versions of Exchange. For example, failover of a clustered Mailbox server in a CCR environment running Exchange 2007 with Service Pack 2 (SP2) completes in about two minutes. By comparison, failover of a mailbox database in an Exchange 2010 environment completes in 30 seconds or less (measured from the time when the failure is detected to when a database copy is mounted, assuming an available copy that's healthy and up to date with log replay). The combination of database-level failovers and significantly faster failover times dramatically improves an organization's overall uptime.

The mailbox resiliency architecture built into Exchange 2010 provides new benefits for organizations and their messaging administrators:

- Multiple server roles can coexist on servers that provide high availability. This enables small organizations to deploy a two-server configuration that provides redundancy of mailbox data and service, while also providing redundant Client Access and Hub Transport services.
- An administrator no longer needs to build a failover cluster to achieve high availability. Failover clusters are now created by Exchange 2010 in a way that's invisible to the administrator. Unlike previous versions of Exchange clusters which used an Exchange-provided cluster resource DLL named ExRes.dll, Exchange 2010 no longer needs or uses a cluster resource DLL. Exchange 2010 isn't a clustered application, and it uses only a small portion of the failover cluster components, namely, its heartbeat capabilities and the cluster database, to provide database mobility.
- Administrators can add high availability to their Exchange 2010 environment after Exchange has been deployed, without having to uninstall Exchange and then redeploy in a highly availability configuration.
- Exchange 2010 provides a view of the event stream that coalesces and combines the events from the operating system with the events from Exchange.

- Because storage group objects no longer exist in Exchange 2010, and because mailbox databases are portable across all Exchange 2010 Mailbox servers, it's easy to move databases when needed.

For more information, see High Availability and Site Resilience.

Flexible Mailbox Protection

Exchange 2010 includes several new features and core changes that, when deployed and configured correctly, can provide flexible mailbox protection that eliminates the need to make traditional backups of your data. Using the high availability features built into Exchange 2010 to minimize downtime and data loss in the event of a disaster can also reduce the total cost of ownership of the messaging system. By combining these features with other built-in features, such as Legal Hold, organizations can reduce or eliminate their dependency on traditional point-in-time backups and realize the cost savings of doing so.

In addition to determining whether Exchange 2010 enables you to move away from traditional point-in-time backups, we also recommend that you evaluate the cost of your current backup infrastructure. Consider the cost of end-user downtime and data loss when attempting to recover from a disaster using your existing backup infrastructure. Also, include hardware, installation and license costs, as well as the management cost associated with recovering data and maintaining the backups. Depending on the requirements of your organization, it is quite likely that a pure Exchange 2010 environment with at least three mailbox database copies will provide lower total cost of ownership than one with backups.

For more information about flexible mailbox protection, see Understanding Backup, Restore and Disaster Recovery.

Changes to High Availability from Previous Versions of Exchange

Exchange 2010 includes many changes to its core architecture. Exchange 2010 combines the key availability and resilience features of CCR and SCR into single high availability solution which handles both onsite data replication and offsite data replication. Mailbox servers can be defined as part of a database availability group (DAG) to provide automatic recovery at the individual mailbox database level instead of at the server level. Each mailbox database can have up to 16 copies. Other new high availability concepts are introduced in Exchange 2010, such as *database mobility* and *incremental deployment*. The concepts of an organization without backups and RAID are also being introduced in Exchange 2010.

To summarize, the key aspects to data and service availability for the Mailbox server role and mailbox databases are:

- Exchange 2010 uses an enhanced version of the same continuous replication technology introduced in Exchange 2007. For more information, see Changes to Continuous Replication from Exchange Server 2007 later in this topic.
- Storage groups no longer exist in Exchange 2010. Instead, there are simply mailbox databases, mailbox database copies, and public folder databases. The primary management interfaces for Exchange databases has moved within the Exchange Management Console from the Mailbox node under **Server Configuration** to the Mailbox node under **Organization Configuration**.
- Some Windows Failover Clustering technology is used by Exchange 2010, but it's now completely managed by Exchange. Administrators don't need to install, build, or configure any aspects of failover clustering when deploying highly available Mailbox servers.

- Each Mailbox server can host as many as 100 databases, and each database can have as many as 16 copies.
- In addition to the transport dumpster feature, a new Hub Transport server feature named *shadow redundancy* has been added. Shadow redundancy provides redundancy for messages for the entire time they're in transit. The solution involves a technique similar to the transport dumpster. With shadow redundancy, the deletion of a message from the transport database is delayed until the transport server verifies that all of the next hops for that message have completed delivery. If any of the next hops fail before reporting back successful delivery, the message is resubmitted for delivery to that next hop. For more information about shadow redundancy, see Understanding Shadow Redundancy.

Incremental Deployment

In previous versions of Exchange, service availability for the Mailbox server roles was achieved by deploying Exchange in a Windows failover cluster. To deploy Exchange in a cluster, you had to first build a failover cluster, and then install the Exchange program files. This process created a special Mailbox server called a clustered Mailbox server (or Exchange Virtual Server in previous versions of Exchange). If you had already installed the Exchange program files on a non-clustered server and you decided you wanted a clustered Mailbox server, you had to build a cluster using new hardware, or remove Exchange from the existing server, install failover clustering, and reinstall Exchange.

Exchange 2010 introduces the concept of incremental deployment, which enables you to deploy service and data availability for all Mailbox servers and databases after Exchange is installed. Service and data redundancy is achieved by using new features in Exchange 2010 such as DAGs and database copies.

Database Availability Groups

A DAG is a set of up to 16 Mailbox servers that provide automatic database-level recovery from failures that affect individual databases. Any server in a DAG can host a copy of a mailbox database from any other server in the DAG. When a server is added to a DAG, it works with the other servers in the DAG to provide automatic recovery from failures that affect mailbox databases, such as a disk failure or server failure.

For more information about DAGs, see Understanding Database Availability Groups.

Mailbox Database Copies

The high availability and site resilience features first introduced in Exchange 2007 are used in Exchange 2010 to create and maintain database copies, thereby enabling you to achieve your availability goals in Exchange 2010. Exchange 2010 also introduces the new concept of database mobility, which is Exchange-managed database-level failovers.

Database mobility disconnects databases from servers, adds support for up to 16 copies of a single database, and provides a native experience for adding database copies to a database. In Exchange 2007, a feature called database portability also enabled you to move a mailbox database between servers. A key distinction between database portability and database mobility, however, is that with database mobility, all copies of a database have the same GUID.

Other key characteristics of database mobility are:

- Because storage groups have been removed from Exchange 2010, continuous replication now operates at the database level. In Exchange 2010, transaction logs are replicated to one or more Mailbox servers and replayed into a copy of a mailbox database that's stored on those servers.

- A failover is an automatic activation process that can occur at either the database level or at the server level. A switchover is a manual activation process that you can perform at the database, server, or data center (site) level.
- Database names for Exchange 2010 must be unique within the Exchange organization.
- When a mailbox database has been configured with one or more database copies, the full path for all database copies must be identical on all Mailbox servers that host a copy.
- Any mailbox database copy (the active or any passive copy) can be backed up using an Exchange-aware Volume Shadow Copy Service (VSS)-based backup application.

For more information about mailbox database copies, see Understanding Mailbox Database Copies.

Changes to Continuous Replication from Exchange Server 2007

The underlying continuous replication technology previously found in CCR and SCR remains in Exchange 2010, and it's been further evolved to support new high availability features such as database copies, database mobility, and DAGs. Some of these new architectural changes are briefly described as follows:

- Because storage groups have been removed from Exchange 2010, continuous replication now operates at the database level. Exchange 2010 still uses an Extensible Storage Engine (ESE) database that produces transaction logs that are replicated to one or more other locations and replayed into one or more copies of a mailbox database.
- Because the log replay functionality that was performed by the Microsoft Exchange Replication service in Exchange 2007 has been moved into the Exchange 2010 version of the Microsoft Exchange Information Store service (store.exe), the performance hit associated with failovers and switchovers (because a new database cache was put into use) no longer exists. When a failover or switchover occurs, the activated database has a warm cache that's ready for use.
- Log shipping and seeding no longer uses Server Message Block (SMB) for data transfer. Exchange 2010 continuous replication uses a single administrator-defined TCP port for data transfer. In addition, Exchange 2010 includes built-in options for network encryption and compression for the data stream.
- Log shipping no longer uses a pull model, where the passive copy pulls closed log files from the active copy. Instead, the active copy pushes the log files to each configured passive copy.
- Seeding is no longer restricted to using only the active copy of the database. Passive copies of mailbox databases can now be specified as sources for database copy seeding and reseeding.
- Database copies are for mailbox databases only. For redundancy and high availability of public folder databases, we recommend that you use public folder replication. Unlike CCR, where multiple copies of a public folder database couldn't exist in the same cluster, each DAG member can host a public folder database, and you can use public folder replication to replicate public folders between public folder databases hosted on DAG members.
- The LogReplayer component of the Microsoft Exchange Replication service includes new logic to suspend log replay if the copy queue length increases beyond a specific threshold. If the number of logs in the copy queue is greater than the number of log files that have been copied to the passive database copy, but not inspected by the passive copy, then the Microsoft Exchange Replication service will suspend log replay for the passive copy and log

Warning event 4110 in the event log. When the number of log files in the copy queue drops below the number of non-inspected copied log files, the Microsoft Exchange Replication service will resume replay for the passive copy and log Informational event 4111 in the event log.

Several concepts used in Exchange 2007 continuous replication also remain in Exchange 2010. These include the concepts of *failover management*, *divergence*, the use of the *auto database mount dial*, and the use of public and private networks.

Changes to Routing Behavior When Hub Transport and Mailbox are Co-Located in a DAG

When the Hub Transport server is co-located with a Mailbox server that is a member of a DAG, there are changes in routing behavior to ensure that the resiliency features in both server roles will provide the necessary protection for messages sent and received by users on that server. The Hub Transport server role was modified so that it now attempts to re-route a message for a local Mailbox server to another Hub Transport server in same site if the Hub Transport server is also a DAG member and it has a copy of the mailbox database mounted locally. This extra hop was added in order to put the message in transport dumpster on a different Hub Transport server.

For example, EX1 hosts the Hub Transport and Mailbox role and is a member of a DAG. When a message arrives in transport for EX1 that is destined for a recipient whose mailbox is also on EX1, transport will re-route the message to another Hub Transport server in the site (for example, EX2), and that server will deliver the message to the mailbox on EX1.

There is a second similar behavior change with respect to the Microsoft Exchange Mail Submission service. This service was modified so that it would prefer to not submit messages to a local Hub Transport role when the Mailbox and Hub Transport server is a member of a DAG. In this scenario, the behavior of transport is to load balance submission requests across other Hub Transport servers in same Active Directory site, and fall back to local Hub Transport server if there are no other available Hub Transport servers in the same site.

End-to-End Availability

Exchange 2010 also includes many features designed to increase end-to-end availability of the system. These features include:

- Transport resilience
- Online move mailbox
- Exchange native data protection
- Incremental resync
- Third Party Replication API

Transport Resilience

Exchange 2007 introduced the transport dumpster feature of the Hub Transport server. The transport dumpster maintains a queue of messages that were delivered to recipients whose mailbox was in a CCR (and in Exchange 2007 SP1, in an LCR) environment. This feature was designed to help protect against data loss by providing an administrator with the option to have a clustered Mailbox server automatically come online on another node with a limited amount of data loss. This is referred to as a lossy failover. When a lossy failover occurred, the system automatically re-delivered the recent e-mail messages sent to users on the failed clustered Mailbox server, by using the transport dumpster where

the e-mail messages were still stored. Although this solution helped to minimize the amount of data lost in a lossy failover, the solution only protected from data loss within a site, and it didn't provide protection for messages in transit.

Exchange 2010 introduces core architectural changes that address both issues. Because DAGs can be stretched across Active Directory sites, it's possible for an individual mailbox database to move between Active Directory sites. Because of this design change, the transport dumpster re-delivery request upon a lossy database failover is now issued to Hub Transport servers in both the database's original and new Active Directory sites.

One other significant change to the transport dumpster is that it now receives feedback from the replication pipeline. When messages in the transport dumpster have been replicated to all mailbox database copies, they're removed from the transport dumpster. This ensures that only non-replicated data is held in the transport dumpster.

In addition to the transport dumpster feature, a new Hub Transport server feature named *shadow redundancy* has been added. Shadow redundancy provides redundancy for messages for the entire time they're in transit. The solution involves a technique similar to the transport dumpster. With shadow redundancy, the deletion of a message from the transport database is delayed until the transport server verifies that all of the next hops for that message have completed delivery. If any of the next hops fail before reporting back successful delivery, the message is resubmitted for delivery to that next hop. For more information about shadow redundancy, see Understanding Shadow Redundancy.

Online Move Mailbox

Exchange 2010 includes a new feature that enables you to move mailboxes asynchronously. In Exchange 2007, when you used the **Move-Mailbox** cmdlet to move a mailbox, the cmdlet logged into both the source database and the target database and moved the content from one mailbox to the other mailbox. There were several disadvantages to having the cmdlets perform the move operation:

- Mailbox moves typically took hours to complete, and during the move, users weren't able to access their mailbox.
- If the command window used to run **Move-Mailbox** cmdlet was closed, the move was terminated and had to be restarted from the beginning.
- The computer used to perform the move participated in the data transfer. If an administrator ran the cmdlets from their workstation, the mailbox data would flow from the source server to the administrator's workstation and then to the target server.

The new move request cmdlets in Exchange 2010 can be used to perform asynchronous moves. Unlike Exchange 2007, the cmdlets don't perform the actual move. The move is performed by the Microsoft Exchange Mailbox Replication Service, a new service that runs on the Client Access server. The **New-MoveRequest** cmdlet sends requests to the Mailbox Replication Service. For more information about online move mailbox, see Understanding Move Requests.

Exchange Native Data Protection

There are several changes to the core architecture of Exchange 2010 that have a direct effect on how you protect your mailbox databases and the mailboxes they contain.

One significant change is the removal of storage groups. In Exchange 2010, each database is associated with a single log stream, represented by a series of 1 megabyte (MB) log files. Each server can host a maximum of 100 databases.

Another significant change for Exchange 2010 is that databases are no longer closely tied to a specific Mailbox server. Database mobility expands the system's use of continuous replication by replicating a database to multiple different servers. This provides better protection of the database and increased availability. In the case of failures, the other servers that have copies of the database can mount the database.

The ability to have multiple copies of a database hosted on multiple servers, means that if you have a sufficient number of database copies, you can use these copies as your backups. For more information on this strategy, see Understanding Backup, Restore and Disaster Recovery.

Incremental Resync

Exchange 2007 introduced the concepts of lost log resilience (LLR) and incremental reseed. LLR is an internal component of ESE that enables you to recover Exchange mailbox databases even if one or more of the most recently generated transaction log files have been lost or damaged. LLR enables a mailbox database to mount even when recently generated log files are unavailable. LLR works by delaying writes to the database until the specified number of log generations have been created. LLR delays recent updates to the database file for a short time. The length of time that writes are delayed depends on how quickly logs are being generated.

Note:
LLR is hard-coded to one log file for all Exchange 2010 mailbox databases.

Incremental reseed provided the ability to correct divergences in the transaction log stream between a source and target storage group, by relying on the delayed replay capabilities of LLR. Incremental reseed didn't provide a means to correct divergences in the passive copy of a database after divergent logs had been replayed, which forced the need for a complete reseed.

In Exchange 2010, *incremental resync* is the new name for the feature that automatically corrects divergences in database copies under the following conditions:

- After an automatic failover for all of the configured copies of a database
- When a new copy is enabled and some database and log files already exist at the copy location
- When replication is resumed following a suspension or restarting of the Microsoft Exchange Replication Service

When divergence between an active database and a copy of that database is detected, incremental resync performs the following tasks:

- It searches historically in the log file stream to locate the point of divergence.
- It locates the changed database pages on the diverged copy.
- It reads the changed pages from the active copy and then copies the necessary log files from the active copy.
- It applies the database page changes to the diverged copy.
- It runs recovery on the diverged copy and replays the necessary log files into the database copy.

Third Party Replication API

Exchange 2010 also includes a new Third Party Replication API that enables organizations to use third-party synchronous replication solutions instead of the built-in continuous replication feature. For information about partner products for Exchange 2010, see the Exchange 2010 Partners Web site. If you're a partner seeking information on the Third Party Replication API, please contact your Microsoft representative.

Features Cut from Exchange Server 2007

The following features in Exchange 2007 and Exchange 2007 SP1 no longer exist in Exchange 2010. Their replacements are noted in the table.

Feature	Replacement
Cluster continuous replication (CCR)	Database availability groups and mailbox

	database copies
Standby continuous replication (SCR)	Database availability groups and mailbox database copies
Local continuous replication (LCR)	Database availability groups and mailbox database copies
Single copy clusters (SCC)	Database availability groups and mailbox database copies; built-in third-party synchronous API available to replace third-party data replication used with SCC
Clustered Mailbox servers	Database availability groups and mailbox database copies
Storage groups	Databases
Recovery Storage Group	Recovery database

1.1.5.4 New Messaging Policy and Compliance Functionality

New Messaging Policy and Compliance Functionality

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-01*

Microsoft Exchange Server 2010 has new messaging policy and compliance features that allow organizations to comply with regulations related to messaging retention, protection of personal information, and fulfilling legal discovery requests for messaging records.

Contents

Messaging Records Management

Messaging records management (MRM) is the records management technology in Exchange that helps organizations to reduce legal risks associated with e-mail and other communications. In Exchange 2010, MRM is accomplished by using the following new retention features:

- **Retention tags** Retention tags are used to apply retention settings to messages and folders. There are three types of retention tags:
  - Default policy tags (DPTs)

  - Retention policy tags (RPTs)
  - Personal tags
- **Retention policies** A retention policy is a group of retention tags that can be applied to a mailbox.

Applying retention policies to the mailboxes in your organization allows you to apply message retention settings without impacting your users' e-mail workflow or e-mail organization methods. Also, with retention tags, users can tag messages and folders based on retention requirements. They no longer need to move messages to folders only for retention purposes (as was required by the managed folders feature in Exchange Server 2007).

Note:
Managed folders, the MRM technology introduced in Exchange 2007, is still available in Exchange 2010. For more information, see Understanding Managed Folders.

To learn more about the retention features in Exchange 2010, see Understanding Retention Tags and Retention Policies.

Return to top

Multi-Mailbox Search

In Exchange 2010, Multi-Mailbox Search helps organizations facing legal discovery requirements (as part of organizational policy, compliance requirements, or lawsuits), to search for relevant content in Exchange mailboxes. Exchange 2010 provides a seamless experience for searching e-mail content in mailboxes across the entire Exchange organization.

To learn more about Multi-Mailbox Search, see Understanding Multi-Mailbox Search.

Return to top

Litigation Hold

In Exchange 2010, Multi-Mailbox Search allows a user who is assigned the Discovery Management role to search mailbox content to comply with discovery requests. However, users who own the mailbox or have permissions to access it can delete messages. Furthermore, if a retention policy or a managed folder mailbox policy is applied to the mailbox, messages can be removed from the mailbox by the Managed Folder Assistant.

In Exchange 2010, you can place mailboxes on litigation hold to protect against intentional, policy-based, or accidental message deletion. This allows deleted messages to be indexed by Exchange Search. As a result, these messages are returned when Multi-Mailbox Search is used to search the mailbox. After a mailbox is placed on litigation hold, any changes made to messages are also preserved as different versions.

To learn more about litigation hold, see Understanding Litigation Hold.

Return to top

Information Rights Management Protection

Protecting critical business information is an important aspect of information protection. Regulations in many countries, regions, and industries (such as financial services and

healthcare), require organizations to protect personal information collected from customers and employees. Most business communication occurs over e-mail, and many users also use e-mail as an information and document repository.

To help protect this critical information, Exchange 2010 includes the following Information Rights Management (IRM) features:

- Support for Active Directory Rights Management Services (AD RMS) rights policy templates.
- Persistent protection of attachments in IRM-protected messages.
- Outlook protection rules protect messages in Microsoft Outlook 2010 based on rule conditions.
- Transport protection rules protect messages based on transport rule conditions.
- Transport decryption decrypts IRM-protected messages on Hub Transport servers, which allows you to apply messaging policies.
- Journal report decryption attaches a decrypted copy of IRM-protected messages to journal reports.
- Support for IRM in Microsoft Office Outlook Web App.
- IRM-protection for Unified Messaging voice mail messages.

To learn more about IRM features, see Understanding Information Rights Management.

Return to top

Personal Archive

Personal archives provide your users with an alternate storage location for storing historical messaging data. Using Outlook 2010 and Outlook Web App, users have seamless access to their personal archive. Using either of these client applications, they can view a personal archive and move or copy messages between their primary mailbox and the archive. Messages can also be automatically moved from the primary mailbox to the archive by using an archive policy.

Personal archives allow you to present your users with a consistent view of their messaging data, and they also eliminate the user overhead required to manage .pst files. Eliminating use of .pst files significantly reduces your organization's exposure to several risks.

To learn more about personal archives, see Understanding Personal Archives.

Return to top

Transport Rule Predicates and Actions

Transport rules inspect messages for conditions specified in the rule. Messages that meet the conditions, and none of the exceptions, have the specified actions applied to them. Exchange 2010 includes several new predicates and actions, providing additional flexibility when creating rules. To learn more, see Transport Rule Predicates and Transport Rule Actions.

The **New-TransportRule** and **Set-TransportRule** cmdlets are also enhanced, allowing you to specify all predicates and actions in a single command. All predicates and actions are now available for use as parameters with these cmdlets. To learn more about these cmdlets, see New-TransportRule and Set-TransportRule.

Return to top

1.1.5.5 New Unified Messaging Functionality and Voice Mail Features

New Unified Messaging Functionality and Voice Mail Features

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-19*

New functionality and many new features have been added to Microsoft Exchange Server 2010 Unified Messaging (UM). This topic explains the new features for Unified Messaging and voice mail that are included in Exchange 2010.

Contents

Call Answering Rules

In Exchange 2010, the Unified Messaging server role allows UM-enabled users to create and customize call answering rules to enhance the experience of people who call them. At the time a user becomes enabled for UM, no call answering rules exist. The Exchange 2010 voice mail is the default call answering behavior. However, users can create up to nine call answering rules.

Call answering rules are similar to the Exchange Server 2007 UM auto attendants. There is usually a greeting, a menu prompt, and a list of options to choose from. The key difference between an auto attendant and a call answering rule that, when the call answering rule processes an incoming call, Unified Messaging already knows who the call is for.

Using call answering rules, a caller can:

- Leave a voice message for the UM-enabled user.
- Transfer to an alternate contact of the UM-enabled user.
- Transfer to the alternate contact's voice mail.
- Transfer to other phone numbers that the UM-enabled user has configured.
- Use the Find-Me feature or locate the UM-enabled user via a supervised transfer.

Additional Language Support

In Exchange 2007, each UM language pack included a Text-to-Speech (TTS) engine and the prerecorded prompts for a specified language. UM language packs for Exchange 2007 are offered in 16 different languages. However, not all the UM language packs contain support for Automatic Speech Recognition (ASR). For ASR, there was only one language—US English.

For Exchange 2010, all available language packs contain the Text-to-Speech (TTS) engine and the prerecorded prompts for a specified language and ASR support. However, only some of the language packs contain support for Voice Mail Preview. The US English (en-US) language pack is included on the Exchange 2010 DVD and additional UM language packs can be downloaded from the Microsoft Download Center.

For more information about UM language packs, see the following topics:

- Client Language Support for Unified Messaging
- Understanding Unified Messaging Languages

Improvements to Name Lookup from a Caller ID

In Exchange 2007 Unified Messaging, a voice message was created after a call was diverted to a Unified Messaging server because of a ring-no-answer or busy condition. After the call was answered, Exchange 2007 Unified Messaging tried to resolve the caller ID. It did this so that it could insert a name, rather than a number, into the sender information.

In Exchange 2007, name lookups for voice mail messages were done using information about the caller who was in the same dial plan as the user being called. Name lookups were performed by using an Exchange Unified Messaging proxy address (EUM proxy address), using the personal contacts of the user receiving the call, or using the **msRTCSIP-Line** attribute in Active Directory if Service Pack 1 (SP1) for Exchange 2007 was installed and Exchange 2007 was integrated with Office Communications Server 2007.

In Exchange 2010, the name lookup methods used in Exchange 2007 have been enhanced. Although Exchange 2010 includes methods that were used to resolve calling IDs in Exchange 2007, eight other Active Directory attributes have been added for resolving a caller ID to a name. You can use the following steps to look up a name from the calling party's information:

1. Use the caller's name if the caller is signed in to their mailbox from Outlook Voice Access or if they use a Unified Communications client such as Office Communicator 2007 or Office Communicator Phone Edition to place the call. The caller's identity is known because they've already been authenticated by Outlook Voice Access, Office Communicator 2007 or Office Communicator Phone Edition.
2. Use the EUM proxy addresses in Active Directory. If the proxy address contains an at sign (@), it's considered to be a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI). If the proxy address begins with a plus sign (+), it's considered to be an E.164 number. If neither of these symbols is present, the address is considered to be an extension within the same dial plan as the called party or an equivalent dial plan.
3. If the caller ID is a valid SIP URI, use Active Directory to resolve the SIP URI using the EUM proxy addresses.
4. If the caller ID is a valid E.164 number, use Active Directory to resolve the number using the calling party's name. For this to work correctly, you must manually configure the `UMCallingLineIds` parameter on the UM-enabled

mailbox for each user. This is useful when you don't want to publish a telephone number, such as a personal cell phone number, in Active Directory, but still want to resolve the calling party's name by using this phone number.

5. Use Active Directory heuristic matching, if it is enabled, to resolve the number using the calling party's name. Active Directory heuristic matching must be enabled on the dial plan, and the user's account in Active Directory must contain information in at least one of the following Active Directory attributes:
   5.a.TelephoneNumber
   5.b.HomePhone
   5.c.Mobile
   5.d.FacsimileTelephoneNumber
   5.e.OtherTelephone
   5.f.OtherHomePhone
   5.g.OtherMobile
   5.h.OtherFacsimileTelephoneNumber
6. Use the personal Contacts of the called party to resolve the number using the calling party's name.
7. If the calling party's name is not resolved using one the methods described previously, the phone number is used in the voice mail message.

Voice Mail Preview

In Exchange 2010, the Unified Messaging server role uses ASR on newly created voice mail messages. When users receive voice messages, the messages contain both a recording and text that's been created from the voice recording. Users see the voice message text displayed in an e-mail message from within Outlook Web App, Outlook 2007, or Outlook 2010.

Message Waiting Indicator

Message Waiting Indicator is a feature found in most legacy voice mail systems and can refer to any mechanism that indicates the existence of a new message. In Exchange 2007, this functionality was provided by a third-party application, which indicated receipt of a new voice message by lighting the lamp on the desk phone. This feature has been added to Exchange 2010, and third-party software isn't needed. Enabling or disabling Message Waiting Indicator is done on the user's mailbox or on a UM mailbox policy.

Missed Call and Voice Mail Notifications Using SMS

When users are members of a hosted or consumer dial plan, and they configure their voice mail settings with their mobile phone number and configure call forwarding, they can receive notifications about missed calls and new voice messages on their cell phones in a text message via the Short Messaging Service (SMS). However, to receive these types of notifications, the users must first configure text messaging and also enable **Notifications** on their account.

Protected Voice Mail

Protected Voice Mail is Unified Messaging functionality that enables users to send private mail. This mail is protected by Active Directory Rights Management Services (AD RMS), and users are restricted from forwarding, copying, or extracting the voice file from e-mail. Protected Voice Mail increases the confidentiality of Unified Messaging, and lets users rely on Unified Messaging if they want to limit the audience for voice messages. This functionality is similar to the way private e-mail messages were handled in Exchange

2007. In Exchange 2010, it applies to voice mail messages as well.

Incoming Fax Support

Exchange 2007 provided built-in support for fax message creation through the Unified Messaging server role. A user with a UM-enabled mailbox could receive fax messages from calls placed to his or her phone number. There's no support in Exchange 2007 UM for inbound fax routing, or for outgoing fax.

In Exchange 2010, direct support for fax has been removed from the Unified Messaging server role. Customers who require a fax solution that works with Exchange 2010 will need to deploy a fax partner solution. Fax partner solutions are available from several fax partners. The fax partner solutions are designed to be tightly integrated with Exchange 2010 and allow UM-enabled users to receive incoming fax messages.

Group Addressing Using Outlook Voice Access

In Exchange 2007, users could use either the telephone user interface (TUI) or voice user interface (VUI) in Outlook Voice Access to send e-mail and voice messages when they logged on to their mailbox. However, users could only send a single e-mail message to a single user in their personal Contacts, to multiple recipients from the directory by adding each recipient individually, or by adding the name of a distribution list from the global address list. In Exchange 2010, when a user signs in to their mailbox using Outlook Voice Access, they can also send e-mail and voice messages to users in a group stored in their personal Contacts.

Built-in Unified Messaging Administrative Roles

A set of roles for managing Unified Messaging and voice mail features have been defined within Exchange 2010. Administrative roles that included UM were available in Exchange 2000. The following UM-specific administrative roles have been added for Exchange 2010:

- UM Mailboxes
- UM Prompts
- Unified Messaging

1.1.5.6 New Mailbox and Recipient Functionality

New Mailbox and Recipient Functionality

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

This topic lists the new functionality available for Mailbox servers, mailboxes, and recipients in Microsoft Exchange Server 2010.

For information about the other mailbox features, see the following topics:

- New Exchange Core Store Functionality
- New High Availability and Site Resilience Functionality

Contents

Calendaring

In Exchange 2010, your users can share information with external users. This information includes calendar, contacts, and free/busy data. For more information about accessing free/busy data from different organizations, see Managing Federated Delegation.

Note:

Contact sharing will be available with the release of Microsoft Outlook 2010. For information about when Outlook 2010 will be available, visit Microsoft Office Online.

Before you can share any information between organizations, a federation trust must be established. For more information, see Federation.

The **MailboxCalendarSettings** commands have been removed. The functionality is replaced by the following cmdlets:

- Get-MailboxCalendarConfiguration
- Set-MailboxCalendarConfiguration
- Get-CalendarProcessing
- Set-CalendarProcessing

Return to top

Calendar Repair Assistant

Calendar Repair Assistant (CRA) is a configurable, time-based mailbox assistant that runs within the Microsoft Exchange Mailbox Assistants service on Exchange 2010 Mailbox servers. CRA automatically detects and corrects inconsistencies for single and recurring meeting items in mailboxes. With this functionality, recipients won't miss meetings or have unreliable meeting information.

For more information about CRA, see Understanding Calendar Repair.

Return to top

Resource Scheduling

You can now use the Exchange Management Console (EMC) to manage resource scheduling by editing the resource mailbox's properties. For more information, see Configure User and Resource Mailbox Properties.

Return to top

Moving Mailboxes

Exchange 2010 includes cmdlets that allow you to move a mailbox while the end user is still accessing it. These cmdlets are for use in moving Exchange 2010 mailboxes between Exchange 2010 databases. Use the **Move-Mailbox** cmdlet in Exchange Server 2007 to move legacy Exchange mailboxes.

For more information, see Understanding Move Requests or Managing Move Requests.

Mailbox moves are now managed by the following cmdlets:

- New-MoveRequest This cmdlet begins the process to move a mailbox. You can test the readiness of a mailbox by including the *WhatIf* parameter in the command.
- Get-MoveRequest This cmdlet retrieves statistics about the status of an ongoing mailbox move that was initiated by using the **New-MoveRequest** cmdlet.
- Remove-MoveRequest This cmdlet cancels an ongoing mailbox move that was initiated by using the **New-MoveRequest** cmdlet.

Return to top

Distribution Groups

Exchange 2010 includes new functionality for both moderated and user-created distribution groups.

Moderated Distribution Groups

You can appoint a moderator to regulate the flow of messages sent to a distribution group. Anyone can send a message to the distribution group alias, but before the message is delivered to all participants, a moderator must review and approve it. This helps prevent inappropriate e-mail messages from being delivered to large audiences. For more information, see Understanding Moderated Transport.

User-Created Distribution Groups

The following is a list of new functionality for user-created distribution groups:

- New parameters have been added to the distribution group cmdlets to allow users to create and manage their own distribution groups in Microsoft Office Outlook Web App and Outlook 2010.
- A new user interface (UI) has been added to allow administrators to manage the distribution group ownership, including how users can be added to the group.
  To view the new UI, open a distribution group's property dialog box (right-click the group, and then click **Properties**). The **Group Information** and the **Membership Approval** tabs include the new functionality.

The following table lists the new parameters that support user-created distribution groups.

New parameters added to distribution group cmdlets

New parameter	Used in cmdlets
MemberDepartRestriction	New-DistributionGroup Set-DistributionGroup

MemberJoinRestriction	New-DistributionGroup Set-DistributionGroup
BypassSecurityGroupManagerCheck	Remove-DistributionGroup Set-DistributionGroup Add-DistributionGroupMember Remove-DistributionGroupMember
MemberDepartRestriction	Set-DistributionGroup
MemberJoinRestriction	Set-DistributionGroup

Also, the *ManagedBy* parameter has been updated to indicate ownership of a distribution group. Users specified in the *ManagedBy* parameter can modify the distribution group settings.

Note:
The *ManagedBy* parameter functionality for dynamic distribution groups didn't change.

For more information about distribution groups, see Understanding Recipients and Managing Distribution Groups.

Return to top

Permission Management for Mailbox Folders

You can manage folder-level permissions for all folders within a user's mailbox. Sharing mailbox folders and calendar folders is managed through a new set of cmdlets. These cmdlets allow you to view, remove, and add permissions for specific users on all designated mailbox folders:

- Add-MailboxFolderPermission
- Get-MailboxFolderPermission
- Remove-MailboxFolderPermission

Return to top

Bulk Recipient Management in the EMC

Exchange 2007 Service Pack 1 (SP1) introduced bulk recipient management for moving, removing, disabling, and enabling mailboxes in the EMC. In Exchange 2010, this functionality is expanded to include the following tasks:

- **Properties** You can select multiple recipients in the result pane, and then click **Properties** in the action pane. Properties that you can't bulk edit are unavailable.

  Note:
  You can only bulk edit recipient properties when the same recipient types are selected.

- **Send Mail** You can select multiple recipients in the result pane, and then click **Send Mail** in the action pane to send an e-mail to multiple recipients. For more information, see the Send Mail section later in this topic.

Return to top

Personal Archive

A personal archive is a specialized mailbox associated with a user's primary mailbox. It appears alongside the primary mailbox folders in Outlook 2010 or Outlook Web App. Users have direct access to e-mail within the archive just as they would their primary mailbox. Users can drag e-mail from .pst files into the personal archive for easier online access.

Through the use of retention policies, e-mail items from the primary mailbox can be automatically offloaded to the personal archive. This reduces the mailbox size and improves application and network performance. In addition, users can use Outlook 2010 or Outlook Web App to search both their personal archive and primary mailbox.

To learn more, see Understanding Personal Archives.

Return to top

Send Mail

You can send mail to multiple recipients from the EMC. Select multiple recipients in the result pane, and then click **Send Mail** in the action pane. You must configure an e-mail account on the computer from which you are sending mail. You can send mail to the following recipient types:

- User mailboxes
- Mail contacts
- Mail users
- Dynamic distribution groups
- Distribution groups

You can't send mail to resource mailboxes.

Return to top

1.1.5.7 New Transport Functionality

New Transport Functionality

Exchange Server 2010 > Getting Started With Exchange 2010 > What's New in Exchange 2010 >

Applies to: *Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-11*

The following is a list of new or improved transport and routing functionality that's included in Microsoft Exchange Server 2010:

- **MailTips** MailTips provide extra information that's displayed to senders while they're composing e-mail messages. MailTips provide information about the messages such as details about the recipients and their availability, or reasons the message wouldn't be delivered. For example, if the person the message is addressed to is out of the office, senders will be informed about this while they're composing the message. To learn more about MailTips, see Understanding MailTips.
- **Shadow redundancy** Messages that are submitted to an Exchange 2010 Hub

Transport server are stored in the transport database until the next hop reports successful delivery of the message. If the next hop doesn't report successful delivery and it fails, the message is resubmitted for delivery. To learn more about shadow redundancy, see Understanding Shadow Redundancy.

- **Moderated transport** Exchange 2010 provides an approval workflow for sending messages to recipients. When you configure a recipient for moderation, all messages sent to that recipient must go through an approval process. To learn more about moderated transport, see Understanding Moderated Transport.
- **End-to-end message tracking** Exchange 2010 transport provides users with the ability to track messages from submission to the final destination. There is a new message tracking tool that makes it easy for any user role, from end-user to administrator, to track messages. For more information, see Understanding Message Tracking.
- **Support for disabling TLS for WAN topologies** In certain topologies where WAN Optimization Controller (WOC) devices are used, the TLS encryption of SMTP traffic may be undesirable. Exchange 2010 supports disabling TLS for hub-to-hub communications for these specific scenarios. For more information, see Disabling TLS Between Active Directory Sites to Support WAN Optimization.
- **Incremental EdgeSync** In Exchange 2010, the EdgeSync process has been changed to keep track of synchronized information and only synchronize the changes since the last replication cycle. This significantly reduces network traffic and greatly improves synchronization efficiency. For more information, see Understanding Edge Subscriptions.
- **Transport rule predicates and actions** Transport rules inspect messages for conditions specified in the rules. Messages that meet the conditions, and none of the exceptions, get the specified actions applied to them. Exchange 2010 includes several new predicates and actions, providing additional flexibility in creating rules and additional options for actions that can be applied to messages. For more information, see Transport Rule Predicates and Transport Rule Actions.
- **Transport rule cmdlet improvements** The **New-TransportRule** and **Set-TransportRule** cmdlets have been enhanced, allowing you to specify all predicates and actions in a single command. All predicates and actions are now available for use as parameters with these cmdlets. For more information, see New-TransportRule and Set-TransportRule.
- **Transport rules integration with AD RMS** Exchange 2010 provides you the ability to create rules that require Active Directory Rights Management Services (AD RMS) protection based on keywords or patterns. For more information, see Understanding Transport Protection Rules.
- **Distribution group expansion improvements** The handling of distribution group expansion has improved in Exchange 2010. First, the amount of memory that's used for caching distribution group membership has been capped by a configurable limit. This change prevents the cache from consuming too much memory, and thereby impacting performance in large environments. Exchange 2010 also queries Active Directory in a more efficient manner when processing large distribution groups with delivery restrictions, improving the performance of message delivery to large distribution groups.
- **Message throttling improvements** In Exchange 2010, you can configure a Receive connector to monitor the rate of message submissions by users, IP addresses, or both. If you configure a Receive connector to monitor the message submission rate for users, it ensures that a specific user doesn't exceed the message rate that it's allowed, regardless of the IP address the connections are coming from. The default client Receive connector created on the Hub Transport servers is configured this way.
- **Latency management** With Exchange 2010 transport, you can measure service levels delivered relative to your service level agreement (SLA) goals. Exchange 2010 provides you the ability to measure latencies for each hop, as well as end-to-end latency.

1.1.6 Discontinued Features

Discontinued Features

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-10*

This topic discusses the components, features, and functionalities that have been removed, discontinued, or replaced in Microsoft Exchange Server 2010. For information about API and development tool changes, see Migrating from Earlier Technologies to Exchange 2010.

Contents

Discontinued Features from Exchange 2010 RTM to Exchange 2010 SP1

This section lists the Microsoft Exchange Server 2010 RTM features that are discontinued in Microsoft Exchange Server 2010 SP1.

Feature	Comments and mitigation
Export-Mailbox and **Import-Mailbox** cmdlets	Use export requests or import requests. For more information, see Understanding Mailbox Import and Export Requests.
Enable-AntispamUpdates	Use Forefront Security for Exchange Server to obtain automatic anti-spam updates. For more information, see Forefront Online Protection for Exchange.
Federated Delivery	Use Tenant Mail Flow control. For more information, see Understanding Transport Options.
ISInteg	Use New-MailboxRepairRequest or New-PublicFolderDatabaseRepairRequest.
Managed folders in the Exchange Management Console (EMC)	In Exchange 2010 SP1, use the Exchange Management Shell to administer managed folder features such as managed default folders, managed custom folders, and managed folder mailbox policies. You can use the EMC and the Shell to manage

	retention policies and retention tags, the new messaging records management (MRM) feature introduced in Exchange 2010. For more information, see Deploying Messaging Records Management.

Discontinued Features from Exchange 2007 to Exchange 2010 RTM

This section lists the Microsoft Exchange Server 2007 features that are discontinued in Exchange 2010.

APIs and Development Features

Feature	Comments and mitigation
Exchange WebDAV	Use Introduction to Web Services or Differences between the EWS Managed API and EWS. Alternatively, you can maintain an Exchange 2007 server for mailboxes that are managed by applications that use WebDAV. For more information, see Migrating from WebDAV to Exchange 2010.

Architecture Features

Feature	Comments and mitigation
DSProxy	Exchange 2010 uses the RPC Client Access service and the Address Book service to perform this functionality. For more information, see Understanding RPC Client Access and Understanding the Address Book Service.
Storage groups	Exchange 2010 uses database copy functionality. For information, see Understanding Mailbox Database Copies.
Extensible Storage Engine (ESE) streaming backup APIs	Exchange 2010 uses Volume Shadow Copy Service (VSS)-based copies, such as Windows Server Backup and the VSS-plug-in included with Exchange 2010. For information, see Understanding Backup, Restore and Disaster Recovery.
User Datagram Protocol (UDP) notifications	Support for User Datagram Protocol (UDP) notifications is removed from Exchange 2010. This impacts the experience when Outlook 2003 clients connect to their mailboxes on an Exchange 2010 server. For more information, see Microsoft Knowledge Base article 2009942, Folders take a long time to update when an Exchange Server 2010 user uses Outlook 2003 in online mode. **Note:** Support for User Datagram Protocol (UDP) notifications is added in Microsoft Exchange Server 2010 Service Pack 1 (SP1) Rollup 3

	(RU3). To obtain Exchange 2010 SP1 Update RU3, see Microsoft Knowledge Base article 2009942, Folders take a long time to update when an Exchange Server 2010 user uses Outlook 2003 in online mode.

High Availability Features

Feature	Comments and mitigation
Cluster continuous replication (CCR)	Exchange 2010 uses database availability groups (DAGs) and mailbox database copies. For information, see High Availability and Site Resilience.
Local continuous replication (LCR)	Exchange 2010 uses DAGs and mailbox database copies. For information, see High Availability and Site Resilience.
Standby continuous replication (SCR)	Exchange 2010 uses DAGs and mailbox database copies. For information, see High Availability and Site Resilience.
Single copy cluster (SCC)	Exchange 2010 uses DAGs and mailbox database copies. For information, see High Availability and Site Resilience.
Setup /recoverCMS	Exchange 2010 uses Setup /m:recoverServer. For information, see Recover a Database Availability Group Member Server.
Clustered mailbox servers	Exchange 2010 uses DAGs and mailbox database copies. For information, see High Availability and Site Resilience.

Client Access Features

Feature	Comments and mitigation
Client authentication using Integrated Windows authentication (NTLM) for POP3 and IMAP4 users	NTLM isn't supported for POP3 or IMAP4 client connectivity in the RTM version of Exchange 2010. Connections from POP3 or IMAP4 client programs using NTLM will fail. If you're running the RTM version of Exchange 2010, the recommended POP3 and IMAP4 setting alternatives to NTLM are: • Kerberos (GSSAPI) • Plain Text Authentication with SSL If you're using the RTM version of Exchange 2010, to use NTLM, you must retain an Exchange 2003 or Exchange 2007 server in your Exchange 2010 organization. Support for NTLM authentication for POP3 and IMAP4 connectivity has been brought back in Exchange 2010 SP1. For more information, see Set-PopSettings and Set-ImapSettings.

Outlook Web App Features

Feature	Comments and mitigation
Document access	Can't use Microsoft Office Outlook Web App to access Microsoft Office SharePoint document libraries and Microsoft Windows file shares.
Web Parts	Web Parts aren't supported in Exchange 2010 RTM. This feature has been brought back in Exchange 2010 SP1.
User-selectable themes	Users can't change the theme in Outlook Web App RTM. This feature has been brought back in Exchange 2010 SP1.
Reading pane at the bottom of the page	There is no option to display the reading pane at the bottom of the Outlook Web App window. This feature has been brought back in Exchange 2010 SP1.

Recipient Related Features

Feature	Comments and mitigation
Move-Mailbox cmdlet set	Use move requests to move mailboxes. For information, see Understanding Move Requests.

Return to top

Discontinued Features from Exchange 2003 to Exchange 2010

This section lists the Exchange Server 2003 features that are discontinued in Exchange 2010.

APIs and Development Features

Feature	Comments and mitigation
Proxy address generators	Use the Shell.
ExCDO 1.2.1	Use Introduction to Web Services.
MAPI32	Use Introduction to Web Services.
CDOEX (CDO 3.0)	Use Introduction to Web Services.
Exchange WebDAV extensions	Use Introduction to Web Services.
ExOLEDB	Use Introduction to Web Services.
Store events	Use Introduction to Web Services.

Return to top

Architecture Features

Feature	Comments and mitigation
Routing groups	Exchange 2010 uses Active Directory site-

	based routing. For information, see Understanding Message Routing.
Administrative groups	Exchange 2010 uses the Exchange 2007 split permissions model that's based on universal security groups. For information, see Understanding Split Permissions.
Intelligent Message Filter	Exchange 2010 uses anti-spam agents in the Hub Transport and Edge Transport server roles. For information, see Understanding Anti-Spam and Antivirus Functionality.
Link state routing	Exchange 2010 uses Active Directory site-based routing. For information, see Understanding Message Routing.
Routing objects	If you need this functionality, retain an Exchange 2003 server in your Exchange 2010 organization.
Network-attached storage	Exchange 2010 supports Internet SCSI (iSCSI).
Exchange Installable File System (ExIFS)	Use Introduction to Web Services or MAPI.
Event service	If you need this functionality, retain an Exchange 2003 server in your Exchange 2010 organization.
Recovery storage group	Exchange 2010 uses the recovery database. For information, see Recovery Databases.
User Datagram Protocol (UDP)	Support for User Datagram Protocol (UDP) notifications is removed from Exchange 2010. This impacts the experience when Outlook 2003 clients connect to their mailboxes on an Exchange 2010 server. For more information, see Microsoft Knowledge Base article 2009942, Folders take a long time to update when an Exchange Server 2010 user uses Outlook 2003 in online mode.

Connector Features

Feature	Comments and mitigation
Microsoft Exchange Connector for Novell GroupWise and migration tools	If you need this functionality, retain an Exchange 2003 server in your Exchange 2010 organization.
Microsoft Exchange Connector for Lotus Notes	Use the appropriate tools for coexisting and migrating from Lotus Notes. These tools are available at the Interoperability Bridges and Lab Center Web site.

Protocol Features

Feature	Comments and mitigation

Network News Transfer Protocol (NNTP)	If you need this functionality, retain an Exchange 2003 server in your Exchange 2010 organization.
POP3 or IMAP4 graphical user interface (GUI) management	Use the Exchange Management Console (EMC) or the Exchange Management Shell. For information, see Managing POP3 and IMAP4.
X.400 message transfer agent (MTA)	If you need this functionality, retain an Exchange 2003 server in your Exchange 2010 organization.
SMTP virtual server instances	Use Exchange 2010 SMTP connectors. For information, see Understanding Send Connectors and Understanding Receive Connectors.

Public Folder Features

Feature	Comments and mitigation
Non-MAPI top-level hierarchies in a public folder store	If you need this functionality, retain an Exchange 2003 server in your Exchange 2010 organization.
Public folder access by using NNTP	If you need this functionality, retain an Exchange 2003 server in your Exchange 2010 organization.
Public folder access by using IMAP4	If you need this functionality, retain an Exchange 2003 server in your Exchange 2010 organization.

Client Access Features

Feature	Comments and mitigation
Client authentication using Integrated Windows authentication (NTLM) for POP3 and IMAP4 users	NTLM isn't supported for POP3 or IMAP4 client connectivity. The recommended POP3 and IMAP4 setting alternatives to NTLM are: • Kerberos (GSSAPI) • Plain Text Authentication with SSL Connections from POP3 or IMAP4 client programs to Exchange 2010 will fail. If you need this functionality, retain an Exchange 2003 or Exchange 2007 server in your Exchange 2010 organization.

Outlook Web App Features

Feature	Comments and mitigation
Calendar search	The search feature isn’t available for the Calendar folder in Outlook Web App.
Views in the Contacts folder	The Address Cards and Detailed Address Cards views are no longer available in Outlook Web App. The option is to use the Reading Pane when viewing Contacts.

	Contacts can't be sorted by location.
Printing	Contacts and Tasks don't include a print option in Exchange 2010 Outlook Web App.

Recipient-Related Features

Feature	Comments and mitigation
Exchange extensions in Active Directory Users and Computers	Exchange 2010 includes recipient management in the EMC. For information, see Managing Mailbox Servers.
Exchange Server Mailbox Merge wizard (ExMerge.exe)	In Exchange Server 2010 RTM, use the **Export-Mailbox** cmdlet or the Move Request cmdlet set. In Exchange Server 2010 SP1, use the Mailbox Repair Request cmdlet set or the Move Request cmdlet set. For information, see Recipient Cmdlets.
Mailbox Manager Policies	Use retention policies, the MRM feature introduced in Exchange 2010, or managed folder mailbox policies, the MRM feature introduced in Exchange 2007 (also available in Exchange 2010). For more information, see Understanding Messaging Records Management.
Recipient Update Service	Use the Update-AddressList and Update-EmailAddressPolicy cmdlets. To replace the full functionality of the Recipient Update Service, you can use the Task Scheduler to schedule these Shell commands. For information, see Task Scheduler.

Tools and Management Features

Feature	Comments and mitigation
Monitoring and status node	Use a monitoring solution such as System Center 2012 Cloud & Datacenter Management.
Message Tracking Center node and tracking mechanism	Use the Tracking Log Explorer and Message Tracking tools. For information, see Understanding Message Tracking.
Mailbox Recovery Center	Use the Restore-Mailbox cmdlet.
Mailbox Management Service	Use messaging records management (MRM) or retention policies. For information, see Understanding Messaging Records Management and Understanding Retention Tags and Retention Policies.
Clean Mailbox tool	In Exchange Server 2010 RTM, use the **Export-Mailbox** cmdlet or the Move Request cmdlet set. In Exchange 2010 SP1, use the **Mailbox**

	Repair Request cmdlet set or the **Move Request** cmdlet set. For information, see Recipient Cmdlets.
Migration wizard	Use the New-MoveRequest cmdlet or the Local Move Request and Remote Move Request wizards to move mailboxes from Exchange 2003 to Exchange 2010. For information, see Understanding Move Requests.
Exchange Profile Redirector tool (ExProfRe)	Use the Autodiscover service. For information, see Understanding the Autodiscover Service.

Return to top

1.1.7 Overview of Exchange 2010 Server Roles

Overview of Exchange 2010 Server Roles

Exchange Server 2010 > Getting Started With Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-20*

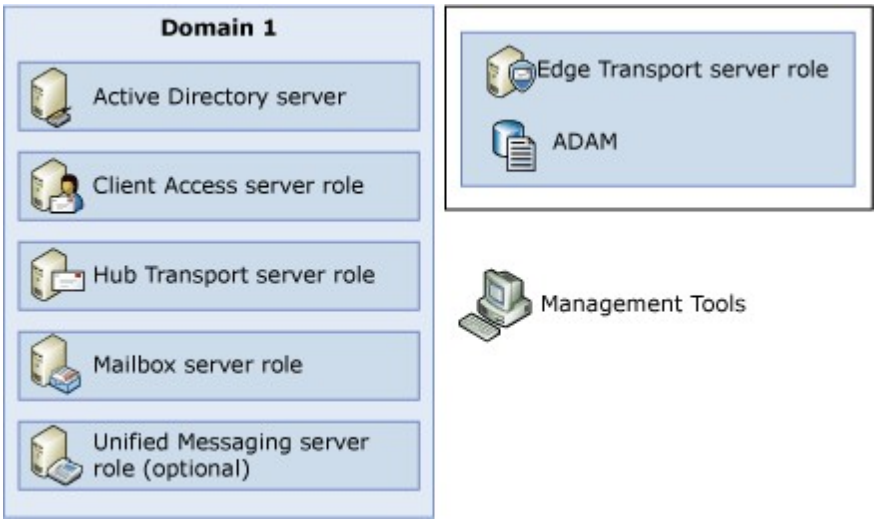
Because organizations tend to group their management tasks around a core set of server roles, Exchange 2010 maps Exchange Server management to this same approach.

A server role is a unit that logically groups the required features and components needed to perform a specific function in the messaging environment. The requirement of a server role is that it is a server that could be run as an atomic unit of scalability. A server role is composed of a group of features.

Server roles, the primary unit of deployment, enable administrators to easily choose which features are installed on an Exchange server. Logically grouping features in server roles offers the following advantages:

- Reduces attack surface on an Exchange server.
- Allows you to install and configure an Exchange server the way you intend to use it.
- Offers the ability to fully customize a server to support your business goals and needs.

The following figure illustrates a domain with each server role deployed.



Exchange 2010 includes the following server roles:

- **Mailbox Server** This server hosts mailboxes and public folders. For more information about the Exchange 2010 Mailbox server role, see Overview of the Mailbox Server Role.
- **Client Access Server** This is the server that hosts the client protocols, such as Post Office Protocol 3 (POP3), Internet Message Access Protocol 4 (IMAP4), Secure Hypertext Transfer Protocol (HTTPS), Outlook Anywhere, Availability service, and Autodiscover service. The Client Access Server also hosts Web services. For more information about the Exchange 2010 Client Access server role, see Client Access.
- **Unified Messaging Server** This is the server that connects a Private Branch eXchange (PBX) system to Exchange 2010. For more information about the Exchange 2010 Unified Messaging server role, see Unified Messaging.
- **Hub Transport Server** This is the mail routing server that routes mail within the Exchange organization. For more information about the Exchange 2010 Hub Transport server role, see Transport and Overview of the Hub Transport Server Role.
- **Edge Transport Server** This is the mail routing server that typically sits at the perimeter of the topology and routes mail in to and out of the Exchange organization. For more information about the Exchange 2010 Edge Transport server role, see Transport and Overview of the Edge Transport Server Role.

1.1.8 Roadmap for Exchange Features

Roadmap for Exchange Features

Exchange Server 2010 > Getting Started With Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This roadmap helps you get acquainted with all the features in Microsoft Exchange Server 2010. The first section lists all the features that can be managed by using either the Exchange Management Console (EMC) or the Exchange Management Shell. This section also shows you how to navigate to the feature in the EMC and provides a link to the

corresponding management topic.

However, not all features and tasks can be managed in the EMC. Therefore, the second section lists the features that can be managed only in the Shell and provides links to the corresponding cmdlet reference topic.

Important:

If you're looking for a feature that was in Exchange Server 2007 or Exchange Server 2003 and you can't find it in this topic, the feature may have been renamed or removed in Exchange 2010. For more information, see Discontinued Features.

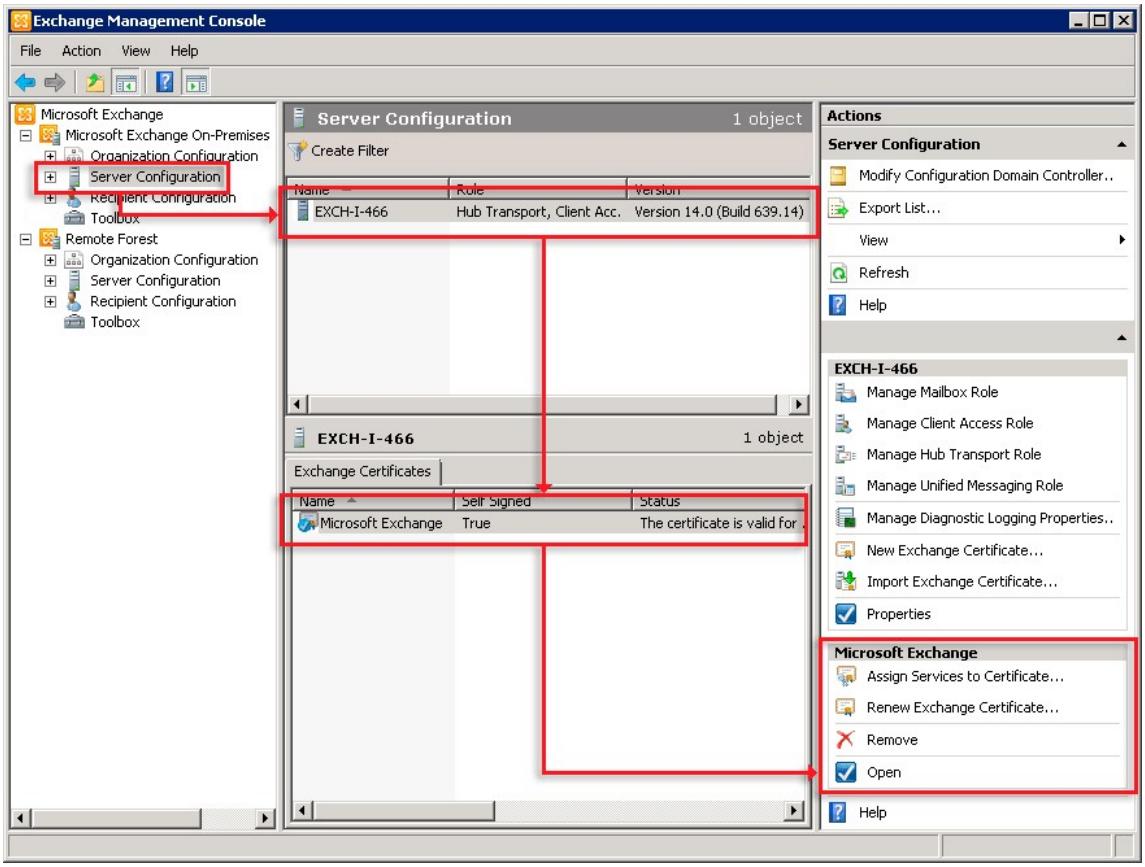
Features Managed in the EMC and the Shell

The following table is organized alphabetically by feature. It includes the click path that shows you how to get to the feature and the related topics that explain how to manage the feature.

Note:

This table shows how to locate features in the EMC. However, because all features can be managed by using the Shell, the management topics include both the EMC and Shell procedures.

The click paths follow the EMC layout from left to right, starting in the console tree and working toward the action pane. For example, consider the following click path for managing Exchange certificates: **Server Configuration** > *(Select Server)* > **Exchange Certificates** > *(Select Certificate)*. The following illustration maps this click path from the console tree, to the result pane, to the work pane, and then finally to the action pane that lists options for managing the specified certificate.



Exchange 2010 features managed in the EMC and Shell

Feature	How to get there in the EMC	Related management topics
Accepted domains	**Organization Configuration** > **Hub Transport** > **Accepted Domains** tab **Edge Transport** > **Accepted Domains** tab	Managing Accepted and Remote Domains
Address book policies	**Organization Configuration** > **Mailbox** > **Address Book Policies** tab	Managing Address Book Policies
Address book policies, apply to user	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Settings** tab > **Address Book Policy** > **Properties**	Assign an Address Book Policy to a Mail User
Address lists	**Organization Configuration** > **Mailbox** > **Address Lists** tab	Managing Address Lists
Archive quotas, apply to mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Settings** tab > **Archive Quota** > **Properties**	Configure Archive Quotas for a Personal (On-Premises) Archive

Best Practices Analyzer	**Toolbox** > **Best Practices Analyzer** > **Open Tool**	Microsoft Exchange Analyzers
Calendar settings, apply to mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) **Properties** > **Calendar Settings** tab	Managing User Mailboxes
Client Access server settings	**Server Configuration** > **Client Access** > (*Select Server*) > **Properties**	Managing Client Access Servers
Content filtering	**Edge Transport** > (*Select Server*) > **Anti-spam** tab > **Content Filtering**	Configure Content Filtering Properties
Customer Experience Improvement Program, opt-in or opt-out organization	**Microsoft Exchange On-Premises** > **Customer Feedback** tab	Opt-in or Opt-out of the Customer Experience Improvement Program
Customer Experience Improvement Program, opt-in or opt-out servers	**Server Configuration** > (*Select Server*) > **Properties** > **Customer Feedback Options** tab **Server Configuration** > (*Select Server Role Node*) > (*Select Server*) > **Properties** > **Customer Feedback Options** tab	Opt-in or Opt-out of the Customer Experience Improvement Program
Database availability group networks	**Organization Configuration** > **Mailbox** > **Database Availability Groups** tab > (*Select Database Availability Group*) > **Networks** tab	Create a Database Availability Group Network Configure Database Availability Group Network Properties
Database availability groups	**Organization Configuration** > **Mailbox** > **Database Availability Groups** tab	Managing Database Availability Groups
Database copies	**Organization Configuration** > **Mailbox** > **Database Management** tab > (*Select Mailbox Database*) > **Database Copies** tab	Managing Mailbox Database Copies
Database switchover	**Organization Configuration** > **Mailbox** > **Database Management** tab **Organization Configuration** > **Mailbox** > **Database Management** tab > (*Select Mailbox Database*) > **Database Copies** tab	Switchovers and Failovers
Databases	**Organization Configuration** > **Mailbox** > **Database Management** tab	Managing Mailbox Databases Managing Public Folder

		Databases
Details Templates Editor	**Toolbox** > **Details Templates Editor** > **Open Tool**	Managing Details Templates
Diagnostic logging	**Server Configuration** > **Mailbox** > (*Select Server*) > **Manage Diagnostic Logging Properties**	Manage Diagnostic Logging Levels
Distribution groups	**Recipient Configuration** > **Distribution Group**	Managing Distribution Groups
Dynamic distribution groups	**Recipient Configuration** > **Distribution Group**	Managing Distribution Groups
Edge Subscriptions	**Organization Configuration** > **Hub Transport** > **Edge Subscriptions** tab	Managing Edge Subscriptions
Edge Transport server settings	**Edge Transport** > (*Select Server*) > **Properties**	Managing Transport Servers
E-mail address policies	**Organization Configuration** > **Hub Transport** > **E-mail Address Policies** tab	Managing E-Mail Address Policies
E-mail addresses, apply to public folder	**Toolbox** > **Public Folder Management Console** > **Default Public Folders** > (*Select Mail-Enabled Public Folder*) > **Properties** > **E-Mail Addresses** tab	Configure Public Folder Properties
E-mail addresses, apply to recipient	**Recipient Configuration** > (*Select Recipient*) > **Properties** > **E-Mail Addresses** tab	Configure User and Resource Mailbox Properties Configure Mail User Properties Configure Mail Contact Properties Configure Distribution Group Properties Configure Dynamic Distribution Group Properties
Exchange ActiveSync mailbox policies	**Organization Configuration** > **Client Access** > **Exchange ActiveSync Mailbox Policies** tab	Managing Exchange ActiveSync with Policies
Exchange ActiveSync mailbox policies, apply to mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Features** tab > **Exchange ActiveSync** > **Properties**	Add Users to an Exchange ActiveSync Mailbox Policy

Exchange Control Panel Web site	**Server Configuration** > **Client Access** > **Exchange Control Panel** tab > (*Select Web Site*) > **Properties**	Configure ECP Virtual Directory Properties
External Client Access domains	**Server Configuration** > **Client Access** > **Configure External Client Access Domain**	Configure External Client Access Namespaces
Federation trusts	**Organization Configuration** > **Federation Trust** tab	Managing Federation
Full Access permission, mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Manage Full Access Permission**	Manage Full Access Permissions
Hub Transport server settings	**Server Configuration** > **Hub Transport** > (*Select Server*) > **Properties**	Managing Transport Servers
IMAP4, configure	**Server Configuration** > **Client Access** > **POP3 and IMAP4** tab > **IMAP4** > **Properties**	View or Configure IMAP4 Properties
IMAP4, enable, disable, or specify the MIME format for a mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Features** tab > **IMAP4**	Enable or Disable IMAP4 Access for a User
IP Allow List providers	**Edge Transport** > (*Select Server*) > **Anti-spam** tab > **IP Allow List Providers**	Configure IP Allow List Providers Properties
IP Allow lists	**Edge Transport** > (*Select Server*) > **Anti-spam** tab > **IP Allow List**	Configure IP Allow List Properties
IP Block lists	**Edge Transport** > (*Select Server*) > **Anti-spam** tab > **IP Block List**	Configure IP Block List Properties
IP Block List providers	**Edge Transport** > (*Select Server*) > **Anti-spam** tab > **IP Block List Providers**	Configure IP Block List Providers Properties
Journal rules	**Organization Configuration** > **Hub Transport** > **Journal Rules** tab	Managing Journaling
License, input key	**Server Configuration** > **Enter Product Key Group**	Enter Product Key
License, view server and client licensing information	**Microsoft Exchange On-Premises** > **Collect Organizational Health Data** tab	Collect Organizational Health Data
Mail contacts	**Recipient Configuration** > **Mail Contact**	Managing Mail Contacts and Mail Users

Mail Flow Troubleshooter	**Toolbox** > **Mail Flow Troubleshooter** > **Open Tool**	NA
Mail users	**Recipient Configuration** > **Mail Contact**	Managing Mail Contacts and Mail Users
Mailbox server settings	**Server Configuration** > **Mailbox** > (*Select Server*) > **Properties**	Managing Mailbox Servers
Mailboxes, configure	**Recipient Configuration** > **Mailbox**	Managing User Mailboxes
Mailboxes, disconnected	**Recipient Configuration** > **Disconnected Mailbox**	Connect to the Disconnected Mailbox Server Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive
Mailboxes, move	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **New Local Move Request** or **New Remote Move Request**	Managing Move Requests
Mailboxes, remote	**Recipient Configuration** > **Mail Contact**	Managing User Mailboxes
MAPI, enable or disable for mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Features** tab > **MAPI**	Enable or Disable MAPI for a User Mailbox
Message delivery	**Organization Configuration** > **Hub Transport** > **Global Settings** tab > (*Select Transport Settings*) > **Properties** > **Message Delivery** tab	Configure Transport Settings Properties
Message delivery restrictions, apply to recipient	**Recipient Configuration** > (*Select Recipient*) > **Properties** > **Mail Flow Settings** tab > **Message Delivery Restrictions** > **Properties**	Configure Message Delivery Restrictions
Message size restrictions, apply to recipient	**Recipient Configuration** > (*Select Recipient*) > **Properties** > **Mail Flow Settings** tab > **Message Size Restrictions** > **Properties**	Configure Message Size Limits for a Mailbox or a Mail-Enabled Public Folder
Message tracking	**Toolbox** > **Message Tracking** > **Open Tool** > (*Log On to Outlook Web App*) > (*Select to Manage My Organization*) > **Reporting** > **Delivery Reports** tab	Track Messages with Delivery Reports
Messaging records	**Organization Configuration**	Deploying Messaging Records

management (MRM) 2.0: Retention policies	> **Mailbox** > **Retention Policies** and **Retention Policy Tags** tabs	Management
Move request, view or remove	**Recipient Configuration** > **Move Request**	Managing Move Requests
Offline address book virtual directory, configure	**Server Configuration** > **Client Access** > **Offline Address Book Distribution** tab	Configure Offline Address Book Distribution Properties
Offline address books (OABs)	**Organization Configuration** > **Mailbox** > **Offline Address Book** tab	Managing Offline Address Books
Organization relationships	**Organization Configuration** > **Organization Relationships** tab	Managing Federated Delegation
Organizational health, update	**Microsoft Exchange On-Premises** > **Organizational Health** tab> **Collect Organizational Health Data**	Collect Organizational Health Data
Organizational health, view	**Microsoft Exchange On-Premises** > **Organizational Health Data** tab	Collect Organizational Health Data
Outlook Anywhere, configure	**Server Configuration** > **Client Access** > (*Select Server*) > **Properties** > **Outlook Anywhere** tab	Managing Outlook Anywhere
Outlook Anywhere, enable or disable	**Server Configuration** > **Client Access** > (*Select Server*) > **Enable Outlook Anywhere**	Enable Outlook Anywhere Disable Outlook Anywhere
Outlook Web App mailbox policies	**Organization Configuration** > **Client Access** > **Outlook Web App Mailbox Policies** tab	Managing Outlook Web App Mailbox Policies
Outlook Web App mailbox policies, apply to mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Features** tab > **Outlook Web App** > **Properties**	Apply an Outlook Web App Mailbox Policy to a Mailbox
Outlook Web App virtual directories, configure	**Server Configuration** > **Client Access** > **Outlook Web App** tab	Managing Outlook Web App Virtual Directories
Performance Monitor	**Toolbox** > **Performance Monitor** > **Open Tool**	Performance and Reliability Monitoring Step-by-Step Guide for Windows Server 2008
Performance Troubleshooter	**Toolbox** > **Performance Troubleshooter** > **Open Tool**	NA

Personal archive, disconnected	**Recipient Configuration** > **Disconnected Mailbox**	Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive
Personal archive, create	**Recipient Configuration** > **New Mailbox**	Create a Personal (On-Premises) or Cloud-Based Archive for a New Mailbox
Personal archive, enable or disable archive on existing mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Enable Archive** or **Disable Archive**	Enable a Personal (On-Premises) or Cloud-Based Archive for an Existing Mailbox
Personal archive, move	**Recipient Configuration** > **Mailbox** > *(Select Archive Mailbox)* > **New Local Move Request** or **New Remote Move Request** > **Move only the archive mailbox**	Create a Local Move Request Create a Remote Move Request That has Exchange 2010 in Both Forests
POP3, configure	**Server Configuration** > **Client Access** > (*Select Server*) > **POP3 and IMAP4** tab > **POP3** > **Properties**	Managing POP3 and IMAP4
POP3, enable or disable for mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Features** tab > **POP3**	Enable or Disable POP3 Access for a User
Public folder databases	**Organization Configuration** > **Mailbox** > **Database Management** tab	Managing Public Folder Databases
Public folder client permissions	**Toolbox** > **Public Folder Management Console** > **Default Public Folders** > (*Select Public Folder*) > **Manage Settings**	Use the Public Folder Management Console to Manage Public Folder Settings
Public folder replication settings	**Toolbox** > **Public Folder Management Console** > **Default Public Folders** > (*Select Public Folder*) > **Properties** > **Replication** tab	Configure Public Folder Replication
Public folder replication update	**Toolbox** > **Public Folder Management Console** > **Default Public Folders** > (*Select Public Folder*) > **Update Content**	Configure Public Folder Replication
Public folders	**Toolbox** > **Public Folder Management Console** > **Default Public Folders**	Managing Public Folders
Queue Viewer	**Toolbox** > **Queue Viewer** > **Open Tool**	Using Queue Viewer
Receive connectors	**Server Configuration** > **Hub Transport** > **Receive Connectors**	Managing Connectors

	Edge Transport > **Receive Connectors**	
Recipient filtering	**Edge Transport** > (*Select Server*) > **Anti-spam** tab > **Recipient Filtering**	Managing Anti-Spam and Antivirus Features
Remote Connectivity Analyzer	**Toolbox** > **Remote Connectivity Analyzer** > **Open Tool**	Exchange Remote Connectivity Analyzer Tool
Remote domains	**Organization Configuration** > **Hub Transport** > **Remote Domains** tab	Managing Accepted and Remote Domains
Reset Exchange Client Access server virtual directories	**Server Configuration** > **Client Access** > (*Select Server*) > **Reset Virtual Directory**	Reset Client Access Virtual Directories
Resource mailbox, configure	**Recipient Configuration** > (*Select Resource Mailbox*) > **Properties**	Managing Resource Mailboxes and Scheduling
Role Based Access Control (RBAC) User Editor	**Toolbox** > **Role Based Access Control (RBAC) User Editor** > **Open Tool** > (*Log On to Outlook Web App*) > **Administrator Roles** tab and **User Roles** tab	Administrator Roles Tab User Roles Tab
Routing Log Viewer	**Toolbox** > **Routing Log Viewer** > **Open Tool**	Using the Routing Log Viewer
Send As permissions, mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Manage Send As Permission**	Manage Send As Permissions for a Mailbox
Send As permissions, mail-enabled public folder	**Toolbox** > **Public Folder Management Console** > **Default Public Folders** > (*Select Mail-Enabled Public Folder*) > **Manage Send As Permission**	Manage Send As Permissions for Mail-Enabled Public Folders
Send connectors	**Organization Configuration** > **Hub Transport** > **Send Connectors** tab **Edge Transport** > **Send Connectors** tab	Managing Connectors
Send on behalf, mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mail Flow Settings** tab > **Delivery Options** > **Properties**	Configure User and Resource Mailbox Properties
Send on behalf, mail-enabled public folder	**Toolbox** > **Public Folder Management Console** >	Configure Public Folder Properties

	Default Public Folders > (*Select Mail-Enabled Public Folder*) > **Properties** > **Mail Flow Settings** tab > **Delivery Options** > **Properties**	
Sender filtering	**Edge Transport** > (*Select Server*) > **Anti-spam** tab> **Sender Filtering**	Managing Anti-Spam and Antivirus Features
Sender ID	**Edge Transport** > (*Select Server*) > **Anti-spam** tab > **Sender ID**	Managing Anti-Spam and Antivirus Features
Sender reputation	**Edge Transport** > (*Select Server*) > **Anti-spam** tab> **Sender Reputation**	Managing Anti-Spam and Antivirus Features
Server switchover	**Server Configuration** > **Mailbox** > (*Select Server*) > **Switchover Server**	Perform a Server Switchover
Sharing policies	**Organization Configuration** > **Mailbox** > **Sharing Policies** tab	Managing Federated Delegation
Sharing policies, apply to mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Settings** tab > **Sharing** > **Properties**	Managing Federated Delegation
Storage quotas, configure for a mailbox	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Settings** tab > **Storage Quotas** > **Properties**	Configure Storage Quotas for a Mailbox
Tracking Log Explorer	**Toolbox** > **Tracking Log Explorer** > **Open Tool**	NA
Transport dumpster	**Organization Configuration** > **Hub Transport** > **Global Settings** tab > **Transport Settings** > **Properties** > **General** tab	Configure Transport Settings Properties
Transport limits	**Organization Configuration** > **Hub Transport** > **Global Settings** tab > (*Select Transport Settings*) > **Properties** > **General** tab	Configure Transport Settings Properties
Transport rules	**Organization Configuration** > **Hub Transport** > **Transport Rules** tab **Edge Transport** > **Transport Rules** tab	Managing Transport Rules

Transport settings	**Organization Configuration** > **Hub Transport** > **Global Settings** tab	Configure Transport Settings Properties
UM auto attendants	**Organization Configuration** > **Unified Messaging** > **UM Auto Attendants** tab	Managing UM Auto Attendants
UM dial plans	**Organization Configuration** > **Unified Messaging** > **UM Dial Plans** tab	Managing UM Dial Plans
UM hunt groups	**Organization Configuration** > **Unified Messaging** > **UM IP Gateways** tab > (*Select IP Gateway*) > **UM Hunt Groups** tab	Managing UM Hunt Groups
UM IP gateways	**Organization Configuration** > **Unified Messaging** > **UM IP Gateways** tab	Managing UM IP Gateways
UM mailbox policies	**Organization Configuration** > **Unified Messaging** > **UM Mailbox Policies** tab	Managing UM Mailbox Policies
UM-enabled users	**Recipient Configuration** > **Mailbox** > (*Select Mailbox*) > **Properties** > **Mailbox Features** tab > **Unified Messaging** > **Properties**	Managing Unified Messaging Users
Unified Messaging server settings	**Server Configuration** > **Unified Messaging** > **Properties**	Managing Unified Messaging Servers
Unified Messaging server, enable or disable	**Server Configuration** > **Unified Messaging** > (*Select UM Server*) > **Disable Immediately** or **Disable After Calls**	Enable Unified Messaging on Exchange 2010 Disable Unified Messaging on Exchange 2010

Features Managed Only in the Shell

The following table lists features managed only by using the Shell and includes links to the corresponding cmdlet reference topics.

Exchange 2010 features managed only in the Shell

Feature	Manage by using
Address rewriting	**AddressRewriteEntry** cmdlet set See Transport Cmdlets
Administrator audit logging	Get-AdminAuditLogConfig Set-AdminAuditLogConfig New-AdminAuditLogSearch

	Search-AdminAuditLog Write-AdminAuditLog
Attachment filter agent	**AttachmentFilterEntry** cmdlet set **AttachmentFilterListConfig** cmdlet set See Anti-Spam Cmdlets
Client access array	**ClientAccessArray** cmdlet set See Client Access Cmdlets
Cmdlet extension agents	**CmdletExtensionAgent** cmdlet set See Cmdlet Extension Agent Cmdlets
Database availability group network encryption and compression	Set-DatabaseAvailabilityGroup
Database availability groups: Datacenter Activation Coordination mode	Set-DatabaseAvailabilityGroup
Database availability groups: replication port	Set-DatabaseAvailabilityGroup
Delivery agent connectors	**DeliveryAgentConnector** cmdlet set See Transport Cmdlets
Edge synchronization (EdgeSync) service settings, configure	**EdgeSyncServiceConfig** cmdlet set See Transport Cmdlets
EdgeSync, forcing or testing	Start-EdgeSynchronization Test-EdgeSynchronization
Exchange ActiveSync connectivity, test	Test-ActiveSyncConnectivity
Exchange ActiveSync log, export	Export-ActiveSyncLog
Exchange Control Panel connectivity, test	Test-EcpConnectivity
Exchange Search	Set-MailboxDatabase, with the *-IndexEnabled* parameter Test-ExchangeSearch Get-FailedContentIndexDocuments
Global address lists (GALs)	**GlobalAddressList** cmdlet set See Mailbox Cmdlets
IMAP4 connectivity, test	Test-ImapConnectivity

Import\export mailbox data	**MailboxImportRequest** cmdlet set **MailboxExportRequest** cmdlet set See Understanding Importing and Exporting Files in the Exchange Management Shell
Information Rights Management (IRM), configure	**IRMConfiguration** cmdlet set See Messaging Policy and Compliance Cmdlets
IP Allow and Block List providers, test	Test-IPAllowListProvider Test-IPBlockListProvider
IP site link costs, Exchange-specific	**ADSiteLink** cmdlet set See Transport Cmdlets
Mailbox audit logging, configure and search	See Managing Mailbox Audit Logging
Message flow, test	Test-Mailflow
Messaging records management (MRM) 1.0: Managed folders	**ManagedFolder** cmdlet set **ManagedFolderMailboxPolicy** cmdlet set Start-ManagedFolderAssistant See Messaging Policy and Compliance Cmdlets
Multi-Mailbox Search	**MailboxSearch** cmdlet set See Messaging Policy and Compliance Cmdlets
Offline address book virtual directory, create	New-OABVirtualDirectory
Outlook client connectivity, test end-to-end	Test-OutlookConnectivity
Outlook Protection Rules	**OutlookProtectionRule** cmdlet set See Messaging Policy and Compliance Cmdlets
Outlook Web App connectivity, test	Test-OwaConnectivity
Outlook Web App virtual directories, create or remove	New-OwaVirtualDirectory Remove-OwaVirtualDirectory
Outlook Web services connectivity, test	Test-OutlookWebServices
POP3 connectivity, test	Test-PopConnectivity
PowerShell, test connectivity	Test-PowerShellConnectivity
PowerShell, virtual directories	**PowerShellVirtualDirectory** cmdlet set See Client Access Cmdlets

RBAC management role assignment Policies	**RoleAssignmentPolicy** cmdlet set See Permissions Cmdlets
RBAC management role groups	**RoleGroup** cmdlet set **RoleGroupMember** cmdlet set See Permissions Cmdlets
RBAC management roles	**ManagementRole** cmdlet set See Permissions Cmdlets
RBAC management role entries	**ManagementRoleEntry** cmdlet set See Permissions Cmdlets
RBAC management role assignments	**ManagementRoleAssignment** cmdlet set See Permissions Cmdlets
RBAC management scopes	**ManagementScope** cmdlet set See Permissions Cmdlets
Recovery database, create	New-MailboxDatabase
Recovery database, extract data	Restore-Mailbox
Recovery items	Set-Mailbox, using the following parameters: • *RecoverableItemsQuota* • *RecoverableItemsWarningQuota* • *SingleItemRecoveryEnabled*
Routing group connectors	**RoutingGroupConnector** cmdlet set See Transport Cmdlets
Safelist aggregation, force	**Update-SafeList** cmdlet set See Transport Cmdlets
Search mailbox and delete items	Search-Mailbox
Sender ID, test	Test-SenderId
Service e-mail channel	**ServiceEmailChannel** cmdlet set See Client Access Cmdlets
Transport agents	**TransportAgent** cmdlet set See Transport Cmdlets
Transport latency, calculating	**MessageLatencyReport** cmdlet set See Transport Cmdlets
Transport pipeline analysis	Get-TransportPipeline
UM connectivity, test	Test-UMConnectivity

UM incoming calls, view active	Get-UMActiveCalls
Web services connectivity, test	Test-WebServicesConnectivity
X.400 authoritative domains	**X400AuthoritativeDomains** cmdlet set See Transport Cmdlets

1.1.9 Exchange 2010: Editions and Versions

Exchange 2010: Editions and Versions

Exchange Server 2010 > Getting Started With Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-04*

Microsoft Exchange Server 2010 is available in two server editions: Standard Edition and Enterprise Edition. Enterprise Edition can scale to 100 databases per server; Standard Edition is limited to 5 databases per server.

These licensing editions are defined by a product key. When you enter a valid license product key, the supported edition for the server is established. Product keys can be used for the same edition key swaps and upgrades only; they can't be used for downgrades. You can use a valid product key to move from the evaluation version (Trial Edition) of Exchange Server 2010 to either Standard Edition or Enterprise Edition. You can also use a valid product key to move from Standard Edition to Enterprise Edition.

You can also license the server again using the same edition product key. For example, if you had two Standard Edition servers with two keys, but you accidentally used the same key on both servers, you can change the key for one of them to the other key that you were issued. You can take these actions without having to reinstall or reconfigure anything. After you enter the product key and restart the Microsoft Exchange Information Store service, the edition corresponding to that product key will be reflected.

No loss of functionality will occur when the Trial Edition expires, so you can maintain lab, demo, training, and other non-production environments beyond 120 days without having to reinstall the Trial Edition of Exchange 2010.

As mentioned earlier, you can't use product keys to downgrade from Enterprise Edition to Standard Edition, nor can you use them to revert to the Trial Edition. These types of downgrades can only be done by uninstalling Exchange 2010, reinstalling Exchange 2010, and entering the correct product key. For more information, see Enter Product Key.

Exchange 2010 Versions

Service Pack 2 (SP2) for Exchange Server 2010 is available and is the most recent version of the product.

Service Pack 1 (SP1) for Exchange Server 2010 and the release to manufacturing (RTM) version of Exchange Server 2010 are also available.

Exchange 2010 Build Versioning

The SP1 version of Exchange 2010 is 14.01.0218.015. The RTM version of Exchange 2010 is 14.00.0639.021. This version information is consistently displayed in the Exchange Management Console, the Exchange Management Shell, and in the **About Exchange**

Server 2010 Help dialog box.

You can also use the Get-ExchangeServer cmdlet and examine the **AdminDisplayVersion** property for the Exchange 2010 build version. For more information about deploying fixes and update rollups for Exchange 2010, see Exchange 2010 Servicing.

Exchange 2010 License Types

Exchange 2010 on-premises is licensed in the Server/Client Access License (CAL) model in the same way that Exchange Server 2007 was licensed. There are three types of licenses:

- **Server Licenses** A license must be assigned for each instance of the server software that is being run. The Server license is sold in two server editions: Standard Edition and Enterprise Edition.
- **Client Access Licenses (CALs)** Exchange 2010 also comes in two client access license (CAL) editions, which are referred to as a Standard CAL and an Enterprise CAL. You can mix and match the server editions with the CAL types. For example, you can use Enterprise CALs with Exchange 2010 Standard Edition. Similarly, you can use Standard CALs with Exchange 2010 Enterprise Edition.
- **External Connector Licenses** This license type allows an unlimited number of clients to access an Exchange server in scenarios where the number of CALs is uncertain.

For more information about Exchange license types, see Licensing and Microsoft Exchange How to Buy.

1.1.10 Exchange Server Build Numbers and Release Dates

Exchange Server Build Numbers and Release Dates

Exchange Server 2010 > Getting Started With Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2, Exchange Server 2010 SP1, Exchange Server 2010*

Topic Last Modified: *2013-02-26*

This topic provides you a central resource for build numbers and release dates for versions of Microsoft Exchange. You can use the information in this topic to verify the version of Exchange that is running in your organization.

This topic is organized in sections that correspond to the major releases of Exchange. Each section lists the build numbers for each service pack level of the specific Exchange release. The "For More Information" section in this topic contains information to help you determine the build number and version of Exchange Server that you're running.

Exchange Server 2010

This section provides the build numbers and general release dates for each version of Microsoft Exchange Server 2010.

To view the build number for the version of Exchange 2010 that you're running, run the following command in the Exchange Management Shell:

```
Get-ExchangeServer | fl name,edition,admindisplayversion
```

Note:
After you install an update rollup for Exchange 2010, the version of Exchange Server isn't updated to show that the update rollup is installed. This issue occurs because the version number that is displayed by the Exchange Management Console or by other administrative mechanisms is obtained from the Exchange Server Object in Active Directory.

For information about the servicing strategy for Exchange 2010, see Exchange 2010 Servicing. For more information about installing an update rollup for Exchange 2010, see Install the Latest Update Rollup for Exchange 2010.

Exchange Server 2010 SP3 build numbers

Product name	Release date	Build number
Microsoft Exchange Server 2010 Service Pack 3 (SP3)	February 12, 2013	14.03.0123.004

Exchange Server 2010 SP2 build numbers

Product name	Release date	Build number
Update Rollup 6 for Microsoft Exchange Server 2010 Service Pack 2 (SP2)	February 12, 2013	14.02.0342.003
Update Rollup 4 v2 for Exchange Server 2010 Service Pack 2	October 9, 2012	14.02.0318.004
Update Rollup 4 for Exchange Server 2010 Service Pack 2	August 13, 2012	14.02.0318.002
Update Rollup 3 for Exchange Server 2010 Service Pack 2	May 29, 2012	14.02.0309.002
Update Rollup 2 for Exchange Server 2010 SP2	April 16, 2012	14.02.0298.004
Update Rollup 1 for Exchange Server 2010 SP2	February 13, 2012	14.02.0283.003
Exchange Server 2010 SP2	December 4, 2011	14.2.247.5

Exchange Server 2010 SP1 build numbers

Product name	Release date	Build number
Update Rollup 7 v2 for Exchange Server 2010 SP1	October 10, 2012	14.01.0421.002
Update Rollup 7 for Exchange Server 2010 SP1	August 8, 2012	14.01.0421.000
Update Rollup 6 for Exchange Server 2010 SP1	October 27, 2011	14.01.0355.002
Update Rollup 5 for Exchange Server 2010 SP1	August 23, 2011	14.1.339.1
Update Rollup 4 for Exchange Server 2010 SP1	July 27, 2011	14.1.323.6
Update Rollup 3 for Exchange	April 6, 2011	14.01.0289.007

Server 2010 SP1		
Update Rollup 2 for Exchange Server 2010 SP1	December 9, 2010	14.01.0270.001
Update Rollup 1 for Exchange Server 2010 SP1	October 4, 2010	14.1.255.2
Exchange Server 2010 SP1	August 23, 2010	14.01.0218.015

Exchange Server 2010 RTM build numbers

Product name	Release date	Build number
Update Rollup 5 for Exchange Server 2010	December 13, 2010	14.0.726.0
Update Rollup 4 for Exchange Server 2010	June 10, 2010	14.0.702.1
Update Rollup 3 for Exchange Server 2010	April 13, 2010	14.0.694.0
Update Rollup 2 for Exchange Server 2010	March 4, 2010	14.0.689.0
Update Rollup 1 for Exchange Server 2010	December 9, 2009	14.0.682.1
Exchange Server 2010	November 9, 2009	14.00.0639.021

Exchange Server 2007

The following table lists the build numbers and general release dates for each version of Microsoft Exchange Server 2007.

The version information for Service Pack 1 (SP1) of Exchange Server 2007 is displayed correctly in the Exchange Management Console, in the Exchange Management Shell, and in the **About Exchange Server 2007** Help dialog box. However, after you apply Exchange 2007 SP1 to an Edge Transport server that is running the release to manufacturing (RTM) version of Exchange 2007, the version information for the Edge Transport server isn't updated in the Exchange Management Console unless the Edge Transport server is resubscribed to the Active Directory site. This is because the Edge Transport server doesn't directly update Active Directory by using any configuration information. Instead, the version information for Edge Transport servers is recorded in Active Directory during the creation of an Edge Subscription.

To view the build number for the version of Exchange 2007 that you're running, run the following command in the Shell:

```
Get-ExchangeServer | fl name,edition,admindisplayversion
```

Exchange Server 2007 SP3 build numbers

Product name	Release date	Build number
Update Rollup 9 for Exchange Server 2007 SP3	December 10, 2012	08.03.0297.002
Update Rollup 8-v3 for Exchange Server 2007 SP3	November 13, 2012	08.03.0279.006

Update Rollup 8–v2 for Exchange Server 2007 SP3	October 9, 2012	08.03.0279.005
Update Rollup 8 for Exchange Server 2007 SP3	August 13, 2012	08.03.0279.003
Update Rollup 7 for Exchange Server 2007 SP3	April 16, 2012	08.03.0264.000
Update Rollup 6 for Exchange Server 2007 SP3	January 26, 2012	8.03.0245.002
Update Rollup 5 for Exchange Server 2007 SP3	September 21, 2011	8.03.0213.001
Update Rollup 4 for Exchange Server 2007 SP3	May 28, 2011	8.03.0192.001
Update Rollup 3-v2 for Exchange Server 2007 SP3	March 30, 2011	8.03.0159.002
Update Rollup 2 for Exchange Server 2007 SP3	December 10, 2010	8.03.0137.003
Update Rollup 1 for Exchange Server 2007 SP3	September 9, 2010	8.03.0106.002
Exchange Server 2007 SP3	June 7, 2010	8.03.0083.006

Exchange Server 2007 SP2 build numbers

Product name	Release date	Build number
Update Rollup 5 for Exchange Server 2007 SP2	December 7, 2010	8.2.305.3
Update Rollup 4 for Exchange Server 2007 SP2	April 9, 2010	8.2.254.0
Update Rollup 3 for Exchange Server 2007 SP2	March 17, 2010	8.2.247.2
Update Rollup 2 for Exchange Server 2007 SP2	January 22, 2010	8.2.234.1
Update Rollup 1 for Exchange Server 2007 SP2	November 19, 2009	8.2.217.3
Exchange Server 2007 SP2	August 24, 2009	8.02.0176.002

Exchange Server 2007 SP1 build numbers

Product name	Release date	Build number
Update Rollup 10 for Exchange Server 2007 SP1	April 13, 2010	8.1.436.0
Update Rollup 9 for Exchange Server 2007 SP1	July 16, 2009	8.1.393.1
Update Rollup 8 for Exchange Server 2007 SP1	May 19, 2009	8.1.375.2
Update Rollup 7 for Exchange	March 18, 2009	8.1.359.2

Server 2007 SP1		
Update Rollup 6 for Exchange Server 2007 SP1	February 10, 2009	8.1.340.1
Update Rollup 5 for Exchange Server 2007 SP1	November 20, 2008	8.1.336.1
Update Rollup 4 for Exchange Server 2007 SP1	October 7, 2008	8.1.311.3
Update Rollup 3 for Exchange Server 2007 SP1	July 8, 2008	8.1.291.2
Update Rollup 2 for Exchange Server 2007 SP1	May 9, 2008	8.1.278.2
Update Rollup 1 for Exchange Server 2007 SP1	February 28, 2008	8.1.263.1
Exchange Server 2007 SP1	November 29, 2007	8.01.0240.006

Exchange Server 2007 RTM build numbers for update rollup packages

Product name	Release date	Build number
Update Rollup 7 for Exchange Server 2007	July 8, 2008	8.0.813.0
Update Rollup 6 for Exchange Server 2007	February 21, 2008	8.0.783.2
Update Rollup 5 for Exchange Server 2007	October 25, 2007	8.0.754.0
Update Rollup 4 for Exchange Server 2007	August 23, 2007	8.0.744.0
Update Rollup 3 for Exchange Server 2007	June 28, 2007	8.0.730.1
Update Rollup 2 for Exchange Server 2007	May 8, 2007	8.0.711.2
Update Rollup 1 for Exchange Server 2007	April 17, 2007	8.0.708.3
Exchange Server 2007	March 8, 2007	8.0.685.25

Exchange Server 2003

The following table lists the build numbers and general release dates for each version of Microsoft Exchange Server 2003. To view the build number of Exchange Server 2003, open the **Properties** dialog box of the server object.

Exchange Server 2003 build numbers

Product name	Release date	Build number
Exchange Server 2003 post-SP2	August 2008	6.5.7654.4

Exchange Server 2003 post-SP2	March 2008	6.5.7653.33
Exchange Server 2003 SP2	October 19, 2005	6.5.7683
Exchange Server 2003 Service Pack 1	May25, 2004	6.5.7226
Exchange Server 2003	September 28, 2003	6.5.6944

Exchange 2000 Server

The following table lists the build numbers and general release dates for each version of Microsoft Exchange 2000 Server. To view the build number of Exchange 2000 Server, open the **Properties** dialog box of the server object.

Exchange 2000 Server build numbers

Product name	Release date	Build number
Exchange 2000 Server post-SP3	August 2008	6.0.6620.7
Exchange 2000 Server post-SP3	March 2008	6.0.6620.5
Exchange 2000 Server post-SP3	August 2004	6.0.6603
Exchange 2000 Server post-SP3	April 2004	6.0.6556
Exchange 2000 Server post-SP3	September 2003	6.0.6487
Exchange 2000 Server SP3	July 18, 2002	6.0.6249
Exchange 2000 Server Service Pack 2	November 29, 2001	6.0.5762
Exchange 2000 Server Service Pack 1	June 21, 2001	6.0.4712
Exchange 2000 Server	November 29, 2000	6.0.4417

Exchange Server 5.5

The following table lists the build numbers and general release dates for each version of Microsoft Exchange Server version 5.5.

Exchange Server 5.5 build numbers

Product name	Release date	Build number
Exchange Server version 5.5 Service Pack 4	November 1, 2000	5.5.2653
Exchange Server version 5.5 Service Pack 3	September 9, 1999	5.5.2650

Exchange Server version 5.5 Service Pack 2	December 23, 1998	5.5.2448
Exchange Server version 5.5 Service Pack 1	August 5, 1998	5.5.2232
Exchange Server version 5.5	February 3, 1998	5.5.1960

Exchange Server 5.0

The following table lists the build numbers and general release dates for each version of Microsoft Exchange Server 5.0.

Exchange Server 5.0 build numbers

Product name	Release date	Build number
Exchange Server 5.0 Service Pack 2	February 19, 1998	5.0.1460
Exchange Server 5.0 Service Pack 1	June 18, 1997	5.0.1458
Exchange Server 5.0	May 23, 1997	5.0.1457

Exchange Server 4.0

The following table lists the build numbers and general release dates for each version of Microsoft Exchange Server 4.0.

Exchange Server 4.0 build numbers

Product name	Release date	Build number
Exchange Server 4.0 Service Pack 5	May5, 1998	4.0.996
Exchange Server 4.0 Service Pack 4	March 28, 1997	4.0.995
Exchange Server 4.0 Service Pack 3	October 29, 1996	4.0.994
Exchange Server 4.0 Service Pack 2	July 19, 1996	4.0.993
Exchange Server 4.0 Service Pack 1	May 1, 1996	4.0.838
Exchange Server 4.0 Standard Edition	June 11, 1996	4.0.837

For More Information

For more information about how to determine the build number and version of Microsoft Exchange that you're running, see Microsoft Knowledge Base article 152439, How to determine the version number, the build number, and the service pack level of Exchange Server.

For more information about Exchange Server 2010 versions, see Exchange 2010: Editions and Versions.

For more information about Exchange Server 2007 versions, see Exchange Server 2007: Platforms, Editions, and Versions.

For more information about how to determine build numbers and version information after you install an update rollup, see the following:

- **Exchange 2010** After you install an update rollup for Exchange 2010, the version of Exchange Server isn't updated to show that the update rollup is installed. This issue occurs because the version number that is displayed by the Exchange Management Console or by other administrative mechanisms is obtained from the Exchange Server Object in Active Directory.
- **Exchange 2007** See How to View the Exchange Server 2007 Version Number After You Install an Update Rollup.

1.1.11 Exchange 2010 Language Support

Exchange 2010 Language Support

[This topic is in progress.]

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 has enhanced language support for both servers and clients. This topic provides information about language packs, including the specific languages that are supported for both servers and clients in Exchange 2010.

Other topics in this section include:

- Language Support for Exchange Management Interfaces
- Client Language Support for Outlook
- Client Languages for Outlook Web App
- Client Language Support for Unified Messaging

Exchange 2010 Language Packs

An Exchange 2010 language pack contains the necessary resources for a supported Exchange language. Language packs are installed during installation of Exchange 2010. Client and server language packs come grouped into a single bundle containing both client and server resource and support files. There are no performance issues with installing all the languages because they're just stored when not in use.

For organizations that have users in multiple languages, we recommend that you do the following:

- On Unified Messaging (UM) servers, only install the UM language pack that you need for your organization. The addition of extra UM language packs introduces more processing when the server builds speech grammar for each language.

UM Language Packs

For a specific language that's supported by Exchange 2010 Unified Messaging, UM language packs allow an Exchange 2010 Unified Messaging server to speak additional languages to callers and recognize other languages when callers use Automatic Speech Recognition (ASR) or when voice messages are transcribed. UM language packs contain:

- Pre-recorded prompts, for example, "After the tone, please record your message. When you've finished recording, hang up, or press the # key for more options." in the language of the UM language pack.
- Grammar files that are used by a Unified Messaging server to look up the names of specific users in the directory in the language of the UM language pack.
- Text-to-Speech (TTS) translation so that content (for example, e-mail, calendar, or contact information) can be read to callers in the language of the UM language pack.
- Support for ASR, which allows callers to interact with Unified Messaging using the Voice User Interface (VUI) in the language of the UM language pack.
- Support for Voice Mail Preview, which allows users to read the transcript of voice mail messages in a specific language from within a supported e-mail client such as Microsoft Outlook or Outlook Web App.

The U.S. English (en-US) language pack contains UM prompts, TTS, ASR, and Voice Mail Preview support for this language.

Important:

The UM language pack must only be installed as an add-in to Exchange 2010 Unified Messaging.

For more information about installing UM language packs, see Install a Unified Messaging Language Pack on a UM Server.

Supported Server Languages for Exchange 2010

The following server languages are supported and available for Exchange 2010:

- Chinese (Simplified)
- Chinese (Traditional)
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Spanish

Beginning in SP1 of Exchange 2010, the following additional languages are supported:

- Arabic
- Hebrew

Supported Client Languages for Exchange 2010

The following client languages are supported and available for Exchange 2010:

Note:

The Windows Server 2008 operating system Multilingual User Interface (MUI) packs aren't needed for client localization.

- Chinese (Simplified)
- English
- French
- German
- Japanese
- Chinese (Traditional)
- Italian
- Korean
- Portuguese
- Russian
- Spanish
- Arabic
- Czech
- Danish
- Dutch
- Finnish
- Greek
- Hebrew
- Hungarian
- Norwegian
- Polish
- Portuguese (Portugal)
- Swedish
- Turkish
- Romanian
- Thai
- Filipino (Philippines)
- Hindi
- Indonesian
- Latvian
- Malay
- Ukrainian
- Vietnamese
- Bulgarian
- Croatian
- Estonian
- Lithuanian
- Serbian
- Slovak
- Slovenian
- Basque
- Catalan
- Chinese (Hong Kong S.A.R.)
- Persian
- Icelandic
- Kazakh
- Serbian (Cyrillic, Serbia)
- Urdu

1.1.11.1 Language Support for Exchange Management Interfaces

Language Support for Exchange Management Interfaces

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-16*

Microsoft Exchange Server 2010 offers a fully localized administrative experience in many languages. Administrators can use the fully localized management interface to administer Exchange 2010 in their chosen language. This topic indicates the languages supported in each type of management interface.

Exchange Management Console and Exchange Management Shell

The following languages are supported in both the Exchange Management Console and the Exchange Management Shell:

- Chinese (Simplified)
- Chinese (Traditional)
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Spanish

For Service Pack 1 (SP1) of Exchange Server 2010, the following additional languages are supported:

- Arabic
- Hebrew

Exchange Control Panel

The Exchange Control Panel (ECP) is localized in the Exchange client languages. For more information about client language support, see Exchange 2010 Language Support.

1.1.11.2 Client Language Support for Outlook

Client Language Support for Outlook

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-17*

In Exchange Server 2010, there are 48 supported languages that Office Outlook 2007 users can use to access their Microsoft Exchange mailbox.

Outlook Client Access

The language of the Outlook user interface that an Outlook user sees, including the content generated by Exchange, depends on the following:

- The language the user is using in Outlook
- Whether the language they're using in Outlook is supported by Exchange 2010
- Whether the language they're using in Outlook has been configured to be available on the Exchange 2010 server

Consider the following scenarios:

- When an Outlook user who's set their language to <Language A> signs in to their Exchange 2010 mailbox and both Outlook and Exchange 2010 support the language the user has specified, <Language A>, the user will see all messages and Exchange-generated mailbox components, for example, the Inbox, in Language A.
- When an Outlook user who's set their language to <Language A> signs in to their Exchange 2010 mailbox that's been set to <Language B>, the Outlook user will see the Outlook user interface in Language A, but will see the content generated by Exchange. For example, by default, folder names such as **Inbox**, **Deleted Items**, and **Sent Items** display in <Language B>.

You can change the Exchange mailbox language setting on the server using Exchange Management Console or the Exchange Management Shell. For information about how to use the Shell to change the language setting for a mailbox on a server, see Set-MailboxRegionalConfiguration.

Supported Languages for Components and Features of Exchange 2010

The following table includes information about the languages that are supported for client and administrative features in Exchange 2010.

Supported languages for Exchange Server 2010

Language	Country/Region	Outlook 2007 client support
Arabic	Saudi Arabia	Available
Basque	Spain	Available
Bulgarian	Bulgaria	Available
Catalan	Spain	Available
Chinese (Cantonese)	China	Available
Chinese (Hong Kong)	China	Available
Chinese (Mandarin)	China	UM language only
Chinese (Simplified)	China	Available
Chinese (Traditional)	Taiwan	Available
Croatian	Croatia	Available
Czech	Czech Republic	Available

Danish	Denmark	Available
Dutch	Netherlands	Available
English	Australia	UM language only
English	United Kingdom	UM language only
English	United States	Available
Estonian	Estonia	Available
Filipino (Tagalog)	Philippines	Available
Finnish	Finland	Available
French	Canada	UM language only
French	France	Available
German	Germany	Available
Greek	Greece	Available
Hebrew	Israel	Available
Hindi	India	Available
Hungarian	Hungary	Available
Icelandic	Iceland	Available
Indonesian (Bahasa)	Indonesia	Available
Italian	Italy	Available
Japanese	Japan	Available
Kazakh	Kazakhstan	Available
Korean	Korea	Available
Latvian	Latvia	Available
Lithuanian	Lithuania	Available
Malay	Malaysia	Available
Norwegian (Bokmal)	Norway	Available
Persian (Farsi)	Iran	Available
Polish	Poland	Available
Portuguese	Brazil	Available
Portuguese	Portugal	Available
Romanian	Romania	Available
Russian	Russia	Available
Serbian (Cyrillic)	Serbia	Available
Slovak	Slovakia	Available

Slovenian	Slovenia	Available
Spanish	Spain	Available
Spanish	Mexico	UM language only
Swedish	Sweden	Available
Thai	Thailand	Available
Turkish	Turkey	Available
Ukrainian	Ukraine	Available
Urdu	Pakistan	Available
Vietnamese	Vietnam	Available

1.1.11.3 Client Languages for Outlook Web App

Client Languages for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-07*

The Exchange 2010 Outlook Web App user interface is available in 54 languages.

For more information about the languages that are supported in Outlook Web App, see Configure Language Settings for Outlook Web App.

Contents

Language and Locale

There are three language settings that you can configure for Outlook Web App.

- The sign-in and error language setting applies to individual Outlook Web App virtual directories. The sign-in and error language is the language that will be used for errors and the forms-based authentication sign-in page. If a value isn't set for this language, the default value is *0*. This means that the default sign-in and error language isn't defined. If the sign-in and error language isn't defined, Outlook Web App will default first to the language set on the Web browser on the client computer. If the language set on the Web browser on the client computer isn't supported by Outlook Web App, Outlook Web App will use the language of the Client Access server.
- The default client language setting applies to individual Outlook Web App virtual directories. The default client language is the client language that's used by Outlook Web App unless the user uses **Regional Settings** in Outlook

Web App to change the language and time zone. The default value for this setting is *0*. This means the default client language isn't defined. If the default client language isn't defined, users will be prompted to choose a language and time zone the first time that they sign in to Outlook Web App. If the default client language value is defined, users won't be prompted to choose a language and the Outlook Web App time zone will use the time zone of the Client Access server. Defining the default client language causes the default folders to be renamed based on the specified language. Users can change the client language and time zone by using **Regional Settings** in Outlook Web App and can rename the default folders after they sign in.

- The client languages are set on individual mailboxes and affect the language that's used in Outlook and Outlook Web App. If multiple languages are configured, the first language in the list that's supported by the Web browser will be used. If none of the languages in the default languages list is supported by the Web browser, the Client Access server language will be used.

Outlook Web App Spelling Checker

In Exchange 2010 Outlook Web App, users can check spelling in 16 languages.

Return to top

Supported Languages for Components and Features of Exchange 2010

The following table includes information about the availability and language support for the client and administrative features in Exchange 2010.

Language	Country/Region	Outlook Web App - user interface	Outlook Web App - spelling checker
Arabic	Saudi Arabia	Available	Available
Basque	Spain	Available	
Bulgarian	Bulgaria	Available	
Catalan	Spain	Available	
Chinese (Hong Kong)	China	Available	
Chinese (Simplified)	China	Available	
Chinese (Traditional)	Taiwan	Available	
Croatian	Croatia	Available	
Czech	Czech Republic	Available	
Danish	Denmark	Available	Available
Dutch	Netherlands	Available	Available
English	Australia	Available	Available
English	United Kingdom	Available	Available
English	Canada	Available	
English	India	Available	

English	United States	Available	Available
Estonian	Estonia	Available	
Filipino (Tagalog)	Philippines	Available	
Finnish	Finland	Available	Available
French	Canada	Available	Available
French	France	Available	Available
Galician	Spain	Available	
German	Germany	Available	Available
Greek	Greece	Available	
Hebrew	Israel	Available	Available
Hindi	India	Available	
Hungarian	Hungary	Available	
Icelandic	Iceland	Available	
Indonesian (Bahasa)	Indonesia	Available	
Italian	Italy	Available	Available
Japanese	Japan	Available	
Kazakh	Kazakhstan	Available	
Korean	Korea	Available	Available
Latvian	Latvia	Available	
Lithuanian	Lithuania	Available	
Malay	Malaysia	Available	
Norwegian (Bokmal)	Norway	Available	Available
Persian (Farsi)	Iran	Available	
Polish	Poland	Available	
Portuguese	Brazil	Available	Available
Portuguese	Portugal	Available	Available
Romanian	Romania	Available	
Russian	Russia	Available	
Serbian (Cyrillic)	Serbia	Available	
Serbian (Latin)	Serbia	Available	
Slovak	Slovakia	Available	
Slovenian	Slovenia	Available	
Spanish	Spain	Available	Available

Spanish	Mexico	Available	
Swedish	Sweden	Available	Available
Thai	Thailand	Available	
Turkish	Turkey	Available	
Ukrainian	Ukraine	Available	
Urdu	Pakistan	Available	
Vietnamese	Vietnam	Available	

1.1.11.4 Client Language Support for Unified Messaging

Client Language Support for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-30*

Microsoft Exchange Unified Messaging language packs are version-specific and platform-specific. Since Exchange Server 2007, there have been separate releases for UM language packs, including Exchange 2007 RTM, Exchange 2007 SP1, SP2, and SP3, the RTM version of Exchange Server 2010, and Exchange 2010 SP1 and SP2. Both 32-bit and 64-bit downloads are available for some of these releases, but only 64-bit downloads are available for others.

It's very important that you install the correct version and platform of the UM language packs on a UM server. Don't install UM language packs on a Unified Messaging server that's running an earlier version of Exchange or that's designed for a 32-bit platform. This topic describes Unified Messaging (UM) language packs and their availability in Microsoft Exchange Server 2010.

What Are Unified Messaging Language Packs?

Unified Messaging language packs allow an Exchange 2010 UM server to speak additional languages to callers and recognize other languages when callers use Automatic Speech Recognition (ASR) or when voice messages are transcribed. UM language packs contain:

- Pre-recorded prompts in the language of the UM language pack, for example, "After the tone, please record your message. When you've finished recording, hang up, or press the # key for more options."
- Grammar files in the language of the UM language pack that are used by a UM server to look up the names of users in the directory.
- Text-to-Speech (TTS) translation so that content, such as e-mail, calendar, and contact information, can be read to callers in the language of the UM language pack.
- Support for ASR, which allows callers to interact with UM using the voice user interface (VUI) in the language of the UM language pack.

In addition, UM language packs provide support for Voice Mail Preview, which allows users to quickly triage their voice messages by reading their transcripts from within a supported

e-mail client such as Outlook or Outlook Web App.

All UM language packs are single files that can be downloaded. These language packs include the pre-recorded prompts, grammar files, Text-to-Speech (TTS) translation, and ASR. However, not all the UM language packs contain support for Voice Mail Preview.

The following UM language packs contain support for all the components and features, including Voice Mail Preview:

1. English (US) - (en-US)
2. French (France) - (fr-FR)
3. Italian - (it-IT)English (Canada) (en-CA)
4. Polish (pl-PL)
5. Portuguese (Portugal) (pt-PT)
6. Spanish (Spain) (es-ES)

Note:

For more information about Voice Mail Preview, see Voice Mail Preview for End Users

By default, when you install the Exchange 2010 Unified Messaging server role, the server will send voice mail previews to UM-enabled users if a supported UM language pack is installed.

There are Exchange 2010 Unified Messaging Voice Mail Preview partners that offer enhanced transcription support for the Voice Mail Preview feature. These partners employ people to correct voice mail transcriptions that were created using Automatic Speech Recognition (ASR). Each Voice Mail Preview partner must meet a set of requirements to be certified to interoperate with Exchange 2010 Unified Messaging.

If you determine that the voice mail previews sent to your users aren't accurate enough, you can contact one of the certified Voice Mail Preview partners listed on the Microsoft PinPoint web page, and sign up with that partner at an additional cost. For more information, see Voice Mail Preview Advisor for Exchange 2010.

The following table includes the supported languages for Exchange 2010 Unified Messaging.

Supported languages for Exchange 2010 UM language packs

Language	Country/ Region	Culture ID	Availability	Prompts	Text-to-Speech	ASR	Voice Mail Preview
Catalan	Spain	ca-ES	Download available	√	√	√	
Chinese (Hong Kong)	China	zh-HK	Download available	√	√	√	
Chinese (Simplified)	China	zh-CN	Download available	√	√	√	
Chinese (Traditional)	Taiwan	zh-TW	Download available	√	√	√	
Danish	Denmark	da-DK	Download available	√	√	√	
Dutch	Netherlands	nl-NL	Download available	√	√	√	

English	Australia	en-AU	Download available	√	√	√	
English	Canada	en-CA	Download available	√	√	√	√
English	India	en-IN	Download available **Caution:** Deploying the Exchange 2010 SP1 English (India) (en-IN) Unified Messaging language pack in organizations that include Exchange Server 2007 servers running on Windows Server 2003 will cause the Exchange 2007 servers to fail. Further details are contained in this Microsoft Knowledge Base article.	√	√	√	
English	United Kingdom	en-GB	Download available	√	√	√	
English	United States	en-US	Download available	√	√	√	√
Finnish	Finland	fi-FL	Download available	√	√	√	
French	Canada	fr-CA	Download available	√	√	√	
French	France	fr-FR	Download available	√	√	√	√
German	Germany	de-DE	Download available	√	√	√	
Italian	Italy	it-IT	Download available	√	√	√	√

	Japan	ja-JP	Download available	√	√	√	
Korean	Korean	ko-KR	Download available	√	√	√	
Norwegian (Bokmal)	Norway	nb-NO	Download available	√	√	√	
Polish	Poland	pl-PL	Download available	√	√	√	√
Portuguese	Brazil	pt-BR	Download available	√	√	√	
Portuguese	Portugal	pt-PT	Download available	√	√	√	√
Russian	Russia	ru-RU	Download available	√	√	√	
Spanish	Spain	es-ES	Download available	√	√	√	√
Spanish	Mexico	es-MX	Download available	√	√	√	
Swedish	Sweden	sv-SE	Download available	√	√	√	

Important:

To ensure that all Unified Messaging features are available in the UM language packs you install, you must install the Exchange 2010 Client and Server Language Pack on each UM server in the dial plan. If you don't install the Client and Server Language Pack, some features may not work as expected. Some features, like Voice Mail Preview, will work in the language that's configured on the dial plan but when only the UM language pack is installed. However, features like Outlook Voice Access and user interface text won't work in the language selected by the user without having both the UM language pack and the Client and Server Language Pack installed. The language pack bundle for Exchange Server 2010 Service Pack 2 (SP2) is integrated into the download for Exchange 2010 SP2. To download SP2 for Exchange 2010, see Microsoft Exchange Server 2010 Service Pack 2 (SP2). However, the language pack bundle for Exchange 2010 SP1 is still available. To download and install additional client and server language packs for Exchange 2010 SP1 on servers in your organization, see the Microsoft Exchange Server 2010 SP1 Language Pack Bundle.

Client Language Selection Process

Exchange 2010 UM language packs enable callers and Outlook Voice Access users to interact with the Unified Messaging system in multiple languages. After you install additional language packs on a Unified Messaging server, callers and Outlook Voice Access users can hear e-mail messages and interact with the Unified Messaging system, and Outlook Web App and Outlook 2010 users can view the transcript of a voice message using Voice Mail Preview in a specific language.

To support a specific language, a UM client language pack for that language must be installed on each UM server in the UM dial plan.

In some cases, if a UM language pack for a specific language hasn't been installed and isn't available, a client fallback language may be used instead of the language that's

needed. For some languages, fallback UM client languages are available to be used, but for other languages, no fallback language is available. If there isn't a UM language pack installed for a specific language, and no fallback language is available for that language, en-US (US English) will be used. By default, the en-US UM language pack is installed on all Unified Messaging servers when you install the Unified Messaging server role. The en-US UM language pack can't be uninstalled.

The following table includes a list of client languages and the fallback languages that are used when a specific UM language pack hasn't been installed on a Unified Messaging server.

Client Fallback Languages for UM

Language	Country/ Region	Culture ID	First language chosen, if installed	Second language chosen, if installed	Third language chosen, if installed
Catalan	Spain	ca-ES	ca-ES	en-US	
Chinese (Hong Kong)	China	zh-HK	zh-HK	zh-CN	zh-TW
Chinese (Simplified)	China	zh-CN	zh-CN	zh-HK	zh-TW
Chinese (Traditional)	Taiwan	zh-TW	zh-TW	zh-HK	zh-CN
Danish	Denmark	da-DK	da-DK	en-US	
Dutch	Netherlands	nl-NL	nl-NL	en-US	
English	Australia	en-AU	en-AU	en-US	
English	Canada	en-CA	en-CA	en-US	
English	India	en-IN	en-IN	en-US	
English	United Kingdom	en-GB	en-GB	en-US	
English	United States	en-US	en-US		
Finnish	Finland	fi-FL	fi-FL	en-US	
French	Canada	fr-CA	fr-CA	fr-FR	en-US
French	France	fr-FR	fr-FR	fr-CA	en-US
German	Germany	de-DE	de-DE	en-US	
Italian	Italy	it-IT	it-IT	en-US	
Japanese	Japan	ja-JP	ja-JP	en-US	
Korean	Korea	ko-KR	ko-KR	en-US	
Norwegian (Bokmal)	Norway	nb-NO	nb-NO	en-US	
Polish	Poland	pl-PL	pl-PL	en-US	
Portuguese	Brazil	pt-BR	pt-BR	pt-PT	en-US

Portuguese	Portugal	pt-PT	pt-PT	pt-BR	en-US
Russian	Russia	ru-RU	ru-RU	en-US	
Spanish	Spain	es-ES	es-ES	es-MX	en-US
Spanish	Mexico	es-MX	es-MX	es-ES	en-US
Swedish	Sweden	sv-SE	sv-SE	en-US	

1.1.12 Exchange 2010 Support for RFC Standards

Exchange 2010 Support for RFC Standards

Exchange Server 2010 > Getting Started With Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-27*

This topic is intended to be a reference for the Request for Comments (RFC) and other standards that are supported in Microsoft Exchange Server 2010. Although every effort has been made to verify this information, omission of an RFC from this list does not necessarily mean that Exchange does not fully or partially support the RFC. RFCs are guidelines, and they frequently contain two types of information: required and optional. Microsoft and other vendors may choose not to implement optional requirements, or they may interpret sections of RFCs differently.

If you are experiencing a problem that you believe is caused because Exchange does not correctly support a particular RFC, open a support incident through Microsoft Customer Support Services (CSS).

Important:
The information that is contained in this topic represents the current view of Microsoft Corporation about the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, this information should not be interpreted to be a commitment on the part of Microsoft. Microsoft cannot guarantee the accuracy of any information that is presented in this topic after the date of publication.
This topic is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

RFC Implementation Statements

All document references are listed in the following format:

Document/RFC: Document or RFC index
Title: Description or title of document
Updated by: RFCs that update this document
Updates: RFCs that are updated by this document
Obsoletes: RFCs that are replaced by this document or are obsolete
Exchange 2010 specific: RFCs that are implemented by or supported by Exchange 2010; if applicable, the component and any other notes about support for the applicable RFC; links to additional information

Note:
For the purposes of this topic, "implemented" means that the RFC has been implemented natively within Exchange 2010, and "supported" means that a technology that is outside Exchange 2010 has implemented the RFC but that Exchange 2010 uses that implementation.

Not all document references contain all fields that are shown in the sample format. In some cases, the information has been merged. Refer to the document source for the latest information.

World Wide Web Consortium (W3C) Standards

Note:
The third-party Web site information in this topic is provided to help you find the technical information you need. The URLs are subject to change without notice.

Document: http://www.w3.org/TR/REC-html32

Title: HTML 3.2 Reference Specification

Exchange 2010 specific: Implemented by Exchange 2010 Text Conversion component

Document: http://www.w3.org/TR/REC-html40

Title: HTML 4.01 Specification

Exchange 2010 specific: Implemented by Exchange 2010 Text Conversion component

Document: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

Title: Simple Object Access Protocol (SOAP) 1.1

Exchange 2010 specific: Partially implemented by Exchange Web Services

Document: Web Services-Interoperability Organization (WS-I) Standards

Title: Basic Profile Version 1.0

Exchange 2010 specific: Implemented by Exchange 2010 Web Services

RFC: 1035 http://www.ietf.org/rfc/rfc1035.txt

Title: Domain Names – Implementation and Specification

Updated by: 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2137, 2181, 2308, 2535, 2845, 3425, 3658, 4033, 4034, 4035, 4343

Obsoletes: 882, 883, 973

Exchange 2010 specific: Supported by Exchange 2010

RFC: 1652 http://www.ietf.org/rfc/rfc1652.txt

Title: SMTP Service Extension for 8bit-MIME transport

Obsoletes: 1426

Exchange 2010 specific: Implemented by Exchange 2010 MIME Conversion Shared Components

RFC: 1731 http://www.ietf.org/rfc/rfc1731.txt

Title: IMAP4 Authentication Mechanisms

Exchange 2010 specific: Implemented by Exchange 2010 IMAP4 Service

RFC: 1740 http://www.ietf.org/rfc/rfc1740.txt

Title: Mime Encapsulation of Macintosh files – MacMIME

Exchange 2010 specific: Implemented by Exchange 2010 MIME Conversion Shared Components

RFC: 1741 http://www.ietf.org/rfc/rfc1741.txt

Title: MIME Content Type for BinHex Encoded Files

Exchange 2010 specific: Implemented by Exchange 2010 MIME Conversion Shared Components

RFC: 1823 http://www.ietf.org/rfc/rfc1823.txt

Title: The LDAP Application Program Interface

Exchange 2010 specific: Supported by Exchange 2010 to communicate with Active Directory

RFC: 1870 http://www.ietf.org/rfc/rfc1870.txt

Title: SMTP Service Extension for Message Size Declaration

Obsoletes: 1653

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service

RFC: 1896 http://www.ietf.org/rfc/rfc1896.txt

Title: The text/enriched MIME Content-type

Obsoletes: 1523, 1563

Exchange 2010 specific: Implemented by Exchange 2010 MIME Conversion Shared Components

RFC: 1939 http://www.ietf.org/rfc/rfc1939.txt

Title: Post Office Protocol – Version 3

Updated by: 1957, 2449

Obsoletes: 1725

Exchange 2010 specific: Implemented by Exchange 2010 POP3 Service

RFC: 2034 http://www.ietf.org/rfc/rfc2034.txt

Title: SMTP Service Extension for Returning Enhanced Error Codes

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service

RFCs: 2045, 2046, 2047, 4289 2049, 4288

http://www.ietf.org/rfc/rfc2045.txt

http://www.ietf.org/rfc/rfc2046.txt

http://www.ietf.org/rfc/rfc2047.txt

http://www.ietf.org/rfc/rfc4289.txt

http://www.ietf.org/rfc/rfc2049.txt

http://www.ietf.org/rfc/rfc4288.txt

Titles: Multipurpose Internet Mail Extensions (MIME) [parts 1-5]

Media Type Specifications and Registration Procedures

Updated by:2184, 2231, 2646, 3798

Obsoletes: 1521, 1522, 1590, 2048

Exchange 2010 specific: Implemented by Exchange 2010

RFC: 2088 http://www.ietf.org/rfc/rfc2088.txt

Title: IMAP4 non-synchronizing literals

Updated by:4466

Exchange 2010 specific: Implemented by Exchange 2010 IMAP4 Service

RFC: 2177 http://www.ietf.org/rfc/rfc2177.txt

Title: IMAP4 IDLE command

Exchange 2010 specific: Implemented by Exchange 2010 IMAP4 Service

RFC: 2181 http://www.ietf.org/rfc/rfc2181.txt

Title: Clarifications to the DNS Specification

Updated by: 2535, 4033, 4034, 4035, 4343

Updates: 1034, 1035, 1123

Exchange 2010 specific: Supported by Exchange 2010

RFC: 2183 http://www.ietf.org/rfc/rfc2183.txt

Title: Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field

Updated by: 2184, 2231

Updates: 1806

Exchange 2010 specific: Implemented by Exchange 2010 MIME Conversion Shared Components

RFC: 2231 http://www.ietf.org/rfc/rfc2231.txt

Title: MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations

Updates: 2045, 2047, 2183

Obsoletes: 2184

Exchange 2010 specific: Implemented by Exchange 2010 MIME Conversion Shared Components

Note:
Although RFC2231-encoded attachment file names are supported during inbound conversion, Exchange 2010 does not generate RFC2231-encoded content in MIME e-mail messages.

RFC: 2247 http://www.ietf.org/rfc/rfc2247.txt

Title: Using Domains in LDAP/X.500 Distinguished Names

Updated by: 4519, 4524

Exchange 2010 specific: Supported by Exchange 2010

RFC: 2311 http://www.ietf.org/rfc/rfc2311.txt

Title: S/MIME Version 2 Message Specification

Exchange 2010 specific: Implemented by Exchange 2010 Outlook Web App and S/MIME control

RFC: 2312 http://www.ietf.org/rfc/rfc2312.txt

Title: S/MIME Version 2 Certificate Handling

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and S/MIME control

RFC: 2342 http://www.ietf.org/rfc/rfc2342.txt

Title: IMAP4 Namespace

Updated by: 4466

Exchange 2010 specific: Implemented by Exchange 2010 IMAP4 Service

RFC: 2387 http://www.ietf.org/rfc/rfc2387.txt

Title: The MIME Multipart/Related Content-type

Updated by: 2112

Exchange 2010 specific: Implemented by Exchange 2010 MIME Conversion Shared Components

RFC: 2445 http://www.ietf.org/rfc/rfc2445.txt

Title: Internet Calendaring and Scheduling Core Object Specification (iCalendar)

Exchange 2010 specific: Implemented by Exchange 2010

RFC: 2446 http://www.ietf.org/rfc/rfc2446.txt

Title: iCalendar Transport-Independent Interoperability Protocol (iTIP) Scheduling Events, BusyTime, To-dos and Journal Entries

Exchange 2010 specific: Implemented by Exchange 2010 (partially supported)

RFC: 2447 http://www.ietf.org/rfc/rfc2447.txt

Title: iCalendar Message-Based Interoperability Protocol (iMIP)

Exchange 2010 specific: Implemented by Exchange 2010 (partially supported)

RFC: 2449 http://www.ietf.org/rfc/rfc2449.txt

Title: POP3 Extension Mechanism

Updated by: 5034

Updates: 1939

Exchange 2010 specific: Implemented by Exchange 2010 POP3 Service

RFC: 2557 http://www.ietf.org/rfc/rfc2557.txt

Title: MIME Encapsulation of Aggregate Documents, such as HTML (MHTML)

Obsoletes: 2110

Exchange 2010 specific: Implemented by Exchange 2010 MIME Conversion Shared Components

RFC: 2595 http://www.ietf.org/rfc/rfc2595.txt

Title: Using TLS with IMAP, POP3 and ACAP

Updated by: 4616

Exchange 2010 specific: Implemented by Exchange 2010 IMAP4 and POP3 services; ACAP not supported

RFC: 2616 http://www.ietf.org/rfc/rfc2616.txt

Title: Hypertext Transfer Protocol – HTTP v1.1

Updated by: 2817

Obsoletes: 2068

Exchange 2010 specific: Implemented by Windows Server 2008; supported by Exchange 2010 Autodiscover Service and Exchange Web Services

RFC: 2617 http://www.ietf.org/rfc/rfc2617.txt

Title: HTTP Authentication: Basic and Digest Access Authentication

Obsoletes: 2069

Exchange 2010 specific: Supported by Exchange 2010 Autodiscover Service and Exchange Web Services

RFC: 2631 http://www.ietf.org/rfc/rfc2631.txt

Title: Diffie-Hellman Key Agreement Method

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App S/MIME Control

RFC: 2634 http://www.ietf.org/rfc/rfc2634.txt

Title: Enhanced Security Services for S/MIME

Exchange 2010 specific: Partially supported by Exchange 2010

RFC: 2782 http://www.ietf.org/rfc/rfc2782.txt

Title: A DNS RR for specifying the location of services (DNS SRV)

Obsoletes: 2052

Exchange 2010 specific: Supported by Exchange 2010

RFC: 2797 http://www.ietf.org/rfc/rfc2797.txt

Title: Certificate Management Messages over CMS

Exchange 2010 specific: Implemented by Exchange 2010 Outlook Web App S/MIME Control

RFC: 2821 http://www.ietf.org/rfc/rfc2821.txt

Title: Simple Mail Transfer Protocol

Updates: 1123

Obsoletes: 821, 974, 1869

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service.

Note:

Note that Exchange 2010 does not currently support IP Literals (RFC 2821, Section 4.1.3).

RFC: 2822 http://www.ietf.org/rfc/rfc2822.txt

Title: Internet Message Format

Obsoletes: 822

Exchange 2010 specific: Implemented by Exchange 2010 MIME Conversion Shared Components

RFC: 3030 http://www.ietf.org/rfc/rfc3030.txt

Obsoletes: 1830

Title: SMTP Service Extensions for Transmission of Large and Binary MIME Messages

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service

RFC: 3207 http://www.ietf.org/rfc/rfc3207.txt

Title: SMTP Service Extension for Secure SMTP over Transport Layer Security

Obsoletes: 2487

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service

RFC: 3217 http://www.ietf.org/rfc/rfc3217.txt

Title: Triple-DES and RC2 Key Wrapping

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service

RFC: 3278 http://www.ietf.org/rfc/rfc3278.txt

Title: Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and S/MIME control

RFC: 3370 http://www.ietf.org/rfc/rfc3370.txt

Title: Cryptographic Message Syntax (CMS) Algorithms

Obsoletes: 2630, 3211

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and S/MIME control

RFC: 3394 http://www.ietf.org/rfc/rfc3394.txt

Title: Advanced Encryption Standard (AES) Key Wrap Algorithm

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and S/MIME control

RFC: 3461 http://www.ietf.org/rfc/rfc3461.txt

Title: Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)

Obsoletes: 1891

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service

Note:
For more information, see Understanding DSNs and NDRs

RFC: 3462 http://www.ietf.org/rfc/rfc3462.txt

Title: The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages
Obsoletes: 1892

Exchange 2010 specific: Partially implemented by Exchange 2010 Transport service

RFC: 3463 http://www.ietf.org/rfc/rfc3463.txt

Title: Enhanced Mail System Status Codes

Updated by: 3886, 4468, 4865, 4954

Obsoletes: 1893

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service

Note:
For more information, see Understanding DSNs and NDRs

RFC: 3464 http://www.ietf.org/rfc/rfc3464.txt

Title: An Extensible Message Format for Delivery Status Notifications

Updated by: 4865

Obsoletes: 1894

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service

RFC: 3501 http://www.ietf.org/rfc/rfc3501.txt

Title: Internet Message Access Protocol – Version 4rev1

Updated by: 4466, 4469, 4551, 5032, 5182

Obsoletes: 2060

Exchange 2010 specific: Implemented by Exchange 2010 (AUTH=PLAIN not supported)

RFC: 3503 http://www.ietf.org/rfc/rfc3503.txt

Title: Message Disposition Notification (MDN) profile for Internet Message Access Protocol (IMAP).

Exchange 2010 specific: Implemented by Exchange 2010 and adheres to the server

implementation section

RFC: 3565 http://www.ietf.org/rfc/rfc3565.txt

Title: Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and S/MIME control

RFC: 3629 http://www.ietf.org/rfc/rfc3629.txt

Title: UTF-8, a transformation format of ISO 10646

Updates: 2279

Exchange 2010 specific: Supported by Exchange 2010

RFC: 3834 http://www.ietf.org/rfc/rfc3834.txt

Title: Recommendations for Automatic Responses to Electronic Mail

Exchange 2010 specific: Implemented by Exchange 2010 Mailbox Server

RFC: 3842 http://www.ietf.org/rfc/rfc3842.txt

Title: A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)

Exchange 2010 specific: Implemented by Exchange 2010 Unified Messaging

RFC: 3850 http://www.ietf.org/rfc/rfc3850.txt

Title: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling

Obsoletes: 2632

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and S/MIME control

RFC: 3851 http://www.ietf.org/rfc/rfc3851.txt

Title: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification

Obsoletes: 2633

Exchange 2010 specific: Implemented by Exchange 2010 Outlook Web App and S/MIME control

RFC: 3852 http://www.ietf.org/rfc/rfc3852.txt

Title: Cryptographic Message Syntax (CMS)

Updated by: 4853, 5083

Obsoletes: 3369

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and S/MIME control

RFC: 3974 http://www.ietf.org/rfc/rfc3974.txt

Title: SMTP Operational Experience in Mixed IPv4/v6 Environments

Exchange 2010 specific: Supported by Exchange 2010 Transport service

RFC: 4120 http://www.ietf.org/rfc/rfc4120.txt

Title: The Kerberos Network Authentication Service (V5)

Updated by: 4537, 5021

Obsoletes: 1510

Exchange 2010 specific: Supported by Exchange 2010 Mailbox, Client Access, Hub Transport, and Unified Messaging (UM) servers that have the MSRPC protocol, and by the Exchange POP3, IMAP4, and SMTP services

RFC: 4262 http://www.ietf.org/rfc/rfc4262.txt

Title: X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and S/MIME control

RFC: 4346 http://www.ietf.org/rfc/rfc4346.txt

Title: The Transport Layer Security (TLS) Protocol Version 1.1

Updated by: 4366, 4680, 4681

Obsoletes: 2246

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service, and by POP3, SMTP, and IMAP4 services

RFC: 4406 http://www.ietf.org/rfc/rfc4406.txt

Title: Sender ID: Authenticating E-Mail

Exchange 2010 specific: Partially implemented; Exchange 2010 does not support MTA forwarding of mail

RFC: 4409 http://www.ietf.org/rfc/rfc4409.txt

Title: Message Submission for Mail

Obsoletes: 2476

Exchange 2010 specific: Partially implemented; Exchange 2010 does not always return

554 DSN (for example, 550 5.7.1)

RFC: 4559 http://www.ietf.org/rfc/rfc4559.txt

Title: SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows

Exchange 2010 specific: Supported by Exchange 2010 Autodiscover Service and by Exchange Web Services

RFC: 4853 http://www.ietf.org/rfc/rfc4853.txt

Title: Cryptographic Message Syntax (CMS) Multiple Signer Clarification

Updates: 3852

Exchange 2010 specific: Implemented by Exchange 2010 Outlook Web Access and S/MIME control

RFC: 4954 http://www.ietf.org/rfc/rfc4954.txt

Title: SMTP Service Extension for Authentication

Updates: 3463

Obsoletes: 2554

Exchange 2010 specific: Implemented by Exchange 2010 Transport Service

RFC: 5008 http://www.ietf.org/rfc/rfc5008.txt

Title: Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and S/MIME control

RFC: 1734 http://www.ietf.org/rfc/rfc1734.txt

Title: POP3 Authentication command

Exchange 2010 specific: Implemented by Exchange 2010 POP3 service (Windows Integrated Authentication – NTLM and GSSAPI)

RFC: 5035 http://www.ietf.org/rfc/rfc5035.txt

Title: Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility

Updates: 2634

Exchange 2010 specific: Supported by Exchange 2010 Outlook Web App and by S/MIME control

For More Information

For more information about Exchange Server RFC and standards compliance in earlier versions of Exchange, see Microsoft Knowledge Base article 262986, Exchange Server RFC

and standards compliance.

For more information about RFCs, visit the following non-Microsoft Web sites:

Note:
The third-party Web site information in this topic is provided to help you find the technical information you need. The URLs are subject to change without notice.

- RFC Editor
- The Internet Engineering Task Force (IETF)
- W3C World Wide Web Consortium
- International Telecommunication Union
- Ecma International

1.2 Planning and Deployment

Planning and Deployment

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-16*

Use this information to help you deploy Microsoft Exchange Server 2010. The following topics are gateways to information about planning for and then deploying Exchange Server 2010.

Planning for Exchange 2010

Topics in this section provide important information to assist you in planning your Exchange 2010 organization, including details about system requirements and upgrading from a previous version of Microsoft Exchange.

Deploying Exchange 2010

Topics in this section can help you understand and manage your deployment of Exchange 2010, whether a new deployment or an upgrade from a previous version of Exchange.

Note:
For information about hybrid deployments, see Hybrid Deployments. For information about cloud-only deployments, see Understanding Cloud-Only Deployments with Exchange 2010 SP3.

In addition to these topics, we also recommend you read:

Exchange 2010 Language Support

Understanding Permissions

Understanding Role Based Access Control

High Availability and Site Resilience

1.2.1 Planning for Exchange 2010

Planning for Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-03*

These topics can help you plan the deployment of Microsoft Exchange Server 2010 into your production environment. Use the following links to access the information to help you make your planning decisions.

After you have completed the planning phase and are ready to deploy, see Deploying Exchange 2010. Also, see Establish a Test Environment later in this topic about installing Exchange 2010 in a test environment prior to deploying into production.

Exchange 2010 System Requirements

Before you install Exchange 2010, make sure that your organization meets the system requirements.

Planning Roadmap for New Deployments

Read this topic to get an overview of the things you need to consider before you begin a new Exchange 2010 deployment.

Exchange 2003 - Planning Roadmap for Upgrade and Coexistence

This topic provides an overview of the things you need to consider before you deploy Exchange 2010 into an Exchange Server 2003 organization.

Exchange 2007 - Planning Roadmap for Upgrade and Coexistence

This topic provides an overview of the things you need to consider before you deploy Exchange 2010 into an Exchange 2007 organization.

Exchange Server Deployment Assistant

Use this tool to generate a customized checklist for planning, installing, or upgrading to Exchange 2010.

Workforce Planning for Exchange

This topic can help you make informed decisions when determining the appropriate workforce levels for your Exchange Server environment.

Planning for High Availability and Site Resilience

Consult this topic to help you with planning to achieve your high availability and site resilience requirements.

Planning Active Directory

Learn about Active Directory requirements and its interaction with your Exchange organization.

Understanding Disjoint Namespace Scenarios

This topic discusses the supported scenarios for deploying Exchange 2010 in a domain that has a disjoint namespace.

Mailbox Server Storage Design

This group of topics discusses storage design, which is a critical piece of a successful Exchange 2010 Mailbox server role deployment.

Understanding Exchange 2010 Virtualization

Read this topic to learn more about how you can deploy Exchange 2010 in a virtualized environment.

Planning for Internal and Third-Party Applications

This topic links to important information about Application Programming Interfaces that are available for applications that use Exchange 2010.

Exchange 2010 Deployment Permissions Reference

Consult this topic to learn about the permissions that are required to set up an Exchange 2010 organization.

Exchange Network Port Reference

Use this topic to find information about ports, authentication, and encryption for all data paths used by Exchange 2010.

Exchange Server Supportability Matrix

Consult this topic to learn about the level of support available for any configuration or required component for all versions of Microsoft Exchange.

Exchange 2010 Solution Accelerator

This topic links to a guide related to infrastructure planning and design for Service Pack 1 for Exchange 2010. The guide provides a step-by-step process for successfully designing an Exchange 2010 infrastructure.

Note:

You can't upgrade an existing Exchange 2000 organization directly to Exchange 2010. You must first upgrade the Exchange 2000 organization to either an Exchange 2003 or Exchange 2007 organization, and then you can upgrade the Exchange 2003 or Exchange 2007 organization to Exchange 2010. We recommend that you upgrade your organization from Exchange 2000 to Exchange 2003, and then upgrade from Exchange 2003 to Exchange 2010. For more information about upgrading from Exchange 2000, see Planning an Upgrade from Exchange 2000 and Upgrading to Exchange 2007.

Establish a Test Environment

Before installing Exchange 2010 for the first time, we recommend that you install it in an isolated test environment. This approach reduces the risk of end-user downtime and negative ramifications to the production environment.

The test environment will act as your “proof of concept” for your new Exchange 2010 design and make it possible to move forward or roll back any implementations before deploying into your production environments. Having an exclusive test environment for validation and testing allows you to do pre-installation checks for your future production environments. By installing in a test environment first, we believe that your organization will have a better likelihood of success in a full production implementation.

For many organizations, the costs of building a test lab may be high because of the need to duplicate the production environment. To reduce the hardware costs associated with a prototype lab, we recommend the use of virtualization by using Windows Server 2008 R2 Hyper-V technologies. Hyper-V enables server virtualization, allowing multiple virtual operating systems to run on a single physical machine.

For more detailed information about Hyper-V, see Virtualization with Hyper-V. For information about Microsoft support of Exchange 2010 in production on hardware virtualization software, see "Hardware Virtualization" in Exchange 2010 System Requirements.

1.2.1.1 Exchange 2010 System Requirements

Exchange 2010 System Requirements

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-02-26*

Before you install Microsoft Exchange Server 2010, we recommend that you review this topic to ensure that your network, hardware, software, clients, and other elements meet the requirements for Exchange 2010. In addition, make sure you understand the coexistence scenarios that are supported for Exchange 2010 and earlier versions of Exchange.

Supported Coexistence Scenarios

The following table lists the scenarios in which coexistence between Exchange 2010 and earlier versions of Exchange are supported.

Coexistence of Exchange 2010 and earlier versions of Exchange Server

Exchange version	Exchange organization coexistence
Exchange 2000 Server	Not supported
Exchange Server 2003	Supported
Exchange 2007	Supported
Mixed Exchange 2007 and Exchange Server 2003 organization	Supported

Exchange 2000 Server

You can't upgrade an existing Exchange 2000 organization directly to Exchange 2010. You must first upgrade the Exchange 2000 organization to either an Exchange 2003 or Exchange 2007 organization, and then you can upgrade the Exchange 2003 or Exchange 2007 organization to Exchange 2010. We recommend that you upgrade your organization from Exchange 2000 to Exchange 2003, and then upgrade from Exchange 2003 to Exchange 2010. For more information about upgrading from Exchange 2000, see Planning an Upgrade from Exchange 2000 and Upgrading to Exchange 2007.

Network and Directory Servers

The following table lists the requirements for the network and the directory servers in your Exchange 2010 organization.

Network and directory server requirements for Exchange 2010

Component	Requirement
Schema master	By default, the schema master runs on the first Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 domain controller installed in a forest. The schema master must be running any of the following: • Windows Server 2003 Standard Edition with Service Pack 2 (SP2) or later (32-bit or 64-bit)

	• Windows Server 2003 Enterprise Edition with SP2 or later (32-bit or 64-bit) • Windows Server 2008 Standard or Enterprise (32-bit or 64-bit) • Windows Server 2008 R2 Standard or Enterprise • Windows Server 2012
Global catalog server	In each Active Directory site where you plan to install Exchange 2010, you must have at least one global catalog server running any of the following: • Windows Server 2003 Standard Edition with SP2 or later (32-bit or 64-bit) • Windows Server 2003 Enterprise Edition with SP2 or later (32-bit or 64-bit) • Windows Server 2008 Standard or Enterprise (32-bit or 64-bit) • Windows Server 2008 R2 Standard or Enterprise • Windows Server 2012 For more information about global catalog servers, see What is the Global Catalog.
Domain controller	In each Active Directory site where you install Exchange 2010, Exchange 2010 must be able to contact at least one writeable domain controller of the domain of which Exchange 2010 is a member. The domain controller can run any of the following: • Windows Server 2003 Standard Edition with SP2 or later (32-bit or 64-bit) • Windows Server 2003 Enterprise Edition with SP2 or later (32-bit or 64-bit) • Windows Server 2008 Standard or Enterprise SP1 or later (32-bit or 64-bit) • Windows Server 2008 R2 Standard or Enterprise SP1 or later • Windows Server 2008 Datacenter RTM or later • Windows Server 2008 R2 Datacenter RTM or later • Windows Server 2012
Active Directory forest	Active Directory must be at Windows Server 2003 forest functionality mode or higher.
IPv6 Support	IPv6 is supported only when IPv4 is also used; a pure IPv6 environment isn't supported. Using IPv6 addresses and IP address ranges is supported only when both IPv6 and IPv4 are enabled on that computer, and the network supports both IP address versions. If Exchange 2010 is deployed in this configuration, all server roles can send data to and receive data from devices, servers, and clients that use IPv6 addresses. Exchange 2010 support is similar to support for Exchange Server 2007. For more information, see Understanding IPv6 Support

	in Exchange 2010.

Directory Server Architecture

The use of 64-bit Active Directory domain controllers increases directory service performance for Exchange 2010. For more information about Exchange 2010, the Mailbox server role and Active Directory ratios, see the "Active Directory Server and Mailbox Server Ratios" section in Understanding Server Role Ratios and Exchange Performance.

Note:

In multi-domain environments, on Windows Server 2008 domain controllers that have the Active Directory language locale set to Japanese, your servers may not receive some attributes that are stored on an object during inbound replication. For more information, see Microsoft Knowledge Base article 949189, A Windows Server 2008 domain controller that is configured with the Japanese language locale may not apply updates to attributes on an object during inbound replication.

Installing Exchange 2010 on Directory Servers

For security and performance reasons, we recommend that you install Exchange 2010 only on member servers and not on Active Directory directory servers. However, you can't run DCPromo on a computer running Exchange 2010. After Exchange 2010 is installed, changing its role from a member server to a directory server, or vice versa, isn't supported.

Hardware

The recommended hardware requirements for Exchange 2010 servers vary depending on a number of factors including the server roles that are installed and the anticipated load that will be placed on the servers. For information about minimum, maximum, and recommended hardware configurations for Exchange 2010 servers, see Performance and Scalability.

Hardware requirements for Exchange 2010

Component	Requirement	Notes
Processor	• x64 architecture-based computer with Intel processor that supports Intel 64 architecture (formerly known as Intel EM64T) • AMD processor that supports the AMD64 platform • Intel Itanium IA64 processors not supported	It's supported to install the Exchange management tools on a computer that has a 64-bit processor. For more information, see Install the Exchange 2010 Management Tools and Prepare Active Directory and Domains.
Memory	Varies depending on Exchange features that are installed	For detailed information about memory requirements for Exchange 2010, see Understanding Memory Configurations and Exchange Performance.
Paging file size	The page file size minimum and maximum must be set to physical RAM plus 10 MB	The recommended page file size also accounts for the memory that's needed to collect

		information if the operating system stops unexpectedly. On 64-bit operating systems, memory can be written as a dump file to the paging file. This file must reside on the boot volume of the server. For more information about the configuration options that are available for memory dump data, see Knowledge Base article 254649, Overview of memory dump file options for Windows Vista, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 2000.
Disk space	• At least 1.2 GB on the drive on which you install Exchange • An additional 500 MB of available disk space for each Unified Messaging (UM) language pack that you plan to install • 200 MB of available disk space on the system drive • A hard disk that stores the message queue database on an Edge Transport server or Hub Transport server with at least 500 MB of free space	The minimum space requirements detailed here don't account for disk subsystem requirements for adequate performance.
Drive	DVD-ROM drive, local or network accessible	None.
Screen resolution	800 x 600 pixels or higher	None.
File format	Disk partitions formatted as NTFS file systems, which applies to the following partitions: • System partition • Partitions that store Exchange binary files • Partitions containing transaction log files • Partitions containing database files • Partitions containing other Exchange files	None.

For more information about planning your hardware for Exchange 2010, see the following

topics:

- Understanding Processor Configurations and Exchange Performance
- Understanding Memory Configurations and Exchange Performance
- Understanding Server Role Ratios and Exchange Performance

Operating System

The following table lists the supported operating systems for Exchange 2010.

Supported operating systems for Exchange 2010

Component	Requirement
Operating system on a computer that has a 64-bit processor	One of the following: • 64-bit edition of Windows Server 2008 Standard with Service Pack 2 (SP2) • 64-bit edition of Windows Server 2008 Enterprise with SP2 • 64-bit edition of Windows Server 2008 R2 Standard with SP1 • 64-bit edition of Windows Server 2008 R2 Enterprise with SP1 • Windows Server 2008 Datacenter RTM or later • Windows Server 2008 R2 Datacenter RTM or later • Windows Server 2012 (Requires Exchange 2010 SP3 or later)
Operating system for installing the Exchange management tools on a computer that has a 64-bit processor	One of the following: • Windows Vista with SP2 for management tools only installation • 64-bit edition of Windows Server 2008 Standard with SP2 • 64-bit edition of Windows Server 2008 Enterprise with SP2 • 64-bit edition of Windows Server 2008 R2 Standard • 64-bit edition of Windows Server 2008 R2 Enterprise • Windows Server 2012 • 64-bit edition of Windows 7 • Windows 8 (Requires Exchange 2010 SP3 or later)

Important:

The release-to-manufacturing (RTM) version of Exchange 2010 doesn't support being run on computers with the United States Federal Information Processing Standards (FIPS) compliant settings enabled. If you have FIPS enabled on computers running Windows Server 2008 SP2 or Windows Server 2008 R2, Exchange 2010 RTM will not function correctly. For more information, see Knowledge Base article 811833, The effects of enabling the "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" security setting in Windows XP and in later versions of Windows.

Support for Outlook and Entourage

Exchange 2010 supports the following versions of Microsoft Office Outlook and Microsoft Entourage for Mac:

- Outlook 2010

- Outlook 2007
- Outlook 2003
- Entourage 2008 for Mac, Web Services Edition
- Outlook for Mac 2011

If you haveclients running Outlook 2003, be aware of the following when you upgrade your organization to Exchange 2010:

- On clients running Outlook 2003, you may notice that folder updates don't occur automatically in a timely manner. This was a known issue in Exchange 2010 RTM and SP1, but it has been resolved in Exchange 2010 SP1 Rollup Update 3. For more information about how to install an Update Rollup, see Install the Latest Update Rollup for Exchange 2010. For more background information about this issue, see Knowledge Base article 2009942, In Outlook 2003, e-mail messages take a long time to send and receive when you use an Exchange 2010 mailbox. Outlook 2007 and Outlook 2010 are not affected by this issue.
- Exchange 2010 RTM: Clients running Outlook 2003 don't use RPC encryption, which RPC Client Access requires by default. You will either need to turn off the RPC encryption requirement or configure Outlook 2003 to use RPC encryption. However, Outlook 2007 and later versions are automatically compatible with the change to RPC Client Access because they support RPC encryption by default. For more information, see Understanding RPC Client Access.
- Exchange 2010 SP1: In Exchange 2010 SP1, the RPC encryption requirement is disabled by default. Any new Client Access Servers (CAS) deployed in the organization will not require encryption. However, any CA servers deployed prior to Exchange 2010 SP1 or upgraded to Exchange 2010 SP1 will retain the existing RPC encryption requirement setting.

For more information, see Concern: Is having Outlook 2003 clients going to prevent me from deploying Exchange 2010?.

Hardware Virtualization

Microsoft supports running Exchange 2010 in production on hardware virtualization software. For more information, see Understanding Exchange 2010 Virtualization.

1.2.1.2 Planning Roadmap for New Deployments

Planning Roadmap for New Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Before proceeding with deployment of Microsoft Exchange Server 2010, we recommend that you read this topic to help you prepare your organization for deployment.

Exchange Organization Planning

Before deploying Exchange 2010, your existing infrastructure must meet certain prerequisites. Review the following topics to help ensure that your organization is ready for Exchange 2010:

- Exchange 2010 System Requirements
- Exchange 2010 Prerequisites

Exchange 2010 Supported Topologies

Exchange 2010 supports the following topologies:

- Single forest, multiple Active Directory sites.
- Multiple forests (resource forest model); multiple Active Directory sites.
- Single Active Directory site.

Exchange 2010 doesn't support the following topologies:

- Installing earlier version of Exchange into a newly created Exchange 2010 organization.

Important:
The addition of earlier versions of Exchange to an Exchange 2010–only organization is not supported.

For more information, see Deploy Multiple Forest Topologies.

Exchange Server 2010 Deployment Assistant

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Active Directory Planning

Exchange 2010 uses Active Directory Lightweight Directory Service (AD LDS) to store and share directory information with Microsoft Windows. For more information, see Planning Active Directory.

Network and Name Resolution Planning

Make sure that you correctly register host records for servers that run Exchange 2010 in the Domain Name System (DNS) server for the Active Directory forest. Clients and other servers use DNS as the name resolution service to locate Exchange servers. You need to confirm that name resolution is correctly configured for your environment. For more information, see the following topics:

- Domain Name System
- Understanding Disjoint Namespace Scenarios
- Exchange Network Port Reference

Hub Transport Server Planning

The Hub Transport server role is a required role in an Exchange 2010 organization that provides routing within a single organizational network by using Active Directory sites. Deployed inside the Active Directory forest, computers that have the Hub Transport server role installed handle all mail flow inside the organization, apply transport rules, apply journal rules, and deliver messages to recipients' mailboxes. Messages that are sent to the Internet are relayed by the Hub Transport server to the Edge Transport server role that is deployed in the perimeter network. Messages that are received from the Internet are processed by the Edge Transport server before they are relayed to the Hub Transport server. The Hub Transport server role stores all its configuration information in Active Directory.

When you plan to deploy the Hub Transport server role, you should consider the following

issues:

- **Topology options** Begin by planning where you will put your Hub Transport servers in the Exchange physical topology. Exchange uses Active Directory sites to route messages; therefore, you must deploy at least one Hub Transport server in each Active Directory site in which you deploy Mailbox servers. For more information about how to plan for placement of the Hub Transport server, see Overview of the Hub Transport Server Role.
- **Server capacity** Planning for server capacity includes determining how you will conduct performance monitoring of the Hub Transport server. Performance monitoring will help you set a performance baseline for your servers. This information will help determine the capacity of your hardware configuration.
- **Transport features** Determine the transport features that you will enable at the Hub Transport server and how they will be configured.
- **Security** The Hub Transport server role is deployed inside the Exchange organization. Planning for Hub Transport server security includes delegation of administrative roles and verification that IP connections are only enabled from authorized servers. Additionally, you should verify that no nonessential services are running and that no unnecessary ports are open. For more information, see Deployment Security Checklist

Internet Connectivity for Hub Transport Servers

To complete mail flow configuration for the Exchange organization and to send and receive e-mail to and from the Internet, you must configure Send connectors and Receive connectors that enable at least one Hub Transport server to connect to the Internet. You can configure Internet connectivity for a Hub Transport by using any of the following methods:

- You can deploy an Edge Transport server and subscribe it to the Exchange organization. This is the recommended deployment method. By default, when you create the Edge Subscription, the required Send connectors are automatically created. You don't have to modify the configuration of the default Receive connector on the Hub Transport server for this scenario. For more information, see Configure Internet Mail Flow Through a Subscribed Edge Transport Server.
- You can deploy an Edge Transport server without subscribing it to the Exchange organization. In this scenario, you would have to manually configure the Send and Receive connectors on your Edge Transport and Hub Transport servers, and you won't be able to use features like recipient filtering or safelist aggregation because there is no data replication. For more information, see Configure Mail Flow Between an Edge Transport Server and Hub Transport Servers Without Using EdgeSync.
- You can send and receive Internet e-mail by relaying through Microsoft Exchange Hosted Services or another third-party SMTP gateway server. In this scenario, you have to create a Send connector and a Receive connector between the Hub Transport server and the external SMTP servers that process and route Internet e-mail. For more information, see Configure Internet Mail Flow Through Exchange Hosted Services or an External SMTP Gateway.
- You can establish Internet mail flow directly through a Hub Transport server. In this scenario, you have to create a Send connector that routes e-mail to the Internet. Also, you have to modify the configuration of the default Receive connector to accept anonymous e-mail submissions. In this scenario, the Exchange 2010 Hub Transport server can be reached directly through the Internet. We don't recommend this topology because it increases security risks by exposing to the Internet the Exchange 2010 server and all roles installed on that server. Instead, we recommend that you implement a perimeter network-based SMTP gateway, such as the Edge Transport server. For more information, see Configure Internet Mail Flow Directly Through a Hub Transport Server.

Note:
If you choose to establish Internet mail flow directly through your Hub Transport servers, we recommend that you install the anti-spam agents on your Hub Transport servers so that they can provide anti-spam protection for your Exchange organization. For more information, see Enable Anti-Spam Functionality on a Hub Transport Server.

Important:
If you configure an Internet-facing Hub Transport server, you can't configure a Send connector to attach a particular IP address to messages that are sent from the Hub Transport server. For example, if more than one IP address is assigned to the Hub Transport server, you can't select which IP address is used by a Send connector to relay e-mail to the Internet. If you use an SMTP relay, such as an Edge Transport server, the IP address of that computer is affixed as the message source.

High Availability and Load Balancing for Hub Transport Servers

Exchange 2010 Transport servers feature shadow redundancy, which provides redundancy for messages for the entire time they are in transit. The solution involves a technique similar to the transport dumpster. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all of the next hops for that message have completed delivery. If any of the next hops fail before reporting back successful delivery, the message is resubmitted for delivery to that next hop.

Shadow redundancy is enabled by default in your Exchange 2010 environment. To learn more about shadow redundancy, see Understanding Shadow Redundancy.

You achieve load balancing for Hub Transport servers when you install more than one Hub Transport server in the same Active Directory site. By default, connections to Hub Transport servers are automatically load balanced if more than one Hub Transport server is deployed in an Active Directory site. If one Hub Transport server is unavailable, the operational Hub Transport servers continue to accept connections. If all Hub Transport servers in an Active Directory site are unavailable, messages are queued until a Hub Transport server becomes available or the messages expire.

Load balancing of outbound connections to remote domains is achieved by specifying more than one Hub Transport server in the same Active Directory site as a source server for the corresponding Send connector. Load balancing doesn't occur when the source servers for a Send connector are located in different Active Directory sites.

Note:
If the Hub Transport server is installed on the same hardware as the Mailbox server role, load balancing may not occur. When the Hub Transport server role is on the same hardware as the Mailbox server role, the local server is preferred for all messages that are sent by users who have mailboxes on that server. Therefore, in this scenario, true load balancing does not occur.

Network Load Balancing (NLB) can be used to provide high availability in the following scenarios:

- Load balancing of inbound SMTP connections for POP and IMAP client connections to the default Receive connector named "Client *<Server Name>*" that is created only on Hub Transport servers.
- Load balancing of inbound SMTP connections for applications that submit e-mail to the Exchange organization.

NLB should not be used to distribute connections for internal routing between Hub Transport servers.

For more information about how to configure Network Load Balancing, see the Network Load Balancing Technical Reference.

Edge Transport Server Planning

The Edge Transport server role is designed to provide improved anti-spam protection for the Exchange organization. The Edge Transport server also applies policies to messages in transport between organizations. This server role is deployed in the perimeter network and outside the Active Directory forest. Edge Transport servers don't have access to Active Directory for configuration and recipient information as do the other Exchange 2010 server roles. The Edge Transport server uses the Active Directory Lightweight Directory Service (AD LDS) to store configuration and recipient information.

You can add an Edge Transport server to an existing Exchange organization making any organizational changes. You don't have to perform any Active Directory preparation steps when you install the Edge Transport server.

When an Edge Transport server is deployed to support an Exchange organization that has not yet deployed Exchange 2010, a limited set of features are available. You can't create an Edge Subscription in this scenario. Therefore, you can't use the Recipient Lookup or safelist aggregation features until you have deployed Exchange 2010 in your organization.

When you're planning to deploy Edge Transport servers, you should consider the following issues:

- **Server Capacity** Planning for server capacity includes planning to conduct performance monitoring of the Edge Transport server. Performance monitoring will help you understand how hard the server is working. This information will determine the capacity of your current hardware configuration.
- **Transport Features** The Edge Transport server can provide anti-spam protection at the edge of the network. As part of your planning process, you should determine the anti-spam features that you will enable at the Edge Transport server and how they will be configured.
- **Security** The Edge Transport server role is designed to have a minimal attack surface. Therefore, it's important to correctly secure and manage both the physical access and network access to the server. Planning for security will help you make sure that IP connections are only enabled from authorized servers and from authorized users. For more information, see the Deployment Security Checklist.
  The recommended practice is to put the Edge Transport server within a perimeter network. To make sure that the server can send and receive e-mail and receive recipient and configuration data updates from the Microsoft Exchange EdgeSync service, you must allow communication through the ports that are listed in the following table.

Communication port settings for Edge Transport servers

Network interface	Open port	Protocol	Note
Inbound from and outbound to the Internet	25/TCP	SMTP	This port must be open for mail flow to and from the Internet.
Inbound from and outbound to the internal network	25/TCP	SMTP	This port must be open for mail flow to and from the Exchange organization.
Local only	50389/TCP	LDAP	This port is used to

			make a local connection to AD LDS.
Inbound from the internal network	50636/TCP	Secure LDAP	This port must be open for EdgeSync synchronization.
Inbound from the internal network	3389/TCP	RDP	Opening this port is optional. It provides more flexibility in managing the Edge Transport servers from inside the internal network by letting you use a remote desktop connection to manage the Edge Transport server.

Note:

The Edge Transport server role uses non-standard LDAP ports. The ports that are specified in this topic are the LDAP communication ports that are configured when the Edge Transport server role is installed. For more information, see Modify AD LDS Configuration.

- **EdgeSync** You can create an Edge Subscription to subscribe the Edge Transport server to the Exchange organization. When you create an Edge Subscription, recipient and configuration data is replicated from Active Directory to AD LDS. You subscribe an Edge Transport server to an Active Directory site. Then the Microsoft Exchange EdgeSync service that is running on the Hub Transport servers in that site periodically updates AD LDS by synchronizing data from Active Directory. The Edge Subscription process automatically provisions the Send connectors that are required to enable mail flow from the Exchange organization to the Internet through an Edge Transport server. If you're using the recipient lookup or safelist aggregation features on the Edge Transport server, you must subscribe the Edge Transport server to the organization.

Configuring DNS Settings for the Edge Transport Server Role

The Edge Transport server role is deployed outside the Exchange organization as a stand-alone server in the perimeter network or as a member of a perimeter network Active Directory domain. You must manually configure the correct DNS suffix for the Edge Transport server role before you install Exchange 2010. If a DNS suffix isn't configured, setup will fail.

Because the Edge Transport server is typically deployed in the perimeter network, it has network interfaces that are connected to multiple network segments. Each of these network segments has a unique IP configuration. The network interface that is connected to the external, or public, network segment should be configured to use a public DNS server for name resolution. This enables the server to resolve SMTP domain names to MX resource records and route mail to the Internet.

The network interface that is connected to the internal, or private, network segment should be configured to use a DNS server in the perimeter network that can resolve the names of the Hub Transport servers in your organization, or should have a Hosts file available. The Edge Transport servers and the Hub Transport servers must be able to use DNS host resolution to locate each other.

To enable name resolution of Hub Transport servers by Edge Transport servers, use one of the following methods:

- Manually create A resource records for Hub Transport servers in a forward lookup zone on the DNS server that's configured on the internal network adapter of the Edge Transport server.
- Edit the Hosts file on the Edge Transport server to include the Host records for the Hub Transport servers. The Hosts file is a local text file in the same format as the 4.3 Berkeley Software Distribution (BSD) UNIX /etc/hosts file. This file maps host names to IP addresses, and the file is stored in the \%Systemroot %\System32\Drivers\Etc folder.

To enable name resolution of Edge Transport servers by Hub Transport servers, use one of the following methods:

- Manually create A resource records for Edge Transport servers in a forward lookup zone on the DNS server that's configured on the Hub Transport server.
- To include the Host records for the Edge Transport servers, edit the Hosts file on the Hub Transport servers that are located in the Active Directory sites to which Edge Transport servers are subscribed.

You must follow these steps to configure DNS settings for the Edge Transport server:

1. Verify that the DNS server settings for each network interface are correct for the network segment.
2. Configure the DNS suffix for the Edge Transport server name using the following steps:
   2.a. Click **Start**, click **Control Panel**, and then double-click **System** to open the **System Properties**.
   2.b. Click the **Computer Name** tab.
   2.c. Click **Change**.
   2.d. On the **Computer Name Changes** page, click **More**.
   2.e. In the **Primary DNS suffix of this computer:** field, type a DNS domain name and suffix for the Edge Transport server.
   This name can't be changed after the Edge Transport server role is installed.
3. Configure DNS host name resolution for Edge Transport servers and Hub Transport servers.

Overriding DNS Settings

In your environment, you may want to specify a DNS server to route mail that differs from the DNS server that is configured in the Exchange server's IP properties. To accomplish this, modify the Internal DNS Lookups and External DNS Lookups settings of the transport server's properties. These settings override the settings on the network adapter to route e-mail messages. For more information, see Configure Edge Transport Server Properties.

Mailbox Server Planning

The Exchange 2010 Mailbox server role hosts mailbox databases and provides e-mail storage and advanced scheduling services for information workers. The Mailbox server role can also host a public folder database, which provides a foundation for workflow, document sharing, and other forms of collaboration. Servers on which the Mailbox server role is installed are called Mailbox servers.

Before installation, we recommend that you take the time to plan for your Mailbox server role deployment. You must consider several factors when planning the size of your mailbox databases.

Sizing Databases

The recommended maximum database size for Exchange 2010 is greater than the recommended maximum size in previous versions of Exchange.

When planning for the size of your databases, you should also plan for how you will enforce limits on database size, either at the database level or at the individual mailbox level. For more information about mailbox limits, see the following topics:

- Understanding Mailbox Database and Log Capacity Factors
- Exchange 2010 Mailbox Server Role Design Example
- Mailbox Server Storage Design

Public Folder Planning

Public folders are an optional feature in Exchange 2010. If all client computers in your organization are running Microsoft Office Outlook 2007 or later, public folders are an optional feature. However, if Outlook 2003 clients are in use, public folders are required. In addition, if you're currently using public folders for collecting, organizing, or sharing documents and other information and you want to continue doing so, you can use public folder replication to move your public folder data to Exchange 2010.

For more information about public folders, see Understanding Public Folders.

Client Access Server Planning

The Client Access server role receives all client connections for Exchange 2010. Computer-based clients, such as Microsoft Outlook and Microsoft Entourage, mobile phones, and browser-based clients all connect through the Client Access server role. The Client Access server role provides the following functionality:

- MAPI access
- POP3 and IMAP4 access

  Note:
  Integrated Windows authentication (formerly called NTLM) isn't supported for POP3 or IMAP4 client connectivity. For more information, see the "Client Access Features" sections in Discontinued Features.

- Outlook Web App access
- The Autodiscover Service which configures client computers that are running Outlook 2010, Outlook 2007, Entourage, and other client applications. The Autodiscover service can also configure supported mobile devices.
- The Availability Service improves information workers' calendaring and meeting scheduling experience by providing secure, consistent and up-to-date free and busy information to computers running Outlook 2007 and later.

When planning your Exchange 2010 deployment, you must have at least one computer with the Client Access server role installed in every Active Directory site that contains Exchange 2010 mailboxes. You can have multiple computers with the Client Access server role installed within each Active Directory site. To provide external client access, at least one Client Access server within your organization must be Internet-facing.

For more information about namespace planning and Client Access servers, see Understanding Client Access Server Namespaces.

Unified Messaging Server Planning

The Unified Messaging server role is designed to provide Unified Messaging (UM) for Exchange 2010 recipients. UM combines voice messaging, fax, and e-mail messaging into one store that can be accessed from a telephone, a user's computer, and a mobile device. Users can access voice messages, e-mail, and calendar information that are located in their Exchange 2010 mailbox from e-mail clients, such as Outlook and Outlook Web App.

The Unified Messaging server depends on the Client Access server, Hub Transport server

and Mailbox server. All voice mail messages that are submitted from a Unified Messaging server for a UM-enabled user are first submitted to an Exchange 2010 Hub Transport server as an SMTP message and then are submitted from a Hub Transport server to the UM-enabled user's mailbox. For a recipient to use Unified Messaging, they must have an Exchange 2010 mailbox. For details, see Understanding Unified Messaging.

Generally, the simpler the Unified Messaging topology, the easier Unified Messaging is to deploy and maintain. Install as few Unified Messaging servers and create as few Unified Messaging objects in Active Directory as you need to support your business and organizational goals. Large enterprises with complex network and telephony environments, multiple business units, or other complexities will require more planning than smaller organizations with relatively straightforward Unified Messaging needs.

Planning Your UM Deployment

You must understand the different aspects of Exchange 2010 Unified Messaging and each component and feature so that you can plan your Unified Messaging infrastructure and deployment appropriately. For details, see Understanding Unified Messaging Components and Understanding Unified Messaging Features.

The following are some of the areas that you should consider and evaluate when planning for Exchange 2010 in your organization:

- Your business needs for Unified Messaging
- Your telephony network and your current voice mail system
- Your current data network design
- Your current Active Directory environment
- The number of users that you will have to support
- The number of Unified Messaging servers you will need
- The storage requirements for users
- The placement of IP gateways, telephony equipment, and Unified Messaging servers

For more information, see Overview of Unified Messaging.

Many deployment options are available for Unified Messaging; each option has several steps in common that are required to create a scalable and highly available system to support large numbers of users. These steps are as follows:

1. Deploy and configure your telephony components for Unified Messaging.
2. Verify that you've correctly installed the Exchange 2010 server roles that are required by Unified Messaging.
3. Install the Unified Messaging server role.
4. Create and configure the required Unified Messaging Active Directory components including UM dial plans, UM IP gateways, UM hunt groups, and UM mailbox policies.
5. Perform post-deployment tasks including deploying certificates for mutual TLS, creating UM auto attendants, and configuring faxing.

For details about deploying Unified Messaging, see the following topics:

- Deploy a New Exchange 2010 RTM UM Environment
- Checklist: Deploy a New Exchange 2010 RTM UM Environment
- Deploy and Configure Incoming Faxing

If you're integrating your Unified Messaging environment with Office Communications Server, there are additional planning considerations. For details, see Understanding Unified Messaging and Communications Server 2007 R2. After you have read Understanding Unified Messaging and Communications Server 2007 R2, details about deploying Unified Messaging and Office Communications Server can be found in the following topics:

- Deploy Unified Messaging and Communications Server 2007 R2
- Checklist: Deploy Office Communications Server 2007 R2 and Exchange 2010

Unified Messaging

Exchange Client Planning

Before you deploy your Exchange 2010 organization, verify that client computers and mobile devices in your organization meet the following requirements.

Requirements	Check
All MAPI clients are running a supported version of Outlook, including Microsoft Outlook 2007, Outlook 2003.	[ ]
All Outlook Web App clients are running a supported Web browser. To use the complete set of features available in Outlook Web App, clients can use the following browsers on a computer running Windows XP, Windows 2003, Windows Vista, or Windows 7: • Internet Explorer 7 and later versions. • Firefox 3.0.1 and later versions. • Chrome 3.0.195.27 and later versions. On a computer running Max OS X, clients can use: • Safari 3.1 and later versions. • Firefox 3.0.1 and later versions. On a computer running Linux, clients can use: • Firefox 3.0.1 and later versions. Clients using a Web browser that doesn't support the full feature set will automatically be directed to the light version of Outlook Web App. The light version of Outlook Web App is optimized for accessibility, such as for users who are blind or have low vision. The light version provides fewer features and is faster for some operations. Clients may want to use the light version if they are on a slow connection or using a computer with unusually strict browser security settings. The light version can be used with almost any browser and has the same features across all browsers.	[ ]
All mobile devices are running a supported operating system. Windows Mobile phones that are Direct Push compatible or mobile phones running another operating system that is compatible with Exchange ActiveSync.	[ ]

1.2.1.3 Exchange 2003 - Planning Roadmap for Upgrade and Coexistence

Exchange 2003 - Planning Roadmap for Upgrade and Coexistence

Exchange Server 2010 > Planning and Deployment > Planning for Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can deploy Microsoft Exchange Server 2010 in an existing Microsoft Exchange Server 2003 organization operating in native mode. Coexistence with these two Exchange versions is supported. This topic provides an overview of the planning considerations and configuration steps that you must take when Exchange 2010 will coexist with Exchange 2003.

Existing Exchange Organization Planning

Before you continue in your planning for Exchange 2010, make sure your current Exchange 2003 organization meets the requirements discussed in the following topics:

- Exchange 2010 System Requirements
- Exchange 2010 Prerequisites

Coexistence

Any organization upgrading from Exchange 2003 will experience a period of coexistence. In a coexistence scenario, any combination of the following versions of Microsoft Exchange is deployed in a single Exchange organization: Exchange 2003, Exchange 2007, and Exchange 2010. This topic is concerned primarily with the coexistence of Exchange 2003 and Exchange 2010.

In a coexistence scenario, multiple versions of Exchange communicate with each other and share data resources, recipient information, and configuration information. Parts of the organization still use Exchange 2003 functionality, and other parts have completed the upgrade to Exchange 2010.

Important:

You can only install additional Exchange 2003 servers in your organization if an Exchange 2003 server was there when the first Exchange 2010 server was installed.

Be aware of the following coexistence issues:

- **Active Directory and domains** When upgrading from Exchange 2003 to Exchange 2010, you must first grant specific Exchange permissions in each domain in which you have run Exchange 2003 DomainPrep. To do this, you run the `setup /PrepareLegacyExchangePermissions` command. Granting these permissions is part of preparing Active Directory and your domains for installing Exchange 2010. For detailed instructions, see Prepare Active Directory and Domains.
- **Management interfaces** In Exchange 2010, you can manage Exchange 2010 servers and mailboxes by using either the Exchange Management Console (EMC) or the Exchange Management Shell. You can also use the EMC to view some attributes on Exchange 2003 servers. For more information, see Exchange Management Console Interoperability.
- **Server role features** The Exchange 2010 server role features available to clients in the Exchange organization during the coexistence period depend on the version of the Exchange server where the user's mailbox is stored and the version of the e-mail client application used to access Exchange.
- **Routing groups** A large organization that has many routing groups must plan its routing topology to maintain mail flow during the coexistence period. When you plan for a period of coexistence between Exchange 2003 and Exchange 2010, you need to understand how each version determines its routing topology. For more information about routing and coexistence, see Upgrade from Exchange 2003 Transport.
- **Native mode** You can only deploy Exchange 2010 in an Exchange 2003 organization that operates in native mode. For more information about how to change your Exchange 2003 organization to native mode, see Understanding

Upgrade to Exchange 2010.

Administration Differences

Exchange 2003 uses administrative groups to organize Exchange objects for delegating permission to manage those objects. Exchange 2010 doesn't use administrative groups as a logical management unit for administrative delegation.

However, to support coexistence between Exchange 2003 and Exchange 2010, all Exchange 2010 servers are automatically put in a single administrative group when Exchange 2010 is installed. This administrative group is recognized in Exchange System Manager of earlier versions of Exchange as Exchange Administrative Group (FYDIBOHF23SPDLT).

Caution:

Don't move Exchange 2010 servers out of Exchange Administrative Group (FYDIBOHF23SPDLT) and don't rename Exchange Administrative Group (FYDIBOHF23SPDLT) by using a low-level directory editor. Exchange 2010 must use this administrative group for configuration data storage. Moving Exchange 2010 servers out of Exchange Administrative Group (FYDIBOHF23SPDLT) or the renaming of Exchange Administrative Group (FYDIBOHF23SPDLT) isn't supported.

You must use Exchange System Manager and utilities to manage the Exchange 2003 servers. In Exchange 2010, you must manage Exchange 2010 servers and mailboxes by using the EMC or the Shell. However, you can use the EMC to view some attributes on Exchange 2003 servers. For more information about EMC interoperability, see Exchange Management Console Interoperability.

Exchange 2007 and Exchange 2003 Mixed Mode Coexistence

When you're ready to upgrade a mixed mode environment, upgrade each Active Directory site individually. If you have Active Directory sites with only Exchange 2007 or Exchange 2003 in them, follow the instructions for upgrade from that version for that Active Directory site. For example, if you have Exchange 2007 in Active Directory site A, follow the upgrade instructions for Exchange 2007. If you have Exchange 2003 installed in Active Directory site B, follow the upgrade instructions for Exchange 2003. For more information about upgrading your Exchange 2003 and Exchange 2007 versions, see Understanding Upgrade to Exchange 2010.

If you have Active Directory sites with both Exchange 2003 and Exchange 2007 installed, follow the upgrade instructions from both Exchange 2003 and Exchange 2007, and perform the upgrade steps required by both. For more information about upgrading to Exchange 2010 in this scenario, see the following topics:

- Understanding Upgrade to Exchange 2010
- Install Exchange 2010 in a Mixed Exchange 2003 and Exchange 2007 Organization

Upgrade Process from Exchange 2003 to Exchange 2010

Here is a high-level overview of the upgrade steps that you follow to upgrade from Exchange 2003 to Exchange 2010.

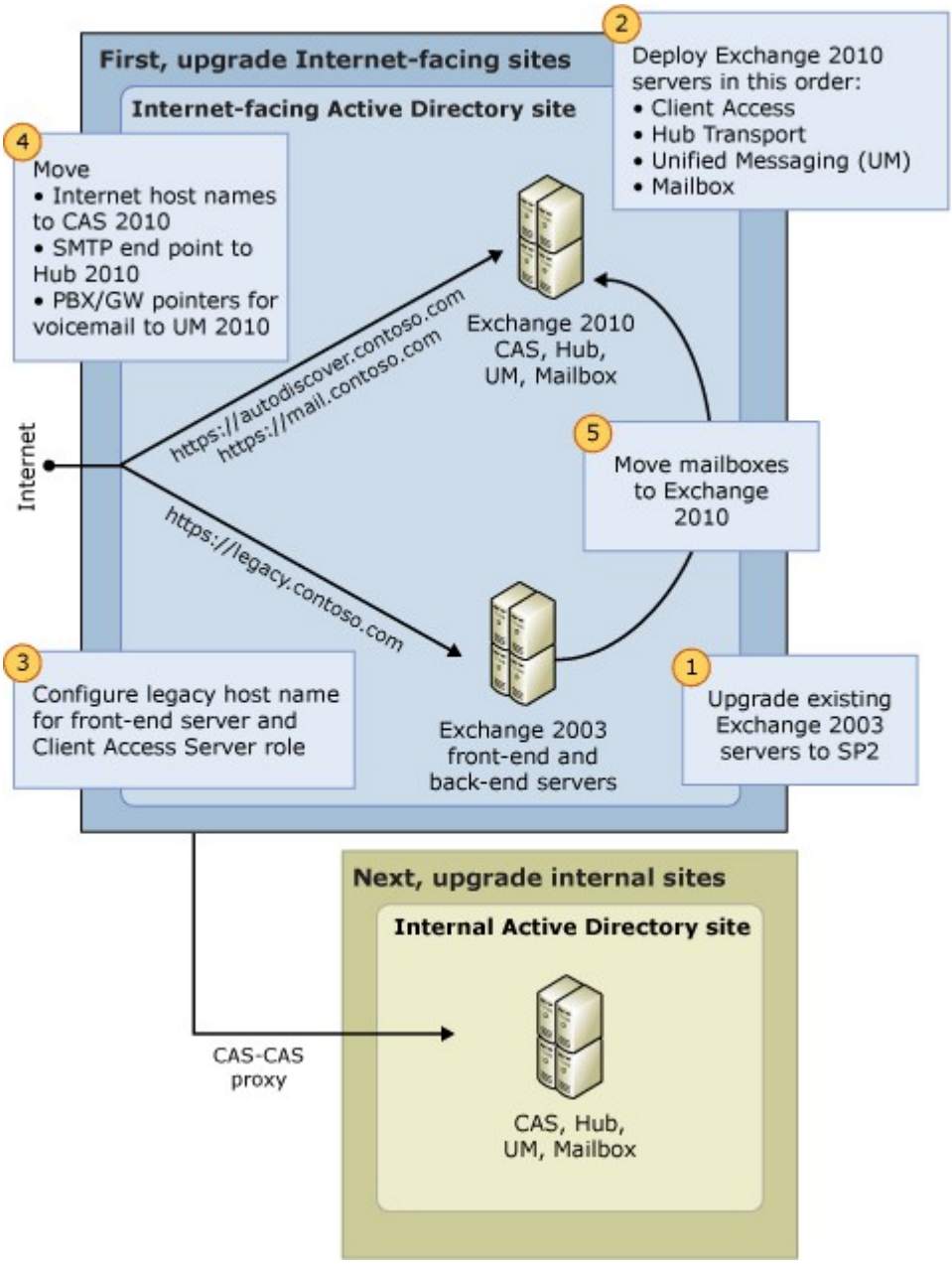
First, you upgrade all Internet-facing Active Directory sites by doing the following:

1. Upgrade existing Exchange 2003 servers to Exchange 2003 Service Pack 2 (SP2).
2. Deploy Exchange 2010 servers in this order:
   2.a. Client Access
   2.b. Hub Transport
   2.c. Unified Messaging

2.d.Mailbox
3. Configure the Exchange 2003 front-end server and the Exchange 2010 Client Access server.
4. Configure the Exchange 2010 Hub Transport server and the Unified Messaging servers.
5. Move mailboxes from Exchange 2003 to Exchange 2010

Then, upgrade all internal Active Directory sites in the same manner.

The following figure illustrates the overview of the upgrade process from Exchange 2003 to Exchange 2010.



Order of Active Directory Sites for Upgrade

As shown in the preceding figure, when you're upgrading your organization to Exchange

2010, you must begin with your servers in the Internet-accessible Active Directory sites, and then upgrade your internal Active Directory sites. This approach is necessary because Client Access server to Client Access server proxying is only supported from the newer Client Access server role versions (Exchange 2010) to the older Client Access server role versions (Exchange 2007) and not the reverse.

Order of Server Roles for Upgrade

Within the first Active Directory site or sites you're upgrading, the first Exchange 2010 server role you install is the Client Access server role. We recommend that you upgrade a single Active Directory site at a time to Exchange 2010. Depending on the size of your Active Directory site, this might be a single Client Access server computer or a load-balanced array of Exchange 2010 Client Access server computers.

We recommend the following order when installing the Exchange 2010 server roles:

1. Client Access server role
2. Hub Transport server role
3. Unified Messaging (UM) server role
4. Mailbox server role

Note:
When upgrading to Exchange 2010, you can't perform an in-place server upgrade on an existing Exchange server.

For detailed information about upgrading server roles, see the following topics:

- Upgrade from Exchange 2003 Client Access
- Upgrade from Exchange 2003 Transport
- Upgrade from Exchange 2003 Mailbox
- Install Exchange 2010 in an Existing Exchange 2003 Organization

You can add the Unified Messaging server role later, or if you want to install it at the same time as the other server roles, you can do so by selecting **Custom Exchange Server Installation**.

Note:
You must deploy the Edge Transport server role in the perimeter network and outside the secure Active Directory forest.

Exchange 2010 Deployment Assistant

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Server Role Coexistence

This section provides details about each Exchange 2010 server role in a coexistence scenario.

Client Access Server Coexistence

The Client Access server role provides new features in addition to all the functionality provided by a front-end server in Exchange 2003. All client connectivity (including Microsoft Outlook MAPI connectivity) now goes through the Client Access server role. There are no longer any clients directly connecting to the Mailbox server role. The Client Access server role can coexist with Exchange 2003 servers. The following list describes the Exchange 2010 Client Access server dependencies and requirements for coexistence with Exchange 2003:

- Whether a user sees the Outlook Web App client of Exchange 2003 or the Outlook Web App client of Exchange 2010 depends on the location of the user's mailbox. For example, if the user's mailbox is located on an Exchange 2003 back-end server and the Client Access server is running Exchange 2010, the user will see Outlook Web Access, the Exchange 2003 client.
- The version of Microsoft Exchange ActiveSync that clients use depends on the server version hosting the user's mailbox. The user's mailbox must be located on a server running Exchange 2003 SP2 or Exchange 2010 to have Direct Push enabled for Exchange ActiveSync.
- When you perform an upgrade from Exchange 2003 to Exchange 2010, you typically upgrade all the Exchange servers in a specific routing group or Active Directory site to Exchange 2010 at the same time, configure coexistence, and then upgrade the next site.

Important:

When upgrading an Exchange 2003 organization, an Exchange 2003 front-end server is required to support the upgrade. For each Exchange 2010 Client Access server, you can only configure one Outlook Web Access 2003 URL for redirection. You can accomplish this with a single Exchange 2003 front-end server or a load-balanced array of Exchange 2003 front-end servers.

For more information about Client Access server coexistence between Exchange 2003 and Exchange 2010, and for information about new Exchange 2010 features, see Upgrade from Exchange 2003 Client Access.

Exchange 2007 introduced the Autodiscover and Availability services, and Exchange 2010 continues to rely on these services:

- The Autodiscover service configures client computers running Microsoft Outlook 2010, Outlook 2007, Entourage, and other client applications. The Autodiscover service can also configure supported mobile devices. The Autodiscover service provides access to Exchange features for Outlook 2010 clients connected to your Exchange messaging environment.
- The Availability service improves information workers' calendaring and meeting scheduling experience by providing secure, consistent, and up-to-date free and busy information to computers running Outlook 2007 or Outlook 2010.

For more information, see Understanding the Autodiscover Service and Understanding the Availability Service.

Hub Transport Server Coexistence

The Hub Transport server role is designed to handle all mail flow for the Exchange organization. It's also responsible for handling transport rules, journaling policies, and message delivery. This server is deployed in the Active Directory forest and is required for Exchange 2010 mailboxes to send and receive messages. Messages sent to the Internet are relayed by the Hub Transport server to the Edge Transport server or a third-party smart host.

You can add an Exchange 2010 Hub Transport server to an existing Exchange organization after you successfully deploy Exchange 2010 Client Access servers. When you introduce Exchange 2010 Hub Transport servers in your Exchange 2003 environment, all Exchange 2010 Hub Transport servers are placed in a single, separate routing group.

To enable mail flow between the Exchange 2010 deployment and your existing Exchange 2003 organization, you need to create a routing group connector. This routing group connector is created during the setup of your first Exchange 2010 Hub Transport server.

To learn more about introducing Exchange 2010 Hub Transport servers to your Exchange 2003 organization, see Upgrade from Exchange 2003 Transport.

Mailbox Server Coexistence

For Exchange 2010 and Exchange 2003 Mailbox servers to coexist, you must be able to send mail among the mailboxes. Exchange 2010 uses the Hub Transport server to send mail. An Exchange 2010 Hub Transport server must be deployed in each Active Directory site that contains an Exchange 2010 Mailbox server. You also need a Client Access server in each Active Directory site where there's a Mailbox server. For more information about upgrading to an Exchange 2010 Mailbox server, see Upgrade from Exchange 2003 Mailbox.

If you move a mailbox from Exchange 2003 to Exchange 2010, and the mailbox is part of an e-mail address policy, the e-mail addresses for that mailbox are automatically updated based on the configuration of the e-mail address policy. If the mailbox had a primary SMTP address that differs from the e-mail address enforced by the e-mail address policy, that SMTP address becomes a secondary SMTP address, and the e-mail address generated by the e-mail address policy becomes the primary SMTP address. For information about how to move mailboxes, see Managing Move Requests.

You can replicate public folder data between Exchange 2010 and Exchange 2003 public folder databases. To do this, you must create a replica of the public folder using the Exchange 2003 Exchange System Manager. For more information about Exchange 2010 and Exchange 2003 public folder coexistence, see Understanding Public Folders.

Unified Messaging Server Coexistence

The Unified Messaging server role is designed to provide Unified Messaging for Exchange 2010 recipients. Unified Messaging combines voice messaging and e-mail messaging into one store that can be accessed from a telephone, a user's computer, or a mobile device. Users can access voice messages, e-mail, and calendar information located in their Exchange 2010 mailbox from e-mail clients, such as Outlook and Outlook Web App.

The Unified Messaging server depends on the Hub Transport server and Mailbox server. All SMTP mail submitted from a Unified Messaging server must be submitted to an Exchange 2010 Hub Transport server. For a recipient to use Unified Messaging, they must have an Exchange 2010 mailbox.

Versions of Exchange earlier than Exchange 2007 can't be upgraded and require you to deploy an Exchange 2010 organization with all the Exchange server roles, including Unified Messaging, and then move the Exchange 2003 (or earlier) mailboxes to an Exchange 2010 Mailbox server. For details, see Move Mailboxes from Exchange 2003 Servers to Exchange 2010 Servers.

Edge Transport Server Coexistence

The Edge Transport server role is designed to provide improved antivirus and anti-spam protection for the Exchange organization. The Edge Transport server also applies policies to messages in transport between organizations. This server role is deployed in the perimeter network and outside the Active Directory forest. The Edge Transport server can be deployed as a smart host and SMTP-relay server for an existing Exchange 2003 organization.

You can add an Edge Transport server to an existing Exchange organization without upgrading the internal Exchange servers or making any organizational changes. You don't have to perform any Active Directory preparation steps when you install the Edge Transport server.

If you're using the Exchange Intelligent Message Filter in Exchange 2003 to perform anti-spam tasks, you can use the Edge Transport server to provide an additional layer of anti-spam protection. The Edge Transport server provides antivirus and anti-spam protection as messages enter the network.

When an Exchange 2010 Edge Transport server is deployed to support an Exchange organization that hasn't yet deployed Exchange 2010, a limited set of features is available. You can't create an Edge Subscription in this scenario. Therefore, you can't use

the Recipient Lookup or safelist aggregation features. For more information about Edge Transport servers and coexistence, see Upgrade from Exchange 2003 Transport.

Supported Topologies

Exchange 2010 supports the following topologies:

- Single forest with multiple Active Directory sites
- Multiple forests (resource forest model) with multiple Active Directory sites
- Single Active Directory site

For more information, see the following topics:

- Deploy Multiple Forest Topologies
- Deploy Exchange 2010 in a Cross-Forest Topology
- Deploy Exchange 2010 in an Exchange Resource Forest Topology

Exchange 2010 doesn't support the following topologies:

- Coexistence with Exchange 2000 Server or earlier
- Coexistence with Exchange 2003 versions prior to SP2
- Installing an older version of Exchange into a newly created Exchange 2010 organization

1.2.1.4 Exchange 2007 - Planning Roadmap for Upgrade and Coexistence

Exchange 2007 - Planning Roadmap for Upgrade and Coexistence

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can deploy Microsoft Exchange Server 2010 in an existing Microsoft Exchange Server 2007 organization. This topic provides an overview of the planning considerations and configuration steps that you must take when Exchange 2010 will coexist with Exchange 2007.

Existing Exchange Organization Planning

Before you continue in your planning for Exchange 2010, make sure your current Exchange 2007 organization meets the requirements discussed in the following topics:

- Exchange 2010 System Requirements
- Exchange 2010 Prerequisites

Coexistence

Any organization that upgrades from Exchange 2007 to Exchange 2010 will experience a period of coexistence when parts of the organization still use Exchange 2007 functionality and other parts have completed the upgrade to Exchange 2010.

Important:

You can only install additional Exchange 2007 servers in your organization if an Exchange

2007 server was there when the first Exchange 2010 server was installed.

Be aware of the following coexistence issues:

- **Management interfaces** In Exchange 2010, you can manage Exchange 2010 servers and mailboxes by using either the Exchange Management Console (EMC) or the Exchange Management Shell. You can also use the EMC to view some attributes on Exchange 2007 servers. For more information, see Exchange Management Console Interoperability.
- **Server role features** The Exchange 2010 server role features available to clients in the Exchange organization during the coexistence period depend on the version of the Exchange server where the user's mailbox is stored and the version of the e-mail client application used to access Exchange.
  For more information about how server-to-server communication occurs, see Understanding Transport Pipeline.
- **Routing groups** A large organization that has many routing groups requires a routing topology that maintains mail flow during the coexistence period. When you plan for a period of coexistence between Exchange 2010 and Exchange 2007, you need to understand how each version determines its routing topology. For more information about routing and coexistence, see Upgrade from Exchange 2007 Transport.

Upgrade Process from Exchange 2007 to Exchange 2010

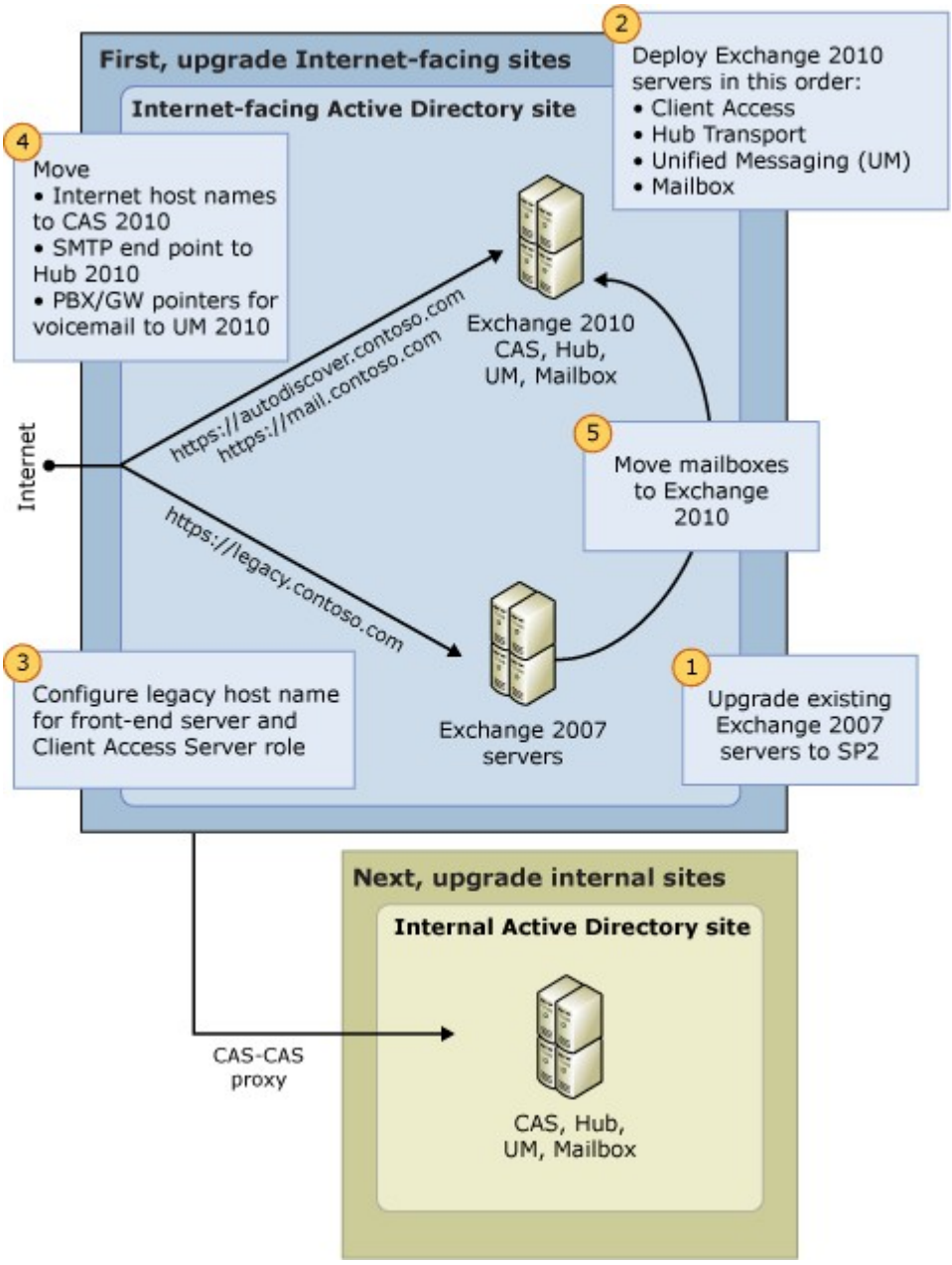
Here is a high-level overview of the upgrade steps that you follow to upgrade from Exchange 2007 to Exchange 2010.

First, you upgrade all Internet-facing Active Directory sites by doing the following:

1. Upgrade existing Exchange 2007 servers to Exchange 2007 Service Pack 2 (SP2).
2. Deploy Exchange 2010 servers in this order:
   2.a.Client Access
   2.b.Hub Transport
   2.c.Unified Messaging
   2.d.Mailbox
3. Configure the Exchange 2010 Client Access server.
4. Configure the Exchange 2010 Hub Transport server and the Unified Messaging servers.
5. Move mailboxes from Exchange 2007 to Exchange 2010

Then, upgrade all internal Active Directory sites in the same manner.

The following figure illustrates the overview of the upgrade process from Exchange 2007 to Exchange 2010.



Order of Active Directory Sites for Upgrade

When you're upgrading your organization to Exchange 2010, you must begin with your servers in the Internet-accessible Active Directory sites, and then upgrade your internal Active Directory sites. Upgrading an internal Active Directory site before all your Internet-accessible sites have been upgraded isn't supported. This is because Client Access server to Client Access server proxying is only supported from the newer Client Access server role versions (Exchange 2010) to older Client Access server role versions (Exchange 2007) and not the reverse.

Order of Server Roles for Upgrade

Within the first Active Directory site or sites you're upgrading, the first Exchange 2010 server role you install is the Client Access server role. We recommend that you upgrade a single Active Directory site at a time to Exchange 2010. Depending on the size of your Active Directory site, this might be a single Client Access server computer or a load-balanced array of Exchange 2010 Client Access server computers.

We recommend the following order when installing the Exchange 2010 server roles:

1. Client Access server role
2. Hub Transport server role
3. Mailbox server role
4. Unified Messaging (UM) server role
5. Edge Transport server role

Note:
When upgrading to Exchange 2010, you can't perform an in-place server upgrade on an existing Exchange server.

For detailed information about upgrading server roles, see the following topics:

- Upgrade from Exchange 2007 Client Access
- Upgrade from Exchange 2007 Transport
- Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging
- Upgrade from Exchange 2007 Mailbox

Exchange 2007 and Exchange 2003 Mixed Mode Coexistence

When you're ready to upgrade a mixed mode environment, upgrade each Active Directory site individually. If you have Active Directory sites with only Exchange 2007 or Exchange 2003 in them, follow the instructions for upgrade from that version for that Active Directory site. For example, if you have Exchange 2007 in Active Directory site A, follow the upgrade instructions for Exchange 2007. If you have Exchange 2003 installed in Active Directory site B, follow the upgrade instructions for Exchange 2003. For more information about upgrading your Exchange 2003 and Exchange 2007 versions, see Understanding Upgrade to Exchange 2010.

If you have Active Directory sites with both Exchange 2003 and Exchange 2007 installed, follow the upgrade instructions from both Exchange 2003 and Exchange 2007, and perform the upgrade steps required by both. For more information about upgrading to Exchange 2010 in this scenario, see the following topics:

- Understanding Upgrade to Exchange 2010
- Install Exchange 2010 in a Mixed Exchange 2003 and Exchange 2007 Organization

Administration Differences

The Exchange Management Console (EMC) is available in both Exchange Server 2010 and Exchange Server 2007. The following lists the tasks and actions that can be performed using the EMC in either Exchange 2010 or Exchange 2007:

- Actions that create objects, such as new mailboxes or a new offline address book (OAB), can only be performed on a version of the EMC that's the same as the target object. For example, creating a mailbox on an Exchange 2007 Mailbox server must be performed with the EMC in Exchange 2007. The following applies:
  - Exchange 2007 Mailbox databases can't be managed from the EMC in Exchange 2010, although these databases can be viewed.
  - The EMC in Exchange 2010 can't enable or disable Exchange 2007 Unified Messaging mailboxes.
  - The EMC in Exchange 2010 can't manage Exchange 2007 mobile devices.
- Actions that require viewing of objects can be performed from any version of the EMC to any version of Exchange objects, with a few exceptions:
  - Exchange 2010 and Exchange 2007 transport rule objects can only be viewed from their corresponding version of the EMC.
  - Exchange 2010 and Exchange 2007 servers can only be viewed from their corresponding version of the EMC.
  - The Queue Viewer tool in the EMC in Exchange 2010 can't connect to an Exchange 2007 server to view queues or messages.

Note:
If an Exchange 2007 object (such as a storage group) is no longer present in Exchange 2010, there's no interoperability expected or provided because Exchange 2010 isn't aware of the feature.

- You can't use message tracking configuration tasks between Exchange 2010 and Exchange 2007. You must use Exchange 2007 messaging tracking tools within your Exchange 2007 servers, and Exchange 2010 messaging tracking tools within your Exchange 2010 servers.

Client Access Server Coexistence

The Client Access server role can coexist with Exchange 2007 Client Access servers. Before you upgrade the first Active Directory site, you must install Exchange 2007 Service Pack 2 (SP2) on all Exchange 2007 Client Access servers within your organization.

After the first Exchange 2010 Client Access server or Client Access server array has been installed in your organization, the Autodiscover service on the Exchange 2007 Client Access servers will redirect users with mailboxes on an Exchange 2010 Mailbox server to the appropriate Exchange 2010 Client Access endpoint.

Installation of Exchange 2010 within your organization requires the creation of a second Domain Name System (DNS) host name. When you install the first Exchange 2010 Client Access server in your organization, you also need to create a host name. If your current host name is http://contoso.com, we recommend creating http://legacy.contoso.com. You install the first Exchange 2010 Client Access server or Client Access server array, copy the appropriate Microsoft Outlook Web Access, Microsoft Exchange ActiveSync, POP3, IMAP4, Exchange Web Services, and Autodiscover service settings, and then configure http://legacy.contoso.com to point to the Exchange 2007 Client Access servers and http://contoso.com to point to the Exchange 2010 Client Access server or Client Access server array. You need the appropriate Secure Sockets Layer (SSL) certificate for both host names. We recommend a Subject Alternative Name that can support multiple host names. For more information, see Upgrade from Exchange 2007 Client Access.

Exchange ActiveSync Coexistence

For coexistence with Exchange ActiveSync, you configure a legacy DNS host name. Users with mailboxes on Exchange 2007 Mailbox servers will be proxied from Exchange 2010 to Exchange 2007.

Note:
When moving a user's mailbox from Exchange 2007 to Exchange 2010, some users are prompted to perform a full synchronization of their mailbox. This is a requirement for many mobile phones and only occurs during the first synchronization of the user phone after the mailbox is moved.

When a user's mailbox is on Exchange 2007, the user will experience the Exchange 2007 version of Exchange ActiveSync during coexistence. That user will have the Exchange 2010 functionality of Exchange ActiveSync when the mailbox is moved to Exchange 2010. For more information about coexisting with Exchange ActiveSync, see Upgrade from Exchange 2007 Client Access.

Outlook Web App Coexistence

If a user with a mailbox on an Exchange 2007 Mailbox server connects to an Exchange 2010 Client Access server in the same Active Directory site, the user will be redirected to an Exchange 2007 Client Access server within that site. If a user with a mailbox on an Exchange 2007 Mailbox server connects to an Exchange 2010 Client Access server in a different Active Directory site and there's no Internet-accessible Client Access server in the destination Active Directory site, the user will be proxied to an Exchange 2007 Client Access server within the destination Active Directory site. As with Exchange 2007, if a user accesses an Exchange 2010 Client Access server in an Active Directory site different from the one where the mailbox resides and there's an Internet-accessible Client Access

server in the Active Directory site that contains the user's mailbox, the user will be redirected to the Client Access server in the destination Active Directory site. When a user's mailbox is on Exchange 2007, the user will experience the Exchange 2007 versions of Microsoft Office Outlook Web App during coexistence. That user will have the Exchange 2010 functionality of Outlook Web App when the mailbox is moved to Exchange 2010.

When upgrading Outlook Web App, there are different authentication scenarios that need to be examined:

- **Forms-based authentication terminating at an Exchange 2007 Client Access server** In this scenario, the Exchange 2010 Client Access server will redirect the user to the legacy Client Access server, and a second sign-on won't be required.
- **Third-party authentication solution in front of the Exchange 2007 Client Access server** This scenario requires a Microsoft Internet Security and Acceleration (ISA) Server or other authentication solution in front of the Exchange servers. In this situation, users will only be required to authenticate at the authentication solution, which will pass the credentials to any required Exchange 2010 or Exchange 2007 servers.
- **Non-forms based authentication terminating at an Exchange 2007 Client Access server** Outlook Web App will redirect the user to a legacy Exchange 2007 Client Access server. Whether the user needs to reauthenticate depends on the authentication mechanism used. For example, if Integrated Windows authentication is used, the user will experience a single sign-on. If Basic authentication is used, the user will need to authenticate twice.

The upgrade and coexistence steps you must take for Outlook Web App depend on which authentication scenario you have chosen. For more information about coexisting with Outlook Web App, see Upgrade from Exchange 2007 Client Access.

Hub Transport Server Coexistence

The Hub Transport server role is designed to handle all mail flow for the Exchange organization. It's also responsible for handling transport rules, journaling policies, and message delivery. This server is deployed in the Active Directory forest and is required for Exchange 2010 mailboxes to send and receive messages. Messages sent to the Internet are relayed by the Hub Transport server to the Edge Transport server or a third-party smart host.

You can add an Exchange 2010 Hub Transport server to an existing Exchange organization after you successfully deploy Exchange 2010 Client Access servers. After you introduce Exchange 2010 Hub Transport servers to your Exchange 2007 environment, you still need to maintain your Exchange 2007 Hub Transport servers. Exchange 2010 Mailbox servers can only communicate with Exchange 2010 Hub Transport servers, and Exchange 2007 Mailbox servers can only communicate with Exchange 2007 Hub Transport servers. When a message is sent from a mailbox on an Exchange 2010 Mailbox server to a mailbox on an Exchange 2007 Mailbox server, the message is first submitted to the closest Exchange 2010 Hub Transport server in the site. This server then relays the message to an Exchange 2007 Hub Transport server in the same site, which finally delivers the message to the Exchange 2007 Mailbox server.

To learn more about introducing Exchange 2010 Hub Transport servers to your Exchange 2007 organization, see Upgrade from Exchange 2007 Transport.

Mailbox Server Coexistence

The Exchange 2010 Mailbox server role can coexist with Exchange 2007 Mailbox servers. If you move a mailbox from Exchange 2007 to Exchange 2010, and the mailbox is part of an e-mail address policy, the e-mail addresses for that mailbox are automatically updated based on the configuration of the e-mail address policy. If the mailbox had a primary SMTP address that differs from the e-mail address enforced by the e-mail address policy, that SMTP address becomes a secondary SMTP address, and the e-mail address generated by the e-mail address policy becomes the primary SMTP address. For information about how

to move mailboxes, see Managing Move Requests.

You can replicate public folder data between Exchange 2010 and Exchange 2007 public folder databases. For more information about Exchange 2010 and Exchange 2007 public folder coexistence, see Understanding Public Folders.

Edge Transport Server Coexistence

The Edge Transport server role is designed to provide improved antivirus and anti-spam protection for the Exchange organization. The Edge Transport server also applies policies to messages in transport between organizations. This server role is deployed in the perimeter network and outside the Active Directory forest. The Edge Transport server can be deployed as a smart host and SMTP-relay server for an existing Exchange 2007 organization.

You can add an Edge Transport server to an existing Exchange organization without upgrading the internal Exchange servers or making any organizational changes. You don't have to perform any Active Directory preparation steps when you install the Edge Transport server. The Edge Transport server provides antivirus and anti-spam protection as messages enter the network.

When an Exchange 2010 Edge Transport server is deployed to support an Exchange organization that hasn't yet deployed Exchange 2010, a limited set of features is available. You can't create an Edge Subscription in this scenario. Therefore, you can't use the Recipient Lookup or safelist aggregation features. For more information about Edge Transport servers and coexistence, see Upgrade from Exchange 2007 Transport.

Unified Messaging Server Coexistence

When you install the first Exchange 2010 Unified Messaging server and add it to an existing Exchange 2007 organization, you must first add the Exchange 2010 Unified Messaging server to an existing UM dial plan that contains Exchange 2007 Unified Messaging servers. Then, configure each IP gateway or IP Private Branch eXchange (PBX) to send all incoming calls to the Exchange 2010 Unified Messaging servers within the UM dial plan and not to the Exchange 2007 Unified Messaging servers. When an incoming call is received by an Exchange 2010 Unified Messaging server and the Unified Messaging-enabled user's mailbox is located on an Exchange 2010 Mailbox server, the Exchange 2010 Unified Messaging server will process the incoming call. If the user's mailbox is located on an Exchange 2007 Mailbox server, the incoming call will be redirected to an Exchange 2007 Unified Messaging server within the same UM dial plan, and the incoming call will be processed.

After all Unified Messaging-enabled user mailboxes have been migrated to an Exchange 2010 Mailbox server, the Exchange 2007 Unified Messaging servers can be removed from the UM dial plan. For more information, see Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging.

Supported Topologies

Exchange 2010 supports the following topologies:

- Single forest with multiple Active Directory sites
- Multiple forests (resource forest model) with multiple Active Directory sites
- Single Active Directory site

For more information, see the following topics:

- Deploy Multiple Forest Topologies
- Deploy Exchange 2010 in a Cross-Forest Topology
- Deploy Exchange 2010 in an Exchange Resource Forest Topology

Exchange 2010 doesn't support the following topologies:

- Coexistence with Exchange 2000 Server or earlier

- Coexistence with Exchange 2003 versions prior to SP2
- Installing an older version of Exchange into a newly created Exchange 2010 organization

1.2.1.5 Exchange Server Deployment Assistant

Exchange Server Deployment Assistant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-15*

Microsoft Exchange Server 2010 introduces the Exchange Server Deployment Assistant or *ExDeploy*, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment. To access ExDeploy, see Exchange Server 2010 Deployment Assistant.

You can use ExDeploy for the following scenarios:

- On-Premises Only
  - Upgrade from Exchange Server 2003
  - Upgrade from Exchange 2007
  - Upgrade from mixed Exchange 2003 and Exchange Server 2007
  - New installation of Exchange 2010

  For more information about this scenario, see Deploying Exchange 2010.
- Hybrid Deployment (On-Premises + Cloud)
  - Exchange 2003
  - Exchange 2007
  - Exchange 2010

  For more information about this scenario, see Hybrid Deployments.
- Cloud Only

  For more information about this scenario, see Understanding Cloud-Only Deployments.

1.2.1.6 Workforce Planning for Exchange

Workforce Planning for Exchange

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-03-08*

You may wonder: "How many IT professionals do I need to manage my Microsoft Exchange Server environment?" Unfortunately, there is no simple answer to this question. But to help you in your planning, this topic describes several major factors you must consider to calculate your optimal workforce level. This topic will help you assess the many facets of your organization so that you can make an informed decision about workforce

levels.

Note:
Although this topic focuses on Microsoft Exchange Server 2010 deployments, you can use its guidance to also estimate workforces for administering previous versions of Exchange.

At a high level, workforce levels are based on organizational maturity and required tasks. Organizational maturity is built on the following principles: operational process maturity, experience, hardware, reliability, and design. The required tasks will vary from company to company, and it's up to the Exchange administrator to assess and manage the process.

Organizational Maturity

Essentially, organizational maturity is determined by the level to which an organization has developed its internal policies and procedures. For example, an organization with very few defined procedures for managing the messaging environment and that has no standard operating procedures for server configuration may experience more incidents and outages than another organization that has carefully documented policies about driver updates, patch installation, and server configuration.

However, organizational maturity is not restricted to the use of policies. It also includes the *means* by which administrators manage an environment. For example, an administrator can apply hotfixes to 10 servers by logging into each server, and then downloading and installing the hotfixes on each one in turn. This process is extremely inefficient. By contrast, one administrator using an automated patch deployment system could easily deploy hotfixes to 100 servers in a few minutes, exponentially increasing efficiency. However, that patch management solution would, itself, have to be actively managed. This requirement would demand more resources, and would have to follow specific policies and procedures to ensure a healthy, accurate solution.

Organizational maturity is built on the following principles:

- **Operational process maturity**: Typically, if you have created well-documented and repeatable operational practices, the need for constant or reactive maintenance is reduced because most tasks will be automated.
- **Experience**: The level of knowledge and relevant work experience possessed by the operations team members has a positive impact on the team's ability to manage an enterprise messaging solution.
- **Hardware**: Efficient systems and good storage practices help maintain a high degree of user satisfaction and can greatly reduce the number of support calls or outages.
- **Reliability**: Related to hardware, reliability is a function of the combination of hardware, software, features that are in use, and the demands on the system. Often, a reliable solution is one that is chosen specifically to meet the full demands of a given workload.

  Note:
  Reliability is *not* a synonym for clustering. A clustering solution introduces additional complexity that may be unsuitable for organizations that don't have experience.

- **Design**: An appropriate design of the Exchange environment increases the effectiveness of all the aforementioned principles. Conversely, a poor design can cause the hardware or staff experience to be less effective.

The principles of organizational maturity are organized into organizational profiles that are known as the *Infrastructure Optimization* model, as shown in the following table.

Infrastructure Optimization model

Level	Characterization

Basic	Systems are complex and incompatible. Most IT personnel spend their time reacting to problems and are just trying to keep things running. If there are few standards and automated tools in use, IT support is labor-intensive and expensive.
Standardized	IT departments are more centralized and effective. But systems remain complex, incompatible, and expensive to maintain. Pockets of standalone systems reside in business groups.
Rationalized	IT and business groups develop strategies and define IT policies, which are enforced through technology. Through standards and careful engineering, applications work together with improved compatibility.
Dynamic	Business agility takes priority over cost savings. IT systems are highly automated, flexible, and respond quickly to changing business conditions.

For more information about Infrastructure Optimization, see Microsoft Infrastructure Optimization.

The key differentiator among the levels of the Infrastructure Optimization model is how technology is used and the standardization of systems across many levels and groups. Generally, the higher the organizational maturity level, the lower the required staffing level for managing the environment. However, technology by itself doesn't increase an organization's maturity level. All solutions must be managed to successfully support accuracy, efficiency, reliability, and stability. An organization's policies should be driven by business need, and the technology should support or facilitate those policies.

Defining Roles and Assigning Tasks

Staffing levels are also heavily dependent upon the demands placed on the enterprise messaging team. These demands can vary greatly from organization to organization. An organization that asks its messaging administrators to deploy, configure, manage, and maintain only the Exchange Server 2010 systems will require fewer staff than one which asks administrators to manage Exchange, backups, messaging hygiene, mobile devices, network, storage, and virtualization technologies.

The following list includes some of the critical questions to consider when you evaluate the role of the messaging administrator in your organization:

- Does your Exchange team have primary responsibility for the underlying Windows operating system on the servers that are running Exchange?
- Is your Exchange team responsible for other technologies, such as Active Directory Domain Services, Microsoft SharePoint Foundation 2010, or Microsoft SQL Server?
- Does your Exchange team manage the physical hardware of the Exchange environment, such as servers, network, and storage? Or, if your Exchange servers are virtualized, do the Exchange administrators manage the virtualization solution?
- Does your Exchange team manage backups (tape-based or disk-based) for the Exchange servers?
- Does your Exchange team manage the messaging hygiene infrastructure?

Does your Exchange team manage non-Exchange software or hardware?
- Does your organization separate the roles of operations and design/ architecture for messaging?
- Does your Exchange team manage network or perimeter security for messaging?
- Does your Exchange team perform direct end-user support? If so, does the team receive all messaging-related tickets or only those that have been escalated from tier 1 and tier 2?
- Do Exchange team members perform standard daily, weekly, monthly, quarterly, or yearly tasks? If so, what are those tasks? What additional tasks should be added to the list?
- Are Exchange team members responsible for responding to security issues involving messaging resources?
- Are Exchange team members asked to perform discovery searches and handle other compliance-related matters?
- Do Exchange team members perform capacity management?

This list isn't exhaustive. There may be critical tasks for messaging administrators in your organization that are not listed above. Additionally, there are other positions, such as operations manager, whose job description and required tasks are markedly different from those of messaging administrator. It's important to consider all positions in the context of the entire team rather than focus on individual positions.

The following list describes the potential responsibilities assigned to roles and functions that are common to many large and medium enterprise messaging deployments. In many cases, the listed role is a subset of an existing role (for example, Director) instead of a specific position. For example, this is the case of Operations Engineers.

- **Director**
  - Provides messaging technology vision based technology capabilities and business need.
  - Coordinates activities of messaging operations and messaging system engineering.
  - Represents all aspects of the enterprise's messaging system to internal and external sources.
- **Manager, Messaging Operations**
  - Makes sure that the messaging system is functioning at peak performance.
  - Makes sure that the messaging operations team is aware of system slowdowns and performance degradation before these problems affect users.
  - Makes sure that all messaging operations technicians and all operations analysts have the tools they need to do their jobs.
  - Represents messaging operations to users.
- **Manager, Messaging System Engineering**
  - Drives the messaging team towards constant analysis and design review with the goal of improving the messaging system's performance.
  - Makes sure that the messaging team has the necessary tools and training to do their jobs.
  - Responds to appropriate escalations from the operations team and allocates resources to those escalations.
- **Associate Operations Analyst**
  - Installs, configures, and documents new production servers in the messaging environment.
  - Performs rudimentary troubleshooting of messaging system problems.
- **Operations Analyst**
  - Installs, configures, and documents new production servers in the messaging environment.
  - Performs all troubleshooting of messaging system problems.
  - Ensures that problems are correctly documented in the daily log.

- **Senior Operations Analyst**
  - Assists with mentoring new Operations Analysts; performs duties of the Operations Analyst when required.
  - Handles escalation issues not resolved by Operations Analyst and Technicians.
  - Makes sure that the daily log remains a useful repository of system troubleshooting information.
- **Associate Operations Engineer**
  - Works with Operations Analysts and Technicians to perform rudimentary analysis and design.
  - Brings ideas and recommendations to other members of the engineering team for further discussion.
- **Operations Engineer**
  - Works with Operations Analysts and Technicians to perform detailed analysis and design.
  - Handles initial escalations from the operations side
  - Troubleshoots and follows up on all escalations from operations team.
  - Evaluates features of released products for usability in the enterprise messaging system.
- **Senior Operations Engineer**
  - Evaluates released and unreleased messaging systems.
  - Provides detailed test plans for features to be implemented.
  - Attempts to minimize all impacts of next generation releases of message product.
  - Handles extreme escalations and interfaces with Microsoft Technical Support, if necessary.
- **Messaging Operations Technician**
  - Handles day-to-day monitoring and reporting on the messaging system.
  - Ensures that events are properly recorded in the daily log.
  - Ensures that all events that transpired during his or her shift have been recorded and reported to appropriate personnel.
  - Also handles escalation requests from standard "PC Helpdesk" department.

To increase the accuracy of any workforce staffing level calculations, it helps if you clearly define the roles of the various messaging team members and then objectively assess the demands of those roles.

Assessing Technology Impact

After your organization has defined the various roles and responsibilities, the next step is to assess the technology, and then map the desired tasks to the technical components of the solution. Often, improvements in the software may let administrators complete specific tasks much quicker than in previous versions, may enable administrators to automate common workflows, or may enable administrators to delegate specific tasks to other individuals or other teams.

Consider this example. Woodgrove Bank administrators often receive requests to restore mailboxes to retrieve mistakenly deleted items. These requests require the involvement of a messaging engineer (who has the necessary permissions to access the Exchange Server 2003 systems), as well as a backup engineer (who handles the actual restore operation). The requirement to restore deleted content will still be present after Woodgrove Bank deploys Exchange Server 2010, but if they choose to enable single item recovery for all users, the actual restoration work could be performed by a messaging administrator (who was granted the appropriate permissions via Role Based Access Control) or by a compliance administrator in the Human Resources department. Because the backup engineer is no longer involved in the restoration operation, the overall process is simpler and presumably can be completed in less time.

Exchange Server 2010 includes several features that could potentially let management reassign tasks at different levels, to different teams, or eliminate the need for the task completely. The following table describes several major features in Exchange Server 2010, together with the changes to tasks that these features may support. The features described in this table aren't an exhaustive list. Of course, you may choose to employ these features at your discretion.

Feature	Possible changes to tasks
Database Availability Groups	By having three or more database copies, Exchange administrators can adopt a native data protection strategy, reducing the demands on the backup team.
Single Item Recovery	Eliminate the need for restoring backups simply to recover a single deleted item.
Role Based Access Control (RBAC)	Lets administrators delegate tasks at a granular level without exposing the organization to major security risks.
PowerShell (expanded in Exchange Server 2010, also present in Exchange Server 2007)	Lets administrators automate common tasks, including many user, group, mailbox, and database maintenance tasks , via PowerShell scripts.
Multi-mailbox search	Combined with RBAC, lets administrators delegate discovery to other individuals, most likely in Human Resources. Lets trusted individuals perform discovery against mailboxes in the environment without third-party tools.
Exchange Control Panel	Lets users manage certain aspects of their messaging experience, including distribution groups and message tracking, thus reducing the demands on the help desk.
Personal Archive	Lets administrators absorb functionality formerly provided by Personal Folders (.pst files), thus removing a common source of support calls.
Retention Policies	Lets administrators control the e-mail lifecycle (by setting a maximum e-mail message age), possibly reducing the number of compliance issues in the messaging environment.

While the above list is specific to Exchange Server 2010, the principle of matching task to technology holds true no matter which version is in use. Using the technology to its fullest lets administrators perform their duties in the most efficient manner possible, freeing their time for other tasks and reducing the demands on other teams as well.

Calculating Staffing Levels

As stated at the beginning of this topic, there is no simple formula to provide a specific recommended number of staff to manage a given Exchange organization. The range of factors is too complex and too varied. Two organizations of similar size and scope may

require vastly different staffing levels based on the required duties of the administrators, the administrators' experience managing Exchange, and the degree of automation in the environment.

The most important factor to consider when calculating staffing levels is the amount of time that is needed to perform all required tasks given the current infrastructure. It may also be appropriate to calculate the amount of time that is required to perform all desired tasks given an idealized infrastructure, if significant changes will be made to the environment which would increase the operational maturity level. The sum total of hours is then translated into a recommended staffing level, taking into account other factors including the length of the work day, the length of the work week, and the average number of vacation and sick days. The staffing level should always be rounded up to the next integer value to ensure that staffing levels exceed the required time rather than fall short.

The following sample Exchange Operations task checklist indicates the level to which tasks should be detailed before staffing levels are calculated.

SAMPLE - Exchange Operations Task Checklist (per location)

Activity	Est. Time (hrs)	Frequency	Annual Work Effort
Planning			
Participation in next-version assessment discussions	8	Annually	8
Feedback from operations	2	Quarterly	8
SLA definitions	4	Annually	4
Operations documentation	1	Annually	1
Exchange Administration			
Backup and Restore	1	Daily	260
Perform regular backup	1	Daily	260
Backup Active Directory system state	1	Daily	260
Verify back up media	1	Monthly	12
Offsite back up media	1	Daily	260
Change backup media regularly	1	Daily	260
Set mailbox and message retention times on all client servers	1	Quarterly	4

Defragment mailbox and public folder stores	1	Monthly	12
Verify integrity of the mailbox and public folder stores	1	Weekly	52
Risk Management			
Identification	1	Annually	1
Analysis and prioritization	.5	Annually	.5
Mitigation and contingency planning	.5	Annually	.5
Additional Work as Assigned			
New projects	100	Annually	100
Help desk escalation support	1	Daily	260
Review open service tickets	2	Daily	520
On-site visit (travel time)	2	Monthly	24
Total			9791.5
Available Hours per Man Year			1635
Percentage of work consumed by Exchange tasks			599%

In this example, the organization determined that the total number of tasks requires 9,792 hours. Given that a full-time employee works 1,635 hours, this analysis suggests that the organization requires 600 percent of a single individual—or, more appropriately, six FTEs—to manage their Exchange organization. Note that this sample task list is for the operations team only. The customer has to perform the same analysis for the engineering and help desk teams, as well.

The number of positions also depends on the complexity and size of the organization. Small organizations may combine roles or omit them entirely, while large organizations may have multiple individuals in certain roles. For example, one large financial services corporation has a messaging team which manages resources for 45,000 users on a 24 hours a day, seven days a week basis. Their messaging services staff typically includes 30-32 individuals in the positions shown in the following table (whose roles and responsibilities are defined in "Defining Roles and Assigning Tasks" earlier in this topic).

Position title	Number of staff
Director	1
Manager, Messaging Operations	1
Sr. Operations Analyst	2

Operations Analyst	3
Assoc. Operations Analyst	0-1
Technicians	17
Manager, Messaging System Engineering	1
Sr. Operations Engineer	2
Operations Engineer	2
Assoc. Operations Engineer	1

Conclusion

To determine the number of engineers, administrators, and other support personnel that are required to manage a specific Exchange environment, you must carefully gather business requirements, consider a variety of factors, and, above all, plan. You can determine your required staffing level only after you determine the needs of the user community, define the roles to fulfill those needs, assess the technology, match the technology to the roles, and then, finally, calculate the time required to perform the desired tasks. It's an involved process, but the ultimate results should closely align the capabilities of the messaging team to the needs of the business (and users) without unnecessarily encumbering either organization or team with superfluous head count.

1.2.1.7 Planning Active Directory

Planning Active Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-07-19*

Microsoft Exchange Server 2010 uses Active Directory to store and share directory information with Microsoft Windows.

Active Directory forest design for Exchange 2010 is similar to Exchange 2007. The main change in Active Directory for Exchange 2010 is in the introduction of Role Based Access Control (RBAC). In Exchange 2007, Active Directory provides ways for you to delegate administrative authority to directory objects by using access control lists (ACLs). In Exchange 2010, you don't need to modify and manage ACLs. RBAC enables you to control, at both broad and granular levels, what administrators and end-users can do. For more information about RBAC, see Understanding Role Based Access Control.

Active Directory and a New Exchange 2010 Organization

For more information about planning for Active Directory in a new Exchange 2010 organization, see the following topics:

- Prepare Active Directory and Domains
- Understanding the Active Directory Driver
- Planning for Access to Active Directory
- Planning to Use Active Directory Sites for Routing Mail

Active Directory and Legacy Exchange Organizations

For more information about planning for Active Directory when your organization includes legacy versions of Exchange, see the following topics:

- Exchange 2010 Active Directory Schema Changes
- Prepare Active Directory and Domains
- Understanding the Active Directory Driver
- Planning for Access to Active Directory
- Planning to Use Active Directory Sites for Routing Mail
- Prepare Legacy Exchange 2003 Permissions
- Exchange Server 2003 and Active Directory
- Discontinued Features

For More Information

For comprehensive Active Directory deployment information, see the Windows Server 2003 Deployment Guide.

For more information about Active Directory forest design for your Exchange organization, see Guidance on Active Directory design for Exchange Server 2007 at the Exchange Team Blog.

Note:

The content of each blog and its URL are subject to change without notice. The content within each blog is provided "AS IS" with no warranties, and confers no rights. Use of included script samples or code is subject to the terms specified in the Microsoft Terms of Use.

1.2.1.7.1 Determine the Exchange Schema Version

Determine the Exchange Schema Version

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-12-26*

To verify that the Exchange schema version has been updated correctly, determine the value of the **rangeUpper** attribute on the property page of the **ms-Exch-Schema-Version-Pt** schema attribute.

To look up the value of the rangeUpper attribute, use a tool such as ADSI Edit, LDP.exe, or DSQuery.

What Do You Want to Do?

- Determine the Exchange Schema version by using ADSI Edit
- Determine the Exchange Schema version by using LDP.exe
- Determine the Exchange Schema version by using DSQuery

Determine the Exchange schema version

by using ADSI Edit

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Organization Management" entry in the Understanding Management Role Groups topic.

1. Sign on to a domain controller in your Active Directory forest.
2. Click **Start**, click **Run**, type **ADSIEdit.msc**, and then click **OK**.
3. In the ADSI Edit console, right-click **ADSI Edit** in the navigation pane, and then click **Connect to**.
4. In the **Connection Settings** dialog box, select **Schema** in the **Select a well known Naming Context** list, and then click **OK**.
5. Expand the schema node in the navigation pane, and then click **CN=Schema,CN=Configuration,DC=contoso,DC=com**.
6. Right-click **CN=ms-Exch-Schema-Version-Pt**, and then click **Properties**.
7. On the property page, locate **rangeUpper** in the **Attribute** list.
8. Verify that the value is correct for the expected Exchange Schema.

Note:

To view the schema version table, see Exchange Server Build Numbers and Release Dates

Determine the Exchange schema version by using LDP.exe

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Organization Management" entry in the Understanding Management Role Groups topic.

1. Sign on to a domain controller in the Active Directory Forest.
2. Click **Start**, click **Run**, type **LDP.exe**, and then click **OK**.
3. In **Ldp**, click **Bind** on the **Connection** menu.
4. In the **Bind type** area, click **Bind as currently logged on user**, and then click **OK**.
5. On the **View** menu, click **Tree**.
6. In the **Tree View** dialog box, select **CN=Schema,CN=Configuration,DC=contoso,DC=com**in the **BaseDN** list, and then click **OK**.
7. Expand the schema node in the navigation pane, and then click **ms-Exch-Schema-Version-Pt**.

   Note:

   If the **ms-Exch-Schema-Version-Pt** schema attribute is not listed, click **General** on the **Options** menu, increase the value of the **Max children** buffer size, click **OK**, and then repeat step 5.
8. In the right pane, scroll down to the bottom and locate the **rangeUpper** attribute.
9. Verify that the value is correct for the expected Exchange schema.

Note:

To view the schema version table, see Exchange Server Build Numbers and Release Dates

Determine the Exchange schema version by using DSQuery

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Organization Management" entry in the Understanding

Management Role Groups topic.

1. Sign on to a domain controller in the Active Directory forest.
2. At a command prompt, type the following command, and then press Enter:
   dsquery * CN=ms-Exch-Schema-Version-Pt,cn=schema,cn=configuration,dc=<Domain>,dc=<local> -scope base -attr rangeUpper

For More Information

Dsquery

DSQUERY Commands

1.2.1.7.2 Exchange 2010 Active Directory Schema Changes

Exchange 2010 Active Directory Schema Changes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

Microsoft Exchange Server 2010 adds new attributes to the Active Directory domain service schema and also makes other modifications to existing classes and attributes. For more information about Active Directory changes when you install Exchange 2010, as well as changes from previous versions of Exchange, see Exchange Server Changes to the Active Directory Schema.

1.2.1.7.3 Prepare Active Directory and Domains

Prepare Active Directory and Domains

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-01-04*

Before you install Microsoft Exchange Server 2010 on any servers in your organization, you must prepare Active Directory and domains.

For information about preparing your domains with legacy Exchange permissions, see Prepare Legacy Exchange 2003 Permissions.

Prerequisites

- The computers on which you plan to install Exchange 2010 must meet the system requirements. For details, see Exchange 2010 System Requirements.
- Your domains and the domain controllers must meet the system requirements in "Network and Directory Servers" in Exchange 2010 System Requirements.
- In each domain in which you install Exchange 2010, you must have at least one domain controller running any of the following:
  - Windows Server 2003 Standard Edition with Service Pack 1 (SP1) or later (32-bit or 64-bit)

- Windows Server 2003 Enterprise Edition with SP1 or later (32-bit or 64-bit)
- Windows Server 2008 Standard or Enterprise (32-bit or 64-bit)
- Windows Server 2008 R2 Standard or Enterprise

- For multiple domain organizations running the following /Prepare* commands, we recommend the following:
  - Run the /Prepare* commands from an Active Directory site with an Active Directory server from every domain.
  - Run the first server role installation or Exchange 2010 service pack upgrade from an Active Directory site with a writeable global catalog server from every domain.
  - Verify that replication of objects from the preceding actions is completed on the global catalog server in the Active Directory site before installing the first Exchange 2010 server (or SP1 upgrade) to that site.
- If you're running the release to manufacturing (RTM) version of Exchange 2010 Setup.com, in each domain (including child domains) where you have the Exchange Enterprise Servers and Exchange Domains Servers security groups (and therefore must run **Setup /PrepareLegacyExchangePermissions**), you must have at least one domain controller running any of the following:
  - Windows Server 2003 Standard Edition with SP1 or later (32-bit or 64-bit)
  - Windows Server 2003 Enterprise Edition with SP1 or later (32-bit or 64-bit)
  - Windows Server 2008 Standard or Enterprise (32-bit or 64-bit)
  - Windows Server 2008 R2 Standard or Enterprise
- If you run the Exchange 2010 Setup wizard with an account that has the permissions required (Schema Admins, Domain Admins, and Enterprise Admins) to prepare Active Directory and the domain, the wizard will automatically prepare Active Directory and the domain. For more information, see Install Exchange Server 2010. However, if you're deploying a new Exchange organization, and you're preparing your Active Directory schema and domains using a computer running Windows Server 2008, you must first install the Active Directory management tools on the Windows Server 2008 computer prior to preparing the schema or domains. To do this, run the following command.

```
ServerManagerCmd -i RSAT-ADDS
```

Prepare Active Directory and domains

To track the progress of Active Directory replication, you can use the Active Directory Replication Monitor tool (replmon.exe), which is installed as part of the Windows Server 2003 Support Tools Setup. By default, it's located at %programfiles%\support tools\. Add your domain controllers as monitored servers so that you can track the progress of replication throughout the domain.

1. If you have any computers in your organization running Microsoft Exchange Server 2003, open a Command Prompt window, and then run one of the following commands:
   - To prepare legacy Exchange permissions in every domain in the forest that contains the Exchange Enterprise Servers and Exchange Domain Servers groups, run the following command.

     setup /PrepareLegacyExchangePermissions or **setup /pl**
   - To prepare legacy Exchange permissions in a specific domain, run the following command.

     setup /PrepareLegacyExchangePermissions:< *FQDN of domain you want to prepare* **>** or **setup /pl:<***FQDN of domain you want to prepare***>**

Note:

You can skip this step and prepare the legacy Exchange permissions as part of Step 2 or Step 3. The advantages of running each step separately are

that you can run each step with an account that has the minimum permissions required for that step, and you can verify completion, success, and replication before continuing to the next step.

Note the following:

- To run this command to prepare every domain in the forest, you must be a member of the Enterprise Admins group. To run this command to prepare a specific domain, or if the forest has only one domain, you must be delegated the Exchange Organization Management role, and you must be a member of the Domain Admins group in the domain that you will prepare.
- If you don't specify a domain, the domain in which you run this command must be able to contact all domains in the forest. If the server can't contact a domain that must have legacy Exchange permissions prepared, it prepares the domains that it can contact, and then returns an error message that it was unable to contact some domains.
- You can run this command from any Windows Server 2008 server in the forest.
- You must run this command on a computer in the same domain and in the same Active Directory site as the schema master. Setup will make all configuration changes to the schema master to avoid conflicts because of replication latency. For more information, see Identify the schema master.
- After you run this command, you must wait for the permissions to replicate across your Exchange organization before continuing to the next step. If the permissions haven't replicated, the Recipient Update Service on your Exchange 2003 computers could fail. The amount of time that replication takes depends on your Active Directory site topology.
- For detailed information about the permissions set by this command, see Prepare Legacy Exchange 2003 Permissions.

2. From a Command Prompt window, run the following command.
setup /PrepareSchema or **setup /ps**

Note:
You can skip this step and prepare the schema as part of Step 3.

Important:
If you have multiple forests in your organization, make sure that you run your forest preparation from the correct Exchange forest. Setup preparation makes configuration changes to your forest, and it could configure a non-Exchange forest incorrectly.

Note:
It isn't supported to use the LDIF Directory Exchange tool (LDIFDE) to manually import the Exchange 2010 schema changes. You must use Setup to update the schema.

This command performs the following tasks:

- Connects to the schema master and imports LDAP Data Interchange Format (LDIF) files to update the schema with Exchange 2010 specific attributes. The LDIF files are copied to the Temp directory, and then deleted after they are imported into the schema.

Note the following:

- To run this command, you must be a member of the Schema Admins group and the Enterprise Admins group.
- You must run this command on a 64-bit computer in the same domain and in the same Active Directory site as the schema master.
- If you haven't completed Step 1, **setup /PrepareSchema** will automatically perform the **PrepareLegacyExchangePermissions** step. To complete the **PrepareLegacyExchangePermissions** step, the domain in which you run this command must be able to contact all domains in the forest. The advantages of running each step separately are that you can run each step with an account that has the minimum permissions required for that

step, and you can verify completion, success, and replication before continuing to the next step.

- If you use the */DomainController* parameter with this command, you must specify the domain controller that is the schema master.
- After you run this command, you should wait for the changes to replicate across your Exchange organization before continuing to the next step. The amount of time this takes is dependent upon your Active Directory site topology.
- For more information, see Exchange Server Changes to the Active Directory Schema.

3. From a Command Prompt window, run the following command.
setup /PrepareAD [/OrganizationName: <*organization name*> **]** or **setup /p [/on:<***organization name***>]**
This command performs the following tasks:
   - If the Microsoft Exchange container doesn't exist, this command creates it under CN=Services,CN=Configuration,DC=<*root domain*>.
   - If no Exchange organization container exists under CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain* >, you must specify an organization name using the */OrganizationName* parameter. The organization container will be created with the name that you specify.
     The Exchange organization name can contain only the following characters:
     A through Z
     a through z
     0 through 9
     Space (not leading or trailing)
     Hyphen or dash
     The organization name can't contain more than 64 characters.
     The organization name can't be blank. If the organization name contains spaces, you must enclose the name in quotation marks (").
   - Verifies that the schema has been updated and that the organization is up to date by checking the **objectVersion** property in Active Directory. The **objectVersion** property is in the CN=<*your organization*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*domain*> container. The **objectVersion** value for Exchange 2010 SP2 is 14247. The **objectVersion** value for Exchange 2010 SP1 is 13214. The **objectVersion** value for Exchange 2010 RTM is 12640.
   - If the containers don't exist, creates the following containers and objects under CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>, which are required for Exchange 2010:
     CN=Address Lists Container,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
     CN=Addressing,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
     CN=Administrative Groups,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
     CN=Client Access,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
     CN=Connections,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
     CN=ELC Folders,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
     CN=ELC Mailbox Policies,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
     CN=Global Settings,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>

CN=Mobile Mailbox Policies,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
CN=Recipient Policies,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
CN=System Policies,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
CN=Transport Settings,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
CN=UM AutoAttendant,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
CN=UM DialPlan,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
CN=UM IPGateway,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>
CN=UM Mailbox Policies,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>

- If it doesn't exist, creates the default Accepted Domains entry, based on the forest root namespace, under CN=Transport Settings,CN=<*Organization Name*>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*>.
- Assigns specific permissions throughout the configuration partition.
- Imports the Rights.ldf file. This adds the extended rights required for Exchange to install into Active Directory.
- Creates the Microsoft Exchange Security Groups organizational unit (OU) in the root domain of the forest and assigns specific permissions on this OU.
- Creates the following management role groups within the Microsoft Exchange Security Groups OU:

  Organization Management
  Recipient Management
  Server Management
  View-Only Organization Management
  Public Folder Management
  UM Management
  Hygiene Management
  Records Management
  Discovery Management
  Delegated Setup
  Exchange All Hosted Organizations
  Exchange Servers
  Exchange Trusted Subsystem
  Exchange Windows Permissions
  Help Desk
  ExchangeLegacyInterop

- Adds the new universal security groups (USGs) that are within the Microsoft Exchange Security Groups OU to the **otherWellKnownObjects** attribute stored on the CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*root domain*> container.
- Creates the Unified Messaging Voice Originator contact in the Microsoft Exchange System Objects container of the root domain.
- Prepares the local domain for Exchange 2010. For information about what tasks are completed to prepare a domain, see Step 4.

Note the following:

- To run this command, you must be a member of the Enterprise Admins group.
- The computer where you run this command must be able to contact all domains in the forest on port 389.
- You must run this command on a computer in the same domain and in the same Active Directory site as the schema master. Setup will make all configuration changes to the schema master to avoid conflicts because of

replication latency.

- If you haven't completed Step 1, **setup /PrepareAD** will automatically perform the **PrepareLegacyExchangePermissions** step. To complete the **PrepareLegacyExchangePermissions** step, the domain in which you run this command must be able to contact all domains in the forest. If you're also a member of the Schema Admins group, and if you haven't completed Step 2, **setup /PrepareAD** will automatically perform the PrepareSchema step. The advantages of running each step separately are that you can run each step with an account that has the minimum permissions required for that step, and you can verify completion, success, and replication before continuing to the next step.
- After you run this command, you should wait for the changes to replicate across your Exchange organization before continuing to the next step. The amount of time this takes is dependent upon your Active Directory site topology.
- To verify that this step completed successfully, make sure that there is a new OU in the root domain called **Microsoft Exchange Security Groups**. This OU should contain the following new Exchange USGs:

  Exchange Security Groups OU:
  Organization Management
  Recipient Management
  Server Management
  View-Only Organization Management
  Public Folder Management
  UM Management
  Hygiene Management
  Records Management
  Discovery Management
  Delegated Setup
  Exchange All Hosted Organizations
  Exchange Servers
  Exchange Trusted Subsystem
  Exchange Windows Permissions
  Help Desk
  ExchangeLegacyInterop

4. From a Command Prompt window, run one of the following commands:
   - Run **setup /PrepareDomain** or **setup /pd** to prepare the local domain. You don't need to run this in the domain where you ran Step 3. Running **setup /PrepareAD** prepares the local domain.
   - Run **setup /PrepareDomain:**<*FQDN of domain you want to prepare*> to prepare a specific domain.
   - Run **setup /PrepareAllDomains** or **setup /pad** to prepare all domains in your organization.

   These commands perform the following tasks:
   - If this is a new organization, creates the Microsoft Exchange System Objects container in the root domain partition in Active Directory and sets permissions on this container for the Exchange Servers, Exchange Organization Administrators, and Authenticated Users groups. This container is used to store public folder proxy objects and Exchange-related system objects, such as the mailbox database's mailbox.
   - Sets the **objectVersion** property in the Microsoft Exchange System Objects container under DC=<*root domain*>. This **objectVersion** property contains the version of domain preparation. The version for Exchange 2010 RTM is 12640. The version for Exchange 2010 SP1 and SP2 is 13040.
   - Creates a domain global group in the current domain called Exchange Install Domain Servers. The command places this group in the Microsoft Exchange System Objects container. It also adds the Exchange Install Domain Servers group to the Exchange Servers USG in the root domain.

   Note:

The Exchange Install Domain Servers group is used if you install Exchange 2010 in a child domain that is an Active Directory site other than the root domain. The creation of this group allows you to avoid installation errors if group memberships haven't replicated to the child domain.

- Assigns permissions at the domain level for the Exchange Servers USG and the Exchange Recipient Administrators USG.

Note the following:

- To run **setup /PrepareAllDomains**, you must be a member of the Enterprise Admins group.
- To run **setup /PrepareDomain**, if the domain that you're preparing existed before you ran **setup /PrepareAD**, you must be a member of the Domain Admins group in the domain. If the domain that you're preparing was created after you ran **setup /PrepareAD**, you must be a member of the Exchange Organization Administrators group, and you must be a member of the Domain Admins group in the domain.
- For domains in an Active Directory site other than the root domain, **/PrepareDomain** might fail with the following messages:
  "PrepareDomain for domain <*YourDomain*> has partially completed. Because of the Active Directory site configuration, you must wait at least 15 minutes for replication to occur, and run PrepareDomain for <*YourDomain*> again."
  "Active Directory operation failed on <*YourServer*>. This error is not retriable. Additional information: The specified group type is invalid.
  Active Directory response: 00002141: SvcErr: DSID-031A0FC0, problem 5003 (WILL_NOT_PERFORM), data 0
  The server cannot handle directory requests."
  If you see these messages, wait for or force Active Directory replication between this domain and the root domain, and then run **/PrepareDomain** again.
- You must run this command in every domain in which you will install Exchange 2010. You must also run this command in every domain that will contain mail-enabled users, even if the domain doesn't have Exchange 2010 installed.

To verify that this step completed successfully, confirm the following:

- You have a new global group in the Microsoft Exchange System Objects container called Exchange Install Domain Servers.

Note:
To view the Microsoft Exchange System Objects container in Active Directory Users and Computers, on the **View** menu, click **Advanced Features**.

- The Exchange Install Domain Servers group is a member of the Exchange Servers USG in the root domain.
- On each domain controller in a domain in which you will install Exchange 2010, the Exchange Servers USG has permissions on the Domain Controller Security Policy\Local Policies\User Rights Assignment\Manage Auditing and Security Log policy.

1.2.1.7.4 Understanding the Active Directory Driver

Understanding the Active Directory Driver

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-02*

The Active Directory driver is the core Microsoft Exchange component that allows Exchange services to create, modify, delete, and query for Active Directory Domain Services (AD DS) data. The Active Directory driver also uses Microsoft Exchange Active Directory Topology (MSExchangeADTopology), which allows the Active Directory driver to use Directory Service Access (DSAccess) topology data. This data includes the list of available domain controllers and global catalog servers available to handle Exchange requests. This topic discusses the relationship between the Active Directory driver and DSAccess.

DSAccess provides directory lookup services for components such as SMTP, message transfer agent (MTA), and the Exchange store. Client requests use the DSProxy service for directory access.

DSAccess implementation has several benefits that Exchange components use, especially related to topology discovery and simplification of Active Directory topology complexity. DSAccess also has several limitations related to paging of results, especially in dealing with large multivalued attributes. One of the major differences between the Active Directory driver and DSAccess is that the Active Directory driver doesn't access and store directory information in a cache. In Microsoft Exchange Server 2010, the Exchange component using DSAccess implements the appropriate cache when needed.

In Exchange 2010, the following services use DSAccess. In these cases, DSAccess is used only to obtain the current topology information and to provide a consistent topology view through all Exchange services running on the server:

- Microsoft Exchange Active Directory Topology (MSExchangeADTopology)
- Microsoft Exchange Information Store (MSExchangeIS)
- Microsoft Exchange System Attendant (MSExchangeSA)
- World Wide Web Publishing Service (WWW service or W3SVC)

1.2.1.7.5 Planning for Access to Active Directory

Planning for Access to Active Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Microsoft Exchange Server 2010 stores all configuration and recipient information in the Active Directory directory service database. When a computer that is running Exchange 2010 requires information about recipients and information about the configuration of the Exchange organization, it must query Active Directory to access the information. Active Directory servers must be available for Exchange 2010 to function correctly.

This topic explains how Exchange 2010 stores and retrieves information in Active Directory

so that you can plan access to Active Directory. This topic also discusses issues you should be aware of if you try to recover deleted Exchange 2010 Active Directory objects.

Exchange Information Stored in Active Directory

The Active Directory database stores information in three types of logical partitions that are described in the following sections:

- The schema partition
- The configuration partition
- The domain partition

The Schema Partition

The schema partition stores two types of information: schema classes and schema attributes. Schema classes define all the types of objects that can be created and stored in Active Directory. Schema attributes define all the properties that can be used to describe the objects that are stored in Active Directory.

When you install the first Exchange 2010 server role in the forest or run the Active Directory preparation process, the Active Directory preparation process adds many classes and attributes to the Active Directory schema. The classes that are added to the schema are used to create Exchange-specific objects, such as agents and connectors. The attributes that are added to the schema are used to configure the Exchange-specific objects and the mail-enabled users and groups. These attributes include properties, such as Microsoft Office Outlook Web Access settings and Microsoft Exchange Unified Messaging (UM) settings. Every domain controller and global catalog server in the forest contains a complete replica of the schema partition.

For more information about schema modifications in Exchange 2010, see Exchange 2010 Active Directory Schema Changes.

The Configuration Partition

The configuration partition stores information about the forest-wide configuration. This configuration information includes the configuration of Active Directory sites, Exchange global settings, transport settings, mailbox policies, and UM dial plans. Each type of configuration information is stored in a container in the configuration partition. Exchange configuration information is stored in a subfolder under the configuration partition's Services container. The information that is stored in this container includes the following:

- Address lists
- Address and display templates
- Administrative groups
- Client access settings
- Connections
- Messaging records management, mobile, and UM mailbox policies
- Global settings
- E-mail address policies
- System policies
- Transport settings

Every domain controller and global catalog server in the forest contains a complete replica of the configuration partition.

The Domain Partition

The domain partition stores information in default containers and in organizational units that are created by the Active Directory administrator. These containers hold the domain-specific objects. This data includes Exchange system objects and information about the computers, users, and groups in that domain. When Exchange 2010 is installed, Exchange

updates the objects in this partition to support Exchange functionality. This functionality affects how recipient information is stored and accessed.

Each domain controller contains a complete replica of the domain partition for the domain for which it is authoritative. Every global catalog server in the forest contains a subset of the information in every domain partition in the forest.

How Exchange 2010 Accesses Information in Active Directory

Exchange 2010 uses an Active Directory API to access information that is stored in Active Directory. The Active Directory Topology service runs on all Exchange 2010 server roles. This service reads information from all Active Directory partitions. The data that is retrieved is cached and is used by Exchange 2010 servers to discover the Active Directory site location of all Exchange services in the organization. For more information about topology and service discovery, see Planning to Use Active Directory Sites for Routing Mail.

Exchange 2010 is an Active Directory site-aware application that prefers to communicate with the directory servers that are located in the same site as the Exchange server to optimize network traffic. Each Exchange 2010 organizational server role must communicate with Active Directory to retrieve information about recipients and information about the other Exchange 2010 server roles. The data that each server role obtains is described in the following sections.

By default, whenever an Exchange 2010 server starts, it binds to a randomly selected domain controller and global catalog server in its own site. You can view the selected directory servers by viewing the properties of the Exchange 2010 server in the Exchange Management Console or by using the **Get-ExchangeServer** cmdlet in the Exchange Management Shell. You can also use the **Set-ExchangeServer** cmdlet to configure a static list of domain controllers to which an Exchange 2010 server should bind or a list of domain controllers that should be excluded.

Important:

A Windows Server 2008 domain controller can be configured as a read-only directory server. This configuration is useful when you want to deploy a domain controller or global catalog server in a remote site for authentication and authorization purposes, but you don't want to allow administrators in that site to write changes to Active Directory. However, you can't deploy an Exchange 2010 server in any site that contains only read-only directory servers.

Hub Transport Server Role

The Hub Transport server role contacts Active Directory when it performs message categorization. The categorizer must query Active Directory to perform recipient lookup and routing resolution. The information that the categorizer retrieves during recipient lookup includes the location of the recipient's mailbox and any restrictions or permissions that may apply to the recipient. The categorizer must also query Active Directory to expand the membership of distribution lists and to perform the Lightweight Directory Access Protocol (LDAP) query processing that is required when mail is sent to a dynamic distribution list.

During routing resolution, the categorizer uses the topology information that is cached by the Active Directory Topology service to discover the routing path for a message. The Hub Transport server uses Active Directory site configuration information to determine the location of other servers and connectors in the topology.

When the Hub Transport server has resolved the location of the recipient's mailbox, it uses Active Directory site information to locate the mailbox store. If the mailbox store is in the same Active Directory site as the Hub Transport server, the Hub Transport server delivers the message directly to the user's mailbox. If the mailbox store is in a different

Active Directory site than the Hub Transport server, the Hub Transport server delivers the message to a Hub Transport server in the remote Active Directory site.

The Hub Transport server stores all configuration information in Active Directory and accesses Active Directory to retrieve this information. The configuration information includes the details of any transport rules, journal rules, and connectors.

Client Access Server Role

The Client Access server role receives connections from the Internet for users who access their mailbox by using Outlook Web App, (POP3, IMAP4, or Microsoft Exchange ActiveSync). When a user connection is received, the Client Access server contacts Active Directory to authenticate the user and to determine the location of the user's mailbox server. If the user's mailbox is in the same Active Directory site as the Client Access server, the user is connected directly to their mailbox. If the user's mailbox is in a different Active Directory site than the Client Access server that received the initial connection, the connection is redirected to a Client Access server in the remote Active Directory site.

Unified Messaging Server Role

The Unified Messaging server role accesses Active Directory to retrieve global configuration information, such as dial plans, IP gateways, and hunt groups. When a message is received by the Unified Messaging server, it searches for Active Directory recipients to match the telephone number to a recipient address. When it has resolved this information, the Unified Messaging server can determine the location of the recipient's mailbox store and then submit the message to a Hub Transport server for routing to the mailbox.

Mailbox Server Role

The Mailbox server role stores configuration information about mailbox users and stores in Active Directory. Additionally, the configuration for agents, address lists, and policies is stored in Active Directory. The Mailbox server retrieves this information to enforce mailbox policies and global settings.

Edge Transport Server Role

The Edge Transport server role is deployed in the perimeter network and is not a domain member. The Edge Transport server doesn't have access to Active Directory and uses Active Directory Lightweight Directory Services (AD LDS, formerly known as Active Directory Application Mode or ADAM) to store schema and configuration information. You can create an Edge Subscription to subscribe the Edge Transport server to an Active Directory site. The Hub Transport servers in that Active Directory site use the Microsoft Exchange EdgeSync service to synchronize Active Directory data to AD LDS.

We recommend that you create an Edge Subscription for each Edge Transport server. This process will automatically provision the Send connectors that are required for end-to-end mail flow. You must create an Edge Subscription if you will be using the recipient lookup or safe list aggregation anti-spam features.

Recovery of Deleted Exchange Objects

Active Directory Recycle Bin helps minimize directory service downtime by enhancing your ability to preserve and recover accidentally deleted Active Directory objects without restoring Active Directory data from backups, restarting Active Directory Domain Services (AD DS), or rebooting domain controllers.

The most important thing to understand about recovering deleted Exchange-related Active Directory objects is that Exchange objects don't exist in isolation. For example, when you mail-enable a user, several different policies and links are calculated for the user based on your current Exchange configuration. Two problems that may arise when you restore a deleted Exchange configuration or recipient object are:

- **Collisions** Some Exchange attributes must be unique across a forest. For example, proxy (e-mail) addresses must not be the same for two different users. Active Directory doesn't enforce proxy address uniqueness—Exchange administrative tools check for uniqueness. Exchange e-mail address policies also automatically resolve possible conflicts in proxy address assignment based on deterministic rules. Therefore, it's possible to restore an Exchange user object and, as a result, create a collision with proxy addresses or other attributes that should be unique.
- **Misconfigurations** Exchange has automated rules that assign various policies or settings. If you delete a recipient, and then change the rules or policies, restoring an Exchange user object may result in a user being assigned to the wrong policy (or even to a policy that no longer exists).

The following guidelines will help you minimize problems or issues when you recover deleted Exchange -related objects:

- If you deleted an Exchange configuration object using Exchange management tools, do not restore the object. Instead, re-create the object using the Exchange management tools (Exchange Management Console or Exchange Management Shell).
- If you deleted an Exchange configuration object without using the Exchange management, recover them as soon as possible. The more administrative and configuration changes that have been made in the system since the deletion, the more likely it is that restoring the objects will result in misconfiguration.
- If you recover deleted Exchange recipients (contacts, users, or distribution groups), monitor closely for collisions and errors relating to the recovered objects. If Exchange policies or other configuration relating to recipients may have been modified since the deletion, re-apply current policies to the restored recipients to ensure that they are configured correctly.

For more information about using Active Directory Recycle Bin, see Active Directory Recycle Bin Step-by-Step Guide.

1.2.1.7.6 Planning to Use Active Directory Sites for Routing Mail

Planning to Use Active Directory Sites for Routing Mail

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-07*

Microsoft Exchange Server 2010 uses Active Directory site topology to determine how messages are transported in the organization. Exchange 2010 uses the existing Active Directory site topology to transport messages between server roles.

The Hub Transport server role provides message transport inside the Exchange organization. When you're deploying a pure Exchange 2010 organization, or introducing Exchange 2010 into a pure Exchange Server 2007 organization, no additional configuration is required to establish routing in the forest. If you're deploying Exchange 2010 in an existing Exchange Server 2003 organization, you must follow specific configuration steps to enable routing between Exchange 2010 and Exchange 2003. For more information about how to configure the Hub Transport server role for coexistence with Exchange 2003, see Upgrade from Exchange 2003 Transport.

Contents

Determining Site Membership

Overview of IP Site Links

Exchange 2010 Placement in Active Directory Sites

How Exchange 2010 Uses Site Membership

Exchange 2010 is a site-aware application. Site-aware applications can determine their own Active Directory site membership and the Active Directory site membership of other servers by querying Active Directory. Exchange 2010 uses site membership to determine which domain controllers and global catalog servers to use for processing Active Directory queries. Additionally, when a server running Exchange has to determine the Active Directory site membership of another Exchange server, it can query Active Directory to retrieve the site name.

In Exchange 2010, the Microsoft Exchange Active Directory Topology service is responsible for updating the site attribute of the Exchange server object. Because the Active Directory site membership is a server object attribute, Exchange doesn't have to query the Domain Name System (DNS) to resolve a server address to a subnet associated with an Active Directory site. Stamping the Active Directory site attribute on an Exchange server object also enables Active Directory site membership to be assigned to a server that isn't a domain member, such as a subscribed Edge Transport server.

The Exchange 2010 server roles use Active Directory site membership information as follows:

- **Mail submission** The Mailbox server role uses Active Directory site membership information to determine which Hub Transport servers are located in the same Active Directory site as the Mailbox servers with the same server version. The Mailbox server submits messages for routing and transport to a Hub Transport server that has the same Active Directory site membership and the same server version as the Mailbox server.
- **Mail delivery** The Hub Transport server performs recipient resolution and queries Active Directory to match an e-mail address to a recipient account. The recipient account information includes the fully qualified domain name (FQDN) of the user's Mailbox server. The Hub Transport server queries Active Directory to determine the Active Directory site of the user's Mailbox server. If the Mailbox server is in the same site as the Hub Transport server, it will deliver the message to that Mailbox server. Otherwise, it will relay the message to another Hub Transport server in the same site as the target Mailbox server for delivery.
- **Message routing** Exchange 2010 Hub Transport servers retrieve information from Active Directory to determine how mail should be routed inside the organization. When a message is submitted to the Microsoft Exchange Transport service, the categorizer uses the header information in the message to query Active Directory for information about where the message must be delivered. If the recipient's mailbox is located on a Mailbox server in the same Active Directory site as the Hub Transport server and the version of the Mailbox server matches the Hub Transport server, the message is delivered directly to that mailbox. If the recipient's mailbox is located on a Mailbox server that has a different server version than the Hub Transport server, the message is relayed to a Hub Transport server in the site that matches the version of the Mailbox server. If the recipient's mailbox is located on a Mailbox server in a different Active Directory site, the message is relayed to a Hub Transport server in that site and then delivered to the Mailbox server.
- **Unified Messaging message submission** The Unified Messaging server role

uses Active Directory site membership information to determine which Hub Transport servers are located in the same Active Directory site as the Unified Messaging server. The Unified Messaging server submits messages for routing to a Hub Transport server within the same Active Directory site. The Hub Transport server performs recipient resolution and queries Active Directory to match a telephone number, or another Unified Messaging property, to a recipient account. After the recipient resolution completes, the Hub transport server will deliver the message to the target mailbox in the same way as a regular e-mail message.

- **Client connections to Client Access server** When the Client Access server receives a user connection request, it queries Active Directory to determine which Mailbox server is hosting the user's mailbox. The Client Access server then retrieves the Active Directory site membership of that Mailbox server. If the Client Access server that received the initial user connection isn't located in the same site as the user's Mailbox server, the connection is redirected to a Client Access server in the same site as the Mailbox server.
- **Public folder referrals** Active Directory site membership and IP site link information is used to prioritize the list of servers used for public folder referrals. Users are directed first to the default public folder database for their mailbox database. If a replica of the public folder being accessed doesn't exist in the default public folder database, the Mailbox store where the default public folder database resides will provide a prioritized referral list of Mailbox servers that hold a replica to the client. Public folder databases in the same Active Directory site as the default public folder database are listed first, and additional referral locations are prioritized based on Active Directory site proximity. Active Directory site proximity is determined by aggregating the costs of the IP site links between the Active Directory site where the default public folder database resides and the Active Directory sites where public folder replicas exist. The list of referrals is prioritized from lowest cost to highest cost. The connecting client will try each referral in the list until a connection is made or all attempts fail.

Determining Site Membership

Active Directory clients assume site membership by matching their assigned IP address to a subnet defined in Active Directory Sites and Services and associated with an Active Directory site. The client then uses this information to determine which domain controllers and global catalog servers exist in that site and communicates with those directory servers for authentication and authorization purposes. Exchange 2010 takes advantage of this relationship by also preferring to retrieve information about recipients from directory servers in the same site as the Exchange 2010 server.

All computers that are part of the same Active Directory site are considered well connected, with a high-speed, reliable network connection. By default, when an Active Directory forest is first deployed, there's a single site named Default-First-Site-Name. If no other sites are manually configured by the administrator, all server and client computers in the forest are considered members of Default-First-Site-Name.

When more than one site is defined, the Active Directory administrator must define the subnets present in the organization and associate those subnets with Active Directory sites.

The Microsoft Exchange Active Directory Topology service checks the site membership attribute on the Exchange server object when the server starts. If the site attribute has to be updated, the Microsoft Exchange Active Directory Topology service stamps the attribute with the new value. The Microsoft Exchange Active Directory Topology service verifies the site attribute value every 15 minutes and updates the value if site membership has changed. The Microsoft Exchange Active Directory Topology service uses the Net Logon service to obtain current site membership. The Net Logon service updates

site membership every five minutes. This means that up to a 20 minute latency period may pass between the time that site membership changes and the new value is stamped on the site attribute.

Overview of IP Site Links

Relationships between Active Directory sites are defined by IP site links. The IP site link consists of two or more Active Directory sites. All Active Directory sites that are part of the link communicate at the same cost. The IP site link properties include a cost assignment, a schedule, and an interval. The schedule and interval properties are only used for determining Active Directory replication frequency. Exchange 2010 uses the cost assignment to determine the lowest cost route for traffic to follow when multiple paths exist to the destination. The cost of the route is determined by aggregating the cost of all site links in a transmission path. The Active Directory administrator assigns the cost to a link based on relative network speed and available bandwidth compared to other available connections.

By default, the Hub Transport server always tries a direct connection to a Hub Transport server in another Active Directory site. Messages in transport don't relay through each Hub Transport server in a site link path. However, Hub Transport servers in intermediate Active Directory sites along the routing path may perform message relay in the following scenarios:

- Direct relay between Hub Transport servers won't occur when a hub site exists along the least cost routing path. You can configure an Active Directory site as a hub site so that messages are routed to the hub site to be processed before the messages are relayed to the target server. Hub sites are discussed later in this topic.
- Exchange 2010 uses the routing path derived from IP site link information when communication to the destination Active Directory site fails. If no Hub Transport server in the destination Active Directory site responds, message delivery backs off along the least cost routing path until a connection is made to a Hub Transport server in an Active Directory site along the routing path. The messages are queued in that Active Directory site and the queue will be in a retry state. This behavior is called *queue at point of failure*.
- The Hub Transport server can also use the IP site link information to optimize routing of messages sent to multiple recipients. The Hub Transport server delays bifurcation of messages until it reaches a fork in the routing paths to the recipients. The bifurcated message is relayed to each recipient destination by a Hub Transport server in the Active Directory site that represents the fork in the individual routing paths. This functionality is called *delayed fan-out*.

Designating Hub Sites

By default, the Hub Transport servers located in Active Directory sites along the path between the source server and the destination server don't process or relay the messages. You can use the **Set-AdSite** cmdlet to override this behavior by configuring an Active Directory site as a hub site. When a hub site exists along the least cost routing path between two Hub Transport servers, the messages are routed to the hub site for processing before they are relayed to the destination server. For this routing behavior to occur, the hub site must exist along the least cost routing path between two Hub Transport servers. This configuration should only be used when it's required by the network topology, such as when firewalls exist between Active Directory sites and prevent direct relay of SMTP communications.

Setting an Exchange-Specific Cost on an IP Site Link

You can use the **Set-AdSiteLink** cmdlet in the Exchange Management Shell to configure an Exchange-specific cost to an Active Directory IP site link. The Exchange-specific cost is a separate attribute used instead of the Active Directory-assigned cost to determine the

Exchange routing path. This configuration is useful when the Active Directory IP site link costs don't result in an optimal Exchange message routing topology.

Setting Message Size Restrictions on IP Site Links

By default, Exchange 2010 doesn't impose a maximum message size limit on messages relayed between Hub Transport servers in different Active Directory sites. If you use the **Set-AdSiteLink** cmdlet to configure a maximum message size on an Active Directory IP site link, routing generates a non-delivery report (NDR) for any message that has a size larger than the maximum message size limit configured on any Active Directory site link in the least cost routing path. This configuration is useful for restricting the size of messages sent to remote Active Directory sites that must communicate over low-bandwidth connections.

Exchange 2010 Placement in Active Directory Sites

For message routing between Exchange 2010 roles to occur correctly, all roles deployed in the forest must belong to an Active Directory site. Make sure that the IP addresses that you have assigned are in subnets that are correctly associated with Active Directory sites.

The first step in planning the placement of Exchange 2010 servers in the Active Directory site topology is to document the current topology. Your documentation should include the following:

- Sites
- Subnets and their site association
- IP site links and their member sites
- IP site link costs
- Directory servers in each site
- Physical network connections
- Firewall locations

After you have diagrammed these objects, plan the placement of Exchange servers. Consider the following information when deciding where to put servers:

- A Hub Transport server must be able to communicate directly with a global catalog server to perform Active Directory lookups.
- Mailbox servers should be located in the same site as a Hub Transport server. We recommend that you deploy more than one Hub Transport server in each Active Directory site to provide load balancing and fault tolerance.
- Unified Messaging servers submit messages to a Hub Transport server for transport to a Mailbox server. A Unified Messaging server may be located in a hub site or near the IP or Voice over IP (VoIP) gateway or IP Private Branch eXchange (IP PBX). The Hub Transport server that has the same site membership as the Unified Messaging server will receive messages for transport and route the messages to other Hub Transport servers and Mailbox servers in the organization.
- Client Access servers provide a connectivity point to the Exchange organization for users who are accessing Exchange remotely. A Client Access server must be deployed in each site that contains Mailbox servers.

After you plan Exchange 2010 server placement, you may identify areas where you can modify the Active Directory site topology to improve communication flow. You may want to adjust IP site links and site link costs to optimize delayed fan-out and queue at point of failure. An efficient Active Directory topology doesn't require any changes to support Exchange 2010.

1.2.1.8 Understanding Disjoint Namespace Scenarios

Understanding Disjoint Namespace Scenarios

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-28*

This topic provides information about the concept of disjoint namespaces and the supported scenarios for deploying Microsoft Exchange Server 2010 in a domain that has a disjoint namespace.

First, some background. Every computer that is on the Internet has a Domain Name System (DNS) name. This is also known as the *machine name* or *host name*. Every computer running the Microsoft Windows operating system with networking capabilities also has a NetBIOS name.

A computer running Windows in an Active Directory directory service domain has both a DNS domain name and a NetBIOS domain name. The DNS domain name consists of one or more subdomains separated by a dot (**.**) and is terminated by a top-level domain name. For example, in the DNS domain name corp.contoso.com, the subdomains are corp and contoso, and the top-level domain name is com. Typically, the NetBIOS domain name is the subdomain of the DNS domain name. For example, if the DNS domain name is contoso.com, the NetBIOS domain name is contoso. If the DNS domain name is corp.contoso.com, the NetBIOS domain name is corp.

A computer in an Active Directory domain also has a primary DNS suffix and can have additional DNS suffixes. By default, the primary DNS suffix is the same as the DNS domain name. For detailed steps about how to change the primary DNS suffix, see the procedures later in this topic.

You define the DNS domain name and NetBIOS domain name of an Active Directory domain when you configure the first domain controller in the domain. For more information about configuring domain controllers, see Domain controller role: Configuring a domain controller.

The procedures in this topic describe how to view the following items on a computer that is running Windows Server 2008 or Windows Server 2003:

- DNS host name
- Primary DNS suffix
- DNS domain name
- NetBIOS name
- NetBIOS domain name

Disjoint Namespaces

In most domain topologies, the primary DNS suffix of the computers in the domain is the same as the DNS domain name.

In some cases, you may require these namespaces to be different. This is called a *disjoint namespace*. For example, a merger or acquisition may cause you to have a topology with a disjoint namespace. In addition, if DNS management in your company is split between administrators who manage Active Directory and administrators who manage networks, you may need to have a topology with a disjoint namespace.

A disjoint namespace scenario is one in which the primary DNS suffix of a computer does not match the DNS domain name where that computer resides. The computer with the

primary DNS suffix that does not match is said to be disjoint. Another disjoint namespace scenario occurs if the NetBIOS domain name of a domain controller does not match the DNS domain name.

Exchange 2010 and Disjoint Namespaces

In Microsoft Exchange 2010, there are three supported scenarios for deploying Exchange in a domain that has a disjoint namespace. The supported scenarios are as follows:

- **Scenario 1** The primary DNS suffix of the domain controller is not the same as the DNS domain name. Computers that are members of the domain can be either disjoint or not disjoint.
- **Scenario 2** A member computer in an Active Directory domain is disjoint, even though the domain controller is not disjoint.
- **Scenario 3** The NetBIOS domain name of the domain controller is not the same as the subdomain of the DNS domain name of that domain controller.

These scenarios are detailed in the following sections.

Note:

It is supported to run Exchange 2010 in the disjoint namespace scenarios described above. If you have a disjoint namespace scenario that is not one of the three scenarios described in this topic, you must work with Microsoft Services to deploy Exchange 2010. For more information, see Microsoft Services.

Scenario 1

In this scenario, the primary DNS suffix of the domain controller isn't the same as the DNS domain name. The domain controller is disjoint in this scenario. Computers that are members of the domain, including Exchange servers and Microsoft Outlook client computers, can have a primary DNS suffix that either matches the primary DNS suffix of the domain controller or matches the DNS domain name.

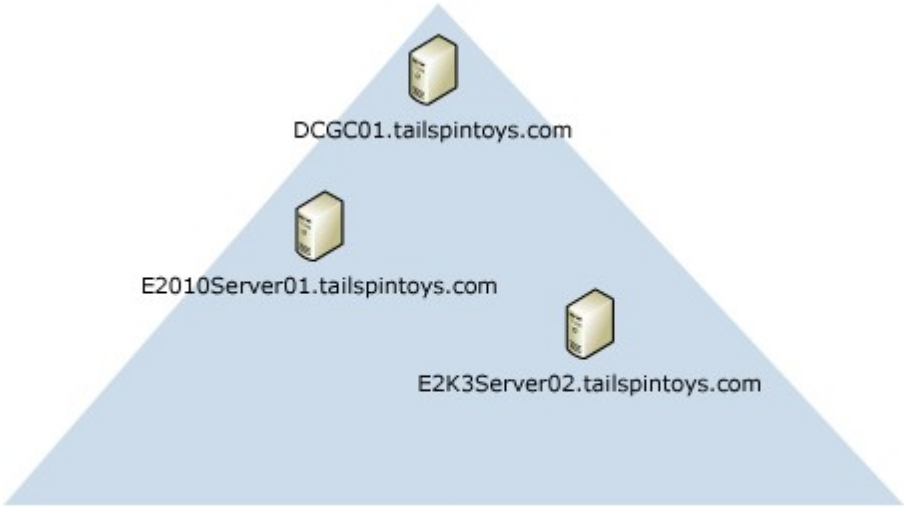
Scenario 2

In this scenario, the primary DNS suffix of a member computer on which Exchange 2010 is installed isn't the same as the DNS domain name, even though the primary DNS suffix of the domain controller is the same as the DNS domain name. In this scenario, you have a domain controller that isn't disjoint and a member computer that is disjoint. Member computers that are running Outlook can have a primary DNS suffix that either matches the primary DNS suffix of the disjoint Exchange server or matches the DNS domain name.

Scenario 3

In this scenario, the NetBIOS domain name of the domain controller isn't the same as the DNS domain name of the same domain controller.

NetBIOS domain name does not match DNS domain name



DNS domain name: tailspintoys.com
Primary DNS suffix for DCGC01, E2010Server01, and E2K3Server02: tailspintoys.com
NetBIOS domain name: CORP

Allow Exchange 2010 servers to access domain controllers that are disjoint

To allow Exchange 2010 servers to access domain controllers that are disjoint, you must modify the **msDS-AllowedDNSSuffixes** Active Directory attribute on the domain object container. You must add both of the DNS suffixes to the attribute. For detailed steps about how to modify the attribute, see The computer's primary DNS suffix does not match the FQDN of the domain where it resides.

In addition, to make sure that the DNS suffix search list contains all DNS namespaces that are deployed within the organization, you must configure the search list for each computer in the domain that is disjoint. The list of namespaces should include not only the primary DNS suffix of the domain controller and the DNS domain name, but also any additional namespaces for other servers with which Exchange may interoperate (such as monitoring servers or servers for third-party applications). You can do this by setting Group Policy for the domain. For more information about Group Policy, see the following topics:

- Group Policy Frequently Asked Questions (FAQ)
- New group policies for DNS in Windows Server 2003

For detailed steps about how to configure the DNS suffix search list Group Policy, see Configure the DNS Suffix Search List for a Disjoint Namespace.

View the DNS host name, primary DNS suffix, DNS domain name, NetBIOS name, and NetBIOS domain name of a computer running Windows Server 2008

1. Click **Start**, right-click **Computer**, and then click **Properties**.
2. In **System**, the DNS host name and primary DNS suffix are displayed under **Computer name, domain, and workgroup settings**, next to **Full computer name**. The DNS domain name is displayed next to **Domain**.
3. Click **Change settings**.
4. In **System Properties**, on the **Computer Name** tab, click **Change**.
5. In **Computer Name/Domain Changes**, click **More**. The primary DNS suffix is displayed under **Primary DNS suffix of this computer**. The NetBIOS computer name is displayed under **NetBIOS computer name**.
   To change the primary DNS suffix, type the new primary DNS suffix under **Primary DNS suffix of this computer**, and then click **OK**.
6. From a Command Prompt window, type **set**. The variable USERDNSDOMAIN displays the DNS domain name. The variable USERDOMAIN displays the

NetBIOS domain name.

View the DNS host name, primary DNS suffix, DNS domain name, NetBIOS name, and NetBIOS domain name of a computer running Windows Server 2003

1. Click **Start**, right-click **My Computer**, and then click **Properties**.
2. In **System Properties**, click the **Computer Name** tab. The DNS host name and primary DNS suffix are displayed next to **Full computer name**. The DNS domain name is displayed next to **Domain**.
3. On the **Computer Name** tab, click **Change**.
4. On the **Computer Name Changes** page, click **More**. The primary DNS suffix is displayed under **Primary DNS suffix of this computer**. The NetBIOS computer name is displayed under **NetBIOS computer name**.
   To change the primary DNS suffix, type the new primary DNS suffix under **Primary DNS suffix of this computer**, and then click **OK**.
5. From a Command Prompt window, type **set**. The variable USERDNSDOMAIN displays the DNS domain name. The variable USERDOMAIN displays the NetBIOS domain name.

Note:
You can also run the command **ipconfig /all** from a Command Prompt window to view the primary DNS suffix. However, if you have a policy that overrides the primary DNS suffix, this command will not display the correct primary DNS suffix.

1.2.1.8.1 Configure the DNS Suffix Search List for a Disjoint Namespace

Configure the DNS Suffix Search List for a Disjoint Namespace

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-08*

You can use the Group Policy Management console (GPMC) to configure the Domain Name System (DNS) suffix search list. In some Microsoft Exchange 2010 scenarios, if you have a disjoint namespace, you must configure the DNS suffix search list to include multiple DNS suffixes.

For more information about Group Policy, see Windows Server Group Policy. For more information about disjoint namespace scenarios, see Understanding Disjoint Namespace Scenarios.

Prerequisites

Confirm that you have installed .NET Framework 3.0 on the computer on which you will install GPMC.

Note:
The current version of GPMC that you can download from the Microsoft Download Center operates on the 32-bit versions of the Windows Server 2003 and Windows XP operating systems and can remotely manage Group Policy objects on 32-bit and 64-bit domain controllers. This version of GPMC doesn't include a 64-bit version, and the 32-bit version doesn't run on 64-bit platforms. The 32-bit version of Windows Server 2008 and the 32-bit version of Windows Vista both include a 32-bit version of GPMC. The 64-bit version of Windows Server 2008 and the 64-bit version of Windows Vista both include a 64-bit version of GPMC.

Configure DNS suffix search list

To perform this procedure, the account you use must be delegated membership in the Domain Admins group.

1. On a 32-bit computer in your domain, install GPMC with Service Pack 1 (SP1). For download information, see Group Policy Management Console with Service Pack 1.

   Note:
   If you have a computer in your domain running Windows Server 2008 or Windows Vista, you can skip this step.

2. Click **Start**, click **Programs**, click **Administrative Tools**, and then click **Group Policy Management**.
3. In **Group Policy Management**, expand the forest and the domain in which you will apply Group Policy. Right-click **Group Policy Objects**, and then click **New**.
4. In **New GPO**, type a name for the policy, and then click **OK**.
5. Right-click the new policy that you created in Step 4, and then click **Edit**.
6. In **Group Policy Management Editor**, expand **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Network**, and then click **DNS Client**.
7. Right-click **DNS Suffix Search List**, click **All Tasks**, and then click **Edit**.
8. On the **DNS Suffix Search List Properties** page, select **Enabled**. In the **DNS Suffixes** box, type the primary DNS suffix of the disjoint computer, the DNS domain name, and any additional namespaces for other servers with which Exchange may interoperate, such as monitoring servers or servers for third-party applications. Click **OK**.
9. In **Group Policy Management**, expand **Group Policy Objects**, and then select the policy that you created in Step 4. On the **Scope** tab, scope the policy so that it applies to only the computers that are disjoint.

1.2.1.9 Mailbox Server Storage Design

Mailbox Server Storage Design

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-08*

Storage design is a critical piece of a successful Microsoft Exchange Server 2010 Mailbox server role deployment. Multiple requirements such as storage performance, capacity, manageability, and cost must all be considered to achieve the optimal storage design for Exchange 2010. This section covers the storage design process as well as the storage design options, support criteria, and best practices related to the Exchange 2010 Mailbox server role. Information is also provided about required storage inputs and storage testing and validation.

Other topics in this section include:

Mailbox Storage Design Process

Understanding High Availability Factors

1.2.1.9.1 Mailbox Storage Design Process

Mailbox Storage Design Process

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

We recommend breaking the storage design process into three steps. The following sections provide detailed information about each of the design steps, including mailbox storage requirements and best practices.

Step 1: Gather Storage Input Requirements

Several Exchange 2010 architectural factors influence mailbox storage design. The following table lists the most important factors that affect mailbox storage design.

Architectural factors in mailbox storage design

Design factor	Description	Storage design impact
Mailbox count	The maximum number of mailboxes targeted to be hosted on a specific Mailbox server.	**Performance** More mailboxes equal more messages delivered and opened per server. This generates more log and database I/O. **Capacity** More mailboxes equal more capacity to store mailbox content. This affects the number of databases and size of databases per server. More mailboxes also equal more logs generated per server per day.

		Reliability In general, the more mailboxes hosted on the Mailbox server, the greater the need for high availability.
Mailbox concurrency	The percentage of users that connect to the Mailbox server at the same time measured over a one hour period.	**Performance** Higher concurrency equals more messages delivered and opened per server. This generates more log and database I/O. In general, 100 percent concurrency is used for standard information worker storage sizing. **Capacity** Higher concurrency equals more logs generated per server per day.
Mailbox size	The maximum mailbox quota per mailbox, for example, maximum mailbox size equals 10 GB. This includes capacity required for the primary mailbox, personal archive, and recoverable items (dumpster) data.	**Performance** Larger primary mailboxes equal more content to process for infrequent database operations, for example, full Microsoft Outlook offline folder files (.ost) sync and new view creation in Microsoft Office Outlook Web App. This can generate slightly more log and database I/O. **Capacity** Larger mailboxes equal more capacity to store mailbox content. This affects the number of databases and size of databases per server.
Mailbox usage profile	The usage characteristics of users on the Mailbox servers, generally defined as messages sent and received per day and average message size in kilobytes (KB).	**Performance** The more intensive the mailbox usage profile, the more log and database I/O that can be generated. **Capacity** A more intensive mailbox usage profile equals more logs generated per server per day.
E-mail client types	The types and percentages of different e-mail clients, for example, Outlook 2003 Cached Exchange Mode, Windows Mobile, Microsoft Exchange ActiveSync, and	**Performance** Different clients exhibit different performance characteristics on the server.

	Microsoft Office Outlook Web App.	
E-mail client extensions	Microsoft and third-party applications that extend the functionality of the e-mail client, for example, Office Communicator and Windows Desktop Search clients.	**Performance** Depending upon implementation, e-mail client extension applications can have a light to very heavy I/O impact on the Mailbox server database I/O.
Server applications	Applications that either run on or against Exchange Mailbox servers, for example, third-party mobile device applications and antivirus applications.	**Performance** Depending on implementation, server applications can have a light to very heavy I/O impact on Mailbox server database I/O.
High availability requirements	Whether Exchange 2010 high availability is used and how it's configured, for example, number of copies, number of sites, and lagged copies.	**Performance** High availability solutions may require slightly more I/O than non-high availability solutions to handle the additional log volume I/O produced by log replication. **Capacity** Using high availability increases the amount of database file storage required (depending upon the number of copies). If circular logging is used, log capacity may be reduced. Using high availability equals more logs generated per server per day. **Reliability** Deploying high availability increases the viable number of storage options. Less reliable storage, storage without RAID or just a bunch of disks (JBOD), may be used when multiple database copies are used in a high availability deployment.

For more information about the features mentioned in the preceding table, see the following topics:

- Understanding Database Availability Groups
- Understanding High Availability and Site Resilience
- Understanding Recoverable Items
- Understanding the Exchange 2010 Store
- Managing Mailbox Databases

Step 2: Design Storage Architecture Based on I/O and Capacity Requirements

After you've completed gathering the Exchange 2010 storage input requirements, you need to design your storage architecture based on I/O and capacity requirements. There are several ways to configure your storage architecture. You can calculate the requirements for the storage architecture manually, or you can use the Exchange 2010 Mailbox Server Role Requirements Calculator. Calculating your requirements manually requires a deeper understanding of mailbox storage design, which is provided by the topics listed in "Calculate the Mailbox Server Role Requirements Manually" later in this topic. When you use the Mailbox Server Role Calculator, it allows you to input your information, and then it provides a recommended best practice for your design.

Calculate the Mailbox Server Role Requirements Manually

Complete the following steps to derive your Mailbox server role architecture:

1. To determine your high availability model, see Understanding High Availability Factors.
2. To calculate your database and log capacity requirements, see Understanding Mailbox Database and Log Capacity Factors.
3. To determine your memory requirements, see Understanding the Mailbox Database Cache.
4. To calculate your database and log performance requirements, see Understanding Database and Log Performance Factors.
5. To determine your logical unit number (LUN) architecture based on your requirements, see Understanding Exchange 2010 LUN Architecture.
6. To determine your storage architecture based on your requirements, see Understanding Storage Configuration.
7. To determine your CPU requirements, see Mailbox Server Processor Capacity Planning.

To see how all this information comes together, review Exchange 2010 Mailbox Server Role Design Example.

Use the Mailbox Server Role Requirements Calculator

The Exchange 2010 Mailbox Server Role Requirements Calculator enables you to determine your requirements for the Mailbox server role by specifying a set of input factors. The calculator can determine the requirements for memory, storage (I/O performance, capacity, and storage configuration), optimal LUN layout, and CPU megacycles. Many variables need to be accounted for before you can design an optimal solution for an Exchange 2010 Mailbox server, and the calculator can help you in your design process. For more information about the calculator (and to download the calculator), see the Exchange Server Team Blog article Exchange 2010 Mailbox Server Role Requirements Calculator.

Note:

The content of each blog and its URL are subject to change without notice. The content within each blog is provided "AS IS" with no warranties, and confers no rights. Use of included script samples or code is subject to the terms specified in the Microsoft Terms of Use.

Step 3: Validate Storage for Performance and Reliability

Before implementing a storage solution in a production environment, it's important that you validate that the solution is configured correctly. This section provides guidance for successfully testing a storage solution for Exchange, beginning with a program that includes solutions that have already been tested.

In addition, you'll find information about several tools that can help you manage, test, and monitor your storage solution. For more information about understanding and troubleshooting I/O performance, see Understanding Database and Log Performance Factors.

Exchange Solution Reviewed Program

When selecting a storage solution, we recommend you choose a solution that has been reviewed by the Microsoft Exchange Solution Reviewed Program (ESRP) for storage, known as ESRP-Storage. ESRP-Storage is an Exchange-specific test, best practices publication framework, and review process to facilitate the creation of known, good Exchange storage solutions. The goals of ESRP-Storage are to:

- Provide storage vendors with prescriptive guidance about Exchange storage testing and best practices publication.
- Develop a mechanism to review storage solutions to make sure that they meet Exchange best practices.
- Provide customers with well-tested and high-quality storage solutions targeted for Exchange deployments.

For more information, see Microsoft Exchange Solution Reviewed Program (ESRP).

Note:
ESRP-Storage isn't a Microsoft certification, qualification, or logo program.

Because storage can be configured in many ways, evaluating tested configurations and using best practices can reduce costs and decrease the time to deployment.

Storage Testing

Before testing a solution, some work is required to understand what it is you're trying to achieve by testing. Some of the keys to successful storage testing include:

- Determine testing goals. For example, consider the performance, throughput, and capacity numbers needed.
- Test with as many servers attached to the storage as you will have in production. This includes non-Exchange servers and workloads.
- Test with production-size databases with the physical disk capacities filled to production level. Most physical disk performance characteristics will change based on the data set size.
- Determine that storage meets the transactional I/O requirements, and determine the maximum performance of the solution within acceptable latencies.
- Determine that storage meets the backup throughput and performance requirements to meet your backup and restore service level agreement (SLA).

Storage-Related Tools

The Microsoft Exchange Server Jetstress tool accurately simulates Exchange I/O characteristics. It includes both a stress test and a performance test, which show the maximum performance of a LUN within acceptable latencies. The Exchange Load Generator simulates Microsoft Office Outlook clients.

Both tools simulate Outlook. Simulating Outlook clients is the only way to measure actual client latency (rather than just the server disk latency). For more information about these tools, including how to download them, see Tools for Performance and Scalability Evaluation.

Important:
The Exchange Jetstress tool should be used on systems prior to placing production data on the server. Jetstress shouldn't be used on systems containing production data.

Important:
The Exchange Load Generator is intended for use in test environments, not in production environments.

Monitoring Server Storage Health

Monitoring your storage solution is critical in identifying hardware and software warnings and error conditions before they lead to data corruption or downtime.

The following tools can help monitor your storage solution. These tools are available in the **Toolbox** node of the Exchange Management Console:

- Best Practices Analyzer Tool
- Performance Monitor
- Performance Troubleshooter

In addition, you can also use Microsoft System Center Operations Manager 2007 to monitor your storage solution, as well as several other aspects of your Exchange organization.

Performance Monitor (perfmon.exe) is the Microsoft Management Console (MMC) performance snap-in for Exchange 2010. Perfmon, which uses the MSExchangeIS performance object to retrieve counter information, provides information that allows you to gauge the health of your storage solution. For more information, see Performance and Scalability Counters and Thresholds.

Monitoring Storage Solution Health

On many storage solutions, there's a way to see performance metrics. Monitoring these metrics can catch performance issues before they affect Exchange. If available, System Center Operations Manager 2007 integration from the storage vendor can assist in making sometimes proprietary metrics easy to understand. Some of the general metrics to watch include:

- **Disk Utilization Percentage** How busy are the physical disks?
- **Read Cache Hit Ratio** How well is the storage controller cache being utilized?
- **Write Pending Requests** How often is the controller waiting for the physical disk?
- **Storage Processor Utilization Percentage** How busy is the storage controller processor?

1.2.1.9.2 Understanding High Availability Factors

Understanding High Availability Factors

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-02*

When planning a highly available Mailbox server and database architecture, design decisions must be considered, such as:

- Will you deploy multiple database copies?
- How many database copies will you deploy?
- Will you have an architecture that provides site resilience?
- What kind of Mailbox server resiliency model will you deploy?
- How many Mailbox servers will you deploy?
- How will you distribute database copies?
- What backup model will you use?
- What storage architecture will you use?

Microsoft Exchange Server 2010 enables you to deploy your Mailbox server infrastructure using standalone Mailbox servers or Mailbox servers configured for mailbox resiliency. Mailbox servers configured for mailbox resiliency employ a database availability group (DAG) with multiple database copies efficiently distributed throughout the DAG. By deploying multiple database copies, you can:

- Design a solution that mitigates the most common reason for using a backup. Database copies provide protection against hardware, software, and data center failures.
- Increase database sizes up to 2 terabytes because your recovery mechanism is another database copy and not restoration from backup.
- Consider storage architecture alternatives to a traditional RAID configuration like just a bunch of disks (JBOD), if you deploy three or more database copies. The combination of JBOD and less expensive disks can result in cost savings for your organization.

By distributing active databases across all the servers that participate within a DAG, you can maximize the efficiency of your hardware.

For more detailed information, see Planning for High Availability and Site Resilience and Understanding Backup, Restore and Disaster Recovery.

Contents

Looking for management tasks related to high availability? See Managing High Availability and Site Resilience.

Planning the Number of Database Copies to Deploy

As discussed in Understanding Mailbox Database Copies, a DAG member can host one copy of each mailbox database, with a maximum of 100 databases per server in the Enterprise Edition of the product (both active and passive copies count toward this limit). This means that there is a limit of 1,600 databases supported by a 16-member DAG (100 database copies per server × 16 servers per DAG ÷ 1 copy per database = 1,600 databases per DAG).

In a high availability configuration, there's no value to deploying a single copy of a database because it doesn't provide data redundancy. You use a formula to determine the number of databases a specific DAG can support. For example, if you choose D to be the number of databases being deployed, C to be the number of copies of each database,

and S to be the number of servers, the following applies:

- D × C = total number of database copies in the DAG
- (D × C) ÷ S = database copies per server

Note:
The resulting number of databases per server must be 100 or less when using the Enterprise Edition and 5 or less when using the Standard Edition.

For example, let's assume that you have a DAG with 6 servers and 84 mailbox databases, with 3 copies of each database. (Note that 6 servers is an integer multiple of 3 copies.) The following applies:

- 84 databases × 3 copies = 252 databases total
- 252 databases ÷ 6 servers = 42 database copies per server

In another example, you have a DAG with 4 servers and 136 mailbox databases, with 3 copies of each database. The following applies:

- 136 databases × 3 copies = 408 databases total
- 408 databases ÷ 4 servers = 102 database copies per server

Because 102 is greater than 100, the proposed scenario isn't a valid DAG design.

Return to top

Database Copy Types

There are two types of database copies:

- Highly available database copies
- Lagged database copies

Highly available database copies are copies configured with a replay lag time of zero. As their name implies, highly available database copies are kept up-to-date by the system, can be automatically activated by the system, and are used to provide high availability for mailbox service and data.

Lagged database copies are copies configured to delay transaction log replay for a period of time. Lagged database copies are designed to provide point-in-time protection, which can be used to recover from store logical corruptions, administrative errors (for example, deleting or purging a disconnected mailbox), and automation errors (for example, bulk purging of disconnected mailboxes).

Typically, lagged database copies aren't activated due to the Active Manager Best Copy Selection algorithm. Because lagged database copies are deployed to mitigate operational risks, they shouldn't be activated. If activated and if a mount request is issued, log replay begins, replaying all required log files to bring the database up-to-date and in a clean shutdown state, thus losing the point-in-time capability.

For more information about how to block activation at the Mailbox server level or suspend activation for one or more database copies to prevent a database copy (such as a lagged database copy) from being automatically activated, see Set-MailboxServer and Suspend-MailboxDatabaseCopy.

Return to top

Site Resilience

Your environment may consist of multiple data centers. As part of your Exchange 2010 design, determine if you will deploy the Exchange infrastructure in a single data center or

distribute it across two or more data centers. Your organization's recovery service level agreements (SLAs) should define what level of service is required following a primary data center failure.

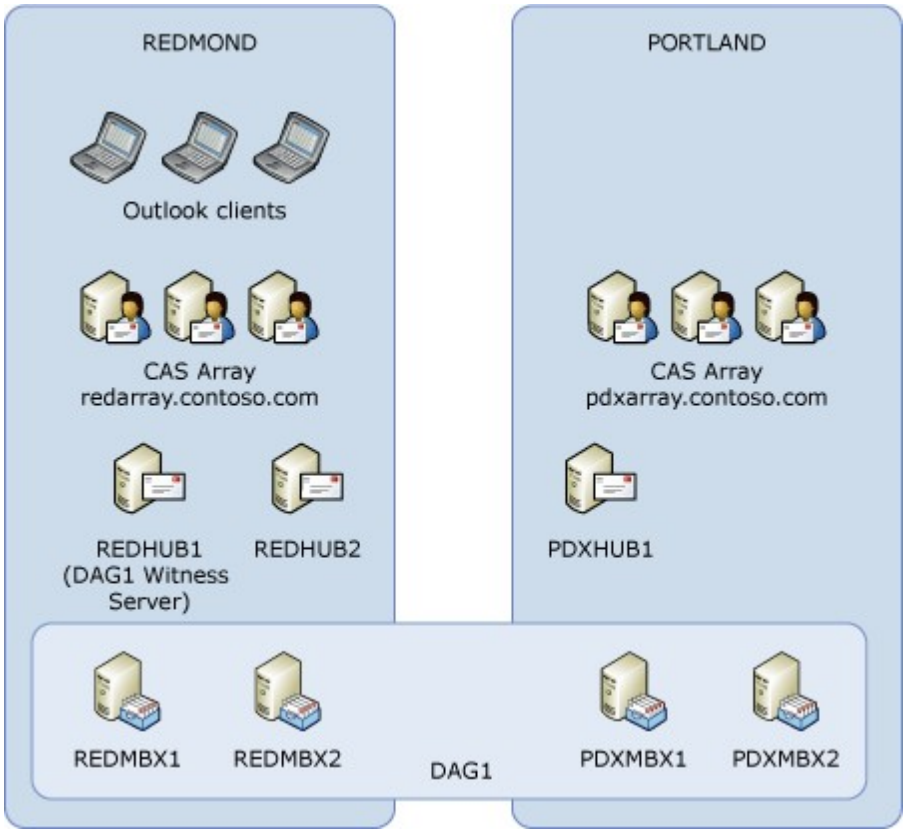
If your Exchange deployment will be deployed across multiple data centers to support site resilience goals, consider which user distribution model applies. There are two types of user distribution models, based on the mailbox locality with respect to the data center:

- Active/passive user distribution model
- Active/active user distribution model

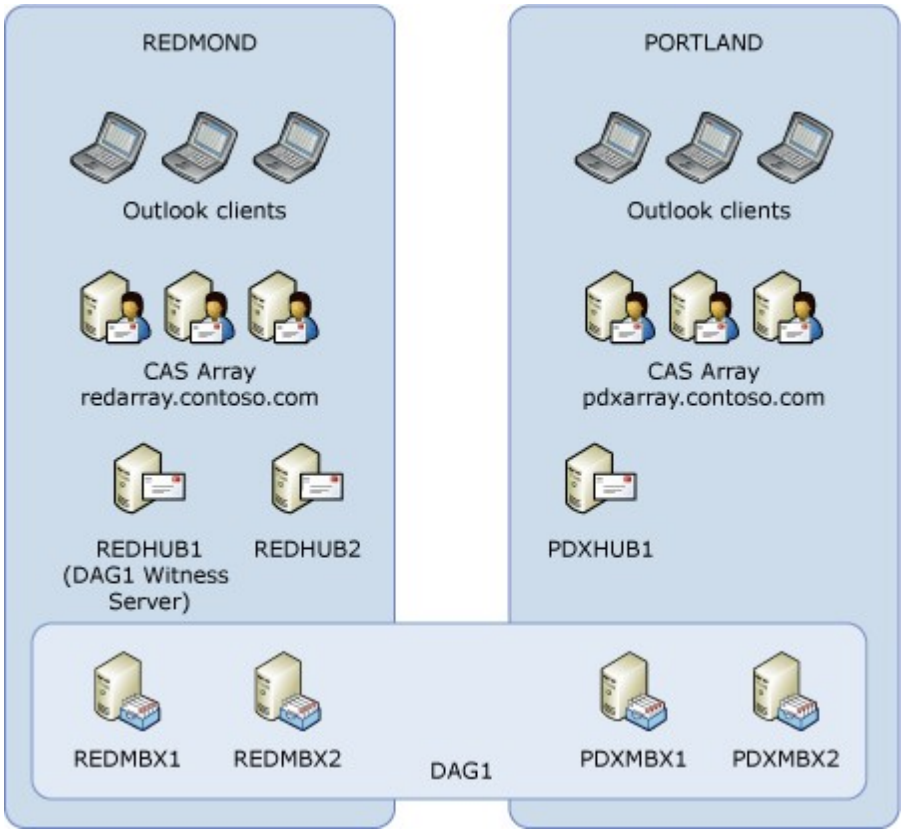
If user mailboxes are primarily located in a single data center (or if users access their data through a single data center) and there's an SLA requirement that the users continue to access their data via the primary data center during normal operations, your architecture is an active/passive user distribution model.

If user mailboxes are dispersed across data centers and there's an SLA requirement that the users continue to access their data via the primary data center during normal operations, your architecture is an active/active user distribution model.

In an active/passive user distribution model, you can deploy your architecture as shown in the following figure, where the active mailboxes are hosted from the primary data center, but database copies are deployed in the secondary data center.

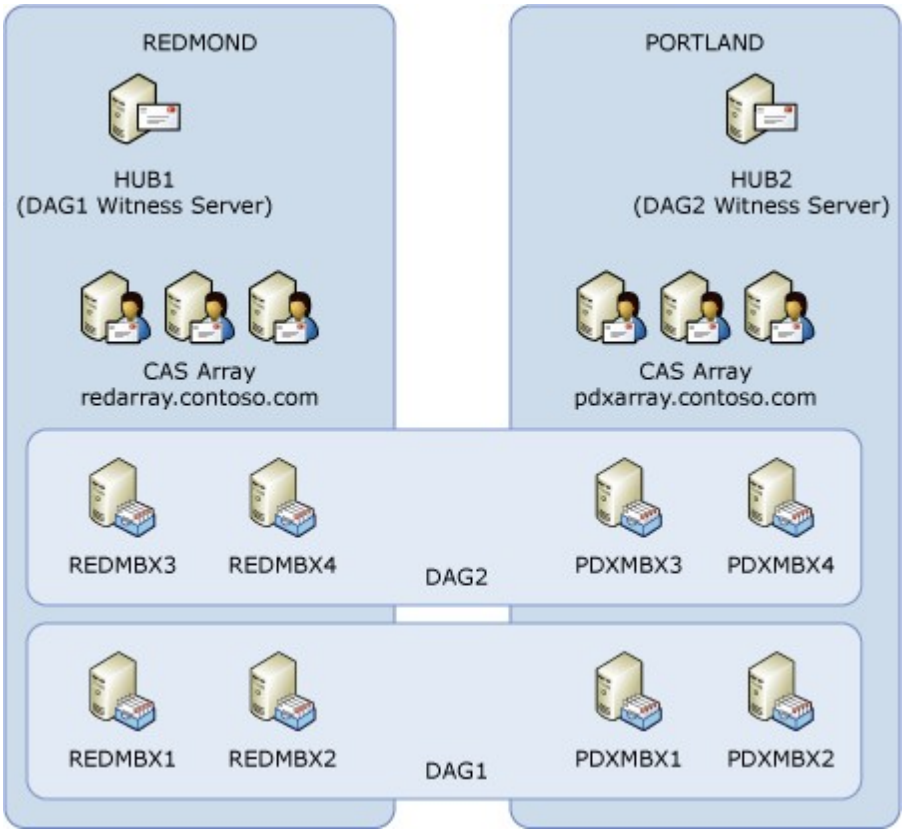


The architecture shown in the following figure could potentially be used for an active/ active user distribution model.



However, there's a risk with the architecture shown in the preceding figure. The wide area network (WAN) is a single point of failure for the DAG. The loss of the WAN will result in the loss of quorum for the DAG members in the second data center. In this example, the Windows failover cluster has a total of five votes (four DAG members plus the witness server), requiring three votes to be available at all times for the failover cluster to remain operational. Three of the votes are located in the Redmond data center, and two of the votes are located in the Portland data center. The loss of the WAN connection results in the Portland data center hosting only two of the votes, which isn't sufficient to maintain quorum. The Redmond data center has three votes, and thus can maintain quorum and continue to service the active mailboxes (as long as those three votes are operational).

To mitigate this risk for active/active user distribution models, we recommend deploying two DAGs, as shown in the following figure.



DAG1 hosts the active mailboxes for the Redmond data center and is implemented as an active/passive user distribution model, with passive database copies deployed in the Portland data center. DAG2 hosts the active mailboxes for the Portland data center and is implemented as an active/passive user distribution model, with passive database copies deployed in the Redmond data center.

This architecture can survive the loss of the WAN:

- In the Redmond data center, the Mailbox server members for DAG2 go into a failed state due to loss of quorum, but the active Mailbox server members for DAG1 remain operational, servicing users.
- In the Portland data center, the Mailbox server members for DAG1 go into a failed state due to loss of quorum, but the active Mailbox server members for DAG2 remain operational, servicing users.

For more information, see Planning for High Availability and Site Resilience.

Return to top

Planning the Mailbox Server Resilience Model

A key aspect to Exchange 2010 Mailbox server capacity planning is determining how many database copies you plan to activate on a per-server basis when configured for mailbox resiliency. A range of designs are possible, but two models are recommended, as described in the following sections.

Design for All Database Copies Activated

You can design your server architecture to handle 100 percent of all hosted database

copies becoming active. For example, if your server hosts 35 database copies, you design the processor and memory to accommodate all 35 databases being active during the peak period of user activity. This solution is usually deployed in pairs. For example, if deploying four servers, one pair is servers 1 and 2, and the second pair is servers 3 and 4. In addition, when designing for this scenario, you size each server for no more than 40 percent available resources for normal run-time operations.

Of the two models discussed in this topic, this model has a higher server count.

Design for Targeted Failure Scenarios

You can design your server architecture to handle the active mailbox load during the worst failure case you plan to accommodate. There are many factors to consider in this model, including site resiliency; RAID storage vs. JBOD; DAG size; and database copy count. This capacity planning model provides a balance between capital costs, availability, and client performance characteristics.

Assuming the database copies are randomly and evenly distributed:

- Design for automatic, single-member server failure in two-member or three-member DAG configurations with two highly available database copies per mailbox database.
- Design for double-member server failure (manual activation after second failure) in three-member DAG configurations with three highly available database copies per mailbox database.
- Design for automatic, double-member server failures where the DAG has four or more members and three or more highly available database copies per mailbox database.

If you choose this capacity planning model, we strongly recommend that you restrict the number of databases that can be activated per server so that a single server doesn't become overloaded and provide a poor client experience.

You can restrict the number of databases by configuring the maximum active databases setting. You can configure this limit in the Exchange Management Shell by running: `Set-MailboxServer -MaximumActiveDatabases`. Configure this limit on each server in the DAG to match the maximum active databases supported by your deployment.

For more information, see Database Availability Group Design Examples.

Return to top

Planning the Number of Mailbox Servers to Deploy

When determining the number of Mailbox servers to deploy, use a multiple of the number of database copies being deployed. For example, if you plan to deploy three database copies, start the design with either 3, 6, 9, 12, or 15 servers.

After you determine the starting point for the number of servers within the DAG, scale the DAG members appropriately based on the number of mailboxes, the failure design model, and other design constraints that may either increase or reduce the number of Mailbox servers required.

One design constraint that many organizations have is a maximum number of mailboxes that can be placed on a server. For example, if an organization has 20,000 mailboxes and only 25 percent can be impacted during a failure event, the maximum number of mailboxes that can be deployed on a single server is 5,000. This requires deploying a minimum of four Mailbox servers.

The selected server hardware and storage model may also cause an adjustment to the number of mailboxes or number of database copies you deploy per server, which can affect the total number of Mailbox servers.

Multiple Role Servers vs. Stand-Alone Role Servers

In Exchange Server 2007, the Client Access and Hub Transport server roles are required to be on servers separate from clustered Mailbox servers. In Exchange 2010, clustered Mailbox servers no longer exist so this restriction no longer applies. Client Access and Hub Transport server roles can be hosted on DAG members, providing improved deployment options.

When deploying multiple role servers (Mailbox, Client Access, and Hub Transport server roles on the same server), most architectures are simplified. Other than the Edge Transport and Unified Messaging servers, all Exchange 2010 servers can be identical. These servers can have the same hardware, software installation process, and configuration options. Consistency across servers can simplify the administration of Exchange implementation.

The multiple role server (in high scale environments) provides more efficient use of high-core-count servers, which provide high megacycle capabilities. Each role, when deployed individually, has a recommended maximum of two populated processor sockets. When combining roles, the recommended maximum number of processor sockets is four. Servers can have larger workloads, which can reduce the overall number of servers in an organization. Deploying fewer servers reduces the cost of managing those servers, because the multiple role server changes cost from a recurring operational expense to a one-time capital expense. A reduced server count can result in significant power, cooling, and data center space reductions, which can further reduce recurring operational expenses.

Although the multiple role concept is efficient, stand-alone server roles may still be appropriate. For example, stand-alone role deployments might be appropriate in certain virtualized environments or when certain hardware architectures (for example, a blade server infrastructure where you can't isolate the hardware appropriately) are being utilized.

When deploying multiple role servers, you must design the processor and memory architecture appropriately. From a processor perspective, you should ensure that the Mailbox server role doesn't consume more than 40 percent of the available megacycles during the failure mode, leaving 40 percent for the Hub Transport and Client Access server roles. To ensure that adequate memory is available for all server roles, follow the memory guidance defined in Understanding the Mailbox Database Cache.

For more information, see Understanding Multiple Server Role Configurations in Capacity Planning.

Return to top

Planning the Database Copy Layout

As part of the high availability design, you need to design a balanced database copy layout. The following design principles should be used when planning the database copy layout:

- Ensure that you minimize multiple database copy failures of a specific mailbox database by isolating each copy. For example, don't place more than a single database copy of a specific mailbox database within the same server rack or in the same storage array. Otherwise, a rack or array failure will result in the failure of multiple copies of the same database, which affects the availability of the database.

- Lay out the database copies in a consistent, distributed way to ensure that the active mailbox databases are evenly distributed after a failure. The sum of the activation preferences of each database copy on any specific server must be equal or close to equal, because this results in an approximately equal distribution after failure, assuming replication is healthy and up-to-date.

For more information, see Database Copy Layout Design.

Return to top

Planning the Backup Model Architecture

Exchange 2010 includes several features and architectural changes that, when deployed and configured correctly, can provide native data protection, which eliminates the need to make traditional backups of your data. Use the following table to decide whether you need to continue utilizing a traditional backup model or whether you can implement the native data protection features in Exchange 2010.

Issue	Mitigation
Software failures	Mailbox resiliency (multiple database copies)
Hardware failures	Mailbox resiliency (multiple database copies)
Site or data center failures	Mailbox resiliency (multiple database copies)
Accidental or malicious deletion of items	Single item recovery and deleted item retention with a window that meets or exceeds the item recovery SLA
Physical corruption scenarios	Single page restore (highly available database copies)
Logical corruption scenarios	Single item recovery Calendar Repair Assistant Mailbox moves **New-MailboxRepairRequest** cmdlet Point-in-time backup
Administrative errors	Point-in-time backup
Automation errors	Point-in-time backup
Rogue administrators	Point-in-time backup (isolated)
Corporate or regulatory compliance requirements	Point-in-time backup (isolated)

Logical corruption is typically a scenario that requires a point-in-time backup. However, with Exchange 2010, there are several options available that can mitigate the need for a point-in-time backup:

- With single item recovery, if the user changes certain properties of an item in any mailbox folder, a copy of the item is saved in the Recoverable Items folder before the modification is written to the database. If the modification of the message results in a corrupted copy, the original item can be restored.
- The Calendar Repair Assistant detects and corrects inconsistencies that occur for single and recurring meeting items for mailboxes homed on that Mailbox

server so that recipients won't miss meeting announcements or have unreliable meeting information.
- During mailbox moves, the Microsoft Exchange Mailbox Replication service detects corrupted items and won't move those items to the target mailbox database.
- Exchange 2010 Service Pack 1 (SP1) introduces the New-MailboxRepairRequest cmdlet, which can fix corruptions with search folders, item counts, folder views, and parent/child folder issues.

A point-in-time backup can be either a traditional backup or a lagged database copy, which both provide the same capabilities. The choice between the two depends on your recovery SLA. The recovery SLA defines the recovery point objective (if a disaster occurs, the data must be restored within a certain timeframe), as well as how long the backups must be retained. If the recovery SLA is 14 days or less, a lagged database copy can be utilized. If the recovery SLA is greater than 14 days, a traditional backup must be used. For the rogue administrator and for corporate or regulatory compliance scenarios, the point-in-time backup typically is maintained separately from the messaging infrastructure and messaging IT staff, which dictates a traditional backup solution.

If you choose to maintain a point-in-time backup, several aspects of the design may change:
- Deploying lagged database copies has storage implications. Additional space must be allocated for the transaction logs on the lagged database copy due to the *ReplayLagTime* settings. In addition, the placement of the lagged database copy can affect your storage architecture. (For details, see "Planning the Storage Model Architecture" later in this topic.)
- Deploying a traditional backup solution has implications on the logical unit number (LUN) layout, depending on the type of Volume Shadow Copy Service (VSS) solution, because hardware-based VSS cloning solutions require two LUNs per database architecture.

Depending on the storage architecture, utilizing a traditional backup solution may require significantly reducing desired user mailbox sizes to meet your backup and restore timeframe SLAs.

When deploying Exchange native data protection, you enable circular logging on the mailbox databases. When enabling circular logging, ensure that sufficient capacity is built into the system so that the solution can survive disaster events that prevent log truncation. At a minimum, you should ensure that there is at least three days of transaction log capacity (excluding lagged copy requirements). For more information about how circular logging functions with continuous replication, see Understanding Backup, Restore and Disaster Recovery.

For additional information about planning backups, see:
- Understanding Exchange 2010 LUN Architecture
- Understanding Mailbox Database and Log Capacity Factors
- Understanding Calendar Repair
- Understanding Recoverable Items

Return to top

Planning the Storage Model Architecture

Exchange 2010 provides flexibility in storage design. Exchange 2010 includes improvements in performance, reliability, and high availability that enable organizations to run Exchange on a range of storage devices. Building on improvements to disk input/output (I/O) introduced in Exchange 2007, the latest version of Exchange requires less storage performance and is more tolerant of storage failures.

Select a storage platform that ensures you're balancing the capacity requirements with the I/O requirements, while ensuring the solution provides acceptable disk latency and a responsive user experience.

RAID or JBOD

Determine whether to implement the storage platform using RAID technology or a JBOD approach (assuming the storage platform allows JBOD configurations). From an Exchange perspective, JBOD means having both the database and its associated logs stored on a single disk. To deploy on JBOD, you must deploy a minimum of three highly available database copies. Utilizing a single disk is a single point of failure, because when the disk fails, the database copy residing on that disk is lost. Having a minimum of three database copies ensures fault tolerance by having two additional copies in the event that one copy (or disk) fails. However, placement of three highly available database copies, as well as the use of lagged database copies, can affect storage design. The following table shows guidelines for RAID or JBOD considerations.

RAID or JBOD considerations

Data center servers	Two highly available copies (total)	Three highly available copies (total)	Two or more highly available copies per data center	One lagged copy	Two or more lagged copies per data center
Primary data center servers	RAID	RAID or JBOD (2 copies)	RAID or JBOD	RAID	RAID or JBOD
Secondary data center servers	RAID	RAID (1 copy)	RAID or JBOD	RAID	RAID or JBOD

To deploy on JBOD with the primary data center servers, you need three or more highly available database copies within the DAG. If mixing lagged copies on the same server hosting highly available database copies (for example, not using dedicated lagged database copy servers), you need at least two lagged database copies.

For the secondary data center servers to use JBOD, you should have at least two highly available database copies in the secondary data center. The loss of a copy in the secondary data center won't result in requiring a reseed across the WAN or having a single point of failure in the event the secondary data center is activated. If mixing lagged database copies on the same server hosting highly available database copies (for example, not using dedicated lagged database copy servers), you need at least two lagged database copies.

For dedicated lagged database copy servers, you should have at least two lagged database copies within a data center to use JBOD. Otherwise, the loss of disk results in the loss of the lagged database copy, as well as the loss of the protection mechanism.

For more information, see Understanding Storage Configuration.

Return to top

Understanding Mailbox Database and Log Capacity Factors

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-24*

This topic explains the factors that you should consider when you plan mailbox database and log capacity as part of your mailbox server storage design in Microsoft Exchange Server 2010.

Mailbox Database Capacity

Many factors influence a sizing capacity plan for Exchange Server 2010 Mailbox databases. This section discusses the following:

- Mailbox storage quotas
- Database white space
- Mailbox database recoverable items
- Actual mailbox size
- Content indexing
- Offline database maintenance
- Recovery database
- Database size
- Database growth overhead

Mailbox Storage Quotas

The first metric to understand is the storage size limit, known as the mailbox *storage quota*, that's in effect in your organization. Knowing the amount of data that an end user is allowed to store in his or her mailbox allows you to determine how many user mailboxes can be housed on the server. Although mailbox storage quotas can change in response to changing organizational requirements, having a goal for the mailbox storage quota is the first step in determining your needed mailbox database capacity.

For example, if you have a server with 5,000 250-MB user mailboxes on it, you need at least 1.25 TB of disk space, excluding space requirements for recoverable items. If a limit isn't set for mailbox storage quotas, you'll find it difficult to estimate database capacity. Mailbox storage quotas for Exchange 2010 need to include the space for both the primary mailbox and personal archive mailbox (when used). For more information, see Managing Mailbox Servers and Managing Archives.

Database White Space

The database size on the physical disk isn't just the number of users multiplied by the mailbox storage quota. When the majority of users aren't approaching their mailbox storage quota, the databases consume less space and white space isn't a capacity concern. The database itself will always have free pages, or white space, spread throughout. During background database maintenance, items marked for removal from the database are removed, which frees these pages. The percentage of white space is constantly changing due to the efforts of the 24x7 online defragmentation process.

You can estimate the amount of white space in the database by knowing the amount of mail sent and received by the users with mailboxes in the database. For example, if you have 100 2-GB mailboxes (total of 200 GB) in a database where users send and receive an average of 10 MB of mail per day, the amount of white space is approximately 1 GB (100 mailboxes × 10 MB per mailbox). The amount of white space can exceed this approximation if background database maintenance isn't able to complete a full pass.

Return to top

Mailbox Database Recoverable Items

Each database has a dumpster that stores soft-deleted items. By default, soft-deleted items are stored for 14 days and calendar items are stored for 120 days in Exchange 2010.

In addition, Exchange 2010 also includes the ability to prevent the purging of data before the deleted item retention window has passed. This functionality is known as *single item recovery*. Single item recovery is disabled by default. However, when single item recovery is enabled, there is an additional 1.2 percent increase in the size of the mailbox for a 14-day deleted item retention window. For calendar version logging data, there is an additional 3 percent increase in the size of the mailbox. Calendar version logging data is enabled by default.

The formula for determining the dumpster space requirements for 14 days of deleted item retention with single item recovery and calendar version logging enabled is:

Dumpster Size = (Daily Incoming/Outgoing Mail x Average Message Size x Deleted Item Retention Window) + (Mailbox Quota Size x 0.012) + (Mailbox Quota Size x 0.03)

For example, if the mailbox size is 2 GB, enabling single item recovery for 14 days of deleted item retention requires an additional 25 MB of space, and the calendar logging feature requires an additional 61 MB.

For more information, see the following topics:

- Exchange 2010 Mailbox Server Role Design Example
- Understanding Recoverable Items
- Managing Recoverable Items
- Understanding Calendar Repair
- Managing Calendars

Actual Mailbox Size

Over time, user mailboxes will reach the mailbox storage quota, so an amount of mail equivalent to the incoming mail will need to be deleted to remain under the mailbox storage quota. This requirement means that the dumpster will increase to a maximum size equivalent to the amount of e-mail sent and received each day multiplied by the number of days within the deleted item retention window. If the majority of users haven't reached the storage quota, only some of the incoming/outgoing mail is deleted. Therefore, the growth is split between the dumpster and the increase in mailbox size.

To determine database size using a 2-GB mailbox without using the personal archive feature, see the "Mailbox Capacity Requirements" section in the Exchange 2010 Mailbox Server Role Design Example topic.

After you have determined the projected actual mailbox size, you can use that value to determine the maximum number of users per database. Divide projected mailbox size by the recommended database size. This value will also help you determine how many databases you will need to handle the projected user count, assuming fully populated databases. Be aware that due to non-transactional input/output (I/O) or because of hardware limitations, you may have to modify the number of users placed on a single server. Some administrators will prefer to use more databases to further reduce the database size. This approach can assist with backup and restore windows at the cost of more complexity in managing more databases per server.

Content Indexing

Content indexing creates an index, or catalog, that allows users to easily and quickly search through their mail items rather than manually search through the mailbox. Exchange 2010 creates an index that is about 10 percent of the total database size, which is placed on the same LUN as the database. Therefore, an additional 10 percent

needs to be factored into the database LUN size for content indexing.

Return to top

Offline Database Maintenance

A database that needs to be compacted offline requires capacity equal to the size of the target database plus 10 percent. Whether you allocate enough space for a single database, or a backup set, additional space must be available to perform these operations.

Important:

Offline maintenance procedures should only be implemented by request of Microsoft Customer Service and Support because offline maintenance procedures invalidate all database copies and require a full reseed of the database.

Recovery Database

If you plan to use a recovery database as part of your disaster recovery plans, sufficient capacity must be available to handle all the databases you want to be able to simultaneously restore on that server. For more information, see Recovery Databases.

Database Size

The database size ultimately determines how many mailboxes you deploy within each database and how many databases you deploy. The database size you deploy depends on several factors:

- **Backup/restore service level agreements (SLAs)** The database size ultimately dictates how fast you can backup and restore the data within a reasonable amount of time.
- **High availability architecture** If you plan to have multiple database copies, you can design your databases to be 2 TB in size because your copies become your first line of defense in terms of recovery operations.
- **Storage architecture** If you plan to deploy on JBOD storage (one disk houses both the database and its corresponding transaction logs), then the size of the disk you use dictates the maximum database size. For example, on a 1 TB disk (with a formatted capacity of about 917 GB), you also need to include space for transaction logs and the content index, and ensure you don't consume all available space.

Database Growth Overhead

After all factors have been considered and calculated, we recommend that you include an additional overhead factor of 20 percent for the database logical unit number (LUN). This value accounts for the other data that resides in the database that isn't necessarily seen when calculating mailbox sizes and white space.

Return to top

Log Capacity

The transaction log files are a record of every transaction performed by the database engine. All transactions are written to the log first, and then lazily written to the database. Unlike Exchange Server 2003, the transaction log files in Exchange 2010 have been reduced in size from 5 MB to 1 MB. This change was made to support the continuous replication features and to minimize the amount of data loss if primary storage fails.

You can use the following table to estimate the number of transaction logs that are generated on an Exchange 2010 Mailbox server where the average message size is 75 KB.

The value for *Number of transaction logs generated per day* is based on the message profile selected and the average message size. It indicates how many transaction logs will be generated per mailbox per day. The log generation numbers per message profile account

for:

- Message size impact
- Amount of data sent/received
- Database health maintenance operations
- Records Management operations
- Data stored in a mailbox that is not a message (tasks, local calendar appointments, contacts)
- Forced log rollover (a mechanism that periodically closes the current transaction log file)

Number of transaction logs generated per mailbox profile

Message profile (75 KB average message size)	Number of transaction logs generated per day
50	10
100	20
150	30
200	40
250	50
300	60
350	70
400	80
450	90
500	100

You can use the following guidelines to understand how message size affects the generation rate of transaction logs:

- If the average message size doubles to 150 KB, the logs generated per mailbox increases by a factor of 1.9. This number represents the percentage of the database that contains the attachments and message tables (message bodies and attachments).
- Thereafter, as message size doubles beyond 150 KB, the log generation rate per mailbox also doubles, increasing from 1.9 to 3.8.

For example, if you have a 100 messages per day and:

- An average message size of 150 KB, the logs generated per mailbox are 20 × 1.9 = 38.
- An average message size of 300 KB, the logs generated per mailbox are 20 × 3.8 = 76.

The following sections discuss factors that affect your log sizing capacity:

- Backup and restore factors
- Move mailbox operations
- Log growth overhead
- High availability factors
- LUN capacity planning

Backup and Restore Factors

Log LUN sizing is partly dependent on your backup and restore design. For example, if your design allows you to go back two weeks and replay all the logs generated since then, you will need two weeks of log file space. If your backup design includes weekly full

and daily differential backups, the log LUN needs to be larger than an entire week of log file space to allow both backup and replay during restore. Most enterprises that perform a nightly full backup allocate two to three times the required daily log generation capacity. This approach is taken to prevent a backup failure from causing the log drive to fill, which would dismount the database.

If you plan on using the mailbox resiliency and single item recovery features within Exchange 2010 as your backup infrastructure (and thus enabling circular logging), as a best practice, you should ensure that you allocated three times the required daily log generation capacity. This ensures that, when replication is suspended or not functioning under normal parameters, the databases don't dismount due to truncation failures.

Move Mailbox Operations

Moving mailboxes is a primary capacity factor for large mailbox deployments. Many large companies move a percentage of their user mailboxes on a nightly or weekly basis to different databases, servers, or sites. If your organization does this, you may find it necessary to provide extra capacity to the log LUN to accommodate mailbox moves.

Although the source server logs the record deletions, which are small, the target server must write all transferred data first to transaction logs. If you generate 10 GB of log files in one day, and keep a three-day buffer of 30 GB, moving 50 2-GB mailboxes (100 GB) would fill your target log LUN and cause downtime. In cases such as these, you may have to allocate additional capacity for the log LUNs to accommodate your move mailbox practices.

Log Growth Overhead Factor

For most deployments, we recommend that you add an overhead factor of 20 percent to the log size (after all other factors have been considered) when creating the log LUN to ensure necessary capacity exists in moments of unexpected log generation.

High Availability Factors

High availability influences log capacity requirements in three significant ways:

- **Database copy count** The log capacity of the entire system is increased based on the number of database copies chosen in the high availability deployment. If you have three database copies spread across three servers, you need to provision log capacity for each copy on each server.
- **Log truncation mechanism** High availability in Exchange 2010, with the ability to have up to 16 copies of each mailbox database, provides the foundation to use continuous replication circular logging as the log truncation/deletion mechanism as opposed to running Full/Incremental backups to truncate/delete the older logs. For more information, see the "Log Truncation without Backups" section in Understanding Backup, Restore and Disaster Recovery and High Availability and Site Resilience.
- **Database copy replay lag** High availability in Exchange 2010 provides the option to lag log replay on passive database copies (configured on a per copy basis). This feature is used to provide a delay for when logs get played in to lagged database copies. This delay can be useful to protect against events which would cause undesirable content to be replicated to all database copies. The content can be stopped from being played in to the lagged database copy by suspending replay before the logs with the undesired content are played in to the database.
  When replay lag is enabled for a database copy, the log capacity requirements change accordingly. If you have a 14-day lag configured, you need to provision for 17 days worth of logs. The additional log capacity is only required for the database copy that has the lag configured, other copies of that database, which don't have a lag, will have normal (non-lagged) log capacity requirements.

For more information, see Understanding High Availability Factors.

LUN Capacity Planning

The capacity requirements for the LUN will be based on the size of the data set (database, transaction logs, content index, and recovery space) and some additional free space. Most operations management programs have capacity thresholds that provide an alert when a LUN is more than 80 percent utilized.

You can use the following formula to determine the appropriate size of the LUN:

LUN Capacity = Data Size / (1 - Free Space Percentage Requirement)

For example, if you had a data size requirement of 3000 MB and a free space requirement of 20 percent, then the LUN that hosts this data must be 3750 MB in size.

Preventing the total consumption of transaction log disk space

To avoid having all your transaction log disk space be consumed, you must first calculate a baseline of your environment to determine the typical log generation rate per day. Second, you must set up monitoring, and take action regarding any alerts that are generated. You should monitor for the following items:

- Transaction Log LUN disk space. Set up several thresholds and different alert mechanisms. For example, if you know your typical log generation baseline, you can set up a threshold to report when you are 20 percent over the baseline.
- Successful completion of your backups (if you aren't leveraging Exchange Native Data Protection).
- The truncation of events in the Application Log.
- Your database copy replication health.

Troubleshooting unexplained growth in Transaction logs

To help troubleshoot unexplained growth in Transaction logs, see Manage Database Log Growth by Using the Troubleshoot-DatabaseSpace.ps1 Script in the Shell.

1.2.1.9.4 Understanding the Mailbox Database Cache

Understanding the Mailbox Database Cache

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-04-23*

The Extensible Storage Engine (ESE) engine uses database cache to reduce I/O operations. In general, the more database cache that is available, the less I/O that is generated on a Microsoft Exchange Server 2010 Mailbox server. The database I/O reduction primarily depends on the amount of database cache available to the server and the user message profile.

Improved Database Cache Effectiveness

The database cache effectiveness has been improved in Exchange 2010 due to several technical changes. One of the most significant changes is increasing the log checkpoint depth target. The log checkpoint depth target is used to ensure that changes made to the log/database cache are written to the database file in a reasonable amount of time. It has been increased from 20 MB per database to 100 MB per database when a database has more than one copy (in a database availability group, or DAG). The following table provides the default log checkpoint depth targets for Exchange 2010.

Default log checkpoint depth target configuration per mailbox database

Database configuration	Log checkpoint depth target (MB)
Stand-alone (one database copy)	20
Mailbox resiliency: Active database copy with two or more copies (DAG)	100
Passive database copy	5

Due to this change, the database write I/O for an active database with two or more copies can be up to 40 percent less than the database write I/O for a stand-alone database. When the database has a higher checkpoint depth target, it's able to retain database file changes in memory for a longer period; thus, improving its ability to combine I/Os (coalescing) and by reducing repeated write I/Os (I/Os that can be saved by delaying the write long enough so multiple database changes can be made in memory prior to writing the change to the database file).

This change was only made for mailbox resiliency solutions because a deeper checkpoint depth target can significantly increase the time it takes the active database to recover the failed database after a failure. This problem has been addressed in mailbox resiliency configurations because if the active database fails, a failover is automatically triggered to another healthy copy. Log replay operations will resume when the failed database is recovered.

The checkpoint depth target has subsequently been reduced on passive database copies to reduce the time a database switchover/failover takes. A passive database copy with a 5 MB checkpoint depth target can be activated much faster than a copy with a higher checkpoint depth target (there are fewer logs to play through when transitioning between the passive and active state). A passive database copy does not have transactional I/O so there is spare capacity to handle the additional write I/O with the lower Checkpoint Depth Target.

Database Cache Minimum Requirements

To ensure the ESE database has sufficient memory to work effectively, there is a required minimum amount of physical memory per server based on database count. These requirements apply to both active and passive database copies. See the following table for the requirements.

Required minimum memory per mailbox server

Database count	Exchange 2010 minimum required physical memory
1-10	2 GB
11-20	4 GB
21-30	6 GB
31-40	8 GB
41-50	10 GB
51-60	12 GB
61-70	14 GB
71-80	16 GB
81-90	18 GB

91-100	20 GB

Database Cache Metrics

In previous versions of Exchange, one of the key metrics needed for sizing storage was the amount of database I/O per second (IOPS) consumed by each user. The two most important factors that can be used to predict Exchange 2010 Mailbox IOPS are the amount of database cache per mailbox and the number of messages each user sends and receives per day.

The following table provides estimated values for IOPS per mailbox based on message activity and database cache. You can use the information in the table to help predict baseline Exchange 2010 mailbox I/O requirements.

These estimates are only valid for database cache sizes between 3 MB and 30 MB per mailbox. These estimates have been validated with users with the following characteristics: High percentage Exchange Cache Mode clients in either Microsoft Office Outlook 2007 or Outlook 2010; 2-GB mailboxes; and a high percentage of Exchange ActiveSync usage. The average message size used for the estimates is 75 KB, but message size isn't a primary factor for IOPS. Other client types and usage scenarios may yield inaccurate results.

Estimated IOPS per mailbox based on message activity and mailbox database cache

Messages sent/ received per mailbox per day (~75KB average message size)	Database cache per user (MB)	Single database copy (Stand-alone): Estimated IOPS per mailbox	Multiple database copies (mailbox resiliency): Estimated IOPS per mailbox
50	3	.060	.050
100	6	.120	.100
150	9	.180	.150
200	12	.240	.200
250	15	.300	.250
300	18	.360	.300
350	21	.420	.350
400	24	.480	.400
450	27	.540	.450
500	30	.600	.500

After you have determined the database cache size requirements, the next step is to determine the minimum memory requirements per server to ensure the database cache size requirements can be met. The database cache size must be factored in to the sizing process to ensure the amount of physical memory per server is adequate to meet the needs of the mailbox count with a given user profile.

The following table lists the default mailbox database cache sizes for both single role Mailbox servers as well as multiple role servers.

Default mailbox database cache sizes

Server physical memory (RAM)	Database cache size: (Mailbox role only)	Database cache size: Multiple-role (for example,

		Mailbox + Hub Transport)
2GB	512 MB	Not supported
4GB	1 GB	Not supported
8GB	3.6 GB	2 GB
16GB	10.4 GB	8 GB
24GB	17.6 GB	14 GB
32GB	24.4 GB	20 GB
48GB	39.2 GB	32 GB
64GB	53.6 GB	44 GB
96GB	82.4 GB	68 GB
128GB	111.2 GB	92 GB

Note:
You can modify the default database cache size values by making changes to the **msExchESEParamCacheSizeMax** and **msExchESEParamCacheSizeMin** attributes in Active Directory. For additional details, see How to modify the Store Database maximum cache size in Exchange 2000 Server. Use 32KB pages for the cache sizing calculations.

To determine server memory requirements, see Exchange 2010 Mailbox Server Role Design Example, which provides information about designing your Mailbox Server role to determine the appropriate memory, capacity, I/O, and CPU performance.

1.2.1.9.5 Understanding Database and Log Performance Factors

Understanding Database and Log Performance Factors

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-12-05*

This topic discusses database and log I/O performance factors in Microsoft Exchange Server 2010. An understanding of these factors is important to your Mailbox server storage design solution. For more information about other key aspects of the design process, see Mailbox Server Storage Design.

Contents

Transactional I/O

Transactional I/O is generally defined as the I/O generated by user activity. Examples of user activity include receiving, sending, and deleting items; syncing a Windows Mobile

client; and logging on via Microsoft Office Outlook Web App.

Transactional I/O is a critical piece of Exchange 2010 storage design because the I/O latency (how long it takes to execute the I/O operation) can directly affect the user experience of online clients such as Microsoft Outlook Online Mode and Outlook Web App. Cached Exchange Mode in Outlook can also be affected by high I/O latency when it's being used for tasks such as delegate access and configuring rules. All clients can be affected by e-mail delivery delays caused by high latency I/O. Transactional I/O can be divided into database volume I/O and log volume I/O.

The transactional I/O requirements in Exchange 2010 have been reduced from those in Exchange Server 2007. Not all I/O that occurs against the Mailbox database and log volumes is considered transactional. For more information, see Understanding the Exchange 2010 Store.

Return to top

Understanding IOPS

For all versions of Exchange, it's important to understand the amount of database I/O per second (IOPS) consumed by each user because it's one of the key transactional I/O metrics needed for adequately sizing storage. The following sections discuss factors that affect IOPS when designing your Mailbox server role storage.

Database Cache

A 64-bit edition of the Windows Server operating system running the 64-bit version of Exchange 2010 substantially increases the virtual address space and allows Exchange to increase its database cache, reduce database read I/O, and enable up to 100 databases per server.

The database read reduction depends on the amount of database cache available to the server and the user message profile. For guidance about memory and databases, see Understanding the Mailbox Database Cache. Following the guidance in that topic can result in up to a 90 percent transactional I/O reduction over Exchange Server 2003. The amount of database cache per user is a key factor in the actual I/O reduction.

The following table demonstrates the increase in actual database cache per mailbox when comparing the default 900 megabytes (MB) of database cache per mailbox in Exchange 2003 versus 6 MB of database cache per mailbox in Exchange 2010 for a user population that uses a 100 messages / day profile. It's the additional database cache In Exchange 2010 that enables more read hits in cache, thus reducing database reads at the disk level.

Database cache sizes based on mailbox count

Mailbox count	Exchange 2003 database cache per mailbox (MB)	Exchange 2010 database cache per mailbox (MB)	Database cache increase over Exchange 2003
4000	0.225	6	27 times
2000	0.45	6	13 times
1000	0.9	6	7 times
500	1.8	6	5 times

Return to top

Determining the Exchange 2010 Mailbox IOPS Profile

The two most significant factors that can be used to predict Exchange 2010 database IOPS are the amount of database cache per user and the number of messages each user sends and receives per day. The following table is based on a standard worker who uses Outlook 2010 in Cached Exchange Mode. The information has been tested to be accurate within plus or minus 20 percent. Other client types and usage scenarios may yield inaccurate results. The predictions are only valid for user database cache sizes between 3 MB and 30 MB. The information hasn't been validated in a scenario where users send and receive over 500 messages per day. The average message size for validation was 75 KB, but message size isn't a primary factor for IOPS.

The table provides estimated values for IOPS per user that you can use to predict your baseline Exchange 2010 IOPS requirements and includes all database I/O (database, content indexing, and NTFS metadata). It doesn't include log volume I/O.

Database cache and estimated IOPS per mailbox based on message activity

Messages sent/ received per mailbox per day	Database cache per mailbox (MB)	Single database copy (stand-alone): Estimated IOPS per mailbox	Multiple database copies (mailbox resiliency): Estimated IOPS per mailbox
50	3	0.06	0.05
100	6	0.120	0.100
150	9	0.18	0.150
200	12	0.240	0.200
250	15	0.300	0.250
300	18	0.360	0.300
350	21	0.420	0.350
400	24	0.480	0.400
450	27	0.540	0.450
500	30	0.600	0.500

Mailbox resiliency refers to a unified high availability and site resilience solution in Exchange 2010. For more information, see Understanding High Availability and Site Resilience.

Return to top

Database Volume I/O

Database volume I/O is I/O associated with database file (.edb) read/write activity, content indexing read/write activity, as well as NTFS metadata read/write activity.

In Exchange 2003, the database read/write ratio is typically 2:1 or 66 percent reads. With Exchange 2010, the larger database cache decreases the number of reads to the database on disk causing the reads to shrink as a percentage of total I/O.

If you follow the recommended memory guidelines, you can expect to see the following I/O ratios for active database copies. For more information about the memory guidelines, see Understanding Memory Configurations and Exchange Performance. This measurement includes all database volume I/O (database, content indexing and NTFS metadata); it doesn't include log volume I/O.

Mailbox database I/O read/write ratios

Messages sent/received per mailbox per day	Stand-alone databases	Databases participating in mailbox resiliency
50	1:1	3:2
100	1:1	3:2
150	1:1	3:2
200	1:1	3:2
250	1:1	3:2
300	2:3	1:1
350	2:3	1:1
400	2:3	1:1
450	2:3	1:1
500	2:3	1:1

For example, if you deploy 24,000 mailboxes across Mailbox servers within a database availability group (DAG) that maintains three database copies, each database has a database read to write ratio of 3:2. Or, in other words, 60 percent of all I/Os to the logical unit number (LUN) hosting the database are read I/Os.

Having more writes as a percentage of total I/O has specific implications when choosing a redundant array of independent disks (RAID) type that has significant costs associated with writes, such as RAID5 or RAID6. For more information about selecting the appropriate RAID solution for your servers, see Understanding Storage Configuration.

Calculating IOPS per Mailbox Server

Calculating IOPS per Mailbox server in Exchange 2010 requires more steps than in previous versions of Exchange because of the following:

- You can now combine databases and logs on the same volume,
- You can host both active and passive database copies on the same server,
- The addition of sequential I/O background tasks (for example, background database maintenance).

Pure sequential I/O operations aren't factored in the IOPS per Mailbox server calculation because storage subsystems can handle sequential I/O much more efficiently than random I/O. These operations include background database maintenance, log transactional I/O, and log replication I/O.

IOPS per Mailbox server is calculated slightly differently depending on how your storage is designed:

- Database files and log files share a single volume.
- Database files are stored on different disk volumes than the transaction log files.

For both storage designs, use Performance Monitor (perfmon.exe) to measure the peak two hour period (at a 5-second sampling interval). This is the time of day where the system is under the most load generated by client activity (for example, 10 A. M. -12 P. M.). This period is often twice the load of the 10 hour daily average (Peak:Average ratio = 2:1).

IOPS per Mailbox Server: Database Files and Log Files Share a Single Volume

In this configuration, the database files and log files are stored on the same disk volume. This example assumes each database is on a different volume backed by a dedicated disk. Fill in the following table for all databases from the collected performance monitor log (described in the previous section).

Database Name	Logical Disk -> Disk Reads/sec	Logical Disk -> Disk Writes/sec	MSExchange DatabaseInstances ->Database Maintenance IO Reads/sec	MSExchange DatabaseInstances ->I/O Database Reads (Recovery) /sec	MSExchange DatabaseInstances ->I/O Database Writes (Recovery) /sec	MSExchange DatabaseInstances ->IO Log Writes/sec
Database 1						
Database 2						
Database 3						
Database 4						
Any additional databases						
Total						

Add the totals from each column, and then perform the following calculation to determine IOPS per Mailbox server.

Calculation summary: Sum of Logical Disk IO - (sum of database maintenance IO + recovery (log replay) IO + Log IO) divided by the number of mailboxes hosted per server during the performance monitor log measurement.

Calculation Detail: ((Logical Disk -> Disk Reads/sec + Logical Disk -> Disk Writes/sec) - (MSExchange Database ==> Instances -> Database Maintenance IO Reads/sec + MSExchange Database ==> Instances -> I/O Database Reads (Recovery)/sec + MSExchange Database ==> Instances -> I/O Database writes (Recovery)/sec + MSExchange Database ==> Instances -> IO Log Writes/sec))/ Number of mailboxes hosted per server during the performance monitor log measurement = IOPS per Mailbox server.

Return to top

IOPS/Mailbox: Dedicated Database File Volume

In this configuration, the database files are stored on different disk volumes than the transaction log files. This example assumes each database is on a different volume backed by a dedicated disk. Fill in the following table for all databases from the collected perfmon log (described in the previous section).

Database Name	Logical Disk -> Disk Reads/sec	Logical Disk -> Disk Writes/sec	MSExchange Database ==> Instances ->Database Maintenance IO Reads/sec	MSExchange Database ==> Instances ->I/O Database Reads (Recovery)/ sec	MSExchange Database ==> Instances ->I/O Database Writes (Recovery)/ sec

Database 1					
Database 2					
Database 3					
Database 4					
Any additional databases					
Total					

Note:
By default, the **MSExchange Database ==> Instances ->Database Maintenance IO Reads/sec** performance counter is not visible in Exchange 2010. You must enable this counter to view it. For more information about how to enable this performance counter, see How to Enable Extended ESE Performance Counters

To determine IOPS per Mailbox server, add the totals from each column and perform the following calculation.

Calculation summary: Sum of Logical Disk IO - (Sum of database maintenance IO + recovery (log replay) IO) divided by the number of mailboxes hosted per server during the perfmon log measurement.

Calculation Detail: ((Logical Disk -> Disk Reads/sec + Logical Disk ->Disk Writes/sec) - (MSExchange Database ==> Instances -> Database Maintenance IO Reads/sec + MSExchange Database ==> Instances -> I/O Database Reads (Recovery)/sec + MSExchange Database ==> Instances -> I/O Database writes (Recovery)/sec))/ Number of mailboxes hosted per server during the performance monitor log measurement = IOPS per Mailbox server.

Measure Baseline IOPS

If you're using a previous version of Exchange, and you have calculated your baseline IOPS, keep in mind that Exchange 2010 affects your baseline in the following ways:

- The number of users on the server affects the overall database cache per user.
- The amount of RAM influences how large your database cache can grow, and a larger database cache causes more cache read hits. This reduces your database read I/O.

The key to this process is that the IOPS on a specific server isn't enough information to plan an entire enterprise. This is because the amount of RAM, number of users, and number of databases will be different on each server. After you have your actual IOPS numbers, always apply a 20 percent I/O overhead factor to your calculations to add some reserve capacity. You don't want a poor user experience because activity is heavier than normal.

Desktop Search Engines and Outlook Online Mode Clients

Unlike Cached Exchange Mode clients, all Online Mode client operations occur against the database. Because of the changes in the store schema and Extensible Storage Engine (ESE), Outlook Online Mode clients now generate the same I/O profile as Outlook Cached Exchange Mode Clients.

In terms of mailbox search capabilities, end users have two options:

- They can use the built-in content index that's available on the Mailbox server.
- They can install a desktop search engine client and have a local index generated on the client of the mailbox's data and perform local searches.

End users that use desktop search engine clients with Outlook Online Mode may incur additional read I/O operations against the database. Currently, the only known desktop search engine that doesn't incur additional read I/Os is Windows Desktop Search 4.0. Windows Desktop Search 4.0 uses synchronization protocols that are similar to how Outlook Cached Exchange Mode synchronization protocols index the mailbox contents.

Therefore, use the following guidelines if you intend to deploy Outlook Online Mode clients with desktop search engines other than Windows Desktop Search 4.0:

- 256 MB Online Mode clients will increase database read operations by a factor of 1.5 when compared with Cached Exchange Mode clients. Below 256 MB, the impact is negligible.
- As mailbox size doubles, the database read IOPS will also double (assuming equal item distribution between key folders remains the same).

As a result of this data, we have two recommendations:

- Deploy Cached Exchange Mode clients where appropriate. For more information, see the "Item Count per Folder" section later in this topic. Otherwise, replace the desktop search engine with Windows Desktop Search 4.0.
- Consider the I/O requirements when you're designing the database storage.

For additional IOPS factors, such as third-party clients, see Optimizing Storage for Exchange Server 2003.

Return to top

Log Volume I/O

Log volume I/O is I/O associated with database logging read/write activity and NTFS metadata read/write activity. Log volume I/O is sequential in nature and, when using a battery-backed write caching array controller, the I/O overhead of log volume I/O is minimal and not a significant factor for Exchange storage sizing.

Because of the reduction in database reads in Exchange 2010, combined with the smaller log file size and the ability to have more databases, the log-to-database write is 40 percent for stand-alone databases and 50 percent for databases that participate in mailbox resiliency. For example, if the database that's participating in mailbox resiliency consumes 12 write I/Os, the log LUN consumes approximately 6 write I/Os.

On Mailbox servers that are hosting databases that are participating in mailbox resiliency, there is overhead associated with using continuous replication. Closed transaction logs must be read and sent to the target database copies. This overhead is an additional 10 percent in log reads for each active database copy that's hosted on the Mailbox server. For example, if the Mailbox server is hosting 10 active database copies, and each transaction log stream is generating 6 write I/Os, you can expect an additional 0.6 read I/Os for each of those 10 active database copies (or a total of 6 read I/Os).

After you measure or predict the transactional log I/O, apply a 20 percent I/O overhead factor to ensure adequate room for busier-than-normal periods.

Item Count per Folder

One way to reduce server I/O is to use Outlook in Cached Exchange Mode. The initial mailbox synchronization is a disk intensive operation, but over time, as the mailbox size grows, the disk subsystem burden is shifted from the Exchange server to the Outlook client. With use of Cached Exchange Mode, having a large number of items in a user's Inbox or a user searching a mailbox will have little effect on the server. This approach also means that Cached Exchange Mode users with large mailboxes may need faster computers than those with small mailboxes (depending on the individual user threshold for acceptable performance).

When you deploy client computers that are running Outlook 2007 in Cached Exchange Mode, consider the following guidelines with respect to mailbox/.ost file sizes:

- **Up to 5 gigabytes (GB)** This size should provide a good user experience on most hardware.
- **Between 5 GB and 10 GB** This size is typically hardware dependent. Therefore, if you have a fast hard disk and a lot of RAM, your experience will be better. However, slower hard drives, such as drives that are typically found on laptops or early generation solid-state drives (SSDs), experience some application pauses when the drives respond.
- **More than 10 GB** This is the size at which short pauses begin to occur on most hardware.
- **Very large, such as 25 GB or larger** This size increases the frequency of the short pauses, especially while you're downloading new e-mail messages. Alternatively, you can use Send/Receive groups to manually synchronize your mail.

This guidance is based on the installation of a cumulative update for Outlook 2007 Service Pack 1 or later, as described in Microsoft Knowledge Base Article 961752, Description of the Outlook 2007 hotfix package (Outlook.msp): February 24, 2009.

If you experience performance-related issues with Outlook 2007 in Cached Exchange Mode deployment, see Knowledge Base Article 940226, How to troubleshoot performance issues in Outlook 2007. For more information about the improvements that are available, see Knowledge Base article 968009, Outlook 2007 improvements in the February 2009 cumulative update.

A challenging scenario occurs when a user has exceeded the number of indexes that Exchange will store. This is 11 indexes in Exchange 2010. When the user chooses to sort a new way, and thereby creates a twelfth index, this causes additional disk I/O activity. Because the index isn't stored, this additional disk activity cost occurs every time that this sort is performed. Because of the high I/O activity that can be generated in this scenario, we strongly recommend that you store no more than 100,000 items in core folders, such as the Inbox and Sent Items folders, and no more than 10,000 items in the Calendar and Contacts folders. The creation of more top-level folders, or of subfolders beneath the Inbox and Sent Items folders, greatly reduces the costs that are associated with this index creation. This is true as long as the number of items in any folder doesn't exceed 100,000.

Return to top

Content Index I/O

In Exchange 2010, messages are indexed as they're received, causing little database disk I/O overhead (because the message is still in the database cache when it's retrieved for indexing). However, write I/O is associated with updating the search catalog store. Because of the overall database I/O reductions in Exchange 2010, the percentage of search catalog I/O is now 10 percent to 15 percent of the database files I/O (depending upon profile). Search catalog read I/O occurs when clients issue search queries, and it's a rare enough occurrence not to be relevant to Exchange 2010 storage design.

Return to top

Non-Transactional I/O

Transactional I/O occurs in response to direct user action and usually has the highest priority, and therefore, it's the focus for storage design. Non-transactional I/O either occurs in the background and is tuned to have a minimal performance impact, or it occurs during a defined maintenance window.

The following sections discuss some of the non-transactional I/O that occurs in the background. Although non-transactional I/O isn't the focus of storage design, it can impact your storage design. For more information, see New Exchange Core Store Functionality.

Background Database Maintenance (Checksumming)

Background database maintenance I/O is sequential database file I/O associated with checksumming both active and passive database copies. Background database maintenance has the following characteristics:

- On active databases, it can be configured to run either 24 × 7 or during the online maintenance window. Background database maintenance (Checksum) runs against passive database copies 24 × 7. For more information, see "Online Database Scanning" in the New Exchange Core Store Functionality topic.
- Reads approximately 5 MB per second for each actively scanning database (both active and passive copies). The I/O is 100 percent sequential, so the storage subsystem can process the I/Os efficiently.
- Stops scanning the database if the checksum pass completes in less than 24 hours.
- Issues a warning event if the scan doesn't complete within three days (not configurable).

Messaging Records Management

Messaging records management (MRM) is the records management technology in Exchange 2010 that helps organizations reduce the legal risks associated with e-mail. MRM makes it easier to retain the messages that are needed to comply with company policy, government regulations, or legal needs, and to remove content that has no legal or business value.

These actions are accomplished through the use of retention policies or managed folders. The Managed Folder Assistant is a Microsoft Exchange Mailbox Assistant that applies message retention settings configured in retention policies or managed folder mailbox policies. The disk I/O required by the assistant depends on the number of mailbox items processed. We recommend that the assistant not run at the same time as either backup or online maintenance. For more information, see Configure the Managed Folder Assistant.

Online Maintenance

You can use the Exchange Management Tools to set the maintenance schedule for a database or allow 24 × 7 database maintenance. Online defragmentation no longer works in Exchange 2010 as it did in previous versions of Exchange. Online defragmentation is continuously performed while the database is being read from and written to. For more information, see "Online Database Scanning" in the New Exchange Core Store Functionality.

Return to top

1.2.1.9.6 Understanding Storage Configuration

Understanding Storage Configuration

Planning and Deployment > Planning for Exchange 2010 > Mailbox Server Storage Design >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-30*

Understanding storage options and requirements for the Mailbox server role in Microsoft Exchange Server 2010 is an important part of your Mailbox server storage design solution. For additional information about other key aspects of the design process, see Mailbox Server Storage Design.

Contents

Storage Architectures

The following table describes supported storage architectures, and provides best practice guidance for each type of storage architecture, where appropriate.

Supported storage architectures

Storage architecture	Description	Best practice
Direct-attached storage (DAS)	DAS is a digital storage system directly attached to a server or workstation, without a storage network in between. For example, DAS transports include Serial Attached Small Computer System Interface (SCSI) and Serial Attached Advanced Technology Attachment (ATA).	Not available.
Storage area network (SAN): Internet Small Computer System Interface (iSCSI)	SAN is an architecture to attach remote computer storage devices (such as disk arrays and tape libraries) to servers in such a way that the devices appear as locally attached to the operating system (for example, block storage). iSCSI SANs encapsulate SCSI commands within IP packets and use standard networking infrastructure as the storage transport (for example, Ethernet).	Don't share physical disks backing up Exchange data with other applications. Use dedicated storage networks. Use multiple network paths for stand-alone configurations.
SAN: Fibre Channel	Fibre Channel SANs encapsulate SCSI commands within Fibre Channel packets and generally utilize specialized Fibre Channel networks as the storage transport.	Don't share physical disks backing up Exchange data with other applications. Use multiple Fibre Channel network paths for stand-alone configurations. Follow storage vendor's best

		practices for tuning Fibre Channel host bus adapters (HBAs), for example, Queue Depth and Queue Target.

Return to top

Physical Disk Types

The following table provides a list of supported physical disk types and provides best practice guidance for each physical disk type where appropriate.

Supported physical disk types

Physical disk type	Description	Supported or best practice
Serial ATA (SATA)	SATA is a serial interface for ATA and integrated device electronics (IDE) disks. SATA disks are available in a variety of form factors, speeds, and capacities. In general, choose SATA disks for Exchange 2010 mailbox storage when you have the following design requirements: • High capacity • Moderate performance • Moderate power utilization	Supported: 512-byte sector disks for Windows Server 2008 and Windows Server 2008 R2. In addition, 512e disks are supported for Windows Server 2008 R2 with the following: • The hotfix described in Microsoft Knowledge Base article 982018, An update that improves the compatibility of Windows 7 and Windows Server 2008 R2 with Advanced Format Disks is available. • Windows Server 2008 R2 with Service Pack 1 (SP1) and Exchange Server 2010 SP1. Support requires that all copies of a database reside on the same physical disk type. For example, it is not a supported configuration to host one copy of a given database on a 512-byte sector disk and another copy of that same database on a 512e disk. Also be aware that 4-kilobyte (KB) sector disks are not supported for any version of Microsoft Exchange and 512e disks are not supported for any version of Exchange prior to Exchange Server 2010 SP1. Best practice: Consider enterprise class SATA disks, which generally have better heat, vibration, and reliability characteristics.

Serial Attached SCSI	Serial Attached SCSI is a serial interface for SCSI disks. Serial Attached SCSI disks are available in a variety of form factors, speeds, and capacities. In general, choose Serial Attached SCSI disks for Exchange 2010 mailbox storage when you have the following design requirements: • Moderate capacity • High performance • Moderate power utilization	Supported: 512-byte sector disks for Windows Server 2008 and Windows Server 2008 R2. In addition, 512e disks are supported for Windows Server 2008 R2 with the following: • The hotfix described in Microsoft Knowledge Base article 982018, An update that improves the compatibility of Windows 7 and Windows Server 2008 R2 with Advanced Format Disks is available. • Windows Server 2008 R2 with Service Pack 1 (SP1) and Exchange Server 2010 SP1. Support requires that all copies of a database reside on the same physical disk type. For example, it is not a supported configuration to host one copy of a given database on a 512-byte sector disk and another copy of that same database on a 512e disk. Also be aware that 4-kilobyte (KB) sector disks are not supported for any version of Microsoft Exchange and 512e disks are not supported for any version of Exchange prior to Exchange Server 2010 SP1. Best practice: Physical disk-write caching must be disabled when used without a UPS.
Fibre Channel	Fibre Channel is an electrical interface used to connect disks to Fibre Channel-based SANs. Fibre Channel disks are available in a variety of speeds and capacities. In general, choose Fibre Channel disks for Exchange 2010 mailbox storage when you have the following design requirements: • Moderate capacity • High performance • SAN connectivity	Supported: 512-byte sector disks for Windows Server 2008 and Windows Server 2008 R2. In addition, 512e disks are supported for Windows Server 2008 R2 with the following: • The hotfix described in Microsoft Knowledge Base article 982018, An update that improves the compatibility of Windows 7 and Windows Server 2008 R2 with Advanced Format Disks is available. • Windows Server 2008 R2 with Service Pack 1

		(SP1) and Exchange Server 2010 SP1. Support requires that all copies of a database reside on the same physical disk type. For example, it is not a supported configuration to host one copy of a given database on a 512-byte sector disk and another copy of that same database on a 512e disk. Also be aware that 4-kilobyte (KB) sector disks are not supported for any version of Microsoft Exchange and 512e disks are not supported for any version of Exchange prior to Exchange Server 2010 SP1. Best practice: Physical disk-write caching must be disabled when used without a UPS.
Solid-state drive (SSD) (flash disk)	An SSD is a data storage device that uses solid-state memory to store persistent data. An SSD emulates a hard disk drive interface. SSD disks are available in a variety of speeds (different I/O performance capabilities) and capacities. In general, choose SSD disks for Exchange 2010 mailbox storage when you have the following design requirements: • Low capacity • Extremely high performance	Supported: 512-byte sector disks for Windows Server 2008 and Windows Server 2008 R2. In addition, 512e disks are supported for Windows Server 2008 R2 with the following: • The hotfix described in Microsoft Knowledge Base article 982018, An update that improves the compatibility of Windows 7 and Windows Server 2008 R2 with Advanced Format Disks is available. • Windows Server 2008 R2 with Service Pack 1 (SP1) and Exchange Server 2010 SP1. Support requires that all copies of a database reside on the same physical disk type. For example, it is not a supported configuration to host one copy of a given database on a 512-byte sector disk and another copy of that same database on a 512e disk. Also be aware that 4-kilobyte (KB) sector disks are not supported for any version of Microsoft Exchange and 512e disks are not supported for any version of Exchange prior to Exchange Server 2010 SP1. Best practice: Physical disk-write

		caching must be disabled when used without a UPS. In general, Exchange 2010 Mailbox servers don't require the performance characteristics of SSD storage.

Factors to Consider When Choosing Disk Types

There are several trade-offs when choosing disk types for Exchange 2010 storage. The correct disk is one that balances performance (both sequential and random) with capacity, reliability, power utilization, and capital cost. The following table of supported physical disk types provides information to help you when considering these factors.

Factors in disk type choice

Disk speed (RPM)	Disk form factor	Interface or transport	Capacity	Random I/O performance	Sequential I/O performance	Power utilization
5,400	2.5-inch	SATA	Average	Poor	Poor	Excellent
5,400	3.5-inch	SATA	Excellent	Poor	Poor	Above average
7,200	2.5-inch	SATA	Average	Average	Average	Excellent
7,200	2.5-inch	Serial Attached SCSI	Average	Average	Above average	Excellent
7,200	3.5-inch	SATA	Excellent	Average	Above average	Above average
7,200	3.5-inch	Serial Attached SCSI	Excellent	Average	Above average	Above average
7,200	3.5-inch	Fibre Channel	Excellent	Average	Above average	Average
10,000	2.5-inch	Serial Attached SCSI	Below average	Excellent	Above average	Above average
10,000	3.5-inch	SATA	Average	Average	Above average	Above average
10,000	3.5-inch	Serial Attached SCSI	Average	Above average	Above average	Below average
10,000	3.5-inch	Fibre Channel	Average	Above average	Above average	Below average
15,000	2.5-inch	Serial Attached SCSI	Poor	Excellent	Excellent	Average
15,000	3.5-inch	Serial Attached	Average	Excellent	Excellent	Below average

		SCSI				
15,000	3.5-inch	Fibre Channel	Average	Excellent	Excellent	Poor
SSD: enterprise class	Not applicable	SATA, Serial Attached SCSI, Fibre Channel	Poor	Excellent	Excellent	Excellent

Return to top

Best Practices for Supported Storage Configurations

This section provides best practice information about supported disk and array controller configurations.

Redundant Array of Independent Disks (RAID) is often used to both improve the performance characteristics of individual disks (by striping data across several disks) as well as to provide protection from individual disk failures. With the advancements in Exchange 2010 high availability, RAID is no longer a required component for Exchange 2010 storage design. However, RAID is still an essential piece to Exchange 2010 storage design for stand-alone servers as well as high availability solutions that require either additional performance or greater storage reliability. The following table provides guidance for the common RAID types that can be used with the Exchange 2010 Mailbox server.

Supported data types for the Exchange 2010 Mailbox server role

Data type	Stand-alone: supported or best practice	High availability: supported or best practice
OS, system, or pagefile volume	Supported: All RAID types. Best practice: RAID1/10. Use a dedicated array group; don't host both system LUN and data LUNs on the same array group.	Supported: All RAID types. Best practice: RAID1/10. Use a dedicated array group; don't host both system LUN and data LUNs on the same array group.
Exchange mailbox database (.edb) file volume	Supported: All RAID types. Best practice: 5,400 or 7,200 disks = RAID1/10 only. RAID5* = Maximum of 7 disks per array group and array controller high priority scrubbing and surface scanning enabled. RAID6* = High priority scrubbing and surface scanning enabled.	Supported: All RAID types. Just a bunch of disks (JBOD) (not RAID) (three or more database copies). Best practice: 5,400 or 7,200 disks = RAID1/10 only or JBOD. When lagged, database copies should have two or more lagged copies, or lagged copies should be protected with RAID. RAID5* = Maximum of 7 disks

		per array group and array controller high priority scrubbing and surface scanning enabled. RAID6* = High priority scrubbing and surface scanning enabled.
Exchange mailbox database log volume	Supported: All RAID types. Best practice: RAID1/10.	Supported: All RAID types. JBOD (not RAID) (three or more database copies). Best practice: RAID1/10. When lagged, database copies should have two or more lagged copies, or lagged copies should be protected with RAID.

*Includes RAID variations such as RAID50 or RAID51 for RAID5

The following table provides guidance about storage array configurations for Exchange 2010.

Supported RAID types for the Exchange 2010 Mailbox server role

RAID type	Description	Supported or best practice
Disk array RAID stripe size (KB)	The stripe size is the per disk unit of data distribution within a RAID set. Stripe size is also referred to as *block size*.	Best practice: 256 KB or greater. Follow storage vendor best practices.
Storage array cache settings	The cache settings are provided by a battery-backed caching array controller.	Best practice: 75 percent write cache and 25 percent read cache (battery-backed cache). Follow storage vendor best practices.
Physical disk write caching	The settings for the cache are on each individual disk.	Supported: Physical disk write caching must be disabled when used without a UPS.

The following table provides guidance about database and log file choices.

Database and log file choices for the Exchange 2010 Mailbox server role

Database and log file options	Description	Stand-alone: supported or best practice	High availability: supported or best practice
File placement:	Database per log isolation refers to placing	Best practice: For recoverability, move	Supported: Isolation of logs and databases isn't

database per log isolation	the database file and logs from the same mailbox database onto different volumes backed by different physical disks.	database (.edb) file and logs from the same database to different volumes backed by different physical disks.	required.
File placement: database files per volume	Database files per volume refers to how you distribute database files within or across disk volumes.	Best practice: Based on your backup methodology.	Supported: When using JBOD, divide a single disk into two volumes (one for database; one for log stream).
File placement: log streams per volume	Log streams per volume refers to how you distribute database log files within or across disk volumes.	Best practice: Based on your backup methodology.	Supported: When using JBOD, divide a single disk into two volumes (one for database; one for log stream). Best practice: When using JBOD, single database per log per volume.
Database size	Database size refers to the disk database (.edb) file size.	Supported: Approximately 16 terabytes. Best practice: • 200 gigabytes (GB) or less. • Provision for 120 percent of calculated maximum database size.	Supported: Approximately 16 terabytes. Best practice: • 2 terabytes or less. • Provision for 120 percent of calculated maximum database size.
Log truncation method	Log truncation method is the process for truncating and deleting old database log files. There are two mechanisms: • Circular logging, in which Exchange deletes the logs. • Log truncation, which occurs after a successful full or incremental Volume Shadow Copy Service (VSS)	Best practice: • Use backups for log truncation (for example, circular logging disabled). • Provision for three days of log generation capacity.	Best practice: • Enable circular logging for deployments that use Exchange 2010 data protection features. • Provision for three days beyond replay lag setting of log generation capacity.

	backup.		

The following table provides guidance about Windows disk types.

Windows disk types for the Exchange 2010 Mailbox server role

Windows disk type	Description	Stand-alone: supported or best practice	High availability: supported or best practice
Basic disk	A disk initialized for basic storage is called a basic disk. A basic disk contains basic volumes, such as primary partitions, extended partitions, and logical drives.	Supported. Best practice: Use basic disks.	Supported. Best practice: Use basic disks.
Dynamic disk	A disk initialized for dynamic storage is called a dynamic disk. A dynamic disk contains dynamic volumes, such as simple volumes, spanned volumes, striped volumes, mirrored volumes, and RAID-5 volumes.	Supported.	Supported.

The following table provides guidance on volume configurations.

Volume configurations for the Exchange 2010 Mailbox server role

Volume configuration	Description	Stand-alone: supported or best practice	High availability: supported or best practice
GUID partition table (GPT)	GPT is a disk architecture that expands on the older master boot record (MBR) partitioning scheme. The maximum NTFS formatted partition size is 256 terabytes.	Supported. Best practice: Use GPT partitions.	Supported. Best practice: Use GPT partitions.
MBR	An MBR, or partition sector, is the 512-byte boot sector that is the first sector (LBA Sector 0) of a partitioned data storage device such as a hard disk. The maximum NTFS formatted partition size is 2 terabytes.	Supported.	Supported.

Partition alignment	Partition alignment refers to aligning partitions on sector boundaries for optimal performance.	Supported: The Windows Server 2008 default is 1 megabyte (MB).	Supported: The Windows Server 2008 default is 1 MB.
Volume path	Volume path refers to how a volume is accessed.	Supported: Drive letter or mount point. Best practice: Mount point host volume must be RAID enabled.	Supported: Drive letter or mount point. Best practice: Mount point host volume must be RAID-enabled.
File system	File system is a method for storing and organizing computer files and the data they contain to make it easy to find and access the files.	Supported: NTFS support only.	Supported: NTFS support only.
NTFS defragmentation	NTFS defragmentation is a process that reduces the amount of fragmentation in Windows file systems. It does this by physically organizing the contents of the disk to store the pieces of each file close together and contiguously.	Supported. Best practice: Not required and not recommended.	Supported. Best practice: Not required and not recommended.
NTFS allocation unit size	NTFS allocation unit size represents the smallest amount of disk space that can be allocated to hold a file.	Supported: All allocation unit sizes. Best practice: 64 KB for both .edb and log file volumes.	Supported: All allocation unit sizes. Best practice: 64 KB for both .edb and log file volumes.
NTFS compression	NTFS compression is the process of reducing the actual size of a file stored on the hard disk.	Supported: Not supported for Exchange database or log files.	Supported: Not supported for Exchange database or log files.
NTFS Encrypting File System (EFS)	EFS enables users to encrypt individual files, folders, or entire data drives. Because EFS provides strong encryption through industry-standard algorithms and public key cryptography, encrypted files are confidential even if an	Supported: Not supported for Exchange database or log files.	Not supported for Exchange database or log files.

	attacker bypasses system security.		
Windows BitLocker (volume encryption)	Windows BitLocker is a data protection feature in Windows Server 2008. BitLocker protects against data theft or exposure on computers that are lost or stolen, and it offers more secure data deletion when computers are decommissioned.	Supported: All Exchange database and log files.	Supported: All Exchange database and log files. Windows failover clusters require Windows Server 2008 R2 or Windows Server 2008 R2 SP1 and the following hotfix: You cannot enable BitLocker on a disk volume in Windows Server 2008 R2 if the computer is a failover cluster node. Exchange volumes with Bitlocker enabled are not supported on Windows failover clusters running earlier versions of Windows. For more information about Windows 7 BitLocker encryption, see BitLocker Drive Encryption in Windows 7: Frequently Asked Questions.

Return to top

Windows Disk Timeouts

Starting with Exchange 2010 Service Pack 1 (SP1), intelligence is included to deal with hung I/O. Before Exchange 2010, Exchange reported slow I/O in the event log, but does not take any other action. Exchange 2010 SP1 will actively fail (bugcheck) the server if the hung I/O is affecting active databases on a DAG node.

The new recovery logic in Exchange 2010 SP1 leverages the built-in Windows bugcheck behavior when certain conditions occur. Specifically, when hung IO occurs. The Extensible Storage Engine (ESE) has been updated to detect hung IO and to take corrective action to automatically recover the server.

ESE maintains an IO watchdog thread that detects when an IO has been outstanding for a specific period of time. By default, if an IO for a database is outstanding for more than one minute, ESE logs an event. If a database has an IO that has been outstanding for more than four minutes, ESE logs a specific failure event, if it is possible to do so.

ESE Event 507, 508, 509, or 510 may or may not be logged, depending on the nature of the hung IO. If the nature of the problem is such that the OS volume is affected or the ability to write to the event log is affected, the events are not logged. If the events are logged, the Microsoft Exchange Replication service (MSExchangeRepl.exe) detects that

condition, and intentionally cause a bugcheck of Windows by terminating the wininit.exe process. The following table describes the recovery logic behavior in Exchange 2010 SP1 and earlier versions.

Exchange Version	I/O Type	I/O Time	Behavior
Exchange Server 2003	Completed	>60 seconds	Write to Event Log
Exchange Server 2007	Completed	>60 seconds	Write to Event Log
Exchange 2010 RTM	Completed	>60 seconds	Write to Event Log ESE performs clean-page overwrite on pages affected by slow I/O
Exchange 2010 SP1	In Flight	>60 seconds	Write to Event Log
Exchange 2010 SP1	In Flight	>4 minutes	Terminate wininit.exe process and bugcheck the server
Exchange Server 2010 SP1	Completed	>30 seconds	Write to event log ESE performs clean-page overwrite on pages affected by slow I/O

Note:

In the **I/O Type** column of the table, **In Flight** describes a slow I/O operation that has not yet successfully finished. and **Completed** describes a slow I/O operation that took more than 30 seconds to finish. The concept of detecting slow I/O in-flight operations is new in Exchange 2010. In earlier versions of Microsoft Exchange, the program reported only after the I/O had finished.

We recommend that you do not change the new recovery logic behavior in Exchange 2010 SP1. However, if you must change the new behavior, see New High Availability and Site Resilience Functionality in Exchange 2010 SP1 for more information about how to do this.

The following table outlines the recommended guidance for setting the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\TimeOutValue** registry subkey for servers that are running the Exchange 2010 Mailbox role.

Scenario	Recommendation
Direct-Attached Storage	Reduce Windows disk TimeOutValue to 20 seconds Refer to hardware manufacturer's guidance Hardware manufacturer's guidance takes priority in the event of a clash
SAN-Attached RAID Storage	Reduce Windows disk TimeOutValue to 20 seconds Refer to hardware manufacturer's guidance

	Hardware manufacturer's guidance takes priority in the event of a clash
JBOD Storage	Increase Windows disk TimeOutValue to 180 seconds Refer to hardware manufacturer's guidance Hardware manufacturer's guidance takes priority in the event of a clash

For more information, see the Exchange Server Team Blog article Windows Disk Timeouts and Exchange Server 2010.

1.2.1.9.7 Understanding Exchange 2010 LUN Architecture

Understanding Exchange 2010 LUN Architecture

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-22*

In many cases, the physical disk, or optimal logical unit number (LUN), that the operating system recognizes is abstracted from the hardware used to present the disk to the operating system. LUN architecture is used in Microsoft Exchange Server 2010.

Although there are many ways to design LUNs in Exchange 2010, we recommend the following designs to limit complexity:

- One LUN per Database
- Two LUNs per Database
- Two LUNs per Backup Set

One LUN per Database

Single LUN per database architecture means that both the database and its corresponding log files are placed on the same LUN. To deploy a LUN architecture that only uses a single LUN per database, you must have a database availability group (DAG) that has two or more copies, and not be using a hardware-based Volume Shadow Copy Service (VSS) solution.

Some of the benefits of this strategy include:

- Simplifies storage administration with fewer LUNs to manage.
- Reduces (potentially) the number of backup jobs.
- Provides flexibility to isolate the performance between databases when not sharing spindles between LUNs.

A concern with this strategy is that it limits the ability to perform hardware-based VSS backup and restore procedures (for example, clone snapshots). For VSS details, see Best Practices for Using Volume Shadow Copy Service with Exchange Server 2003.

Return to top

Two LUNs per Database

With Exchange 2010, in the maximum case of 100 databases, the number of LUNs you provision will depend upon your backup strategy. If your recovery time objective is small, or if you use VSS clones for fast recovery, it may be best to place each database on its own transaction log LUN and database LUN. This approach will exceed the number of available drive letters; therefore, volume mount points must be used.

Some of the benefits of this strategy include:

- Enables hardware-based VSS at a database level, providing single database backup and restore.
- Provides flexibility to isolate the performance between databases when not sharing spindles between LUNs.
- Increases reliability because a capacity or corruption problem on a single LUN will only impact one database. This is an important consideration when you aren't leveraging the built-in mailbox resiliency features.

Some of the concerns with this strategy include:

- 100 databases require 200 LUNs, which could exceed some storage array maximums.
- A separate LUN for each database causes more LUNs per server, which increases administrative costs and complexity.

Return to top

Two LUNs per Backup Set

A backup set is the number of databases fully backed up in a night. A solution that performs a full backup on 1/7th of the databases nightly (for example, using a weekly or bimonthly full backup with daily incremental or differential backups) can reduce complexity by placing all of the databases to be backed up on the same log and database LUN. This can reduce the number of LUNs on the server.

Some of the benefits of this strategy include:

- Simplifies storage administration with fewer LUNs to manage.
- Reduces (potentially) the number of backup jobs.

Some of the concerns with this strategy include:

- The ability to perform hardware-based VSS backup and restore procedures (for example, clone snapshots) is limited. For VSS details, see Best Practices for Using Volume Shadow Copy Service with Exchange Server 2003.
- A capacity or corruption problem on a single LUN could impact more than one database.

Return to top

1.2.1.9.8 Understanding Exchange 2010 Page Zeroing

Understanding Exchange 2010 Page Zeroing

Planning and Deployment > Planning for Exchange 2010 > Mailbox Server Storage Design >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

By default, most storage systems (file systems and databases) don't write over the actual data when it's deleted. They delete the pointer to the data and add the pages and blocks backing the data to a free or available list. The data is eventually deleted when the pages and blocks are re-used. *Data zeroing* is a mechanism that writes either zeros or a binary pattern over deleted data in an attempt to make the data much more difficult to recover. This action is taken for security reasons. Data zeroing occurs prior to the pages and blocks being re-used by the storage system.

Page Zeroing in Exchange 2010 SP1

In Service Pack 1 (SP1) for Exchange Server 2010, page zeroing is on by default. There is no mechanism to disable it. Page zeroing operations are recorded in the transaction log files so that all copies of a database are page-zeroed in a similar manner. That is, zeroing a page on the active database causes the page to get zeroed on a passive database after the passive database replays the transaction log with the page zeroing log record. There is no mechanism for the Extensible Storage Engine (ESE) to prioritize the reutilization of zeroed pages over allocating new space. Tables which have sequential space allocation assigned will intentionally skip fragmented or zeroed pages in favor of using new or free sequential pages. This approach reduces the database I/O footprint of the server.

In Exchange 2010 SP1, improvements to database page zeroing help to reduce the performance impact on servers when they're performing zeroing functions. Key improvements are:

- **Optimized storage and network capacity** The Extensible Storage Engine (ESE) writes a page-zeroing record to the transaction log file instead of logging the entire page image. This approach reduces log write I/O, keeps the capacity footprint of the logs as low as possible, and reduces the bandwidth requirements to ship the logs from active to passive copies.
- **Optimized database disk I/O** In previous versions of Exchange 2010, page zeroing occurred only during a backup or scheduled maintenance process (when configured), and caused significant database disk I/O. In Exchange 2010 SP1, page zeroing occurs by default and happens primarily at transaction time. For the majority of cases, the zeroing occurs immediately after the hard delete. This design allows the database to utilize the checkpoint depth capability of the engine, which ensures dirty pages stay in cache for a certain amount of time so additional page updates that occur in close time proximity don't cause additional database write I/O. Because of this design, page zeroing has no significant database I/O impact, which is why it's enabled by default.

Implementation of Page Zeroing in the ESE Database

The ESE database uses pages as its unit of storage and has implemented *page zeroing*. ESE page zeroing writes a binary pattern once over a hard-deleted record. The page-zeroing pattern is specific to the ESE engine operation and is different for run-time operations vs. maintenance operations. The following table lists the fill patterns that correspond to specific run-time operations.

Fill pattern of page zeroing per ESE run-time operation

ESE run-time operation	Fill pattern
Replace	R
Record/long value delete	D

Freed page space	H

The following table lists the fill patterns that correspond to specific operations that occur during ESE background database maintenance.

Fill pattern of page zeroing per ESE background database maintenance operation

ESE background database maintenance operation	Fill pattern
Record delete	D
Long value delete	L
Freed page space of partially used page	Z
Freed page space of unused page	U

Background Database Maintenance

Configured by default, background database maintenance is a process which continuously checksums and scans the database in the background. Its primary function is to checksum the database pages, but it also handles cleaning up after Exchange 2010 Store crashes (cleaning up space and zeroing out records and pages which did not occur due to the crash). Background database maintenance processes approximately 5 MB per second per database. If timely page zeroing is a priority, you can reduce database sizes to ensure page zeroing occurs for the crash recovery cases in a shorter time period (for example, 24 hours). For more information, see New Exchange Core Store Functionality.

Background database maintenance is a continuous process, so there are no events associated with its start and completion. You can track the progress of background database maintenance completion with the following performance counter:

- MSExchange Database =>Instances->Database Maintenance Duration: This performance counter indicates the number of seconds that have passed since maintenance last completed for a given database.

Process of ESE Database Page Zeroing

The following table discusses database delete scenarios, and when page zeroing functions occur.

ESE background database maintenance operation

Database delete scenario	ESE process and timeframe to zero database data
• Scenario 1: Single item recovery is disabled and user purges item from the Recoverable Items folder. • Scenario 2: Single item recovery is disabled and the Recoverable Items retention period is set to zero. • Scenario 3: Single item recovery is enabled and the item expires based on the deleted item retention period.	An asynchronous thread writes a binary pattern over the deleted data. This action occurs within milliseconds of the record deletion. If the Store process crashes while the asynchronous zeroing work is still outstanding (or version store cleanup is cancelled due to version store growth), the zeroing is completed when background database maintenance (24x7) processes that section of the database. For more

	information about background database maintenance, see New Exchange Core Store Functionality.
View Scenario: Expiration of items from Outlook/ Outlook Web Access folder view (for example, Conversation view)	Data zeroing occurs when background database maintenance (24x7) processes this section of the database.
Move Mailbox/Delete Mailbox Scenario: Deletion of source mailbox (expiry of deleted mailbox from dumpster)	Data zeroing occurs when background database maintenance (24x7) processes this section of the database.

Monitoring Page Zeroing Behavior

You can measure and monitor page zeroing functionality with the following ESE performance counters:

- MSExchange Database->Database Maintenance Pages Zeroed: This performance counter indicates the number of pages zeroed by the database engine since the performance counter was invoked.
- MSExchange Database->Database Maintenance Pages Zeroed/sec: This performance counter indicates the rate at which pages are zeroed by the database engine.

Note:
To learn how to enable these counters, see How to Enable Extended ESE Performance Counters.

Page zeroing is a database maintenance function, so performance information related to both page zeroing for run-time transactions and page zeroing due to background database maintenance is included in these counters.

Exchange 2010 Mailbox Data and Page Zeroing

Only the Mailbox database file (.edb) has provisions for page zeroing. The following Exchange 2010 Mailbox data types have no provisions for page zeroing:

- Mailbox database transaction logs (.log)
  When transaction logs are deleted (due to truncation via backup or circular logging), there is no process to zero the blocks in the NTFS file system backing the log file. It's likely that NTFS will quickly re-utilize that free space for newly created logs, but there is no guarantee that this will happen.
- Content index catalog files
  Exchange 2010 uses Exchange Search (MSExchangeSearch) for search indexing functionality. The search index catalog is comprised of several dozen files stored on the same volume as the mailbox database file. When a message is hard-deleted from the mailbox database, the associated content in the search catalog isn't immediately deleted. The content deletion occurs when MS Search does a shadow, or master merge, of many small catalog files in to a single larger file. After the master merge completes, the smaller catalog files are deleted. There is no process to zero the blocks which backed the deleted catalog files. To ensure the catalog files are fully zeroed, use the following process:
  .1.Stop the MSExchangeSearch and Microsoft Search (MSSearch) processes on affected servers.

.2.Delete the catalog directory for each affected database (on all copies).
.3.Re-start the MSExchangeSearch and MSSearch processes.
.4.Zero-out the freed block using a NTFS block zeroing tool.

Note:
Deleting the content index catalog files severely impacts the client user experience on the Exchange 2010 server. Outlook Web App and Exchange ActiveSync server searches will be broken until the content index rebuilds the catalog by re-crawling each database. This rebuild could take several days to several weeks to complete.

1.2.1.9.9 Mailbox Server Processor Capacity Planning

Mailbox Server Processor Capacity Planning

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-19*

Mailbox server capacity planning has changed significantly from previous versions of Exchange due to mailbox resiliency provided in Microsoft Exchange Server 2010. Exchange 2010 has been reengineered with the concept of mailbox resiliency, in which the architecture changed so that automatic failover protection is now provided at the individual mailbox database level instead of at the server level. There are two primary changes that affect the Mailbox server role capacity planning process:

- Hosting active and passive database copies on the same server
- Providing database copy count

You can use the information in this topic to better understand these changes and as design guidance for sizing Mailbox servers when configured for mailbox resiliency.

Contents

Hosting Active and Passive Database Copies on the Same Server

In Exchange 2010, you can host both active and passive database copies on the same server when the server is configured for mailbox resiliency. The processors on each server service the workload from both active mailboxes (hosted on active, mounted databases) as well as passive mailboxes (hosted on passive databases). The processor requirements for passive mailboxes and databases must be considered when performing Exchange 2010 mailbox capacity planning. A passive database copy uses CPU resources to check or validate replicated logs, to replay replicated logs into the database, and to maintain the content index associated with the database copy. In general, each passive mailbox

(hosted on a passive database copy) equates to 15 percent of the CPU utilization required to host the active mailbox (hosted on an active database copy).

A key aspect of Exchange 2010 mailbox capacity planning is determining how many database copies you plan to activate on a per-server basis when configured for mailbox resiliency. There is a range of designs from which you can choose, but we recommend the following models:

- **Design for all database copies activated** In this model, you design your server to handle 100 percent of hosted database copies becoming active.
- **Design for targeted failure scenarios** In this model, you design your server to handle the active mailbox load during the worst failure case.

For more information, see the following topics:

- Understanding High Availability Factors
- Understanding Processor Configurations and Exchange Performance
- Understanding Memory Configurations and Exchange Performance

Return to top

Database Copy Count

Using Exchange 2010 mailbox resiliency, you can configure multiple database copies (up to 16 copies per database). Each additional database copy increases the CPU work the server hosting the active copy must do. This additional work on the server with the active copy is primarily log replication and content indexing because each passive copy will retrieve content to index from the active copy.

The per-mailbox CPU requirements of the server hosting the active database copy must be increased by 10 percent for each additional database copy (for example, one copy = 10 percent, two copies = 20 percent, and so on). This factor is only applied to the CPU requirements for the server hosting the active database copy. The CPU used to host passive database copies isn't applied to this calculation. For more information, see Understanding Processor Configurations and Exchange Performance.

Return to top

Design Steps

Due to new sizing factors, additional steps are required to size Mailbox servers when configured for mailbox resiliency. The general steps are as follows:

1. Consider high availability requirements for the overall solution architecture. Consider mailbox resiliency or a stand-alone solution, site resiliency, the number of database copies required, and the number of servers or database availability groups (DAGs) to handle common failure cases.
2. If using mailbox resiliency, choose which database activation model to design for. (Design for targeted failure scenario or design for all database copies activated.)
3. Use the following table to estimate CPU and memory requirements based on design. Consider CPU and memory requirements for active mailboxes, CPU requirements for passive mailboxes, and CPU requirements on the active mailbox for additional database copies. Use the activation model choice to define the maximum number of mailboxes the design can accommodate.

The following table provides estimated values based on user profile. The estimated values are based on a peak two-hour period during the knowledge worker workday (for example, from 10:00 until noon). This peak period is often twice the 8 to 10-hour daily average load. The user profile description has been omitted because the range of profiles has grown as e-mail usage has increased.

Per mailbox database cache, IOPS, and CPU estimates based on user profile and message activity

Messages sent or received per mailbox per day	Database cache per mailbox in megabytes (MB)	Single database copy (stand-alone) with estimated IOPS per mailbox	Multiple database copies (mailbox resiliency) with estimated IOPS per mailbox	Megacycles for active mailbox or stand-alone mailbox	Megacycles for passive mailbox
50	3	0.06	0.05	1	0.15
100	6	0.12	0.1	2	0.3
150	9	0.18	0.15	3	0.45
200	12	0.24	0.2	4	0.6
250	15	0.3	0.25	5	0.75
300	18	0.36	0.3	6	0.9
350	21	0.42	0.35	7	1.05
400	24	0.48	0.4	8	1.2
450	27	0.54	0.45	9	1.35
500	30	0.6	0.5	10	1.5

Note:
You must increase the megacycles per active mailbox by 10 percent for each additional database copy after the one active copy.

Calculating the Megacycles for Different Processor Configurations

The example in the next section "Example of Capacity Planning for a Mailbox Server" uses a baseline processor configuration, 2 x 4 core Intel Xeon x5470 3.33-gigahertz (GHz) processors, which yields 3,333 megacycles per processor core. However, this processor configuration most likely isn't the processor configuration you're deploying. You can use the following steps to perform a megacycle adjustment to determine the available megacycles your server design can support.

1. Open a Web browser, and then go to Standard Performance Evaluation Corporation.
2. Click **results**, highlight **CPU2006**, and then select **Search CUP2006 Results**.
3. In the **Available Configurations** drop-down box, select **SPECint2006 Rates**. In **Search Form Request**, select the **Simple** option and then click **Go**. Under **Simple Request**, enter the search criteria (for example, **Processor Matches x5550**).
4. Find the server and processor you're planning to deploy, click **Execute Simple Fetch**, and note the resulting value.

For example, consider that you're deploying a Dell PowerEdge M710 8-core server with Intel x5550 2.67GHz processors (2,670 megahertz (MHz)). For this configuration, the SPECint_rate2006 results value is 240, with a value of 30 per core (known in the formula as *new platform per core value*).

The baseline system HP DL380 G5 x5470 3.33GHz, 8 cores (3,333 MHz), has a

SPECint_rate2006 results value of 150, or 18.75 per core (known in the formula as *baseline per core value*).

To determine the megacycles of the M710 platform example, use the following formula:

((New platform per core value) × (Hertz per core of baseline platform)) ÷ (Baseline per core value) = Adjusted megacycles per core

30 × 3,333 ÷ 18.75 = 5,333 megacycles per core or 42,662 megacycles per server

Example of Capacity Planning for a Mailbox Server

The following example illustrates the processor sizing process. The example has the following design assumptions:

- **Mailbox count** 12,000.
- **Mailbox profile** 150 messages sent or received per day.
- **Availability requirements** Mailbox resiliency within a single site, tolerance for double-server failures.
- **Storage architecture** Just a bunch of disks (JBOD) (not RAID) storage with three database copies, 300 mailboxes per database, 40 databases with 30 database copies per server (or 120 database copies per DAG). The three database copies are randomly distributed across the four nodes so no two servers look alike.
- **Activation model** Targeted failure scenario, where double-server failures are tolerated with minimal outage. This results in 20 databases out of 30 copies per server being activated after two server failure events.
- **Server platform** 2 x 4 core Intel Xeon x5470 3.33-GHz processors.

The following process applies.

1. **Calculate server count** A four-node DAG is required to tolerate double-server failures, so the design needs to begin with four Mailbox servers within the DAG.
2. **Calculate maximum active mailboxes per server based on the activation model** Assuming the active databases are equally distributed across the nodes, each server would ideally host 3,000 active mailboxes (12,000 ÷ 4). To calculate the active mailbox count after a double-node failure (based on this example), the mailbox count would be divided by the remaining two nodes, which equals 6,000 active mailboxes per node (12,000 ÷ 2).
   In this example, the *MaximumActiveDatabases* parameter on the **Set-MailboxServer** cmdlet is configured for 20.
3. **Calculate active mailbox CPU requirements** Multiply the maximum number of active mailboxes (20 × 300 = 6,000 active mailboxes) by the megacycles per active mailbox (6,000 × 3 megacycles = 18,000 megacycles), based on the preceding table. Multiply this value by 10 percent for each additional database copy.
   In this example, there's one active copy and two passive copies for every database, so the 18,000 megacycles is increased by 20 percent (18,000 × 1.2 = 21,600 megacycles).
4. **Calculate passive mailbox CPU requirements** Multiply the number of passive mailboxes (when a server is hosting the maximum number of active mailboxes) by the megacycles per passive mailbox (3,000 × .45 megacycles = 1,350 megacycles), based on the preceding table.
5. **Add active and passive CPU requirements to get total CPU requirement** In this example, 21,600 active mailbox megacycles + 1,350 passive mailbox megacycles = 22,950 megacycles total CPU requirement.
6. **Apply total CPU requirement to hardware platform** This example uses a 2 x 4 core Intel Xeon x5470 3.33-GHz processor-based server. This equates to 26,664 megacycles (8 × 3,330 MHz). Divide the required megacycles by the available megacycles based on the server platform to estimate the CPU utilization at peak period after a double-node failure (22,950 ÷ 26,664 = 86

percent predicted CPU utilization). The 86 percent CPU utilization rate represents a fully utilized server with almost no space, but because this is based on a double-failure condition that occurs during the peak period, this rate may be acceptable.
We recommend that stand-alone servers be designed to not exceed 70 percent utilization during peak period, and two-node and three-node configurations that can only tolerate a single-node failure be designed not to exceed 80 percent utilization at the peak period (during a node failure).

Virtualization

If you're sizing a new virtualized deployment, you don't want to oversubscribe processors. Therefore, you want to have a 1:1 ratio of logical cores to virtual CPUs on your host. From there, use the physical sizing guidance discussed in this topic and then account for 10 percent hypervisor CPU overhead. For example, if you sized your physical deployment for 500 users per core, your virtual deployment would be sized for 450 users per core.

Calculating the Number of Required Mailbox Cores per Data Center

As discussed in Understanding Server Role Ratios and Exchange Performance, you will need to size your Hub Transport server, Client Access server, and global catalog server based on the load of the Mailbox servers.

It's a common assumption that the processor core ratio guidance is based on the total number of mailbox cores being deployed; however, that isn't the case. Generally, the Mailbox servers aren't running at 100 percent CPU utilization 100 percent of the time. A well-designed solution should never have 100 percent CPU utilization for an extended duration of time based on the 70 percent and 80 percent design thresholds described in the previous section.

To calculate the minimum number of Hub Transport server, Client Access server, and global catalog server processor cores, you need to determine the number of mailbox cores required to support the active mailbox databases during the worst failure model.

The formula to calculate the required mailbox cores within a data center is:

Required mailbox cores = (active mailbox CPU requirements) ÷ (adjusted megacycles per core) × (number of remaining servers) × (number of DAGs)

If you aren't deploying a high availability solution, the formula is:

Required mailbox cores = (active mailbox CPU requirements) ÷ (adjusted megacycles per core) × (number of Mailbox servers within the data center)

Example of Calculating the Number of Required Mailbox Cores per Data Center

Continuing with the previous example, the solution can sustain two server failures, with each remaining server requiring 18,000 megacycles. Therefore:

Required mailbox cores = (18,000 ÷ 3,333) × 2

= 5.4 × 2

= 11 total cores

This means that, within this data center, a total of 11 cores will be used out of the available 16 mailbox cores during the targeted failure model (or 5.5 cores per remaining Mailbox server).

Based on this data, the minimum number of processor cores that should be deployed

within the data center for the Hub Transport server, Client Access server, and global catalog server is:

Minimum Hub Transport server (with antivirus) processor cores per data center = (number of required mailbox cores per data center) ÷ 5

= 11 ÷ 5

= 3 cores

Minimum Client Access server processor cores per data center = (number of required mailbox cores per data center) × 3 ÷ 4

= 11 × 3 ÷ 4

= 33 ÷ 4

= 9 cores

Minimum global catalog server (64-bit) processor cores per data center = (number of required mailbox cores per data center) ÷ 8

= 11 ÷ 8

= 2 cores

Return to top

1.2.1.9.10 Exchange 2010 Mailbox Server Role Design Example

Exchange 2010 Mailbox Server Role Design Example

Planning and Deployment > Planning for Exchange 2010 > Mailbox Server Storage Design >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-01*

This topic provides an example of how to determine the appropriate memory, capacity, I/O, and CPU performance requirements for the Mailbox server role and its accompanying architecture.

You can use the Exchange Server 2010 Mailbox Server Role Requirements Calculator to determine the appropriate requirements for the Mailbox server role by specifying your set of input factors. The calculator can determine the requirements discussed in this example. For more information about the calculator (and to download it), see the Exchange Server Team Blog article Exchange 2010 Mailbox Server Role Requirements Calculator.

Note:

The content of each blog and its URL are subject to change without notice. The content within each blog is provided "AS IS" with no warranties, and confers no rights. Use of included script samples or code is subject to the terms specified in the Microsoft Terms of Use.

For more information about the Mailbox Server role storage design, see Mailbox Server Storage Design.

The scenario used in this example is that of a three database copy solution that makes use of JBOD (just a bunch of disks) storage. For the purposes of this example, consider the following architecture requirements:

- Six Mailbox servers participating in a single database availability group (DAG)
- Exchange Mailbox server also hosts the Hub Transport and Client Access server roles
- Three high availability mailbox database copies, no lagged database copies
- 7.2 K (7,200 RPM) 1-terabyte SATA spindles are used
- JBOD storage configuration (1 logical unit number (LUN) / Database LUN architecture)
- For backup architecture, using the native data protection features provided via single item recovery and mailbox resiliency
- A restore LUN is deployed for maintenance and recovery operations
- Each LUN has at minimum 20 percent free space
- The solution should survive double server failure events
- The only server role installed is the Mailbox server role

Contents

Mailbox Capacity Requirements

The following example illustrates appropriate sizing for an environment in which there are 24,000 2-GB 100 messages per day profile mailboxes spread across six Mailbox servers that are participating within a DAG with each database having three copies. These mailboxes receive an average of 37 MB of mail per five-day work week, with an average message size of 75 KB. Single item recovery is enabled with a 14-day deleted item retention window. The following calculations are used to determine the mailbox size:

Mailbox Size = Mailbox Limit + Whitespace + Dumpster

Whitespace = 100 messages per day x 75/1024 MB = 7.32 MB

Dumpster = (100 messages per day x 75/1024 MB * 14 days) + (2048 MB x 0.012) + (2048 MB x 0.03) = 188.6 MB

Example values for determining actual mailbox size on disk

Mailbox quota	Dumpster size (two weeks)	White space	Total size on disk
2 GB	188.7 MB	7.3 MB	2.19 GB (+12%)

Because this environment leverages JBOD storage, the maximum database size that can be deployed is dependent on the size of the disk. To determine the maximum database size for the JBOD scenario, use the following formula where the formatted capacity of a 1TB disk is 931 GB, the Free Space Percentage Requirement is 20 percent, and the Content Index Percentage is 10 percent:

Maximum Database Size = [Formatted Disk Capacity x (1 – Free Space Percentage Requirement)] / (1 + Content Index Percentage)

= [931 GB x (1 - .2)] / (1+ .10)

= 744.8 GB / 1.1

= 677 GB

In this environment, each user's mailbox consumes 2.25 GB of disk space. To support 24,000 mailboxes, with a 677 GB database size, it's necessary to have 102 databases. This requirement results in a final count of 235 mailboxes per database.

However, because this solution is leveraging a JBOD storage architecture, it's vital to ensure that the number of mailboxes per database not exceed the amount of random I/O that can be achieved on the single disk. Because this solution is leveraging large form factor 7.2K SATA spindles, the spindle can achieve a maximum of 55 random I/O per second (IOPS) when fully utilized. Factoring in a 20 percent I/O overhead growth buffer, this means that the spindle can handle a total of 44 random IOPS.

Provided that the user base has a 100 messages per day profile, each mailbox is expected to consume 0.1 IOPS; therefore, the disk can support a maximum of 440 mailboxes with this IOPS profile. Because the capacity calculations determined that the maximum number of mailboxes that can be supported is 235 and this is below the 440 mailboxes determined based on the IOPS profile, this solution can be deployed on a single disk.

To determine the actual database size, use the following formula:

Database Size = Number of Mailboxes x Mailbox Size on Disk x Database Overhead Growth Factor

Based on the number of mailboxes, the actual size of the mailboxes, and the database growth overhead factor of 20 percent, the database size is 619 GB as shown in the following table.

Database capacity requirements

Mailboxes per database	Total number of databases	Database size requirements
235	102	619 GB

To ensure that the Mailbox server doesn't sustain any outages as a result of space allocation issues, the transaction logs also need to be sized to accommodate all of the logs that will be generated during the backup set. Provided that this architecture is leveraging the mailbox resiliency and single item recovery features as the backup architecture, the log capacity should allocate for three times the daily log generation rate in the event that a failed copy isn't repaired for three days. (Any failed copy prevents log truncation from occurring.)

A 100 messages per day profile mailbox generates 20 transaction logs per day on average, so a 24,000 mailbox environment will generate 576,000 transaction logs each day. Therefore, each database will generate 5,647 logs per day. One percent of the mailboxes are moved per week on one day (Saturday). The solution makes use of the native data protection features within Exchange and, therefore, doesn't perform backups and is sized to tolerate three days without log truncation.

As shown in the following table, this server requires 23 GB of space for each database copy.

Log capacity requirements

Logs per database	Log file size	Daily log size	Move mailbox size ÷ database	Truncation failure tolerance	Log size requirements
5647	1 MB	5.65 GB	6 GB (240 × 2.19 GB x 1.2 / 102)	16.5 GB (3 × 5.65 GB)	23 GB (16.5 GB + 6 GB)

Provided that this is a Mailbox Resiliency and JBOD configuration with three copies, each database and its corresponding transaction logs will be placed on the same LUN. The LUN size required is:

LUN Capacity = Database Size ÷ (1 - Free Space Percentage Requirement)

= (Database Size + Transaction Log Size + Content Index Size) ÷ (1 - 0.2)

= (619 GB + 23 GB + 61.9 GB) / 0.8

= 879 GB

Determining required LUN size

Database size	Transaction log size	Content index size	Database LUN size
619 GB	23 GB	61.9 GB	879 GB

Return to top

Database Copy Requirements

Provided that there are a total of 102 databases required to support 24,000 mailboxes and that each database has three copies, the DAG will support a total of 306 databases. 306 databases spread across six Mailbox servers means that each Mailbox server will house 51 database copies. The database copies should be distributed across the servers in the DAG in such a way that server level failures cause active databases to fail over to as many remaining servers as possible (database copies aren't distributed in a symmetric fashion).

To maximize the efficiency of the Mailbox servers participating in the DAG, the active databases will be equally distributed across all Mailbox servers. As a result, when all six Mailbox servers are functioning, each server should be hosting 17 active database copies.

In the event that a single Mailbox server fails, the 17 databases will be redistributed across the remaining Mailbox servers increasing the active database copy count per server to 21.

In the event that two Mailbox servers fail, the 34 databases will be redistributed across the remaining Mailbox servers, increasing the active database copy count per server to 26. It's this active copy count that will be used to size the memory and CPU requirements for the Mailbox server.

For more information about how to distribute the database copies across the Mailbox servers, see Database Copy Layout Design.

Return to top

Mailbox Memory Requirements

With a message profile of 100 messages / day, the minimum required memory per mailbox to support the database cache is 6 MB. With a worst case active mailbox database count per server being 26, each server could host a total of 6,110 live mailboxes. In addition, there are a total of 51 databases per server. The Mailbox server requires a minimum database cache of 12 GB. Therefore, the amount of memory required to support the database cache is:

Minimum Required Database Cache = MAX((Number of Live Mailboxes x Memory Required / Mailbox), Minimum Memory for Databases)

= MAX(6110 x 6/1024 GB, 12 GB)

= MAX (36 GB, 12 GB)

= 36 GB

When deploying a multi-role architecture, the total physical memory required to support this configuration is 64 GB, based on the table in Understanding the Mailbox Database Cache.

Return to top

Mailbox I/O Requirements

Each mailbox sends or receives 100 messages / day. Therefore, each mailbox has an IOPS profile of 0.1. Each database houses 235 mailboxes. Therefore, the total amount of database volume I/O is:

Database Volume I/O = Number of Mailboxes x IOPS Profile x (1 + I/O Overhead Growth Factor)

= 235 x 0.1 x 1.2

= 28.2 IOPS

The amount of database read I/O percentage for this architecture is 60 percent. Therefore, each database volume generates 16.92 IOPS of read I/O and 11.28 IOPS of write I/O.

In this architecture, each log stream generates 50 percent of the database write I/O. Therefore, the log write I/O per volume is 5.64 IOPS.

The 26 active database copies also generate log read I/O that's 10 percent of the log write I/O; therefore the log read I/O for these databases is 0.56 IOPS.

Considering each large form factor 7.2K SATA disk generates 55 random IOPS, there are no concerns that the disk can't handle the I/O requirements of the database.

Return to top

Mailbox CPU Requirements

During a double server failure event, the remaining servers each host 26 databases for a total of 6,110 active mailboxes per server. Based on the calculations found in Mailbox Server Processor Capacity Planning, each server has the following CPU megacycle

requirements.

Determining CPU megacycle requirements

Active mailbox CPU megacycle requirements	Passive mailbox CPU megacycle requirements	Total CPU megacycle requirements
14,682	1,765	16,447

Provided that the chosen server platform can support a total of 26,400 megacycles, the server CPU platform can support the environment during a double server failure event.

Return to top

1.2.1.10 Understanding Exchange 2010 Virtualization

Understanding Exchange 2010 Virtualization

Exchange Server 2010 > Planning and Deployment > Planning for Exchange 2010 >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-11-13*

You can deploy Microsoft Exchange Server 2010 in a virtualized environment. This topic provides an overview of the scenarios that are supported for deploying Exchange 2010 on hardware virtualization software.

Contents

The following terms are used in this topic to discuss Exchange virtualization:

- **Cold boot** Refers to the action of bringing a system from a power-off state into a clean start of the operating system. No operating system state has been persisted in this case.
- **Saved state** When a virtual machine is powered off, hypervisors typically have the ability to save the state of the virtual machine, so when the machine is powered back on, it returns to that saved state rather than going through a cold boot startup.
- **Planned migration** When a system administrator initiates the move of a virtual machine from one hypervisor host to another, the action is a *planned migration*. The action could be a single migration, or a system administrator could configure automation to move the virtual machine on a timed basis. A planned migration could also be the result of some other event that occurs in the system, other than hardware or software failure. The key point is that the Exchange virtual machine is operating normally and needs to be relocated for some reason. This relocation can be done via technology, like Live Migration or vMotion. However, if the Exchange virtual machine or the hypervisor host where the virtual machine is located experiences some sort of failure condition, the outcome isn't characterized as a planned migration.

Requirements for Hardware Virtualization

Microsoft supports Exchange 2010 in production on hardware virtualization software only when all the following conditions are true:

- The hardware virtualization software is running one of the following:
  - Windows Server 2008 with Hyper-V technology
  - Windows Server 2008 R2 with Hyper-V technology
  - Microsoft Hyper-V Server 2008
  - Microsoft Hyper-V Server 2008 R2
  - Microsoft Hyper-V Server 2012
  - Any third-party hypervisor that has been validated under the Windows Server Virtualization Validation Program.

  Note:
  Deployment of production Exchange servers on Windows Azure virtual machines is not supported.
- The Exchange guest virtual machine has the following conditions:
  - It is running Exchange 2010. This includes Exchange 2010 Hosting Mode, available in Exchange 2010 SP1 and Exchange 2010 SP2.
  - It is deployed on Windows Server 2008 with SP2 (or later versions) or on Windows Server 2008 R2 RTM (or later versions).

  Note:
  When you install Exchange 2010 in a Hyper-V environment, you may receive the following error message: "Hub Transport Server role installation failed." For virtualized Active Directory servers, we recommend that you disable the time sync integration component, and then set the time to a reliable external time provider before you install the Hub Transport role. This recommendation is especially important if your host is joined to the domain that the virtual machine is hosting.

For deployments of Exchange 2010 SP2 or of Exchange 2010 SP1:

- All Exchange 2010 server roles, including Unified Messaging, are supported in a virtual machine. Unified Messaging virtual machines have the following special requirements:
  - Four virtual processors are required for the virtual machine. Memory should be sized using standard best practices guidance. For more information, see Understanding Memory Configurations and Exchange Performance.
  - Four physical processor cores are available for use by each Unified Messaging role virtual machine at all times. This requirement means that no processor oversubscription can be in use. This requirement affects the ability of the Unified Messaging role virtual machine to use physical processor resources. For more information, see the Virtualizing Unified Messaging Servers section.
- Exchange server virtual machines (including Exchange Mailbox virtual machines that are part of a database availability group, or DAG), may be combined with host-based failover clustering and migration technology, as long as the virtual machines are configured such that they will not save and restore state on disk when moved or taken offline. All failover activity must result in a cold boot when the virtual machine is activated on the target node. All planned migration must either result in shutdown and cold boot, or an online migration that makes use of a technology like Hyper-V Live Migration. Hypervisor migration of virtual machines is supported by the hypervisor vendor; therefore, you must ensure that your hypervisor vendor has tested and supports migration of Exchange virtual machines. Microsoft supports Hyper-V Live Migration of these virtual machines.

For deployments of the release to manufacture (RTM) version of Exchange 2010:

- Exchange 2010 server roles except for Unified Messaging are supported in a virtual machine.
- Microsoft doesn't support combining Exchange high availability solutions (such as DAGs) with hypervisor-based clustering, high availability, or migration solutions that will move or automatically failover mailbox servers that are members of a DAG between clustered root servers. DAGs are supported in hardware virtualization environments, provided the virtualization environment doesn't employ clustered root servers, or the clustered root servers have been configured to never failover or automatically move mailbox servers that are members of a DAG to another root server.
- The storage used by the Exchange guest machine for storage of Exchange data (for example, mailbox databases or Hub transport queues) can be virtual storage of a fixed size (for example, fixed virtual hard disks (VHDs) in a Hyper-V environment), SCSI pass-through storage, or Internet SCSI (iSCSI) storage. Pass-through storage is storage that's configured at the host level and dedicated to one guest machine. All storage used by an Exchange guest machine for storage of Exchange data must be block-level storage because Exchange 2010 doesn't support the use of network attached storage (NAS) volumes. Also, NAS storage that's presented to the guest as block-level storage via the hypervisor isn't supported. The following virtual disk requirements apply for volumes used to store Exchange data:
  - Virtual disks that dynamically expand aren't supported by Exchange.
  - Virtual disks that use differencing or delta mechanisms (such as Hyper-V's differencing VHDs or snapshots) aren't supported.

  Note:
  In a Hyper-V environment, each fixed VHD must be less than 2,040 GB. For supported third-party hypervisors, check with the manufacturer to see whether any disk size limitations exist.
- Only management software (for example, antivirus software, backup software, or virtual machine management software) can be deployed on the physical root machine. No other server-based applications (for example, Exchange, SQL Server, Active Directory, or SAP) should be installed on the root machine. The root machine should be dedicated to running guest virtual machines.
- Some hypervisors include features for taking snapshots of virtual machines. Virtual machine snapshots capture the state of a virtual machine while it's running. This feature enables you to take multiple snapshots of a virtual machine and then revert the virtual machine to any of the previous states by applying a snapshot to the virtual machine. However, virtual machine snapshots aren't application aware, and using them can have unintended and unexpected consequences for a server application that maintains state data, such as Exchange. As a result, making virtual machine snapshots of an Exchange guest virtual machine isn't supported.
- Many hardware virtualization products allow you to specify the number of virtual processors that should be allocated to each guest virtual machine. The virtual processors located in the guest virtual machine share a fixed number of logical processors in the physical system. Exchange supports a virtual processor-to-logical processor ratio no greater than 2:1. For example, a dual processor system using quad core processors contains a total of 8 logical processors in the host system. On a system with this configuration, don't allocate more than a total of 16 virtual processors to all guest virtual machines combined.
- When you calculate the total number of virtual processors required by the root machine, you must also account for both I/O and operating system requirements. In most cases, the equivalent number of virtual processors required in the root operating system for a system hosting Exchange virtual machines is 2. This value should be used as a baseline for the root operating system virtual processor when calculating the overall ratio of physical cores to virtual processors. If performance monitoring of the root operating system indicates you're consuming more processor utilization than the equivalent of 2

processors, you should reduce the count of virtual processors assigned to guest virtual machines accordingly, and verify that the overall virtual processor-to-physical core ratio is no greater than 2:1.

- The operating system for an Exchange guest machine must use a disk that has a size equal to at least 15 GB plus the size of the virtual memory that's allocated to the guest machine. This requirement is necessary to account for the operating system and paging file disk requirements. For example, if the guest machine is allocated 16 GB of memory, the minimum disk space needed for the guest operating system disk is 31 GB.
  In addition, it's possible that guest virtual machines may be prevented from directly communicating with fibre channel or SCSI host bus adapters (HBAs) installed in the root machine. In this event, you must configure the adapters in the root machine's operating system and present the LUNs to guest virtual machines as either a virtual disk or a pass-through disk.
- Exchange Jetstress 2010 is supported for use in virtual guest instances deployed on one of the following hypervisors. Jetstress is not supported when used in virtual guest instances running under any other hypervisor.
  - Windows Server 2008 R2 (or newer) with Hyper-V technology
  - Hyper-V Server 2008 R2 (or newer)
  - VMware ESX 4.1 (or newer)

We support running the Microsoft Exchange Server Jetstress 2010 tool in a guest virtual machine if it’s deployed on one of the following host computers:

1. Microsoft Windows Server 2008 R2, or a later version
2. Microsoft Hyper-V Server 2008 R2, or a later version
3. VMware ESX 4.1, or a later version

Root Machine Storage Requirements

The minimum disk space requirements for each root machine are as follows:

- Root machines in some hardware virtualization applications may require storage space for an operating system and its components. For example, when running Windows Server 2008 with Hyper-V, you will need a minimum of 10 GB to meet the requirements for Windows Server 2008. For more details, see Windows Server 2008 R2 System Requirements. Additional storage space is also required to support the operating system's paging file, management software, and crash recovery (dump) files.
- Some hypervisors maintain files on the root machine that are unique to each guest virtual machine. For example, in a Hyper-V environment, a temporary memory storage file (BIN file) is created and maintained for each guest machine. The size of each BIN file is equal to the amount of memory allocated to the guest machine. In addition, other files may also be created and maintained on the host machine for each guest machine.

Exchange Storage Requirements

Requirements for storage connected to a virtualized Exchange server are as follows:

- Each Exchange guest machine must be allocated sufficient storage space on the root machine for the fixed disk that contains the guest's operating system, any temporary memory storage files in use, and related virtual machine files that are hosted on the host machine. In addition, for each Exchange guest machine, you must also allocate sufficient storage for the message queues on the Hub Transport and Edge Transport servers and sufficient storage for the databases and log files on Mailbox servers.
- Storage used by Exchange should be hosted in disk spindles that are separate from the storage that's hosting the guest virtual machine's operating system.
- Configuring iSCSI storage to use an iSCSI initiator inside an Exchange guest virtual machine is supported. However, there will be reduced performance in

this configuration if the network stack inside a virtual machine isn't full-featured (for example, not all virtual network stacks support jumbo frames).

Exchange Memory Requirements and Recommendations

Some hypervisors have the ability to oversubscribe or dynamically adjust the amount of memory available to a specific guest machine based on the perceived usage of memory in the guest machine as compared to the needs of other guest machines managed by the same hypervisor. This technology makes sense for workloads in which memory is needed for brief periods of time and then can be surrendered for other uses. However, it doesn't make sense for workloads that are designed to use memory on an ongoing basis. Exchange, like many server applications with optimizations for performance that involve caching of data in memory, is susceptible to poor system performance and an unacceptable client experience if it doesn't have full control over the memory allocated to the physical or virtual machine on which it's running.

Many of the performance gains in recent versions of Exchange, especially those related to reduction in I/O, are based on highly efficient usage of large amounts of memory. When that memory is no longer available, the expected performance of the system can't be achieved. For this reason, memory oversubscription or dynamic adjustment of virtual machine memory should be disabled for production Exchange servers.

Size the memory for guest machines using the same methods as used for physical deployments. You can find details about memory sizing for Exchange 2010 server roles in Understanding Memory Configurations and Exchange Performance. For additional guidance, see the "Application Considerations" section of a white paper written by the Microsoft Hyper-V team, available for download at Implementing and Configuring Dynamic Memory.

Host-based Failover Clustering and Migration for Exchange

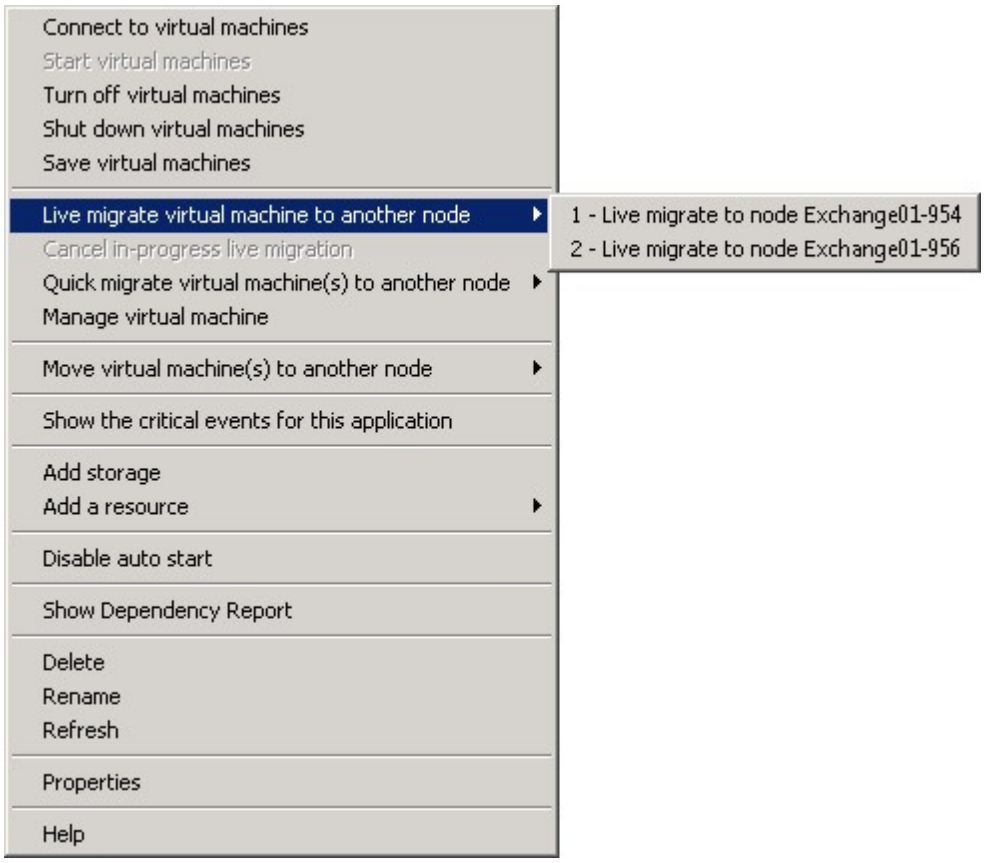
Here are answers to some frequently asked questions about host-based failover clustering and migration technology with Exchange 2010 DAGs.

- **Does Microsoft support third-party migration technology?**
  Microsoft can't make support statements for the integration of third party hypervisor products using these technologies with Exchange, because these technologies aren't part of the Server Virtualization Validation Program (SVVP). The SVVP covers the other aspects of our support for third-party hypervisors. You need to ensure that your hypervisor vendor supports the combination of their migration and clustering technology with Exchange. Simply put, if your hypervisor vendor supports their migration technology with Exchange, then we support Exchange with their migration technology.
- **How does Microsoft define host-based failover clustering?**
  Host-based failover clustering refers to any technology that provides the automatic ability to react to host-level failures and start affected virtual machines on alternate servers. Use of this technology is supported given that, in a failure scenario, the virtual machine is coming up from a cold boot on the alternate host. This technology helps to make sure that the virtual machine never comes up from a saved state that is persisted on disk because it will be stale relative to the rest of the DAG members.
- **What does Microsoft mean by migration support?**
  Migration technology refers to any technology that allows a planned move of a virtual machine from one host machine to another host machine. This move could also be an automated move that occurs as part of resource load balancing, but it isn't related to a failure in the system. Migrations are

supported as long as the virtual machines never come up from a saved state that is persisted on disk. This means that technology that moves a virtual machine by transporting the state and virtual machine memory over the network with no perceived downtime is supported for use with Exchange. A third-party hypervisor vendor must provide support for the migration technology, while Microsoft will provide support for Exchange when used in this configuration.

Warning:

In the case of Microsoft Hyper-V, the live migration option is supported, but the quick migration option is not supported. It's important to note that when you select the Move operation on a virtual machine in a Hyper-V environment, the default behavior is actually to perform a quick migration. To stay in a supported state with Exchange SP1 and Exchange SP2 DAG members, it's critical that you use the live migration option, as shown in the following figure.



Virtualizing Unified Messaging Servers

Unlike Exchange 2010 RTM, Exchange 2010 SP1 and SP2 support the Unified Messaging (UM) role on Hyper-V and other supported hypervisors. Exchange 2010 SP1 or Exchange 2010 SP2 must be deployed for UM support because the UM role is dependent on a media component provided by Microsoft Lync. Prior to the release of Exchange 2010 SP1, the Lync engineering team had enabled high-quality, real-time audio processing in a virtual deployment. Beginning with Exchange 2010 SP1, the changes were integrated into the UM role.

1.2.1.11 Planning for Internal and Third-Party Applications

Planning for Internal and Third-Party Applications

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 introduces many changes to the set of Application Programming Interfaces (APIs) that are available for application development. Upgrading your Exchange servers to Exchange 2010 can affect both internal applications and third-party applications that may use the Exchange APIs over the network or on your Exchange server. Use the sections in this topic to review potential effects on your internal or third-party applications that interact with Exchange 2010.

Important:
We recommend that you contact third-party software vendors to confirm that the products you use are supported for use with Exchange 2010.

Use this topic as a guide to help you investigate whether your Exchange Server applications will be affected by an upgrade to Exchange 2010.

Exchange 2010 APIs

Exchange 2010 supports fewer APIs than previous versions of Exchange Server support. For a list of Exchange 2010 APIs, see Development Technologies for Exchange 2010 on MSDN.

Earlier versions of Exchange Server contain APIs that have been removed from Exchange 2010. For a list of APIs that are available in earlier versions of Exchange, see the following topics on MSDN:

- Development Technologies for Exchange 2007
- Development Technologies for Exchange 2003

The following table identifies the development technologies that are available for use with Exchange 2010.

Development Technology	Exchange 2003	Exchange 2007	Exchange 2010
Exchange Web Services		X	X
Exchange Web Services Managed API (available as a separate download.)		X	X
Messaging Application Programming Interface (MAPI)	X	X	X
Outlook Object Model (OOM) (available as a separate download.)	X	X	X
Outlook web application	X	X	X
Outlook web		X	X

application customization			
Transport Agents		X	X

The following table lists the development technologies that are not available in Exchange 2010, and the product versions that they are available in.

Development Technology	Exchange 2003	Exchange 2007
Active Directory Services Interface (ADSI)	X	X
Collaboration Data Objects for Windows 2000 (CDOSYS)	X	X
CDOSYS SMTP/NNTP Event Sinks	X	X
Collaboration Data Objects for Exchange (CDOEX)	X	X
CDOEXM	X	
CDOWF	X	
Exchange Backup and Restore API	X	X
Exchange Writer for the Windows Volume Shadow Copy Service	X	X
Exchange OLE DB Provider	X	X
Exchange Store Event Sinks	X	X
Incremental Change Synchronization (ICS)	X	X
Lightweight Directory Access Protocol (LDAP)	X	X
SMTP Event Sinks	X	X
Web Forms	X	X
WebDAV	X	X
WebDAV Notifications	X	X
Windows Management Instrumentation (WMI)	X	

Migrating Applications to Exchange 2010

For information about migration your applications to Exchange 2010 technologies, see Migrating from Exchange 2000, Exchange 2003, and Exchange 2007 APIs on MSDN.

Exchange 2007 and Exchange 2010 Application Coexistence

Exchange Web Services does not allow delegation of mailbox access across versions. If either the principal's or the delegate's mailbox is on an Exchange server that is running a different version of Exchange, delegate access attempts will not succeed.

Exchange HTTP Proxying

Cross-site proxying to a site that has an external URL set for an Exchange server that is running the Client Access server role is only allowed for the delegate access scenario where the source and destination mailboxes are in different Active Directory sites or when accessing public folders. The preferred method is to use Autodiscover to get the correct Client Access server URL to directly access a mailbox instead of using the cross-site Client Access server to Client Access server proxy feature. For more information about Client Access server proxying, see Understanding Proxying and Redirection.

1.2.1.12 Exchange 2010 Deployment Permissions Reference

Exchange 2010 Deployment Permissions Reference

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic describes the permissions that are required to set up a Microsoft Exchange Server 2010 organization. The universal security groups (USGs) that are associated with management role groups, and other Windows security groups and security principals, are added to the access control lists (ACLs) of various Active Directory objects. ACLs control what operations can be performed on each object. By understanding what permissions are granted to each role group, security group, or security principal, you can determine what minimum permissions are required to install Exchange 2010.

In some cases, the ACL isn't applied on the usual property, **ntSecurityDescriptor**, but on another property, such as **msExchMailboxSecurityDescriptor**. The directory service can't enforce security that isn't specified in the Windows security descriptor. In most cases, these ACLs are replicated to store ACLs on appropriate objects by the store service. Unfortunately, there is no tool to view these ACLs as anything other than raw binary data.

The columns of each permissions table include the following information:

- **Account** The security principal granted or denied the permissions.
- **ACE type** Access control entry (ACE) type
  - **Allow ACE** An allow ACE allows the user or group associated with the ACE to access an item.
  - **Deny ACE** A deny ACE prevents the user or group associated with the ACE from accessing an item.
- **Inheritance** The type of inheritance used for child objects.
  - **All** indicates that the permissions apply to the object and all sub-objects.
  - **Desc** indicates the permissions apply to the object class listed in the **On Property/Applies To**row.
  - **None** indicates those permissions only apply the object.

- **Permissions** The permissions granted to the account.
- **On Property/Applies To** In some cases, permissions apply only to a given property, property set, or object class. These limited permissions are specified here.
- **Comments** When applicable, this column explains why the permissions are required or provides other information about the permissions.

The permissions are generally listed in the table by the names that are used on the Active Directory Service Interfaces (ADSI) Edit (AdsiEdit.msc) **Security** property page in the **Advanced** view on the **View/Edit** tab. The ADSI Edit **Security** property page lists a much more condensed view of the permissions. The LDP tool (Ldp.exe) displays the access mask directly as a numeric value. The setup code refers to the permissions by predefined constants.

The following table shows the relationships between these values.

ADSI Edit Summary page	ADSI Edit Advanced view, View/Edit tab	ACL entries applied to a given object	Binary value (access mask in LDP)
Full Control	Full Control	WRITE_OWNER | WRITE_DAC | READ_CONTROL | DELETE | ACTRL_DS_CONTROL_ACCESS | ACTRL_DS_LIST_OBJECT | ACTRL_DS_DELETE_TREE | ACTRL_DS_WRITE_PROP | ACTRL_DS_READ_PROP | ACTRL_DS_SELF | ACTRL_DS_LIST | ACTRL_DS_DELETE_CHILD | ACTRL_DS_CREATE_CHILD	0x000F01FF
Read	List Contents + Read All Properties + Read Permissions	ACTRL_DS_LIST | ACTRL_DS_READ_PROP | READ_CONTROL	0x00020014
Write	Write All Properties + All Validated Writes	ACTRL_DS_WRITE_PROP | ACTRL_DS_SELF	0x00000028
	List Contents	ACTRL_DS_LIST	0x00000004
	Read All Properties	ACTRL_DS_READ_PROP	0x00000010
	Write All Properties	ACTRL_DS_WRITE_PROP	0x00000020
	Delete	DELETE	0x00010000
	Delete Subtree	ACTRL_DS_DELETE_TREE	0x00000040
	Read Permissions	READ_CONTROL	0x00020000
	Modify Permissions	WRITE_DAC	0x00040000
	Modify Owner	WRITE_OWNER	0x00080000

	All Validated Writes	ACTRL_DS_SELF	0x00000008
	All Extended Rights	ACTRL_DS_CONTROL_ACCESS	0x00000100
Create All Child Objects	Create All Child Objects	ACTRL_DS_CREATE_CHILD	0x00000001
Delete All Child Objects	Delete All Child Objects	ACTRL_DS_DELETE_CHILD	0x00000002
		ACTRL_DS_LIST_OBJECT	0x00000080

Extended rights are custom rights specified by individual applications. They are specified in the ACL. However, they are meaningless to Active Directory. The specific application enforces any extended rights. Examples of Exchange extended rights are "Create public folder" or "Create named properties in the information store."

Note:

For information about permissions that are set during a Microsoft Exchange Server 2003 installation, see Working with Active Directory Permissions in Exchange Server 2003. For information about permissions that are set during a Microsoft Exchange Server 2007 installation, see Exchange 2007 Setup Permissions Reference.

Prepare Legacy Exchange Permissions

The permissions tables in this section show the permissions set when you execute the `setup /PrepareLegacyExchangePermissions` command.

Distinguished name of the object: DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Exchange Enterprise Servers	Allow ACE	All	Write Property	Exchange Information
Authenticated Users	Allow ACE	All	Read Property	Exchange Information

Distinguished name of the object: CN=AdminSDHolder,CN=System,DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Exchange Enterprise Servers	Allow ACE	All	Read Property Write Property	Exchange Information

Distinguished name of the object: CN=<organization>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Exchange Domain Servers	Allow ACE	All	Write Property	Exchange Information

Prepare Active Directory Permissions

The permissions tables in this section show the permissions set when you execute the `Setup /PrepareAD` command.

Microsoft Exchange Container Permissions

The following table shows the permissions that are set on the Microsoft Exchange container within the configuration partition.

Distinguished name of the object: CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
Installation Account	Allow ACE	All	Full Control		This is the account that is used to run /PrepareAD.
Organization Management	Allow ACE	All	Full Control		
Exchange Trusted Subsystem	Allow ACE	All	Full Control		
Exchange Servers	Allow ACE	All	Read		
Authenticated Users	Allow ACE	None	Read Property List Contents		
Public Folder Management	Allow ACE	All	Read Permissions List Contents Read Property List Object		
Delegated Setup	Allow ACE	All	Read Permissions List Contents Read Property List Object		

Microsoft Exchange Autodiscover Container Permissions

The following table shows the permissions set on the Microsoft Exchange Autodiscover container within the configuration partition.

Distinguished name of the object: CN=Microsoft Exchange Autodiscover,CN=Services,CN=Configuration,DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/

				Applies to
Exchange Servers	Allow ACE	All	Read	

Microsoft Exchange Organization Container Permissions

The permissions tables in this section show the permissions set on the Microsoft Exchange Organization and sub-containers within the configuration partition.

Distinguished name of the object: CN=<organization>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<domain>

Account(s)	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
Enterprise Admins Root Domain Admins Installation Account Organization Management	Deny ACE	All	Send As Receive As		Windows administrators aren't allowed to open mailboxes.
Enterprise Admins Schema Admins Root Domain Admins Installation Account Organization Management	Deny ACE	All	Exchange Web Services Impersonation Exchange Web Services Token Serialization		Extended right
Enterprise Admins Schema Admins Root Domain Admins Installation Account Organization Management Exchange Servers	Deny ACE	All	Store Transport Access Store Constrained Delegation Store Read Access Store Read Write Access		
Authenticated	Deny ACE	Desc	Read Property	msExchAvail	

Users				abilityUserPassword / msExchAvailabilityAddressSpace	
Exchange Servers	Allow ACE	All	Control Access		
Organization Management	Allow ACE	All	Read Permissions List Contents Read Property List Object		
Public Folder Management	Allow ACE	All	Read Permissions List Contents Read Property List Object		
NT Authority \Network Service	Allow ACE	All	Read		
Exchange Servers	Allow ACE	All	Write Property	groupType	
Exchange Servers	Allow ACE	All	Write Property	msExchOwningServer	
Exchange Servers	Allow ACE	All	Write Property	msExchMailboxSecurityDescriptor	
Exchange Servers	Allow ACE	All	Write Property	msExchUMServerWritableFlags	
Exchange Servers	Allow ACE	All	Write Property	msExchDatabaseCreated	
Exchange Servers	Allow ACE	All	Write Property	msExchUserCulture	
Exchange Servers	Allow ACE	All	Write Property	msExchMobileMailboxFlags	
Exchange Servers	Allow ACE	All	Write Property	siteFolderGUID	
Exchange Servers	Allow ACE	All	Write Property	siteFolderServer	
Exchange Servers	Allow ACE	All	Write Property	msExchEDBOffline	

Exchange Servers	Allow ACE	All	Write Property	userCertificate	
Exchange Servers	Allow ACE	All	Write Property	msExchUMDtmfMap	
Exchange Servers	Allow ACE	All	Write Property	msExchBlockedSendersHash	
Exchange Servers	Allow ACE	All	Write Property	Personal Information	
Exchange Servers	Allow ACE	All	Write Property	Public Information	
Exchange Servers	Allow ACE	All	Write Property	Exchange Information	
Exchange Servers	Allow ACE	All	Write Property	msExchPatchMDB	
Exchange Servers	Allow ACE	All	Write Property	publicDelegates	
Exchange Servers	Allow ACE	All	Write Property	msExchUMSpokenName	
Exchange Servers	Allow ACE	All	Write Property	msExchUMPinChecksum	
Exchange Servers	Allow ACE	All	Write Property	legacyExchangeDN	
Exchange Servers	Allow ACE	All	Write Property	msExchSafeSendersHash	
Organization Management	Allow ACE	All	Create top level public folder		
Public Folder Management	Allow ACE	All	Create top level public folder		
Organization Management	Allow ACE	All	View information store status		
Public Folder Management	Allow ACE	All	View information store status		
Organization Management	Allow ACE	All	Administer information store		
Public Folder Management	Allow ACE	All	Administer information store		
Organization Management	Allow ACE	All	Create named properties in		

			the information store		
Public Folder Management	Allow ACE	All	Create named properties in the information store		
Organization Management	Allow ACE	All	Modify public folder ACL		
Public Folder Management	Allow ACE	All	Modify public folder ACL		
Organization Management	Allow ACE	All	Modify public folder quotas		
Public Folder Management	Allow ACE	All	Modify public folder quotas		
Organization Management	Allow ACE	All	Modify public folder admin ACL		
Public Folder Management	Allow ACE	All	Modify public folder admin ACL		
Organization Management	Allow ACE	All	Modify public folder expiry		
Public Folder Management	Allow ACE	All	Modify public folder expiry		
Organization Management	Allow ACE	All	Modify public folder replica list		
Public Folder Management	Allow ACE	All	Modify public folder replica list		
Organization Management	Allow ACE	All	Modify public folder deleted item retention		
Public Folder Management	Allow ACE	All	Modify public folder deleted item retention		
Organization Management	Allow ACE	All	Create public folder		
Public Folder Management	Allow ACE	All	Create public folder		
Everyone NT Authority \Anonymous Logon	Allow ACE	All	Create named properties in the information store		

Everyone NT Authority \Anonymous Logon	Allow ACE	All	Create public folder		
Everyone NT Authority \Anonymous Logon	Allow ACE	Desc	Read Permissions List Contents Read Property List Object	/msExchPrivateMDB	
Everyone NT Authority \Anonymous Logon	Allow ACE	Desc	Read Permissions List Contents Read Property List Object	/msExchPublicMDB	
Exchange Servers	Allow ACE	Desc	Read Permissions List Contents Read Property List Object	/siteAddressing	

Distinguished name of the object: CN=All Address Lists,CN=Address Lists Container,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated Users	Allow ACE	All	List Contents	
Organization Management	Allow ACE	All	Write Property	msExchLastAppliedRecipientFilter msExchRecipientFilterFlags
Public Folder Management	Allow ACE	All	Write Property	msExchLastAppliedRecipientFilter msExchRecipientFilterFlags

Distinguished name of the object: CN=Offline Address Lists,CN=Address Lists Container, CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated	Allow ACE	All	Download Offline	

Users			Address Book	

Distinguished name of the object: CN=Addressing,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated users	Allow ACE	All	Read	

Distinguished name of the object: CN=Recipient Policies,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Organization Management	Allow ACE	All	Write Property	msExchLastAppliedRecipientFilter msExchRecipientFilterFlags
Public Folder Management	Allow ACE	All	Write Property	msExchLastAppliedRecipientFilter msExchRecipientFilterFlags

Configuration Partition Container Permissions

The permissions tables in this section show the permissions set by the `Setup /PrepareAD` command on various containers within the configuration partition.

Distinguished name of the object: CN=Sites,CN=Configuration,DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Organization Management Exchange Trusted Subsystem	Allow ACE	All	Write Property	msExchVersion / site
Organization Management Exchange Trusted Subsystem	Allow ACE	All	Write Property	msExchVersion / site-link
Organization Management Exchange Trusted Subsystem	Allow ACE	All	Write Property	msExchPartnerId / site

Organization Management Exchange Trusted Subsystem	Allow ACE		Write Property	msExchTransportSiteFlags / site
Organization Management Exchange Trusted Subsystem	Allow ACE	All	Write Property	msExchCost / site-link
Organization Management Exchange Trusted Subsystem	Allow ACE	Desc	Read Permissions List Contents Read Property List Object	/ msExchEdgeSyncEHFConnector
Organization Management Exchange Trusted Subsystem	Allow ACE	Desc	Read Permissions List Contents Read Property List Object	/ msExchEdgeSyncMservConnector
Organization Management Exchange Trusted Subsystem	Allow ACE	Children	Create Child Delete Child Delete Tree	msExchEdgeSyncServiceConfig / site
Organization Management Exchange Trusted Subsystem	Allow ACE	Desc	Read Permissions List Contents Read Property List Object	/ msExchEdgeSyncServiceConfig
Organization Management Exchange Trusted Subsystem	Allow ACE	Children	Create Child Delete Child Delete Tree	msExchEdgeSyncMservConnector / msExchEdgeSyncServiceConfig
Organization Management Exchange Trusted Subsystem	Allow ACE	Children	Create Child Delete Child Delete Tree	msExchEdgeSyncEHFConnector / msExchEdgeSyncServiceConfig

Distinguished name of the object: CN=Deleted Objects,CN=Configuration,DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
Exchange Servers	Allow ACE	All	List Contents		
Organization Administration	Allow ACE	All	Read Permission Write Permission List Contents Read Property List Object		
Installation Account	Allow ACE	All	Read Permission Write Permission List Contents Read Property List Object		This is the account that is used to run /PrepareAD.
Exchange Trusted Subsystem	Allow ACE	All	Read Permission List Contents Read Property List Object		

Exchange Administrative Group Permissions

The Setup /PrepareAD command also configures the following permissions on the administrative groups within the organization.

Distinguished name of the object: CN=<admin group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
Organization Management	Allow ACE	Desc	Access Recipient Update Service	msExchExchangeServer	Allows Exchange Recipient Administrators to stamp recipients with proxy address information.
NT AUTHORITY \SYSTEM	Allow ACE	Desc	Access Recipient Update	msExchExchangeServer	Allows the servers to stamp

			Service		recipients with proxy address information.
Public Folder Management	Allow ACE	Desc	Access Recipient Update Service	msExchExchangeServer	Allows Exchange Public Folder Administrators to stamp recipients with proxy address information.

Distinguished name of the object: CN=Advanced Security Settings,CN=<admin group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated Users	Allow ACE	None	List Contents	

Distinguished name of the object: CN=Encryption,CN=Advanced Security Settings,CN=<admin group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated Users	Allow ACE	None	Read Property	

Distinguished name of the object: CN=Arrays,CN=<admin group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated Users	Allow ACE	None	List Contents	

Distinguished name of the object: CN=Database Availability Groups,CN=<admin group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated Users	Allow ACE	None	List Contents	

Distinguished name of the object: CN=Databases,CN=<admin group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated Users	Allow ACE	None	List Contents	

Distinguished name of the object: CN=Servers,CN=<admin

group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
Exchange Servers	Deny ACE	All	Receive As		Exchange Servers aren't allowed to open mailboxes.
Authenticated Users	Allow ACE	None	List Contents		

Microsoft Exchange Security Groups Container Permissions

The permissions tables in this section show the permissions set on the Microsoft Exchange Security Groups container within the root domain partition.

Distinguished name of the object: OU=Microsoft Exchange Security Groups,DC=<root domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Organization Management	Allow ACE	All	Full Control	
Exchange Trusted Subsystem	Allow ACE	All	Create Child Delete Child	/ Group
Exchange Trusted Subsystem	Allow ACE	Desc	Write Property	Member / group

Distinguished name of the object: CN=Organization Management,OU=Microsoft Exchange Security Groups,DC=<root domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Organization Management	Allow ACE	All	Full Control	

Distinguished name of the object: CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security Groups,DC=<root domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Organization Management	Allow ACE	All	Full Control	

Distinguished name of the object: CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=<root domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Organization	Allow ACE	All	Full Control	

Management				
Root Domain Administrators	Allow ACE	All	Read Members Write Members	
Child Domain Administrators	Allow ACE	All	Read Members Write Members	

Prepare Domain

The following tables show the permissions set when you execute the `Setup /PrepareDomain` command.

Distinguished name of the object: DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
Authenticated Users	Allow ACE	All	Read Property	Exchange Information	
NT AUTHORITY \NETWORK	Allow ACE	All	Read Property	Exchange Personal Information	Grants Transport service read permissions.
Exchange Servers	Allow ACE	All	Write Property	groupType	
Exchange Servers	Allow ACE	All	Write Property	msExchMailboxSecurityDescriptor	
Exchange Servers	Allow ACE	All	Write Property	msExchUMServerWritableFlags	
Exchange Servers	Allow ACE	All	Read Property	userAccountControl	
Exchange Servers	Allow ACE	All	Read Property	canonicalName	
Exchange Servers	Allow ACE	All	Read Property	Exchange Personal Information	
Exchange Servers	Allow ACE	All	Read Property	Exchange Information	
Exchange Servers	Allow ACE	All	Write Property	msExchUserCultulre	
Exchange Servers	Allow ACE	All	Read Property	memberOf	
Exchange Servers	Allow ACE	All	Read Property	garbageCollPeriod	
Exchange	Allow ACE	All	Replication		Extended right

Servers			Synchronization		
Exchange Servers	Allow ACE	All	Create Child Delete Chile List Children	msExchActiveSyncDevices / User	
Exchange Servers	Allow ACE	All	Write Property	msExchSafeSendersHash	
Exchange Servers	Allow ACE	All	Write Property	msExchPublicDelegates	
Exchange Servers	Allow ACE	All	Write Property	msExchMobileMailboxFlags	
Exchange Servers	Allow ACE	All	Write Property	msExchSafeRecipientsHash	
Exchange Servers	Allow ACE	All	Write Property	userCertificate	
Exchange Servers	Allow ACE	All	Write Property	msExchUMDtmfMap	
Exchange Servers	Allow ACE	All	Write Property	msExchBlockedSendersHash	
Exchange Servers	Allow ACE	All	Write Property	msExchUMSpokenName	
Exchange Servers	Allow ACE	All	Write Property	msExchUMPinChecksum	
Organization Management	Allow ACE	All	Read		
Organization Management	Allow ACE	All	Write Property	Exchange Information	
Organization Management	Allow ACE	All	Write Property	garbageCollPeriod	
Organization Management	Allow ACE	All	Write Property	legacyExchangeDN	
Organization Management	Allow ACE	All	Write Property	msExchPublicDelegates	
Organization Management	Allow ACE	All	Write Property	textEncodedORAddress	
Organization Management	Allow ACE	All	Write Property	proxyAddresses	
Organization Management	Allow ACE	All	Write Property	mail	
Organization	Allow ACE	All	Write Property	displayName	

Management				Printable	
Organization Management	Allow ACE	All	Write Property	showInAddressBook	
Organization Management	Allow ACE	All	Write Property	Exchange Personal Information	
Organization Management	Allow ACE	All	Full Control	/msExchDynamicDistributionList	
Organization Management	Allow ACE	All	Write Property	adminDisplayName	
Organization Management	Allow ACE	All	Write Property	displayName	
Exchange Trusted Subsystem	Allow ACE	All	Read		
Exchange Trusted Subsystem	Allow ACE	All	Write Property	displayName	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	Public Information	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	msExchPublicDelegates	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	adminDisplayName	
Exchange Trusted Subsystem	Allow ACE	All	Full Control	/msExchDynamicDistributionList	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	Exchange Information	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	Exchange Personal Information	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	garbageCollPeriod	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	textEncodedORAddress	
Exchange Trusted	Allow ACE	All	Write Property	showInAddressBook	

Subsystem					
Exchange Trusted Subsystem	Allow ACE	All	Write Property	legacyExchangeDN	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	Personal Information	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	proxyAddresses	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	displayNamePrintable	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	mail	
Exchange Windows Permissions	Allow ACE	All	Write Property	pwdLastSet	
Exchange Windows Permissions	Allow ACE	All	Delete Tree WriteDACL	/ user	
Exchange Windows Permissions	Allow ACE	All	Delete Tree WriteDACL	/ inetOrgPerson	
Exchange Windows Permissions	Allow ACE	All	Write Property	sAMAccountName	
Exchange Windows Permissions	Allow ACE	All	Create Child Delete Child	/ contact	
Exchange Windows Permissions	Allow ACE	All	Create Child Delete Child	/ user	
Exchange Windows Permissions	Allow ACE	All	Create Child Delete Child	/ organizationUnit	
Exchange Windows Permissions	Allow ACE	All	Create Child Delete Child	/ group	
Exchange Windows Permissions	Allow ACE	All	Create Child Delete Child	/ computer	
Exchange Windows Permissions	Allow ACE	All	Write Property	Member	

Exchange Windows Permissions	Allow ACE	All	Write Property	wwwHomePage	
Exchange Windows Permissions	Allow ACE	All	Write Property	countryCode	
Exchange Windows Permissions	Allow ACE	All	Write Property	userAccount Control	
Exchange Windows Permissions	Allow ACE	All	Write Property	managedBy	
Exchange Windows Permissions	Allow ACE	All	Reset Password		Extended right
Exchange Windows Permissions	Allow ACE	All	Change Password		Extended right

Distinguished name of the object: CN=AdminSDHolder,CN=System,DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
Exchange Servers	Allow ACE	All	Write Property	groupType	
Exchange Servers	Allow ACE	All	Write Property	msExchMailboxSecurityDescriptor	
Exchange Servers	Allow ACE	All	Write Property	msExchUMServerWritableFlags	
Exchange Servers	Allow ACE	All	Read Property	userAccount Control	
Exchange Servers	Allow ACE	All	Read Property	canonicalName	
Exchange Servers	Allow ACE	All	Read Property	Exchange Personal Information	
Exchange Servers	Allow ACE	All	Read Property	Exchange Information	
Exchange Servers	Allow ACE	All	Write Property	msExchUserCultulre	
Exchange Servers	Allow ACE	All	Read Property	memberOf	
Exchange Servers	Allow ACE	All	Read Property	garbageColl Period	
Exchange	Allow ACE	All	Replication		Extended right

Servers			Synchronization		
Exchange Servers	Allow ACE	All	Create Child Delete Chile List Children	msExchActiveSyncDevices / User	
Exchange Servers	Allow ACE	All	Write Property	msExchSafeSendersHash	
Exchange Servers	Allow ACE	All	Write Property	msExchPublicDelegates	
Exchange Servers	Allow ACE	All	Write Property	msExchMobileMailboxFlags	
Exchange Servers	Allow ACE	All	Write Property	msExchSafeRecipientsHash	
Exchange Servers	Allow ACE	All	Write Property	userCertificate	
Exchange Servers	Allow ACE	All	Write Property	msExchUMDtmfMap	
Exchange Servers	Allow ACE	All	Write Property	msExchBlockedSendersHash	
Exchange Servers	Allow ACE	All	Write Property	msExchUMSpokenName	
Exchange Servers	Allow ACE	All	Write Property	msExchUMPinChecksum	
Organization Management	Allow ACE	All	Read		
Organization Management	Allow ACE	All	Write Property	Exchange Information	
Organization Management	Allow ACE	All	Write Property	garbageCollPeriod	
Organization Management	Allow ACE	All	Write Property	legacyExchangeDN	
Organization Management	Allow ACE	All	Write Property	msExchPublicDelegates	
Organization Management	Allow ACE	All	Write Property	textEncodedORAddress	
Organization Management	Allow ACE	All	Write Property	proxyAddresses	
Organization Management	Allow ACE	All	Write Property	mail	
Organization	Allow ACE	All	Write Property	displayName	

Management				Printable	
Organization Management	Allow ACE	All	Write Property	showInAddressBook	
Organization Management	Allow ACE	All	Write Property	Exchange Personal Information	
Organization Management	Allow ACE	All	Full Control	/ msExchDynamicDistributionList	
Organization Management	Allow ACE	All	Write Property	adminDisplayName	
Organization Management	Allow ACE	All	Write Property	displayName	
Exchange Trusted Subsystem	Allow ACE	All	Read		
Exchange Trusted Subsystem	Allow ACE	All	Write Property	displayName	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	Public Information	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	msExchPublicDelegates	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	adminDisplayName	
Exchange Trusted Subsystem	Allow ACE	All	Full Control	/ msExchDynamicDistributionList	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	Exchange Information	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	Exchange Personal Information	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	garbageCollPeriod	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	textEncodedORAddress	
Exchange Trusted	Allow ACE	All	Write Property	showInAddressBook	

Subsystem					
Exchange Trusted Subsystem	Allow ACE	All	Write Property	legacyExchangeDN	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	Personal Information	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	proxyAddresses	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	displayNamePrintable	
Exchange Trusted Subsystem	Allow ACE	All	Write Property	mail	

Distinguished name of the object: CN=Microsoft Exchange System Objects,DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
NT AUTHORITY \NETWORK	Allow ACE	All	Read Property	Exchange Personal Information
Authenticated Users	Allow ACE	All	Read Permissions	
Authenticated Users	Allow ACE	All	Read Property	garbageCollPeriod
Authenticated Users	Allow ACE	All	Read Property	adminDisplayName
Authenticated Users	Allow ACE	All	Read Property	modifyTimeStamp
Exchange Servers	Deny ACE	All	Delete Tree	
Exchange Servers	Allow ACE	All	Read Delete Tree	
Exchange Servers	Allow ACE	All	Create Child Delete Child	/ msExchSystemMailbox
Exchange Servers	Allow ACE	All		/ publicFolder
Exchange Servers	Allow ACE	Desc	Write Property	/ publicFolder
Exchange Servers	Allow ACE	Desc	Write Property	/ msExchSystemMa

				ilbox
Organization Management	Allow ACE	All	Read	
Organization Management	Allow ACE	Desc	Write Property	/ msExchSystemMailbox
Organization Management	Allow ACE	All	Create Child Delete Child	/ msExchSystemMailbox
Organization Management	Allow ACE	Desc	Read Property Write Property	mail / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	displayNamePrintable / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	displayName / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	textEncodedORAddress / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	proxyAddresses / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	cn / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	showInAddressBook / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	Exchange Information / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	legacyExchangeDN / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	Exchange Personal Information / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	msDSPhoneticDisplayName / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	msExchPFContacts / publicFolder
Organization	Allow ACE	Desc	Read Property	garbageCollPer

Management			Write Property	iod / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	name / publicFolder
Organization Management	Allow ACE	Desc	Read Property Write Property	msExchPublicDelegates / publicFolder
Public Folder Management	Allow ACE	All	Read	
Public Folder Management	Allow ACE	Desc	Read Property Write Property	mail / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	displayNamePrintable / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	displayName / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	textEncodedORAddress / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	proxyAddresses / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	cn / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	showInAddressBook / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	Exchange Information / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	legacyExchangeDN / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	Exchange Personal Information / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	msDSPhoneticDisplayName / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	msExchPFContacts / publicFolder

Public Folder Management	Allow ACE	Desc	Read Property Write Property	garbageCollPeriod / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	name / publicFolder
Public Folder Management	Allow ACE	Desc	Read Property Write Property	msExchPublicDelegates / publicFolder
Exchange Trusted Subsystem	Allow ACE	All	Read	
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	mail / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	displayNamePrintable / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	displayName / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	textEncodedORAddress / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	proxyAddresses / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	cn / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	showInAddressBook / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	Exchange Information / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	legacyExchangeDN / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	Exchange Personal Information / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	msDSPhoneticDisplayName / publicFolder
Exchange	Allow ACE	Desc	Read Property	msExchPFContac

Trusted Subsystem			Write Property	ts / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	garbageCollPeriod / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	name / publicFolder
Exchange Trusted Subsystem	Allow ACE	Desc	Read Property Write Property	msExchPublicDelegates / publicFolder

Server Role Installation

During installation of the Client Access, Hub Transport, Unified Messaging, and Mailbox server roles, Setup adds the Organization Management USG to the administrator security group on the local computer so that members of the management role group named Organization Management can manage the server.

The following permissions table shows the permissions set when you install the Client Access, Hub Transport, Unified Messaging, or Mailbox server roles.

Distinguished name of the object: CN=<server>,CN=Servers,CN=<admin group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
MACHINE$	Allow ACE	All	Read		
MACHINE$	Allow ACE	None	Write Property	msExchServerSite msExchEdgeSyncCredential	
Exchange Servers	Allow ACE	All	Store Transport Access Store Constrained Delegation Store Read Only Access Store Read and Write Access		Extended rights
NT AUTHORITY \NETWORK	Allow ACE	All	Exchange Web Services Token Serialization		Extended right Only granted on Client

					Access server role objects.
NT AUTHORITY\NETWORK	Allow ACE	All	Read		Only granted on Hub Transport server role objects.
Delegated Setup	Allow ACE	All	Full Control		
Delegated Setup	Allow ACE	All	Read		
Delegated Setup	Deny ACE	All	Create Child Delete Child	/msExchPublicMDB	
Authenticated Users	Allow ACE	All	Read Property		
Delegated Setup	Deny ACE	All	Receive As Send As		Extended right

Database Availability Groups

The permissions tables in this section show the permissions set with regards to the database availability groups and its members.

Distinguished name of the object: CN=<DAGName>,CN=Database Availability Groups,CN=<admin group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated Users	Allow ACE	None	Read Properties	

Distinguished name of the object: CN=<DAGName>,CN=Computers,DC=<domain>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Mailbox Server Computer Account$	Allow ACE	None	Delete Read Permissions List Contents Read Property Delete Tree List Object	
Mailbox Server Computer	Allow ACE	None	Write Property	Logon Information

Account$				
Mailbox Server Computer Account$	Allow ACE	None	Write Property	description
Mailbox Server Computer Account$	Allow ACE	None	Write Property	displayName
Mailbox Server Computer Account$	Allow ACE	None	Write Property	sAMAccountName
Mailbox Server Computer Account$	Allow ACE	None	Write Property	Account Restrictions
Mailbox Server Computer Account$	Allow ACE	None	Write Property	Validated write to DNS host name
Mailbox Server Computer Account$	Allow ACE	None	Write Property	Validated write to service principal name

Edge Transport

If you install an Edge Transport server and establish an Edge Subscription with the Exchange organization, the permissions in the following permissions table are set when the Edge Transport server is instantiated into the organization.

Distinguished name of the object: CN=<server>,CN=Servers,CN=<admin group>,CN=Administrative Groups,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
Exchange Servers	Allow ACE	All	Write Property		
Authenticated Users	Allow ACE	None	Read Properties		ACE is defined in schema for msExchExchangeServer class objects defaultSecurityDescriptor.

Client Access Server Installation

During installation of the first Client Access server, the following container is created. The following permissions table shows the permissions that are applied.

Distinguished name of the object: CN=Availability Configuration,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
Exchange	Allow ACE	Desc	Read Property	msExchAvail	Extended right

Servers				abilityUser Password / msExchAvail abilityAddr essSpaceObj ects	

Hub Transport Server Installation

During installation of each Hub transport server, the following permissions are set.

Distinguished name of the object: CN=Default <Server>,CN=SMTP Receive Connectors,CN=Protocols,CN=<Server>,CN=Servers,CN=<admin group>,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
ExchangeLegacyInterop	Deny ACE	All	Accept Forest Headers		
ExchangeLegacyInterop	Deny ACE	All	Accept Organization Headers		
Exchange Servers	Allow ACE	All	Accept Any Sender		
ExchangeLegacyInterop	Allow ACE	All	Accept Any Sender		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Accept Any Sender		This is the well-known security identifier (SID) for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Accept Any Sender		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Accept Any Sender		This is the well-known SID for externally secured servers.
Exchange Servers	Allow ACE	All	Accept EXCH50		
ExchangeLegacyInterop	Allow ACE	All	Accept EXCH50		
S-1-9-1419165041-1139599005-	Allow ACE	All	Accept EXCH50		This is the well-known SID for Hub

3936102811-1022490595-21					Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Accept EXCH50		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Accept EXCH50		This is the well-known SID for externally secured servers.
Exchange Servers	Allow ACE	All	Submit Messages to any Recipient		
ExchangeLegacyInterop	Allow ACE	All	Submit Messages to any Recipient		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Submit Messages to any Recipient		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Submit Messages to any Recipient		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Submit Messages to any Recipient		This is the well-known SID for externally secured servers.
Exchange Servers	Allow ACE	All	Accept XShadow		
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Accept XShadow		This is the well-known SID for Edge Transport servers.
Exchange Servers	Allow ACE	All	Accept Routing Headers		
ExchangeLega	Allow ACE	All	Accept Routing		

cyInterop			Headers		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Accept Routing Headers		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Accept Routing Headers		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Accept Routing Headers		This is the well-known SID for externally secured servers.
Exchange Servers	Allow ACE	All	Accept Forest Headers		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Accept Forest Headers		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Accept Forest Headers		This is the well-known SID for Edge Transport servers.
Exchange Servers	Allow ACE	All	Accept Authentication Flag		
ExchangeLegacyInterop	Allow ACE	All	Accept Authentication Flag		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Accept Authentication Flag		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Accept Authentication Flag		This is the well-known SID for Edge Transport servers.

S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Accept Authentication Flag		This is the well-known SID for externally secured servers.
Exchange Servers	Allow ACE	All	Bypass Anti-Spam		
ExchangeLegacyInterop	Allow ACE	All	Bypass Anti-Spam		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Bypass Anti-Spam		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Bypass Anti-Spam		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Bypass Anti-Spam		This is the well-known SID for externally secured servers.
Exchange Servers	Allow ACE	All	Bypass Message Size Limit		
ExchangeLegacyInterop	Allow ACE	All	Bypass Message Size Limit		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Bypass Message Size Limit		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Bypass Message Size Limit		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-	Allow ACE	All	Bypass Message Size Limit		This is the well-known SID for externally secured

23					servers.
Exchange Servers	Allow ACE	All	Accept Organization Headers		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Accept Organization Headers		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Accept Organization Headers		This is the well-known SID for Edge Transport servers.
Exchange Servers	Allow ACE	All	Submit Messages to Server		
ExchangeLegacyInterop	Allow ACE	All	Submit Messages to Server		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Submit Messages to Server		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Submit Messages to Server		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Submit Messages to Server		This is the well-known SID for externally secured servers.
Exchange Servers	Allow ACE	All	Accept Authoritative Domain Sender		
ExchangeLegacyInterop	Allow ACE	All	Accept Authoritative Domain Sender		
S-1-9-1419165041-	Allow ACE	All	Accept Authoritative		This is the well-known

1139599005-3936102811-1022490595-21			Domain Sender		SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Accept Authoritative Domain Sender		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Accept Authoritative Domain Sender		This is the well-known SID for externally secured servers.
Authenticated Users	Allow ACE	All	Submit Messages to any Recipient		
Authenticated Users	Allow ACE	All	Accept Routing Headers		
Authenticated Users	Allow ACE	All	Bypass Anti-Spam		
Authenticated Users	Allow ACE	All	Submit Messages to Server		

Distinguished name of the object: CN=Client <Server>,CN=SMTP Receive Connectors,CN=Protocols,CN=<Server>,CN=Servers,CN=<admin group>,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to
Authenticated Users	Allow ACE	All	Submit Messages to any Recipient	
Authenticated Users	Allow ACE	All	Accept Routing Headers	
Authenticated Users	Allow ACE	All	Bypass Anti-Spam	
Authenticated Users	Allow ACE	All	Submit Messages to Server	

SMTP Send Connector Creation

The following table shows the permissions set when you create Send connectors.

Distinguished name of the object: CN=<Connector Name>,CN=Connections,CN=<routing group>,CN=Routing Groups,CN=<admin group>,CN=<organization>

Account	ACE type	Inheritance	Permissions	On property/ Applies to	Comments
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Send Organization Headers		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Send Organization Headers		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Send Forest Headers		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Send Forest Headers		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Send XShadow		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Send XShadow		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-10	Allow ACE	All	Send Routing Headers		This is the well-known SID for partner servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Send Routing Headers		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-	Allow ACE	All	Send Routing Headers		This is the well-known

1139599005-3936102811-1022490595-22					SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Send Routing Headers		This is the well-known SID for externally secured servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-24	Allow ACE	All	Send Routing Headers		This is the well-known SID for Legacy Exchange servers.
NT AUTHORITY\ANONYMOUS LOGON	Allow ACE	All	Send Routing Headers		
S-1-9-1419165041-1139599005-3936102811-1022490595-21	Allow ACE	All	Send Exch50		This is the well-known SID for Hub Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-22	Allow ACE	All	Send Exch50		This is the well-known SID for Edge Transport servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-23	Allow ACE	All	Send Exch50		This is the well-known SID for externally secured servers.
S-1-9-1419165041-1139599005-3936102811-1022490595-24	Allow ACE	All	Send Exch50		This is the well-known SID for Legacy Exchange servers.

1.2.1.13 Default Authentication Settings for Exchange-related Virtual Directories

Default Authentication Settings for Exchange-related Virtual Directories

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-08*

Microsoft Exchange Server 2010 automatically configures multiple Internet Information Services (IIS) virtual directories during installation. This topic contains information about the default IIS authentication settings and default Secure Sockets Layer (SSL) settings for the Client Access and Mailbox server roles.

Client Access Server Role

The following table lists the default settings on a stand-alone Exchange 2010 Client Access server.

Default Client Access server IIS authentication and SSL settings

Virtual directory	Authentication method	SSL settings	Management method
Default Web site	• Anonymous	• Required	IIS ,management console
aspnet_client	• Anonymous authentication	• SSL required • Requires 128-bit encryption	IIS management console
Autodiscover	• Anonymous authentication • Basic authentication • Windows authentication	• SSL required • Require 128-bit encryption	Exchange Management Shell (Shell)
ecp	• Anonymous authentication • Basic authentication	• SSL required • Requires 128-bit encryption	Exchange Management Console (EMC) or Shell
EWS	• Anonymous authentication • Windows authentication	• SSL required • Requires 128-bit encryption	Shell
Microsoft-Server-ActiveSync	• Basic authentication	• SSL required • Requires 128-bit encryption	EMC or Shell
OAB	• Windows authentication	• Not required	EMC or Shell
owa	• Basic	• SSL required • Requires 128-bit encryption	EMC or Shell
Powershell	• Anonymous authentication	• Not required	Shell
Rpc	• Basic authentication • Windows authentication	• SSL required • Requires 128-bit encryption	Shell
RpcWithCert	By default, all authentication methods are disabled	• Required	

Mailbox Server Role

The following table lists the default settings on a stand-alone Exchange 2010 mailbox server.

Default Mailbox server IIS authentication and SSL settings

Virtual directory	Authentication method	SSL settings	Management method
Default Web site	• Anonymous authentication	• SSL required • Requires 128-bit encryption	This virtual directory isn't configurable by the user.
PowerShell	• Anonymous authentication	• Not required	Shell.

1.2.1.14 Exchange Server Supportability Matrix

Exchange Server Supportability Matrix

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-02-26*

The Exchange Server Supportability Matrix provides a central source for Microsoft Exchange administrators to easily locate information about the level of support available for any configuration or required component for all versions of Microsoft Exchange.

Support Lifecycle

For more information about the support lifecycle for a specific version of Exchange, or of the Microsoft Windows server or client operating systems, see the Microsoft Support Lifecycle page. For more information about the Microsoft Support Lifecycle, see the Microsoft Support Lifecycle Policy FAQ.

Release Model

The following table identifies the release model used for updates and hotfixes for each version of Exchange. With Exchange, each update rollup package is cumulative with regard to the whole product. Therefore, if you apply an update rollup package to Microsoft Exchange Server 2010, you apply all the fixes contained in that update rollup package. This includes all the fixes contained in each earlier update rollup package. For more information, see Exchange 2010 Servicing.

When an update or a hotfix for earlier versions of Exchange is created, one or more of the binary files included in the update or included in the hotfix are cumulative. They are cumulative with regard to the contents of the files. However, they aren't cumulative with regard to the whole Exchange product. The release model used by a product is identified by an X character.

Servicing release model	Exchange 2013	Exchange 2010	Exchange 2007	Exchange 2003

Cumulative Updates	X			
Update rollups		X	X	
Hotfixes				X
Security Hotfixes Delivered Separately	X			X

Important:
Update rollups for Exchange 2010 and Exchange 2007 are a cumulative set of the hotfixes. Cumulative Updates (CU's) for Exchange 2013 are released as a full refresh of Exchange 2013, similar to a product upgrade or a service pack release.

Supported Operating System Platforms

The following table identifies the operating system platforms on which each version of Exchange can run. Supported platforms are identified by an X character.

Operating system platform	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
Windows 2000 Server SP4					X
Windows XP Professional SP2				X*	X**
Windows XP Professional SP3				X*	X**
Windows Vista SP1				X*	X***
Windows Vista SP2		X*	X*	X*	X***
Windows Server 2003 SP2				X	X
Windows Server 2003 R2 SP2				X	X
Windows Server 2008				X	
Windows Server 2008 SP2		X	X	X	
Windows Server 2008 R2		X	X	X	

Windows Server 2008 R2 SP1	X	X	X	X	
Windows 7	X*	X*	X*	X*	
Windows 8	X*	X*			
Windows Server 2012	X	X			

*Only for Exchange management tools

**Only for Exchange 2003 or Exchange 2000 System Manager

***Only together with Exchange 2003 System Manager for Windows Vista

Supported Active Directory Environments

The following table identifies the Active Directory environments with which each version of Exchange can communicate. Supported environments are identified by an X character. An Active Directory server refers both to global catalog servers and to domain controllers.

Operating system environment	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
Windows 2000 Server SP4 Active Directory servers					X
Windows Server 2003 SP1 Active Directory servers				X	X
Windows Server 2003 SP2 Active Directory servers	X	X	X	X	X
Windows Server 2008 Active Directory servers	X	X	X	X	X
Windows Server 2008 SP2 Active Directory servers	X	X	X	X	X
Windows Server 2008 R2 Active	X	X	X	X	X

Directory servers					
Windows Server 2008 R2 SP1 Active Directory servers	X	X	X	X	X
Windows Server 2008 read-only Active Directory servers					
Windows Server 2008 R2 read-only Active Directory servers					
Windows Server 2012 Active Directory servers	X	X	X	X	
Windows Server 2012 read-only Active Directory servers					

Domain and forest functional level	**Exchange 2013**	**Exchange 2010 SP3**	**Exchange 2010 SP2**	**Exchange 2007 SP3**	**Exchange 2003 SP2**
Windows 2000 Server mixed domain functional level					X
Windows 2000 Server native functional level				X	X
Windows Server 2003 interim domain functional level					X
Windows	X	X	X	X	X

Server 2003 domain functional level					
Windows Server 2008 domain functional level	X	X	X	X	X
Windows Server 2008 R2 domain functional level	X	X	X	X	X
Windows Server 2012 domain functional level	X	X	X	X	
Windows 2000 Server forest functional level				X	X
Windows Server 2003 interim forest functional level					X
Windows Server 2003 forest functional level	X	X	X	X	X
Windows Server 2008 forest functional level	X	X	X	X	X
Windows Server 2008 R2 forest functional level	X	X	X	X	X
Windows Server 2012 forest functional level	X	X	X	X	

Web Browsers Supported for Use with the Premium Version of Outlook Web App or Outlook Web Access

The following table identifies the Web browsers supported for use together with the premium version of Microsoft Office Outlook Web App for Microsoft Exchange Server 2010, Office Outlook Web Access for Exchange 2007 or Exchange 2003, or Outlook Web Access for Exchange 2000. Supported browsers are identified by an X character.

Browser	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
Internet Explorer 10	X	X			
Internet Explorer 9	X	X	X	X	
Internet Explorer 8	X	X	X	X	X**
Internet Explorer 7		X	X	X	X***
Internet Explorer 6				X	X
Firefox 3.0.1 or later		X	X		
Firefox 12 or later	X	X	X		
Safari 3.1 or later		X	X		
Safari 5.0 or later	X	X	X		
Chrome 3.0.195 or later		X	X		
Chrome 18 or later	X	X	X		

Support is added by Exchange 2010 SP2 RU5.

**Requires the hotfix described in Microsoft Knowledge Base article 963664, Error message when you click the flag icon of a message in the message list view in Outlook Web Access 2003 when you are using Internet Explorer 8: "'firstchild.firstchild' is null or not an object".

***Requires the hotfix described in Microsoft Knowledge Base article 911829, You receive an error message when you try to perform any editing tasks, or you must click to enable the compose frame in Outlook Web Access.

Web Browsers Supported for Use with the Basic Version of Outlook Web App or Outlook Web Access

The following table identifies the Web browsers that are supported for use together with the light (basic) version of Outlook Web App for Exchange 2010 or Microsoft Outlook Web Access for Microsoft Exchange Server 2007, for Microsoft Exchange Server 2003, or for Microsoft Exchange 2000. Supported browsers are identified by an X character.

Note:

Outlook Web App Basic (Outlook Web App Light) is supported for use in mobile browsers. However, if rendering or authentication issues occur in a mobile browser, determine whether the issue can be reproduced by using Outlook Web App Light in the full client of a supported browser. For example, test the use of Outlook Web App Light in Safari, Chrome, or Internet Explorer. If the issue can't be reproduced in the full client, we recommend that you contact the mobile device vendor for help. In these cases, we collaborate with the vendor as appropriate.

Browser	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
Internet Explorer 10	X	X			
Internet Explorer 9	X	X*	X*	X	
Internet Explorer 8	X	X	X	X	X**
Internet Explorer 7	X	X	X	X	X***
Internet Explorer 6		X	X	X	X
Safari	X	X	X	X	X****
Firefox	X	X	X	X	X****
Netscape				X	X****
Opera	X	X	X	X	X****

*Requires Exchange 2010 SP2 RU5-v2, described in Microsoft Knowledge Base article 2785908, Description of Update Rollup 5 version 2 for Exchange Server 2010 Service Pack 2.

**Requires the hotfix described in Microsoft Knowledge Base article 963664, Error message when you click the flag icon of a message in the message list view in Outlook Web Access 2003 when you are using Internet Explorer 8: "'firstchild.firstchild' is null or not an object".

***Requires the hotfix described in Microsoft Knowledge Base article 911829, You receive an error message when you try to perform any editing tasks, or you must click to enable the compose frame in Outlook Web Access.

****Browser should support HTML 3.2, European Computer Manufacturers Association (ECMA) script standards, and JavaScript.

Web Browsers Supported for the Use of S/MIME with Outlook Web App or Outlook Web Access

The following table identifies the Web browsers that are supported for the use of S/MIME together with Outlook Web App for Exchange 2010 or Outlook Web Access for Exchange 2007, Exchange 2003, or Exchange 2000. Supported browsers are identified by an X character.

Browser	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
Internet Explorer 10		X			
Internet Explorer 9		X	X	X	
Internet Explorer 8		X	X	X	X*
Internet Explorer 7		X	X	X	X***
Internet Explorer 6					X

**Requires Update Rollup 8 for Exchange Server 2007 Service Pack 1 (SP1) or later versions. For more information, see Description of Update Rollup 8 for Exchange Server 2007 Service Pack 1.

***Requires the hotfix described in Microsoft Knowledge Base article 924334, The Compose Message form stops responding after you install Internet Explorer 7.0 and the S/MIME control on an Outlook Web Access client in Exchange Server 2003.

Clients

The following table identifies the mailbox clients that are supported for use together with each version of Exchange. Supported clients are identified by an X character.

Client	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
Outlook 2002					X
Outlook 2003		X	X	X	X
Outlook 2007	X**	X	X	X	X
Outlook 2010	X***	X	X	X	X
Windows Mobile 5.0	X	X	X	X	X

Windows Mobile 6.0	X	X	X	X	X
Windows Mobile 6.1	X	X	X	X	X
Windows Mobile 6.5	X	X	X	X	X
Windows Phone 7	X	X	X	X	X
Windows Phone 7.5	X	X	X	X	X
Entourage X				X*	X
Entourage 2004 (DAV)				X**	X
Entourage 2008 (DAV)				X**	X
Entourage 2008 (EWS)	X****	X****	X****	X	

*WebDav: Contacts, Events, IMAP: Mail

**Requires Outlook 2007 Service Pack 3 and the November 2012 Public Update or later.

***Requires Outlook 2010 Service Pack 1 and the November 2012 Public Update or later.

****EWS only. There is no DAV support for Exchange 2010.

Tools

The following table identifies the version of Microsoft Exchange that can be used together with the Microsoft Exchange Inter-Organization Replication tool (Exscfg.exe; Exssrv.exe). The tool is used to replicate public folder information (including free/busy information) between Exchange organizations. For more information, see Microsoft Exchange Server Inter-Organization Replication. Supported versions are identified by an X character.

Note:

You must run the Inter-Organization Replication tool on a 32-bit operating system that has Exchange 2003 Management Tools installed.

Important:

If you want to use the Inter-Organization Replication tool, one of the Exchange replication endpoints must be an Exchange 2003 server.

Tool	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
Inter-Organization Replication tool		X	X	X	X

Microsoft .NET Framework

The following table identifies the version of the Microsoft .NET Framework that can be used together with each version of Exchange. Supported versions are identified by an X character.

.NET Framework	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
.NET Framework 1.0 SP1					X
.NET Framework 1.1 SP1					X
.NET Framework 2.0					
.NET Framework 2.0 SP1				X	
.NET Framework 3.0				X	
.NET Framework 3.5		X*****		X***	
.NET Framework 3.5 SP1		X	X	X	
.NET Framework 4.0		X*****	X****	X***	
.NET Framework 4.5	X	X*****	X****		

***Supported versions of the .NET Framework are included in the .NET Framework 3.5 and in the .NET Framework 3.5 SP1.

****Applies only when upgrading the system from the .NET Framework 3.5 and the .NET Framework 3.5 SP1. Uninstalling the .NET Framework 3.5 and the .NET Framework 3.5 SP1 isn't supported.

***** If you are using Windows Server 2012, the .NET Framework 3.5 must be installed before you can use Exchange 2010 SP3.

Windows PowerShell

The following table identifies the version of the Windows PowerShell command-line interface that can be used together with each version of Exchange. Supported versions

are identified by an X character.

PowerShell	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
PowerShell 1.0				X	
PowerShell 2.0		X	X	X	
PowerShell 3.0	X				

Microsoft Management Console

The following table identifies the version of Microsoft Management Console (MMC) that can be used together with each version of Exchange. Supported versions are identified by an X character.

MMC	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
MMC 2.0					X
MMC 3.0	X	X	X	X	

Windows Installer

The following table identifies the version of Windows Installer that is used together with each version of Exchange. Supported versions are identified by an X character.

Windows Installer	Exchange 2013	Exchange 2010 SP3	Exchange 2010 SP2	Exchange 2007 SP3	Exchange 2003 SP2
Windows Installer 3.0					
Windows Installer 3.1 v1					
Windows Installer 3.1 v2					
Windows Installer 4.0					
Windows Installer 4.5	X	X	X	X	
Windows Installer 5.0	X				

1.2.1.15 Exchange 2010 Solution Accelerator

Exchange 2010 Solution Accelerator

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-24*

The Infrastructure Planning and Design (IPD) Guide for Exchange Server 2010 with Service Pack 1 (SP1) provides the IT architect with a step-by-step process for successfully designing an Exchange Server 2010 infrastructure. Exchange 2010 supports a variety of infrastructure topologies that enable IT departments to deploy the messaging architecture that best suits their business needs. The guide helps organizations make informed decisions about the design of fault tolerance and scalability so that their overall requirements are met.

For more information about the IPD guide, see Infrastructure Planning and Design - Exchange Server 2010.

1.2.2 Deploying Exchange 2010

Deploying Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-08*

The deployment phase is the period during which you install Microsoft Exchange Server 2010 into your production environment. Before you begin the deployment phase, you should plan your Exchange organization. For more information, see Planning for Exchange 2010.

Use the following links to access the information you need to help you with deploying Exchange 2010. Also, see Exchange Server Deployment Assistant for information about a Web-based tool that can help you with your deployment.

Understanding Deployment of Exchange 2010

This section includes topics related to understanding your Exchange 2010 deployment, including important information about prerequisites and security. Also, start here to get insight into upgrading from previous versions of Microsoft Exchange.

Understanding a New Installation of Exchange 2010

This section discusses the scenario in which you install Exchange 2010 into a new Exchange organization.

Understanding Upgrade from Exchange 2003 to Exchange 2010

See this section for information that will help you upgrade from Microsoft Exchange Server 2003 to Exchange 2010.

Understanding Upgrade from Exchange 2007 to Exchange 2010

See this section for information that will help you upgrade from Microsoft Exchange Server 2007 to Exchange 2010.

Understanding Upgrade from Exchange 2003 and Exchange 2007 to Exchange 2010

See this section for information that will help you upgrade from a mixed environment of Exchange 2003 and Exchange 2007 to Exchange 2010.

Understanding Unified Messaging Deployments

See this section for information that will help you understand deploying Exchange 2010 Unified Messaging, whether a new deployment or an upgrade.

Managing Deployment of Exchange 2010

In this section you'll find the procedures that will help you prepare your organization and install Exchange 2010 server roles or upgrade existing server roles. This section also contains information that will help you move your mailboxes from one version of Exchange to another.

Deploy Multiple Forest Topologies

This section includes information to help you deploy Exchange 2010 in a resource forest or cross-forest topology.

Exchange 2010 Post-Installation Tasks

See this section for mandatory and optional post-installation tasks to complete your Exchange 2010 installation.

Modify an Exchange 2010 Installation

See this section for procedures to help you remove or modify your Exchange 2010 installation.

Installation Guide Templates

This section provides document templates you can use to create customized installation guides for your organization's Exchange 2010 server role installations.

Exchange 2010 Servicing

This section provides guidance about how to deploy fixes for Exchange 2010 and provides information about how to apply the appropriate updates.

1.2.2.1 Understanding Deployment of Exchange 2010

Understanding Deployment of Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-13*

Before you begin the deployment phase, you should plan your Microsoft Exchange Server 2010 organization. For more information, see Planning for Exchange 2010.

This section includes the following topics:

Exchange 2010 Prerequisites

Understanding Exchange 2010 Setup

Overview of Services Installed by Exchange Setup

Deployment Security Checklist

Exchange Management Console Interoperability

Understanding Upgrade to Exchange 2010

1.2.2.1.1 Exchange 2010 Prerequisites

Exchange 2010 Prerequisites

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-02-26*

This topic provides the steps for installing the necessary Windows Server 2008 Service Pack 2 (SP2) or later, Windows Server 2008 R2 or later, and Windows Server 2012 operating system prerequisites for all Microsoft Exchange Server 2010 server roles. It also includes the steps for installing the Windows 8, Windows 7, and Windows Vista operating system prerequisites for the Exchange management tools.

Prerequisites

- Make sure that the functional level of your forest is at least Windows Server 2003, and that the schema master is running Windows Server 2003 with Service Pack 1 (SP1) or later. For more information about the Windows functional level, see Managing Domains and Forests.
- The full installation option of Windows Server 2008 with SP2 or later, Windows Server 2008 R2 RTM or later, or Windows Server 2012 must be used for all servers running Exchange 2010 server roles or management tools.
- For all server roles other than the Edge Transport server role, you must first join the computer to the appropriate internal Active Directory forest and domain.

Note:
If you're installing the Mailbox server role and you intend the server to be a member of a database availability group (DAG), you must be running the Enterprise Edition of Windows Server 2008 or Windows Server 2008 R2. The Standard Edition doesn't support the features needed for DAGs. You can't upgrade Windows when Exchange is installed on the server. This does not apply to Windows Server 2012 because Windows Server 2012 Standard and Windows Server 2012 Datacenter both support failover clustering.

Note:
If you're installing the Mailbox server role, the Task Scheduler and Windows Firewall must be enabled and running. In addition, if the Mailbox server will be a member of a DAG and host replicated databases, it's required that the script is scheduled and run automatically. For more information about the script, see "CheckDatabaseRedundancy.ps1 Script" in the Monitoring High Availability and Site Resilience topic.

Install the Exchange 2010 Hotfixes for Windows Server 2008 SP2

The following hotfixes are required for Windows Server 2008 SP2:

- Install the update described in Microsoft Knowledge Base article 977624, AD RMS clients do not authenticate federated identity providers in Windows Server 2008 or in Windows Vista. Without this update, Active Directory Rights Management Services (AD RMS) features may stop working.

- Install the update described in Knowledge Base article 979744, A .NET Framework 2.0-based Multi-AppDomain application stops responding when you run the application.
- Install the update described in Knowledge Base article 979917, Two issues occur when you deploy an ASP.NET 2.0-based application on a server that is running IIS 7.0 or IIS 7.5 in Integrated mode. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB979917 - QFE for Sharepoint issues - Perf Counter fix & User Impersonation.
  - For the available downloads, see KB979917 - QFE for Sharepoint issues - Perf Counter fix & User Impersonation.
- Install the update described in Knowledge Base article 973136, FIX: ArgumentNullException exception error message when a .NET Framework 2.0 SP2-based application tries to process a response with zero-length content to an asynchronous ASP.NET Web service request: "Value cannot be null".
- Install the update described in Knowledge Base article 977592, RPC over HTTP clients cannot connect to the Windows Server 2008 RPC over HTTP servers that have RPC load balancing enabled.

Install the Exchange 2010 Hotfixes for Windows Server 2008 R2

Warning:
The following hotfixes only apply to Windows Server 2008 R2 RTM. If you're installing Exchange on Windows Server 2008 R2 SP1, you don't need to apply these hotfixes.

The following hotfixes are required for the Client Access server for Windows Server 2008 R2 RTM:

- Install the update described in Knowledge Base article 979099, An update is available to remove the application manifest expiry feature from AD RMS clients. Without this update, the AD RMS features may stop working.
- Install the update described in Knowledge Base article 979744, A .NET Framework 2.0-based Multi-AppDomain application stops responding when you run the application.
- Install the update described in Knowledge Base article 983440, An ASP.NET 2.0 hotfix rollup package is available for Windows 7 and for Windows Server 2008 R2. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB983440 - Win7 rollup package (PR for QFE 810219).
  - For the available downloads, see KB983440 - Win7 rollup package (PR for QFE 810219).
- Install the update described in Knowledge Base article 977020, FIX: An application that is based on the Microsoft .NET Framework 2.0 Service Pack 2 and that invokes a Web service call asynchronously throws an exception on a computer that is running Windows 7.

The following hotfix is required for Hub Transport and Mailbox servers for Windows Server 2008 R2:

- Install the update described in Knowledge Base article 979099, An update is available to remove the application manifest expiry feature from AD RMS clients. Without this update, the AD RMS features may stop working.

The following hotfix is strongly recommended for Mailbox servers running Windows Server 2008 R2 that are members of a database availability group (DAG):

- Install the update described in Knowledge Base article 2550886, A transient communication failure causes a Windows Server 2008 R2 failover cluster to stop working. Without this update, the underlying cluster for a DAG could

experience a race condition that causes a loss of quorum in the cluster and a loss of functionality in the DAG.

Install the Exchange 2010 Hotfixes for Windows 7 and Windows Vista

The following hotfixes are required for Windows 7 and Windows Vista:

- Install the update described in Knowledge Base article 977020, FIX: An application that is based on the Microsoft .NET Framework 2.0 Service Pack 2 and that invokes a Web service call asynchronously throws an exception on a computer that is running Windows 7.
- Install the update described in Knowledge Base article 983440, An ASP.NET 2.0 hotfix rollup package is available for Windows 7 and for Windows Server 2008 R2. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB983440 - Win7 rollup package (PR for QFE 810219).
  - For the available downloads, see KB983440 - Win7 rollup package (PR for QFE 810219).

Install the Windows Server 2008 SP2 operating system prerequisites

1. Install Microsoft .NET Framework 3.5 Service Pack 1 (SP1). For details, see Microsoft .NET Framework 3.5 Service Pack 1.
2. Install the Microsoft .NET Framework 3.5 Family Update for Windows Vista x64 and Windows Server 2008 x64 updates. For details, see Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 and Knowledge Base article 959209, An update for the .NET Framework 3.5 Service Pack 1 is available.
3. Install Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu). For details, see Knowledge Base article 968930, Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0).
4. On servers that will host the Hub Transport or Mailbox server role, install the Microsoft Filter Pack. For Exchange 2010 release to manufacturing (RTM), see 2007 Office System Converter: Microsoft Filter Pack. For Exchange 2010 SP1, see Microsoft Office 2010 Filter Packs. For more information about registering the Filter Pack, see Register Filter Pack IFilters with Exchange 2010.

   Note:
   On Exchange 2010 RTM, you can meet the prerequisite by installing 2007 Office System Converter: Microsoft Filter Pack. However, we recommend that you upgrade to the Microsoft Office 2010 Filter Packs.

5. Open an elevated command prompt, navigate to the \Scripts folder on the Exchange 2010 installation media, and then use one of the following commands to install the necessary operating system components:
   - This example is for a server that will have the typical installation of the Client Access, Hub Transport, and Mailbox server roles.

     ```
     sc config NetTcpPortSharing start= auto
     ServerManagerCmd -ip Exchange-Typical.xml -Restart
     ```

   - This example is for a server that will host the Client Access, Hub Transport, Mailbox, and Unified Messaging server roles.

     ```
     sc config NetTcpPortSharing start= auto
     ServerManagerCmd -i Desktop-Experience
     ServerManagerCmd -ip Exchange-Typical.xml -Restart
     ```

- This example is for a server that will host the Client Access and Hub Transport server roles.

```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

- This example is for a server that will host the Hub Transport and Mailbox server roles.

```
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

- This example is for a server that will host the Client Access and Mailbox server roles.

```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

- This example is for a server that will host only the Client Access server role.

```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-CAS.xml -Restart
```

- This example is for a server that will host only the Hub Transport server role.

```
ServerManagerCmd -ip Exchange-Hub.xml -Restart
```

- This example is for a server that will host only the Mailbox server role.

```
ServerManagerCmd -ip Exchange-MBX.xml -Restart
```

- This example is for a server that will host only the Unified Messaging server role.

```
ServerManagerCmd -ip Exchange-UM.xml -Restart
```

- This example is for a server that will host the Edge Transport server role.

```
ServerManagerCmd -ip Exchange-Edge.xml -Restart
```

Install the Exchange 2010 Hotfixes for Windows Server 2008 SP2

The following hotfix is required for Windows Server 2008 SP2 and must be installed after the operating system prerequisites have been installed:

- Install the hotfix described in Knowledge Base article 982867, WCF services that are hosted by computers together with a NLB fail in .NET Framework 3.5 SP1. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.
  - For the available downloads, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.

After installing the preceding prerequisites and hotfix, and before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Install the Windows Server 2008 R2 operating system prerequisites

1. On servers that will host the Hub Transport or Mailbox server role, install the Microsoft Filter Pack. For Exchange 2010 RTM, see 2007 Office System Converter: Microsoft Filter Pack. For Exchange 2010 SP1, see Microsoft Office 2010 Filter Packs. For more information about registering the Filter Pack, see Register Filter Pack IFilters with Exchange 2010.

   Note:

   On Exchange 2010 RTM, you can meet the prerequisite by installing 2007 Office System Converter: Microsoft Filter Pack. However, we recommend that you upgrade to the Microsoft Office 2010 Filter Packs.

2. On the Start menu, navigate to **All Programs** > **Accessories** > **Windows PowerShell**. Open an elevated Windows PowerShell console, and run the following command.

   ```
   Import-Module ServerManager
   ```

3. Use the **Add-WindowsFeature** cmdlet to install the necessary operating system components:
   - This example is for a server that will have the typical installation of the Client Access, Hub Transport, and Mailbox server roles.

     ```
     Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Ba
     ```

   - This example is for a server that will host the Client Access, Hub Transport, Mailbox, and Unified Messaging server roles.

     ```
     Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Ba
     ```

   - This example is for a server that will host the Client Access and Hub Transport server roles.

     ```
     Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Ba
     ```

   - This example is for a server that will host the Hub Transport and Mailbox server roles.

     ```
     Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Ba
     ```

   - This example is for a server that will host the Client Access and Mailbox server roles.

     ```
     Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Ba
     ```

   - This example is for a server that will host only the Client Access server role.

     ```
     Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Ba
     ```

   - This example is for a server that will host the Hub Transport or the Mailbox server role.

     ```
     Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Ba
     ```

   - This example is for a server that will host only the Unified Messaging server role.

     ```
     Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Ba
     ```

- This example is for a server that will host the Edge Transport server role.

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,ADLDS -Restart
```

Install the Exchange 2010 Hotfixes for Windows Server 2008 R2

The following hotfix is required for Windows Server 2008 R2 and must be installed after the operating system prerequisites have been installed:

- Install the hotfix described in Knowledge Base article 982867, WCF services that are hosted by computers together with a NLB fail in .NET Framework 3.5 SP1. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.
  - For the available downloads, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.

After installing the preceding prerequisites and hotfix, and before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Install the Windows Server 2012 operating system prerequisites

Follow the instructions in this section to install the Service Pack 3 (SP3) for Exchange Server 2010 prerequisites on your Windows Server 2012 computer. The prerequisites that are required to install Exchange 2010 SP3 on a Windows Server 2012 computer depend on which Exchange roles you want to install.

1. On the Start screen, right-click **Windows PowerShell** and then click **Run as administrator**. Then, run the following command.

```
Import-Module ServerManager
```

2. Use the **Add-WindowsFeature** cmdlet to install the necessary operating system components for the Exchange 2010 SP3 roles you want to install. Following are examples of installations:
   - This example is for a server that will have the typical installation of the Client Access, Hub Transport, and Mailbox server roles.

```
Add-WindowsFeature NET-Framework-Features,NET-HTTP-Activatic
```

   - This example is for a server that will host the Client Access, Hub Transport, Mailbox, and Unified Messaging server roles.

```
Add-WindowsFeature NET-Framework-Features,Desktop-Experience
```

   - This example is for a server that will host the Client Access and Hub Transport server roles.

```
Add-WindowsFeature NET-Framework-Features,NET-HTTP-Activatic
```

   - This example is for a server that will host the Hub Transport and Mailbox server roles.

```
Add-WindowsFeature NET-Framework-Features,RSAT-Clustering,WA
```

   - This example is for a server that will host the Client Access and Mailbox server roles.

```
Add-WindowsFeature NET-Framework-Features,NET-HTTP-Activatic
```

- This example is for a server that will host only the Client Access server role.

```
Add-WindowsFeature NET-Framework-Features,NET-HTTP-Activatic
```

- This example is for a server that will host only the Hub Transport server role.

```
Add-WindowsFeature NET-Framework-Features,Web-Mgmt-Console,W
```

- This example is for a server that will host only the Mailbox server role.

```
Add-WindowsFeature NET-Framework-Features,RSAT-Clustering,We
```

- This example is for a server that will host only the Unified Messaging server role.

```
Add-WindowsFeature NET-Framework-Features,Desktop-Experience
```

- This example is for a server that will host the Edge Transport server role.

```
Add-WindowsFeature ADLDS,NET-Framework-Features -Restart
```

After you have installed the operating system roles and features, install the following software components in the order presented:

1. Client Access and Unified Messaging servers
   1.a. Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit
2. Mailbox and Hub Transport servers
   2.a. Microsoft Office 2010 Filter Pack 64 bit
   2.b. Microsoft Office 2010 Filter Pack SP1 64 bit

Install the Windows Vista SP2 operating system prerequisites for the Exchange management tools

1. Install Microsoft .NET Framework 3.5 SP1. For details, see Microsoft .NET Framework 3.5 Service Pack 1.
2. Install the Microsoft .NET Framework 3.5 Family Update for Windows Vista x64 and Windows Server 2008 x64 updates. For details, see Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 and Knowledge Base article 959209, An update for the .NET Framework 3.5 Service Pack 1 is available.
3. Install Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu). For details, see Knowledge Base article 968930, Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0).
4. Install the necessary operating system components:
   4.a. Open Control Panel, and then select **Programs**.
   4.b. Click **Turn Windows features on or off**.
   4.c. Navigate to **Internet Information Services** > **Web Management Tools** > **IIS 6 Management Compatibility**.
   4.d. Select the check box for **IIS 6 Management Console**, and then click **OK**.

Install the Windows 7 operating system prerequisites for the Exchange management tools

1. Open Control Panel, and then select **Programs**.
2. Click **Turn Windows features on or off**.
3. Select **Microsoft .NET Framework 3.5.1**.
4. Navigate to **Internet Information Services** > **Web Management Tools** > **IIS 6 Management Compatibility**.
5. Select the check box for **IIS 6 Management Console**, and then click **OK**.

Install the Windows 8 operating system prerequisites for the Exchange management tools

Note:
To install the Exchange Management Tools on Windows 8, you must install Exchange 2010 SP3 or later.

The Exchange management tools can be installed on a domain-joined computer with a default install of Windows 8 64-bit.

1.2.2.1.2 Understanding IPv6 Support in Exchange 2010

Understanding IPv6 Support in Exchange 2010

Planning and Deployment > Deploying Exchange 2010 > Understanding Deployment of Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-07-11*

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP). IPv6 is intended to correct many of the shortcomings of IPv4, which was the previous version of the IP. In Microsoft Exchange Server 2010, IPv6 is supported only when IPv4 is also used; a pure IPv6 environment isn't supported. Using IPv6 addresses and IP address ranges is supported only when both IPv6 and IPv4 are enabled on the computer running Exchange 2010, and the network supports both IP address versions. If Exchange 2010 is deployed in this configuration, all server roles can send data to and receive data from devices, servers, and clients that use IPv6 addresses.

This topic discusses IPv6 addressing in Exchange 2010. For additional background information about IPv6, see IPv6 and IPv6 Support in Exchange 2007 SP1 and SP2.

Contents

Disable or Enable IPv6

Looking for management tasks related to deploying Exchange 2010? See Managing Deployment of Exchange 2010.

IPv6 Addresses

An IPv6 address is 128-bits long. The address is described by using colon-hexadecimal notation. Colon-hexadecimal notation describes the 128-bit address by using eight 16-bit, 4-digit hexadecimal numbers separated by the colon character (:). An example of an IPv6 address in colon-hexadecimal notation is 2001:0DB8:0000:0000:02AA:00FF:C0A8:640A.

You can express an IPv6 address by using the following methods:

- **Suppress leading zeros** You can omit the leading zeros in any of the eight 4-digit hexadecimal numbers in an IPv6 address.
- **Double-colon compression** You can use two colons (::) to represent contiguous 16-bit hexadecimal digits that contain all zeros. These all-zero digits may exist at the beginning, middle, or end of the IPv6 address. You can only use double-colon compression one time in an IPv6 address.
- **Trailing dotted-decimal notation** You may express the last 32 bits at the end of an IPv6 address in dotted-decimal notation by separating the 8-bit digits with a period (.). Trailing dotted-decimal notation is frequently used with IPv4-compatible addresses.

The following table provides examples of the IPv6 address notation and the equivalent IPv6 address syntax.

IPv6 address notation and syntax

IPv6 address notation	IPv6 address syntax
Full IPv6 address	2001:0DB8:0000:0000:02AA:00FF:C0A8:640A
IPv6 address that uses suppressed leading zeros	2001:DB8:0:0:2AA:FF:C0A8:640A
IPv6 address that uses double-colon compression	2001:DB8::2AA:FF:C0A8:640A
IPv6 address that uses trailing dotted-decimal notation	2001:DB8::2AA:FF:192.168.100.10

IPv6 addresses are categorized into the following types:

- **Unicast address** A packet is delivered to one interface.
- **Multicast address** A packet is delivered to multiple interfaces.
- **Anycast address** A packet is delivered to the nearest of multiple interfaces. The distance between interfaces is defined by the routing cost.

IPv6 unicast addresses have the following possible scopes:

- **Link local** The scope of the IPv6 address is the local subnet. IPv6 link local addresses are comparable to IPv4 link local addresses used in Automatic Private IP Addressing (APIPA).
- **Site local** The scope of the IPv6 address is the local organization. Site local addresses were deprecated by RFC 3879 and replaced by unique local addresses as defined in RFC 4193. IPv6 site local addresses and IPv6 unique local addresses are comparable to IPv4 private IP addresses.

- **Global** The scope of the IPv6 address is the whole world. IPv6 global addresses are comparable to IPv4 public IP addresses.

The following table provides a comparison of IPv4 elements and IPv6 elements.

IPv4 vs. IPv6 elements

Item	IPv4	IPv6
Private IP address	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	FD00::/8
Link local address	169.254.0.0/16	FE80::/64
Loopback address	127.0.0.1	::1
Unspecified address	0.0.0.0	::
Address resolution	Address Resolution Protocol (ARP)	Neighbor Discovery (ND)
Domain Name System (DNS) host name resolution	Address record (A record)	AAAA record or A6 record

For more information about IPv6 addressing, see IPv6 Address Types.

Supported IPv6 Address Input Formats

The following types of IPv6 address input formats are supported in Exchange 2010:

- A single IPv6 address
- An IPv6 address range
- An IPv6 address together with a subnet mask
- An IPv6 address together with a subnet mask that uses Classless Interdomain Routing (CIDR) notation

The following table provides examples of the acceptable IPv6 address input formats in Exchange 2010 on Windows Server 2008.

IPv6 address examples

Type	Example of an IPv6 address
Single address	2001:DB8::2AA:FF:C0A8:640A
Address range	2001:DB8::2AA:FF:C0A8:640A- 2001:DB8::2AA:FF:C0A8:6414
Address together with subnet mask	2001:DB8::2AA:FF:C0A8:640A (FFFF:FFFF:FFFF:FFFF::)
Address together with subnet mask that uses CIDR notation	2001:DB8::2AA:FF:C0A8:640A/64

In Exchange 2010 on Windows Server 2008, the following input formats are supported:

- Suppression of leading zeros
- Double-colon compression
- Trailing dotted-decimal notation

Return to top

IPv6 Support in Exchange 2010 Components

The following table describes the components in Exchange 2010 affected by IPv6.

Exchange 2010 components and IPv6

Server role on the source computer	Feature	IPv6 supported	Comments
Transport	IP Allow list and IP Block list	Yes	For more information about the IP Allow list, see Enable or Disable Connection Filtering and Understanding Connection Filtering.
Transport	IP Allow List providers and IP Block List providers	No	Currently, there is no widely accepted industry standard protocol for looking up IPv6 addresses. Most IP Block List providers don't support IPv6 addresses. If you allow anonymous connections from unknown IPv6 addresses on a Receive connector, you increase the risk that spammers will bypass IP Block List providers and successfully deliver spam into your organization. For more information about IP Block list providers, see "IP Block List Providers" in Understanding Connection Filtering.
Transport	Sender reputation	No	The Protocol Analysis agent doesn't compute the sender reputation level (SRL) for messages that originate from IPv6 senders. For more information about sender reputation, see Understanding Sender Reputation.
Transport	Sender ID	Yes	For more information, see Understanding Sender ID.
Transport	Receive connectors	Yes	IPv6 addresses are accepted for the following components: • Local IP address bindings • Remote IP addresses • IP address ranges We strongly recommend against configuring Receive connectors to accept anonymous

			connections from unknown IPv6 addresses. If your organization must receive mail from senders who use IPv6 addresses, create a dedicated Receive connector that restricts the remote IP addresses to the specific IPv6 addresses that those senders use. For more information, see Understanding Receive Connectors.
Transport	Send connectors	Yes	IPv6 addresses are accepted for the following components: • Smart host IP addresses • The *SourceIPAddress* parameter for Send connectors configured on Edge Transport servers **Note:** If you want to specify an IPv6 address for the *SourceIPAddress* parameter, make sure that the appropriate DNS AAAA and mail exchange (MX) records are configured correctly. This helps ensure message delivery if a remote messaging server tries any kind of reverse lookup test on the specified IPv6 address. For more information, see Understanding Send Connectors.
Transport	Incoming message rate limits	Partial	Incoming message rate limits that you can set on a Receive connector, such as the *MaxInboundConnectionPercentagePerSource* parameter, the *MaxInboundConnectionPerSource* parameter, and the *TarpitInterval* parameter, only apply to a global IPv6 address. Link local IPv6 addresses and site local IPv6 addresses aren't affected by any specified incoming message rate limits. For more information about incoming message rate limits, see Understanding Message Throttling.

Unified Messaging	All features	No	Unified Messaging doesn't support IPv6 in any version of Exchange 2010. For more information about Unified Messaging, see Unified Messaging.
Mailbox (Database availability group member)	IPv6 addresses	Yes	Static IPv6 addresses are supported by Windows Server 2008 and the Cluster service. However, using static IPv6 addresses goes against best practices. Exchange 2010 on Windows Server 2008 doesn't support the configuration of static IPv6 addresses during setup. Failover clusters support Intra-site Automatic Tunnel Addressing Protocol (ISATAP). They support only IPv6 addresses that allow for dynamic registration in DNS. Link local addresses can't be used in a cluster. For more information, see New High Availability and Site Resilience Functionality.

Return to top

Disable IPv6

Exchange servers fully support IPv6 networks. Therefore, you do not have to disable IPv6 on your Exchange servers. To learn more about IPv6 support in Microsoft Windows, see IPv6 for Microsoft Windows: Frequently Asked Questions.

Return to top

1.2.2.1.3 Understanding Exchange 2010 Setup

Understanding Exchange 2010 Setup

Planning and Deployment > Deploying Exchange 2010 > Understanding Deployment of Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-29*

This topic provides an overview of Microsoft Exchange Server 2010 Setup. You can use different types and modes of Exchange 2010 Setup to install and maintain the various editions and versions of Exchange 2010. Improvements have also been made to Setup in Exchange Server 2010 Service Pack 1 (SP1) to enhance the Setup log and the scenario of

a failed installation.

For a list of the various services installed by Exchange Setup, see Overview of Services Installed by Exchange Setup.

Exchange Editions and Versions

Exchange Server 2010 is available in two server editions: Standard Edition and Enterprise Edition. These are licensing editions that are defined by a product key. The release to manufacturing (RTM) and service pack 1 (SP1) versions of Exchange Server 2010 are now available. For more information, see Exchange 2010: Editions and Versions.

Types of Exchange Setup

You have the following options for Exchange 2010 Setup:

Exchange Setup UI Setup.exe is an interactive experience where you are guided by the Exchange 2010 Setup wizard.

Exchange Unattended Setup Setup.com is an unattended experience where you provide command-line switches interactively or through a script. Setup.com is available from the Exchange 2010 DVD or the downloaded source files.

Modes of Exchange Setup

Setup for Exchange 2010 includes several installation modes:

Install Use this mode when you're installing a new server role or adding a server role to an existing installation (maintenance mode). You can use this mode from both the Exchange Setup wizard and the unattended install.

Uninstall Use this mode when you're removing the Exchange installation or removing a single server role from an existing installation (maintenance). You can use this mode from both the Exchange Setup wizard and the unattended install.

Upgrade Select this mode used when you have an existing installation of Exchange and you're installing the new version. This mode is used for a Service Pack installation. You can use this mode from both the Exchange Setup wizard and the unattended install.

RecoverServer Use this mode when there has been a catastrophic failure of a server, and you need to recover data. You must install a server using the same fully qualified domain name (FQDN) as the failed server, and then run Setup with the **/m:RecoverServer** switch. Don't specify the roles to restore. Setup detects the Exchange Server object in Active Directory and installs the corresponding files and configuration automatically. After you recover the server, you can restore databases and reconfigure any additional settings. To run in RecoverServer mode, you can't have Exchange installed on the server. The Exchange server object must exist in Active Directory. You can only use this mode during an unattended installation.

Note:

You must complete one mode of Setup before you can use another mode.

Exchange 2010 SP1 Setup Improvements

There have been several improvements to Setup in Exchange 2010 SP1:

- **Failed Installations** Unlike Exchange 2010 RTM, Setup in Exchange 2010 SP1

now supports resuming a failed installation. (In Exchange 2010, if you have a failed installation, you can't use the Uninstall mode to correct it.) A watermark in the registry identifies where Setup failed. You will not have to answer the Exchange 2010 Setup wizard questions again when you resume a failed Setup. You can resume the failed install, and let it succeed.

- **Exchange Setup Log** Exchange SP1 improves the Exchange Setup Log by reducing the amount of non-essential information and correctly noting errors. The Setup Log is divided into discrete sections so it's easy to see where Setup failed. For more information, see Verify an Exchange 2010 Installation.
- **Windows Roles and Features** Exchange 2010 SP1 adds the ability to install Windows roles and features that are required for your server roles.

For more information about these improvements, see New Deployment Functionality in Exchange 2010 SP1.

1.2.2.1.4 Overview of Services Installed by Exchange Setup

Overview of Services Installed by Exchange Setup

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-06-21*

During the installation of Microsoft Exchange Server 2010, Setup runs a set of tasks that install new services. A service is a background process that can be launched during operating system startup by the Service Control Manager in Microsoft Windows. Services are executable files designed to operate independently and without administrative intervention. A service can run using either a graphical user interface (GUI) mode or a console mode.

Services aren't new to Exchange 2010. All previous versions of Exchange included components implemented as services. Each server role includes services that are part of, or may be needed by, the server role to perform its functions. Although Setup installs all services whether they're immediately needed or not, some services only become active when specific features are used.

The following table lists by name and by short name the various services installed by Exchange 2010. Also included is a description of each service, the server role that installs the service, and whether the service is required or optional. In the table, *optional* means that the service is installed by Setup, but you can disable it if you determine that the function provided by the service isn't needed by your organization.

Services installed by Exchange Setup

Service name	Service short name	Security context	Description and dependencies	Default startup type	Server roles	Required (R) or optional (O)
Microsoft Exchange Active Directory Topology	MSExchangeADTopology	Local System	Provides Active Directory topology information to Exchange	Automatic	Mailbox, Hub Transport, Client Access, Unified	R

			services. If this service is stopped, most Exchange services are unable to start. This service has no dependencies.		Messaging	
Microsoft Exchange ADAM	ADAM_MSExchange	Network Service	Stores configuration data and recipient data on the Edge Transport server. This service represents the named instance of Active Directory Lightweight Directory Service (AD LDS) that's automatically created by Setup during Edge Transport server installation. This service is dependent upon the COM+ Event System service.	Automatic	Edge Transport	R
Microsoft Exchange Address Book	MSExchangeAB	Local System	Manages client address book connections. This service is dependent upon the Microsoft Exchange Active Directory	Automatic	Client Access	R

			Topology service.			
Microsoft Exchange Anti-spam Update	MSExchangeAntispamUpdate	Local System	Provides the Microsoft Forefront Protection 2010 for Exchange Server anti-spam update service. On Hub Transport servers, this service is dependent upon the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent upon the Microsoft Exchange ADAM service.	Automatic	Hub Transport, Edge Transport	O
Microsoft Exchange Credential Service	MSExchangeEdgeCredential	Local System	Monitors credential changes in AD LDS and installs the changes on the Edge Transport server. This service is dependent upon the Microsoft Exchange ADAM service.	Automatic	Edge Transport	R
Microsoft Exchange EdgeSync	MSExchangeEdgeSync	Local System	Connects to an AD LDS instance on subscribed Edge Transport	Automatic	Hub Transport	O

			servers over a secure LDAP channel to synchronize data between a Hub Transport server and an Edge Transport server. This service is dependent upon the Microsoft Exchange Active Directory Topology service. If Edge Subscription isn't configured, this service can be disabled.			
Microsoft Exchange File Distribution	MSExchangeFDS	Local System	Distributes offline address book (OAB) and custom Unified Messaging prompts. This service is dependent upon the Microsoft Exchange Active Directory Topology and Workstation services.	Automatic	Client Access, Unified Messaging	R
Microsoft Exchange Forms-Based Authentication	MSExchangeFBA	Local System	Provides forms-based authentication to Microsoft Office Outlook Web App	Automatic	Client Access	R

			and the Exchange Control Panel. If this service is stopped, Outlook Web App and the Exchange Control Panel won't authenticate users. This service has no dependencies.			
Microsoft Exchange IMAP4	MSExchangeIMAP4	Network Service	Provides IMAP4 service to clients. If this service is stopped, clients won't be able to connect to this computer using the IMAP4 protocol. This service is dependent upon the Microsoft Exchange Active Directory Topology service.	Manual	Client Access	O
Microsoft Exchange Information Store	MSExchangeIS	Local System	Manages the Exchange Information Store. This includes mailbox databases and public folder databases. If this service is stopped, mailbox	Automatic	Mailbox	R

			databases and public folder databases on this computer are unavailable. If this service is disabled, any services that explicitly depend on it will fail to start. This service is dependent on the RPC, Server, Windows Event Log, and Workstation services.			
Microsoft Exchange Mail Submission Service	MSExchangeMailSubmission	Local System	Submits messages from the Mailbox server to Exchange 2010 Hub Transport servers. This service is dependent upon the Microsoft Exchange Active Directory Topology service.	Automatic	Mailbox	R
Microsoft Exchange Mailbox Assistants	MSExchangeMailboxAssistants	Local System	Performs background processing of mailboxes in the Exchange store. This service is dependent upon the Microsoft Exchange	Automatic	Mailbox	R

			Active Directory Topology service.			
Microsoft Exchange Mailbox Replication Service	MSExchange MailboxRepli cation	Local System	Processes mailbox moves and move requests. This service is dependent upon the Microsoft Exchange Active Directory Topology and Net.Tcp Port Sharing service.	Automatic	Client Access	O
Microsoft Exchange Monitoring	MSExchange Monitoring	Local System	Allows applications to call the Exchange diagnostic cmdlets. This service has no dependenci es.	Manual	All	O
Microsoft Exchange POP3	MSExchange POP3	Network Service	Provides POP3 service to clients. If this service is stopped, clients can't connect to this computer using the POP3 protocol. This service is dependent upon the Microsoft Exchange Active Directory Topology service.	Manual	Client Access	O
Microsoft Exchange	MSExchange ProtectedSe	Local System	Provides a host for	Automatic	Hub Transport,	R

Protected Service Host	rviceHost		several Exchange services that must be protected from other services. This service is dependent upon the Microsoft Exchange Active Directory Topology service.		Client Access	
Microsoft Exchange Replication Service	MSExchangeRepl	Local System	Provides replication functionality for mailbox databases on Mailbox servers in a database availability group (DAG) and database mount functionality for all Mailbox servers. This service is dependent upon the Microsoft Exchange Active Directory Topology service.	Automatic	Mailbox	R
Microsoft Exchange RPC Client Access	MSExchangeRPC	Network Service	Manages client RPC connections for Exchange. This service is dependent upon the Microsoft Exchange Active	Automatic	Mailbox, Client Access	O (Mailbox), R (Client Access)

			Directory Topology service.			
Microsoft Exchange Search Indexer	MSExchange Search	Local System	Drives indexing of mailbox content, which improves the performance of content search. This service is dependent upon the Microsoft Exchange Active Directory Topology and Microsoft Search (Exchange Server) services.	Automatic	Mailbox	O
Microsoft Exchange Server Extension for Windows Server Backup	WSBExchange	Local System	Enables Windows Server Backup users to back up and recover application data for Microsoft Exchange. This service has no dependencies.	Manual	Mailbox	O
Microsoft Exchange Service Host	MSExchange ServiceHost	Local System	Provides a host for several Exchange services. On internal server roles, this service is dependent upon the Microsoft Exchange Active	Automatic	All	R

			Directory Topology service. On Edge Transport servers, this service is dependent upon the Microsoft Exchange ADAM service.			
Microsoft Exchange Speech Engine	MSSpeechService	Network Service	Provides speech processing services for Unified Messaging. This service is dependent upon the Windows Management Instrumentation (WMI) service.	Automatic	Unified Messaging	R
Microsoft Exchange System Attendant	MSExchangeSA	Local System	Forwards directory lookups to a global catalog server for legacy Outlook clients, generates e-mail addresses and OABs, updates free/busy information for legacy clients, and maintains permissions and group memberships for the server. If this service is disabled, any services that	Automatic	Mailbox	R

			explicitly depend on it will fail to start. This service is dependent on the RPC, Server, Windows Event Log, and Workstation services.			
Microsoft Exchange Throttling	MSExchange Throttling	Network Service	Limits the rate of user operations. This service is dependent upon the Microsoft Exchange Active Directory Topology service.	Automatic	Mailbox	R
Microsoft Exchange Transport	MSExchange Transport	Network Service	Provides SMTP server and transport stack. On Hub Transport servers, this service is dependent upon the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent upon the Microsoft Exchange ADAM service.	Automatic	Hub Transport, Edge Transport	R
Microsoft Exchange Transport	MSExchange TransportLogSearch	Local System	Provides remote search	Automatic	Hub Transport, Mailbox,	O

Log Search			capability for Microsoft Exchange Transport log files. On Hub Transport servers, this service is dependent upon the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent upon the Microsoft Exchange ADAM service.		Edge Transport	
Microsoft Exchange Unified Messaging	MSExchangeUM	Local System	Enables Microsoft Exchange Unified Messaging features. This allows voice and fax messages to be stored in Exchange and gives users telephone access to e-mail, voice mail, calendar, contacts, or an auto attendant. If this service is stopped, Unified Messaging isn't available. This service is	Automatic	Unified Messaging	R

			dependent upon the Microsoft Exchange Active Directory Topology and the Microsoft Exchange Speech Engine service.			
Microsoft Search (Exchange Server)	msftesql-Exchange	Local System	This is a Microsoft Exchange-customized version of Microsoft Search. This service is dependent on the RPC service.	Manual	Hub Transport, Mailbox	O

1.2.2.1.5 Deployment Security Checklist

Deployment Security Checklist

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-05-11*

Microsoft Exchange Server 2010 features are designed to help improve the security of your messaging environment. Generally, for Exchange 2010, the following conditions are true:

- Accounts that are used by Exchange 2010 have the minimum rights that are required to perform the given task sets.
- By default, services are started only when they are required.
- Access control list (ACL) rights for Exchange objects are minimized.
- Administrative permissions are set according to the scope of change on the object that a given modification requires.
- By default, all internal default message paths are encrypted.

This topic lists steps that we recommend you take to harden the messaging environment before you install Microsoft Exchange. We recommend that you refer to this checklist every time that you install a new Exchange server role.

Before installing Exchange 2010, perform the following procedures.

Procedure	Done?
Run Microsoft Update.	

Run the Microsoft Windows Malicious Software Removal Tool. The Malicious Software Removal Tool is included with Microsoft Update. More information about the tool can be found at Malicious Software Removal Tool.	
Run the Microsoft Baseline Security Analyzer.	

1.2.2.1.6 Exchange Management Console Interoperability

Exchange Management Console Interoperability

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

The Exchange Management Console (EMC) is a Microsoft Management Console-(MMC) based tool that provides Exchange administrators with a GUI to manage the configuration of Exchange organizations. You can also add the Exchange Management Console snap-in to custom MMC-based tools. This topic discusses interoperability between the EMC in Microsoft Exchange Server 2010 and earlier versions of Exchange, specifically Exchange Server 2003 and Exchange Server 2007.

For more information about the improvements to the Exchange Management Console, see New Administrative Functionality in the Exchange Management Console.

Interoperability with Exchange 2003

You can't manage Exchange 2010 objects using the Exchange Server 2003 System Manager. You can use the EMC in Exchange 2010 to view certain properties and objects, like the routing group connector in Exchange Server 2003. You can't perform message tracking configuration tasks between Exchange 2010 and Exchange 2003. You must use Exchange 2003 messaging tracking tools within your Exchange 2003 organization, and Exchange 2010 messaging tracking tools within your Exchange 2010.

Interoperability with Exchange 2007

The Exchange Management Console (EMC) is available in both Exchange Server 2010 and Exchange Server 2007. The following lists the tasks and actions that can be performed using the EMC in either Exchange 2010 or Exchange 2007:

- Actions that create objects, such as new mailboxes or a new offline address book (OAB), can only be performed on a version of the EMC that's the same as the target object. For example, creating a mailbox on an Exchange 2007 Mailbox server must be performed with the EMC in Exchange 2007. The following applies:
  - Exchange 2007 Mailbox databases can't be managed from the EMC in Exchange 2010, although these databases can be viewed.
  - The EMC in Exchange 2010 can't enable or disable Exchange 2007 Unified Messaging mailboxes.
  - The EMC in Exchange 2010 can't manage Exchange 2007 mobile devices.
- Actions that require viewing of objects can be performed from any version of

the EMC to any version of Exchange objects, with a few exceptions:

- Exchange 2010 and Exchange 2007 transport rule objects can only be viewed from their corresponding version of the EMC.
- Exchange 2010 and Exchange 2007 servers can only be viewed from their corresponding version of the EMC.
- The Queue Viewer tool in the EMC in Exchange 2010 can't connect to an Exchange 2007 server to view queues or messages.

Note:
If an Exchange 2007 object (such as a storage group) is no longer present in Exchange 2010, there's no interoperability expected or provided because Exchange 2010 isn't aware of the feature.

- You can't use message tracking configuration tasks between Exchange 2010 and Exchange 2007. You must use Exchange 2007 messaging tracking tools within your Exchange 2007 servers, and Exchange 2010 messaging tracking tools within your Exchange 2010 servers.

The following is a list of Exchange 2010-only and Exchange 2007-only objects. These objects are available for viewing, managing, and creating only in the corresponding version of the EMC.

Note:
Be aware that managing an object in the Exchange 2010 Exchange Control Panel can upgrade the object. As a result, it can't be managed by the Exchange 2007 management tools (EMC, Shell) that created the object.

Exchange 2007 objects no longer present in Exchange 2010:

- Storage groups
- Exchange Administrators
- WebDAV

Exchange 2010 Management Console-only objects:

- Database availability group
- Certificate creation
- Database copies
- Federation trust
- Sharing relationships
- Sharing policies
- Microsoft Office Outlook Web App mailbox policies
- Customer Experience Program properties

Side-by-Side Management Console

To use the side-by-side EMC feature, the Exchange 2007 EMC must first be installed on a non-Exchange administrative machine. After the Exchange 2007 EMC is installed, you can then install the Exchange 2010 EMC to run in a side-by-side scenario.

Note:
Exchange 2010 EMC can only be administered from a 64-bit machine. Therefore, for side-by-side management, the Exchange 2007 EMC must be installed on a 64-bit machine. Side-by-side management for Exchange Server 2003 and Exchange 2010 management tools isn't supported, because Exchange Server 2003 management tools can only be run on 32-bit machines. However, you can use 32-bit Windows PowerShell 2.0 and remotely access your Exchange 2010 environment.

For more information, see Install the Exchange 2010 Management Tools.

Understanding Upgrade to Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Microsoft Exchange Server 2010 can be deployed in an Active Directory forest that has an existing messaging system. You have a coexistence scenario if the following conditions are true:

- Exchange Server 2010 is deployed in an existing Exchange organization.
- More than one version of Microsoft Exchange provides messaging services to the organization.

You can't upgrade an existing Exchange 2000 organization directly to Exchange 2010. You must first upgrade the Exchange 2000 organization to either an Exchange 2003 or Exchange 2007 organization, and then you can upgrade the Exchange 2003 or Exchange 2007 organization to Exchange 2010. We recommend that you upgrade your organization from Exchange 2000 to Exchange 2003, and then upgrade from Exchange 2003 to Exchange 2010. For more information about upgrading from Exchange 2000, see Planning an Upgrade from Exchange 2000 and Upgrading to Exchange 2007.

When an organization gradually transitions a messaging system from Exchange Server 2003 or Exchange Server 2007 to Exchange 2010, the organization will probably have to maintain more than one version of Exchange during that time.

The following table lists the scenarios in which coexistence between Exchange 2010 and earlier versions of Exchange are supported.

Coexistence of Exchange 2010 and earlier versions of Exchange Server

Exchange version	Exchange organization coexistence
Exchange 2000 Server	Not supported
Exchange Server 2003	Supported
Exchange 2007	Supported
Mixed Exchange 2007 and Exchange Server 2003 organization	Supported

The following topics provide information about upgrading your organization to Exchange 2010:

Understanding Upgrade from Exchange 2003 to Exchange 2010

Understanding Upgrade from Exchange 2007 to Exchange 2010

Understanding Upgrade from Exchange 2003 and Exchange 2007 to Exchange 2010

Also, see Exchange Server Deployment Assistant for information about a Web-based tool that can help you with your deployment.

1.2.2.2 Understanding a New Installation of Exchange 2010

Understanding a New Installation of Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

The following topics provide information about deploying a new installation of Microsoft Exchange 2010 in your organization:

Checklist: Perform a New Installation of Exchange 2010

Managing Deployment of Exchange 2010

Deploy a New Exchange 2010 RTM UM Environment

Install or Upgrade to Exchange 2010 SP2 Unified Messaging

In addition, see Understanding Deployment of Exchange 2010 for information about prerequisites to installation of Exchange 2010 and see Exchange Server Deployment Assistant for information about a Web-based tool that can help you with your deployment.

1.2.2.2.1 Checklist: Perform a New Installation of Exchange 2010

Checklist: Perform a New Installation of Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-28*

Use this checklist to deploy Microsoft Exchange Server 2010. Before you start working with this checklist, make sure you're familiar with the concepts discussed in:

- Planning for Exchange 2010
- Understanding Exchange 2010 Setup
- Planning Roadmap for New Deployments
- Deployment Security Checklist
- Deployment Checklist for Multi-Tenancy

This checklist is generic in that it provides guidance for a typical scenario. For more customized step-by-step guidance about how to deploy Exchange 2010, see the Exchange Server Deployment Assistant.

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Checklist for a New Installation of Exchange 2010

Done?	Task	Topic
	1. Verify system requirements	Exchange 2010 System Requirements
	2. Confirm prerequisite steps are done	Exchange 2010 Prerequisites
	3. Configure disjoint namespace **Note:** This step is optional. It's only necessary if your organization is running a disjoint namespace.	Configure the DNS Suffix Search List for a Disjoint Namespace
	4. Install the Client Access server role	Install Exchange Server 2010
	5. Add digital certificates on the Client Access server	Create a New Exchange Certificate
	6. Enable Outlook Anywhere **Note:** This step is optional. It's only necessary if you want to use the Outlook Anywhere component of Exchange 2010.	Enable Outlook Anywhere
	7. Configure settings on virtual directories, including OAB, Web Services, ECP, Outlook Web App, and Exchange ActiveSync virtual directories **Note:** This step is necessary if you want to use Exchange Web Services, Outlook Anywhere, or the offline address book. It also may be required if you need to change any of the default settings for ECP, Outlook Web App, or Exchange ActiveSync.	Create an Offline Address Book Virtual Directory Configure ECP Virtual Directory Properties View or Configure Outlook Web App Virtual Directories View or Configure Exchange ActiveSync Virtual Directory Properties
	8. Install the Hub Transport server role	Install Exchange Server 2010
	9. Install the Mailbox server role	Install Exchange Server 2010

	10. Use public folders	Configure Public Folder Replication
	11. Install the Edge Transport server role **Note:** This step is optional. It's only necessary if you want to use the Edge server role in your organization.	Install Exchange Server 2010
	12. Subscribe the Edge Transport server **Note:** This step is optional. It's only necessary if you want to use the Edge server role in your organization.	Create an Edge Subscription File on an Edge Transport Server Import an Edge Subscription File to an Active Directory Site
	13. Install the Unified Messaging server role **Note:** This step is optional. It's only necessary if you want to use Unified Messaging in your organization.	Install Exchange Server 2010
	14. Configure Unified Messaging **Note:** This step is optional. It's only necessary if you want to use Unified Messaging in your organization.	Deploy a New Exchange 2010 RTM UM Environment
	15. Post-installation tasks	Exchange 2010 Post-Installation Tasks

Return to top

1.2.2.3 Understanding Upgrade from Exchange 2003 to Exchange 2010

Understanding Upgrade from Exchange 2003 to Exchange 2010

Exchange Server 2010 > Planning and Deployment > Deploying Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

When you're upgrading your existing Microsoft Exchange Server 2003 organization to Exchange Server 2010, there's a period of time when both Exchange 2003 and Exchange 2010 will coexist within your organization. This section discusses key points about both the upgrade process and coexistence as they apply to the Client Access, Transport, and Mailbox server roles.

You can only deploy Exchange 2010 in an Exchange 2003 organization that operates in

native mode. Use Exchange System Manager to change the Exchange organization to native mode on an Exchange 2003 server, as follows:

1. Start Exchange System Manager. Click **Start** > **Programs** > **Microsoft Exchange** > **System Manager**.
2. Right-click the organization, and then click **Properties**.
3. Click the **General** tab, and then, under **Change Operations Mode**, click **Change Mode**. Click **Yes** if you are sure that you want to permanently switch the organization's mode to native mode.

For more information, see the following topics:

Checklist: Upgrading from Exchange 2003

Upgrade from Exchange 2003 Client Access

Upgrade from Exchange 2003 Transport

Upgrade from Exchange 2003 Mailbox

For more information about the Exchange 2003 to Exchange 2010 planning and upgrade process, see the following topics:

Exchange 2003 - Planning Roadmap for Upgrade and Coexistence

Understanding Upgrade to Exchange 2010

Managing Deployment of Exchange 2010

Exchange Server Deployment Assistant

1.2.2.3.1 Checklist: Upgrading from Exchange 2003

Checklist: Upgrading from Exchange 2003

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-29*

Use this checklist to upgrade from Microsoft Exchange Server 2003 to Exchange Server 2010. Before you start working with this checklist, make sure you're familiar with the concepts discussed in:

- Planning for Exchange 2010
- Deployment Security Checklist
- Exchange 2003 - Planning Roadmap for Upgrade and Coexistence

This checklist is generic in that it provides guidance for a typical upgrade scenario. For more customized step-by-step guidance about how to upgrade your Exchange 2003 organization, see the Exchange Server Deployment Assistant.

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment.

ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Checklist for Upgrading from Exchange 2003 to Exchange 2010

Done?	Task	Topic
	1. Verify system requirements	Exchange 2010 System Requirements
	2. Confirm prerequisite steps are done	Exchange 2010 Prerequisites
	3. Configure disjoint namespace **Note:** This step is optional. It's only necessary if your organization is running a disjoint namespace.	Configure the DNS Suffix Search List for a Disjoint Namespace
	4. Install the Client Access server role	Install Exchange 2010 in an Existing Exchange 2003 Organization
	5. Add digital certificates on the Client Access server	Create a New Exchange Certificate
	6. Enable Outlook Anywhere **Note:** This step is optional. It's only necessary if you want to use the Outlook Anywhere component of Exchange 2010.	Enable Outlook Anywhere
	7. Configure OAB and Web Services virtual directories **Note:** This step is necessary if you want to use Exchange Web Services, Outlook Anywhere, or the offline address book. It also may be required if you need to change any of the default settings for Exchange Control Panel, Microsoft Office Outlook Web App, or Exchange ActiveSync.	Create an Offline Address Book Virtual Directory Configure ECP Virtual Directory Properties View or Configure Outlook Web App Virtual Directories View or Configure Exchange ActiveSync Virtual Directory Properties
	8. Install the Hub Transport server role	Install Exchange Server 2010
	9. Configure a legacy host	Upgrade from Exchange

	name	2003 Client Access
	10. Configure Exchange ActiveSync authentication	Configure Authentication for Exchange ActiveSync
	11. Install the Unified Messaging server role **Note:** This step is optional. It's only necessary if you want to use Unified Messaging in your organization.	Install Exchange Server 2010
	12. Configure Unified Messaging **Note:** This step is optional. It's only necessary if you want to use Unified Messaging in your organization.	Install Exchange Server 2010 Checklist: Deploy a New Exchange 2010 RTM UM Environment
	13. Install the Mailbox server role	Install Exchange Server 2010
	14. Change the offline address book (OAB) generation server	Move the Offline Address Book Generation Process to Another Server
	15. Install the Edge Transport server role **Note:** This step is optional. It's only necessary if you want to use the Edge server role in your organization.	Install Exchange Server 2010 Upgrade from Exchange 2003 Transport
	16. Move Internet mail flow from Exchange 2003 to Exchange 2010	Move Internet Mail Flow from Exchange 2003 to Exchange 2010
	17. Move mailboxes from Exchange 2003 to Exchange 2010	Create a Local Move Request
	18. Move public folder data from Exchange 2003 to Exchange 2010	Move Public Folder Content from One Public Folder Database to Another Public Folder Database
	19. Post-installation tasks	Exchange 2010 Post-Installation Tasks

Return to top

Upgrade from Exchange 2003 Client Access

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you're upgrading your existing Microsoft Exchange Server 2003 organization to Exchange Server 2010, there's a period of time when both Exchange 2003 and Exchange 2010 will coexist within your organization. This topic describes the various steps you must take to upgrade an Exchange 2003 organization to Exchange 2010.

Important:

When you upgrade your organization to the RTM version of Exchange 2010, your clients running Outlook 2003 don't use RPC encryption, and RPC Client Access requires it by default. This can cause connection issues between Exchange 2010 and Outlook 2003. In Exchange 2010 SP2, RPC Client Access doesn't require RPC encryption by default. If you have Outlook 2003 clients within your organization, we recommend that you install Exchange 2010 SP2 to avoid connection issues between Exchange 2010 RTM and Outlook 2003. For more information, see Understanding RPC Client Access.

Overview of the Upgrade Process

The upgrade process includes the following steps:

1. Installing Exchange 2010 within your organization on new hardware.
2. Configuring Exchange 2010 Client Access.
3. Creating a set of legacy host names and associating those host names with your Exchange 2003 infrastructure.

   Note:

   Your legacy host name should be in the format "legacy.contoso.com", where contoso.com matches your current host name.

   Note:

   Configuring a legacy host name is necessary only if you'll need Exchange 2003 and Exchange 2010 to coexist in the same organization. If you have a small number of mailboxes and can move all your mailboxes from Exchange 2003 to Exchange 2010 during the downtime you've scheduled for the upgrade, this step isn't necessary.
4. Obtaining a digital certificate with the names you'll be using during the coexistence period and installing it on your Exchange 2010 Client Access server.
5. Associating the host name you currently use for your Exchange 2003 infrastructure with your newly installed Exchange 2010 infrastructure.
6. Moving mailboxes from Exchange 2003 to Exchange 2010.
7. Decommissioning your Exchange 2003 infrastructure.

Note:

Throughout this topic, mail.contoso.com will be used as the primary namespace and legacy.contoso.com will be used as the legacy namespace. When you perform your upgrade you'll substitute the names of your own primary and legacy namespaces.

Understanding Legacy Host Names

An important part of the upgrade process is configuring a legacy host name and associating that host name with your Exchange 2003 infrastructure. This is a necessary step if your organization has a significant number of mailboxes that can't all be moved from Exchange 2003 to Exchange 2010 during the downtime scheduled for the upgrade

and if your organization supports Outlook Web Access for Internet users.

If your organization has a small number of mailboxes, and you're able to schedule downtime over an evening or a weekend, you can skip the step of configuring a legacy host name and move all mailboxes during this downtime. Doing this eliminates the need for Exchange 2003 and Exchange 2010 to coexist.

You'll have to configure a legacy host name to be published to the Internet and associated with the virtual directories of the various services you have on Exchange 2003, such as Microsoft Exchange ActiveSync, Microsoft Outlook Web Access, POP3, and IMAP4 if:

- You have a significant number of mailboxes to move from Exchange 2003 to Exchange 2010
  or
- You don't want to move all mailboxes at once
  and
- You have users who access Outlook Web Access from the Internet.

After a legacy host name has been configured and associated with your Exchange 2003 infrastructure, and your current host name has been associated with your Exchange 2010 infrastructure, users will experience a seamless transition. Exchange 2010 will redirect users from the Exchange 2010 Client Access server to the Exchange 2003 front-end server. Users won't have to learn a new URL to access Outlook Web Access (called Outlook Web App in Exchange 2010) or reconfigure their Exchange ActiveSync devices. POP3, IMAP4, and Outlook Anywhere users can also continue to access their mailboxes without interruption.

How to create a legacy host name

The steps to perform this task will vary for each organization. That's because the exact steps depend on your Internet provider and firewall configuration. Example steps for GoDaddy are provided below to give you an idea of how things work. The steps you need to follow may vary. But, in general, you need to:

1. Create a DNS host (A) record in your internal and external DNS servers that points to the IP address of your legacy Internet-facing Exchange server (for example, your Exchange 2007 Client Access server or Exchange 2003 front-end server) in internal DNS or the public IP address on your reverse proxy or firewall solution (external DNS). The host name should be in the format of legacy.*domain*.com (for example, legacy.contoso.com).
2. Create a publishing rule for the legacy host name in your reverse proxy or firewall solution to point to your legacy Internet-facing Exchange server. Refer to your proxy/firewall solution's user manual for instructions for how to do this.
3. Configure the existing DNS host (A) record in your internal and external DNS servers for your original host name (for example, mail.contoso.com) to point to your Exchange 2010 organization. For example, point to the IP address of your Client Access server or array (internal DNS) or the public IP address on your reverse proxy or firewall solution (external DNS).
   So, for example, if your provider is GoDaddy.com, you can use the following steps to create a DNS host (A) record and associate it with your legacy Exchange infrastructure:
   3.a. From your GoDaddy account management home page, click **Domain Manager** under the **My Products** heading in the left sidebar.
   3.b. If you're prompted to log in to your account, log in.
   3.c. In the **Total DNS** section of the Domain Manager information screen, click **Total DNS Control**.
   3.d. In the **A (Host)** section of the Total DNS Control screen, click **Add new A record**.
   3.e. Enter the host name, for example legacy.contoso.com and enter the IP address of your legacy Exchange server in the **Points to IP address** box.
   3.f. Choose a **TTL** (time to live) value. If you're performing this step well in

advance of your Exchange 2010 installation, you can choose 1 day or 1 week from the drop-down list. Otherwise, choose the default of 1 hour or 1/2 hour.

3.g.Click **OK** to complete your changes.

How to verify the legacy host name can be accessed from the Internet

From outside your firewall, using your specific domain name instead of contoso, perform the following steps:

1. Navigate to https://mail.contoso.com/owa, and verify that you can access Outlook Web App for a user whose mailbox is on an Exchange 2010 server.
2. Navigate to https://legacy.contoso.com/exchange, and verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.
3. Navigate to https://mail.contoso.com/owa, and verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.

You can also use the Exchange Server Remote Connectivity Analyzer to verify connectivity for the legacy namespace.

You'll find ExRCA at: https://www.testexchangeconnectivity.com.

Certificate Planning for Upgrade

To support coexistence of Exchange 2003 and Exchange 2010, you'll likely have to obtain a new commercial certificate. We recommend that you obtain a certificate that supports Subject Alternative Names. However, a wildcard certificate is also supported. For more information about certificates, see Understanding Digital Certificates and SSL.

Return to top

Installing Exchange 2010

After you've ensured that the prerequisites are met and you've obtained the correct certificates, you can begin your upgrade. Do this using the following steps.

Note:

In the following steps, replace <CAS2010> with the name of your Exchange 2010 Client Access server.

1. Install the Exchange 2010 Client Access server role.
2. During Setup, you can enter the primary external namespace for your virtual directories. This value should be the primary host name that your users use to connect to Exchange services from the Internet, for example: mail.contoso.com.
   - If you're upgrading through the graphical user interface Setup experience, you'll be prompted to configure an external Client Access domain.
   - If you're upgrading from a command prompt, use the setup property /`ExternalCASServerDomain` and specify your domain, for example: mail.contoso.com.
3. If your organization requires Outlook Anywhere access, enable Outlook Anywhere.
   - This can be done using the following command: `Enable-OutlookAnywhere -Server:<CAS2010> -ExternalHostName:mail.contoso.com -SSLOffloading $false`
4. If you didn't configure a primary external namespace during setup, you'll have to run the following commands to configure the virtual directories for the Offline Address Book, Exchange Web Services, Exchange ActiveSync, Outlook Web App, and Exchange Control Panel. You can do that with the following commands:
   - Offline Address Book: `Set-OABVirtualDirectory <CAS2010>\OAB* -ExternalURL https://mail.contoso.com/OAB`

- Web Services: `Set-WebServicesVirtualDirectory <CAS2010>\EWS* -ExternalURL https://mail.contoso.com/ews/exchange.asmx`
- Exchange ActiveSync: `Set-ActiveSyncVirtualDirectory -Identity <CAS2010>\Microsoft-Server-ActiveSync -ExternalURL https://mail.contoso.com`
- Outlook Web App:`Set-OWAVirtualDirectory <CAS2010>\OWA* -ExternalURL https://mail.contoso.com/OWA`
- Exchange Control Panel: `Set-ECPVirtualDirectory <CAS2010>\ECP* -ExternalURL https://mail.contoso.com/ECP`

5. Configure the Exchange 2003 URL property on the /owa virtual directory. This is necessary for Exchange 2003 and Exchange 2010 to coexist. To configure this property, use the following command.
   - `Set-OWAVirtualDirectory <CAS2010>\OWA* -Exchange2003URL https://legacy.contoso.com/exchange`

   Note:
   You must enable forms-based authentication on the Exchange 2003 front-end server to allow your users to access their mailboxes through a single sign-on during the coexistence period.

6. Change the Offline Address Book generation server and enable web distribution on the Exchange 2010 Client Access server using the following steps:
   - Move the Offline Address Book using the following command: `Move-OfflineAddressBook "Default Offline Address List" -Server <MBX2010>`
   - Add the Exchange 2010 Client Access server as a web distribution point using the following commands:
   - `$OABVDir=Get-OABVirtualDirectory -Server <CAS2010>`
   - `$OAB=Get-OfflineAddressBook "Default Offline Address List"`
   - `$OAB.VirtualDirectories += $OABVdir.DistinguishedName`
   - `Set-OfflineAddressBook "Default Offline Address List" -VirtualDirectories $OAB.VirtualDirectories`
7. Enable Integrated Windows authentication on the Microsoft-Server-ActiveSync virtual directory on the Exchange 2003 back-end server. This allows the Exchange 2010 Client Access server and the Exchange 2003 back-end server to communicate using Kerberos authentication.
   - Install the hotfix located here, and then use Exchange System Manager to adjust the authentication settings of the Exchange ActiveSync virtual directory.
   - Or, set the **msExchAuthenticationFlags** attribute to a value of 6 on the **Microsoft-Server-ActiveSync** object within the configuration container on each Exchange 2003 mailbox server. An example script is provided here.

     Important:
     Don't use IIS Manager to change the authentication setting on the ActiveSync virtual directory, because the DS2MB process within the System Attendant will overwrite the settings that are stored in Active Directory.

8. Create a legacy host name in your external DNS infrastructure and associate this host name with your Exchange 2003 front-end server or with your proxy infrastructure.
9. Reconfigure your External DNS settings or the publishing rules for your reverse proxy infrastructure to have your original namespace of mail.contoso.com point to your Exchange 2010 Client Access server or Client Access server array.
10. Test all client connections and re-enable Internet protocol client usage.

Upgrade from Exchange 2003 Transport

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-09*

When upgrading from Microsoft Exchange Server 2003 to Exchange Server 2010, there will be a period of time where both versions coexist in production. You can use the information summarized in the following table to help ensure that message flow isn't negatively affected during this period of coexistence.

Important:

If you deploy Exchange 2010 as a new organization, you can't later install Exchange 2003 in the Exchange 2010 organization. This isn't a supported scenario. If you anticipate requiring Exchange 2003 functionality in your organization in the future, you must first install an Exchange 2003 organization and maintain at least one Exchange 2003 server.

Summary by feature of required and optional actions for upgrading Exchange 2003 Transport to Exchange 2010

Feature	Required actions for coexistence	Optional actions and best practices
Routing Topology Differences When you plan for coexistence between Exchange 2010 and Exchange 2003, you must understand the differences in how each version determines its routing topology. This section provides an overview of the differences between the topologies, including a discussion of: • Routing group connectors • Link state updates in a coexistence environment	• Specify an Exchange 2003 bridgehead server for the first routing group connector that is created during setup of Exchange 2010. • Verify that every Exchange 2003 routing group has at least one connector to another routing group before you introduce the first Exchange 2010 server. • Suppress minor link state updates for each server in the Exchange 2003 organization. • Make sure that the Exchange 2010 routing group isn't the only communication path between Exchange 2003	• Specify more than one source server and more than one target server for the routing group connectors between your Exchange 2010 routing group and Exchange 2003 routing groups to provide redundancy and server availability • Create additional routing group connectors between Exchange 2003 and Exchange 2010 to optimize mail flow if necessary.

	routing groups to ensure that major links state updates continue to occur.	
Send and Receive Connectors Exchange 2003 uses SMTP virtual server interfaces for each protocol to send and receive messages between Exchange servers. The Exchange 2010 Hub Transport servers use an implicit connector called the intra-organization Send connector to route messages between sites.	• None. The default configuration of Send and Receive connectors on Exchange 2010 support coexistence with Exchange 2003.	• Create explicit Send connectors and Receive connectors if you want to create a connector that sends messages to a specific address space or receives messages from a specific address range.
X-EXCH50 Data Exchange 2003 uses the proprietary verb X-EXCH50 to transmit information about messages and recipients that can't be included in the e-mail message. Exchange 2010 supports a mapping between MAPI and MIME and doesn't require Exch50 data to reliably transmit message properties.	• None. The routing group connectors support the propagation of EXCH50 data.	• Make sure that the connector permissions allow the routing of EXCH50 data if you're connecting Exchange 2010 to an Exchange 2003 server in a cross-forest scenario.
Message Tracking Significant difference between the versions in that events logged by Exchange 2010 message tracking don't correspond directly to the message tracking events logged by Exchange 2003.	• None.	• Use the Exchange 2003 message tracking tool to search for messages that are transferred to or received from the Exchange 2003 organization.
Edge Transport Server Coexistence When an Edge Transport server is deployed to support an Exchange organization that hasn't yet deployed Exchange 2010, certain features can't be used.	• Create specific Send and Receive connectors on the Edge Transport server and update the configuration of the Exchange 2003 bridgehead servers if you're deploying an Edge Transport server before introducing Exchange 2010 to your Exchange 2003 organization.	• Deploy Exchange 2010 Hub Transport servers in your Exchange 2003 organization and then use EdgeSync.

Routing Topology Differences

Exchange 2003 use routing groups to define an Exchange-specific routing topology. Typically, routing groups are used to specify a set of well-connected Exchange servers. Servers in the same routing group can communicate with each other without the use of connectors. Ideally, the routing groups defined in your existing environment are based on IP subnets and closely mirror the Active Directory site configuration.

When more than one routing group is defined in an Exchange 2003 organization, you must manually create routing group connectors to enable mail flow between Exchange 2003 servers in different routing groups. The routing group connector must specify a source server and a target server as the connector endpoints. A routing group connector defines a one-way connection, and a reciprocal connector must be created to establish mail flow in both directions. The source and target servers are the bridgehead servers for the routing group. The bridgehead servers relay e-mail to other routing groups on behalf of other servers in their routing group and receive e-mail from other routing groups for delivery to other servers in their routing group.

In Exchange 2010, you don't have to define an Exchange-specific routing configuration. Exchange 2010 uses the existing Active Directory site topology to define its routing topology. However, you can make Exchange-specific configuration changes to Active Directory sites and IP site link costs to control mail flow. E-mail routed to Exchange servers located in different sites must be relayed by Hub Transport servers. Hub Transport servers send e-mail to Hub Transport servers in remote sites by using the intra-organization Send connector. The intra-organization Send connector is an implicit connector computed by using Active Directory site and IP site link information. To learn more about how Exchange 2010 uses Active Directory sites to route messages, see Planning to Use Active Directory Sites for Routing Mail.

Routing Group Connectors

To support coexistence between these two routing topologies, all Exchange 2010 servers are automatically added to a single routing group when Exchange 2010 is installed. The Exchange 2010 routing group is recognized in Exchange System Manager in Exchange 2003 as Exchange Routing Group (DWBGZMFD01QNBJR) within Exchange Administrative Group (FYDIBOHF23SPDLT).

During the installation of the first Exchange 2010 Hub Transport server in an existing Exchange organization, you must specify an Exchange 2003 bridgehead server to which to establish the first routing group connector. We recommend that you select a bridgehead server located in a hub routing group or in a routing group that has many mailboxes. The routing group connector links the routing group where the Exchange 2003 server resides and the Exchange 2010 routing group. The Exchange 2010 routing group includes all Exchange 2010 servers, regardless of the Active Directory site in which they reside.

Caution:

Don't move Exchange 2010 servers out of Exchange Routing Group (DWBGZMFD01QNBJR), and don't rename Exchange Routing Group (DWBGZMFD01QNBJR) by using a low-level directory editor. Neither action is supported. Exchange 2010 must use this routing group for communication with Exchange 2003.

The Hub Transport server that you're installing and the Exchange 2003 bridgehead server that you select are configured as the source and target servers on two reciprocal routing group connectors. The selected bridgehead server is automatically added to the membership of the ExchangeLegacyInterop universal security group and is granted the permissions needed to send e-mail to and receive e-mail from Exchange 2010. This routing group connector creates a single connection point between Exchange 2003 and

Exchange 2010.

You can modify the list of source and target servers by using the **Set-RoutingGroupConnector** cmdlet in the Exchange Management Shell. It's a best practice to specify more than one source server and more than one target server to provide redundancy and server availability.

Important:
Placing Exchange 2010 servers and Exchange 2003 servers in the same routing group isn't supported.

Every Exchange 2003 routing group should have at least one connector to another routing group before you introduce the first Exchange 2010 server. Event ID 5006 is logged for each Microsoft Exchange message database (MDB) located in a routing group that doesn't have a routing group connector path from the Exchange 2010 routing group. For more information about the Exchange 2003 routing topology, see the Exchange Server Transport and Routing Guide.

If your existing Exchange environment includes more than one routing group, you may want to create additional connection points between Exchange 2003 and Exchange 2010 to optimize mail flow. To create additional connection points, follow these steps:

1. Determine how you will upgrade the organization to Exchange 2010. The order in which you decommission routing groups will determine which Exchange 2003 routing groups should connect directly with Exchange 2010.
2. Modify the registry to suppress minor link state updates on all the Exchange 2003 servers. This configuration change prevents connector state messages from being relayed throughout the organization by using link state updates, but doesn't prevent configuration change messages from being relayed. For more information, see Suppress Link State Updates.
3. Use the **New-RoutingGroupConnector** cmdlet in the Shell to create all routing group connectors that specify Exchange 2010 Hub Transport servers as source or target servers. Configure a routing group connector from the Exchange Routing Group (DWBGZMFD01QNBJR) to each Exchange 2003 routing group with which Exchange 2010 will communicate directly, and configure the corresponding reciprocal routing group connectors. You can use the *Bidirectional* parameter with the **New-RoutingGroupConnector** cmdlet to create both connectors in a single operation. These connectors will enable mail flow between Exchange 2003 and Exchange 2010.

   Important:
   When you use the **New-RoutingGroupConnector** cmdlet, the specified legacy Exchange servers are automatically added to the membership of the ExchangeLegacyInterop universal security group, and the permissions required to allow a legacy Exchange server to send mail to and receive mail from an Exchange 2010 Hub Transport server are automatically granted. If you use Exchange System Manager to create a routing group connector between the Exchange 2010 routing group and any Exchange 2003 routing group, this group membership isn't updated and the connector won't work correctly. Therefore, always use the Shell to create or update routing group connectors between Exchange 2010 and Exchange 2003.

For more information, see Create Additional Routing Group Connectors from Exchange 2010 to Exchange 2003.

Link State Updates in a Coexistence Environment

When connecting the Exchange 2010 routing group to the Exchange 2003 organization, you must consider the behavior of link state routing. Exchange 2003 servers maintain a link state routing table that's updated through communication with the routing group master. Each connector that has been created between Exchange 2003 routing groups is

considered a link. Exchange 2003 servers determine how a message is routed inside the organization by using the cost assigned to these links. If a particular routing group is inaccessible by using the lowest cost route, the link state table is updated by the routing group master to show the state of that link as down. This data is communicated to every routing group in the Exchange organization. When the data is received, the link state table is updated, and another route is calculated.

Link state routing isn't used by Exchange 2010 Hub Transport servers. Exchange 2010 can't propagate link state updates, and it doesn't recalculate routes. Hub Transport servers always try to communicate directly with other Hub Transport servers. When a connection to a site is unavailable, Exchange 2010 uses the IP site link costs associated with Active Directory sites to determine the closest site at which to queue the message. This behavior is known as *queue at point of failure*. The message queue generated at the point of failure is put in a retry state.

If multiple paths exist between the Exchange 2010 routing group and any Exchange 2003 routing group, minor link state updates must be suppressed to make sure that message looping doesn't occur when a route is recalculated. We recommend that minor link state updates be suppressed for each server in the Exchange 2003 organization. When link state updates are suppressed, Exchange 2003 servers also queue at point of failure, instead of recalculating the route.

Configuration changes, such as the addition of connectors, are still communicated between Exchange 2003 servers by using link state. However, to ensure that major links state updates continue to occur, you must make sure that the Exchange 2010 routing group isn't the only communication path between Exchange 2003 routing groups. For more information about how to suppress link state updates, see Suppress Link State Updates.

Return to top

Send and Receive Connectors

Exchange 2003 uses SMTP virtual server interfaces for each protocol to send and receive messages between Exchange servers. Configuration is required only when you modify the default values or create connectors specific to another organization.

The Exchange 2010 Hub Transport servers use an implicit connector to route messages between sites. This connector is called the intra-organization Send connector. During installation, explicit Receive connectors are automatically created on each Hub Transport server. One Receive connector is configured to receive SMTP traffic from all sources by listening on port 25. A second Receive connector is configured to receive SMTP traffic from non-MAPI clients by listening on port 587. Explicit Send connectors and Receive connectors are created on Hub Transport servers only when you want to create a connector that sends messages to a specific address space or receives messages from a specific address range. For more information about connectors in Exchange 2010, see Understanding Send Connectors and Understanding Receive Connectors.

Return to top

X-EXCH50 Data

Exchange 2003 uses the proprietary verb X-EXCH50 to transmit information about messages and recipients that can't be included in the e-mail message. The information is transmitted as the Exch50 binary large object. Exch50 contains data such as spam confidence level, address rewriting information, and other MAPI properties that don't have MIME representation. Because X-EXCH50 is a proprietary Extended Simple Mail Transfer Protocol (ESMTP) verb, Exch50 data can't be propagated by a non-Exchange server.

Exchange 2010 supports a mapping between MAPI and MIME and doesn't require Exch50 data to reliably transmit message properties. To correctly coexist with Exchange 2003, Exchange 2010 servers can propagate the Exch50 data to Exchange 2003 servers. On incoming SMTP connections, Exch50-related properties used by Exchange 2010 are promoted to Exchange 2010-equivalent properties. Properties that aren't used by Exchange 2010 but are used by Exchange 2003 are preserved. On outgoing SMTP connections, the Exchange 2010 server can form the Exch50 data by promoting the Exchange 2010 properties and appending them to the preserved Exchange 2003 data.

Routing group connectors between Exchange 2010 and Exchange 2003 are automatically configured to support sending and receiving Exch50 data. If you are connecting Exchange 2010 to an Exchange 2003 server in a cross-forest scenario, make sure that the connector permissions allow the routing of Exch50 data. For more information, see Configure Cross-Forest Connectors.

Return to top

Message Tracking

The message tracking schema in Exchange 2010 is significantly different from the message tracking schema in Exchange 2003. The events logged by Exchange 2010 message tracking don't correspond directly to the message tracking events logged by Exchange 2003. Messages sent and received by Exchange 2010 can only be tracked by Exchange 2010 servers. There is no Microsoft Windows Management Instrumentation (WMI) support in Exchange 2010. Therefore, an Exchange 2003 server can't query for message tracking logs on an Exchange 2010 server. If a message tracking query in Exchange 2010 indicates that the message was transferred to an Exchange 2003 server, you must use the Exchange 2003 message tracking tool to continue to search for the message.

Return to top

Edge Transport Server Coexistence

The Edge Transport server role is designed to provide improved antivirus and anti-spam protection for the Exchange organization. The Edge Transport server also applies policies to messages in transport between organizations. This server role is deployed in the perimeter network and outside the Active Directory forest. The Edge Transport server can be deployed as a smart host and SMTP-relay server for an existing Exchange 2003 organization.

You can add an Edge Transport server to an existing Exchange organization without upgrading the internal Exchange servers or making any organizational changes. Because it deployed outside Active Directory, you don't have to perform any Active Directory preparation steps when you install the Edge Transport server. If you are using the Exchange Intelligent Message Filter in Exchange 2003 to perform anti-spam tasks, you can use the Edge Transport server to provide an additional layer of anti-spam protection.

When an Edge Transport server is deployed to support an Exchange organization that hasn't yet deployed Exchange 2010, certain features can't be used. You can't create an Edge Subscription in this scenario. Therefore, you can't use the Recipient Lookup or safelist aggregation features. For more information about using the Edge Transport server role with an Exchange 2003 organization, see Deploy the Edge Transport Server Role in an Existing Exchange 2003 Organization Before Upgrading to Exchange 2010.

Return to top

1.2.2.3.4 Upgrade from Exchange 2003 Mailbox

Upgrade from Exchange 2003 Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-29*

The Microsoft Exchange Server 2010 Mailbox server role can coexist with Exchange Server 2003 and Exchange 2007. If you're upgrading from an Exchange 2003 organization to Exchange 2010, the first server role you need to upgrade is the Client Access server role.

Then, after Mailbox servers have been deployed, you can move mailboxes from Exchange 2003 to Exchange 2010. To move mailboxes to Exchange 2010, you can use either the move request cmdlets or the Exchange Management Console, depending on your Exchange version. For more information about how to move mailboxes, see the following topics:

Move Mailboxes from Exchange 2003 Servers to Exchange 2010 Servers

Move Mailboxes from Exchange 2010 Servers to Exchange 2003 Servers

Exchange 2003 and Exchange 2010 Coexistence

The following topics provide more details about Mailbox server role feature coexistence between Exchange 2003 and Exchange 2010:

Understanding Public Folders

Understanding Exchange Search

Understanding E-Mail Address Policies

For more information about upgrading from previous versions of Exchange, see the following topics:

Exchange 2007 - Planning Roadmap for Upgrade and Coexistence

Exchange 2003 - Planning Roadmap for Upgrade and Coexistence

1.2.2.4 Understanding Upgrade from Exchange 2007 to Exchange 2010

Understanding Upgrade from Exchange 2007 to Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-29*

When you're upgrading your existing Microsoft Exchange Server 2007 organization to Exchange Server 2010, there's a period of time when both Exchange 2007 and Exchange 2010 will coexist within your organization. This section discusses key points about both the upgrade process and coexistence as they apply to the Client Access, Transport, Mailbox, and Unified Messaging server roles. For more information, see the following topics:

Checklist: Upgrading from Exchange 2007

Upgrade from Exchange 2007 Client Access

Upgrade from Exchange 2007 Transport

Upgrade from Exchange 2007 Mailbox

Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging

For more information about the Exchange 2007 to Exchange 2010 planning and upgrade process, see the following topics:

Exchange 2007 - Planning Roadmap for Upgrade and Coexistence

Understanding Upgrade to Exchange 2010

Managing Deployment of Exchange 2010

Exchange Server Deployment Assistant

1.2.2.4.1 Checklist: Upgrading from Exchange 2007

Checklist: Upgrading from Exchange 2007

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-24*

Use this checklist to upgrade from Microsoft Exchange Server 2007 to Exchange Server 2010. Before you start working with this checklist, make sure you're familiar with the concepts discussed in:

- Planning for Exchange 2010
- Deployment Security Checklist
- Exchange 2007 - Planning Roadmap for Upgrade and Coexistence

This checklist is generic in that it provides guidance for a typical upgrade scenario. For more customized step-by-step guidance about how to upgrade your Exchange 2007 organization, see the Exchange Server Deployment Assistant.

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Checklist for Upgrading from Exchange 2007 to Exchange 2010

Done?	Task	Topic
	1. Verify system requirements	Exchange 2010 System Requirements
	2. Confirm prerequisite steps are done	Exchange 2010 Prerequisites
	3. Configure disjoint namespace **Note:** This step is optional. It's only necessary if your organization is running a disjoint namespace.	Configure the DNS Suffix Search List for a Disjoint Namespace
	4. Install the Client Access server role	Upgrade from Exchange 2007 Client Access Install Exchange Server 2010
	5. Add digital certificates on the Client Access server	Create a New Exchange Certificate
	6. Enable Outlook Anywhere **Note:** This step is optional. It's only necessary if you decide to deploy Outlook Anywhere.	Enable Outlook Anywhere
	7. Configure settings on virtual directories, including OAB, Exchange Web Services, ECP, Outlook Web App, and Exchange ActiveSync virtual directories **Note:** This step is necessary if you want to use Exchange Web Services, Outlook Anywhere, or the offline address book. It also may be required if you need to change any of the default settings for the Exchange Control Panel, Outlook Web App, or Exchange ActiveSync.	Create an Offline Address Book Virtual Directory Configure ECP Virtual Directory Properties View or Configure Outlook Web App Virtual Directories View or Configure Exchange ActiveSync Virtual Directory Properties
	8. Install the Hub Transport server role	Upgrade from Exchange 2007 Transport Install Exchange Server 2010

	9. Configure a legacy host name	Upgrade from Exchange 2007 Client Access
	10. Install the Unified Messaging server role **Note:** This step is optional. It's only necessary if you want to use Unified Messaging in your organization.	Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging Install the Exchange 2010 Unified Messaging Server Role
	11. Configure and transition Unified Messaging **Note:** This step is optional. It's only necessary if you want to use Unified Messaging in your organization.	Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging Checklist: Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM UM
	12. Install the Mailbox server role	Install Exchange Server 2010 Upgrade from Exchange 2007 Mailbox
	13. Move OAB generation to Exchange 2010	Move the Offline Address Book Generation Process to Another Server
	14. Install the Edge Transport server role **Note:** This step is optional. It's only necessary if you want to use the Edge server role in your organization.	Upgrade from Exchange 2007 Transport Install Exchange Server 2010
	15. Subscribe and transition Edge Transport services **Note:** This step is optional. It's only necessary if you want to use the Edge server role in your organization.	Create an Edge Subscription File on an Edge Transport Server Import an Edge Subscription File to an Active Directory Site
	16. Move Exchange 2007 mailboxes to Exchange 2010	Create a Local Move Request
	17. Move public folder data to Exchange 2010	Configure Public Folder Replication
	18. Post-installation tasks	Exchange 2010 Post-Installation Tasks

Return to top

1.2.2.4.2 Upgrade from Exchange 2007 Client Access

Upgrade from Exchange 2007 Client Access

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you're upgrading your existing Microsoft Exchange Server 2007 organization to Exchange Server 2010, there's a period of time when both Exchange 2007 and Exchange 2010 will coexist within your organization. This topic describes the various steps you must take to upgrade an Exchange 2007 organization to Exchange 2010.

Note:
The information provided in this topic is applicable regardless of whether you have Exchange Server 2003 mailbox servers within your Exchange 2007 organization. For information about upgrading an organization running only Exchange 2003 to Exchange 2010, see Upgrade from Exchange 2003 Client Access.

Important:
When you upgrade your organization to the RTM version of Exchange 2010, your clients running Outlook 2003 don't use RPC encryption, and RPC Client Access requires it by default. This can cause connection issues between Exchange 2010 and Outlook 2003. In Exchange 2010 SP2, RPC Client Access doesn't require RPC encryption by default. If you have Outlook 2003 clients within your organization, we recommend that you install Exchange 2010 SP2 to avoid connection issues between Exchange 2010 RTM and Outlook 2003. For more information, see Understanding RPC Client Access.

Overview of the Upgrade Process

The upgrade process includes the following steps:

1. Installing Exchange 2010 within your organization on new hardware.
2. Configuring Exchange 2010 Client Access.
3. Creating a set of legacy host names that will be associated with the version of Exchange you're upgrading from.

   Note:
   Your legacy host name should be in the format "legacy.contoso.com", where contoso.com matches your current host name.

   Note:
   Configuring a legacy host name is necessary only if you'll need Exchange 2007 and Exchange 2010 to coexist in the same organization. If you have a small number of mailboxes and can move all your mailboxes from Exchange 2007 to Exchange 2010 during the downtime you've scheduled for the upgrade, this step isn't necessary.
4. Obtaining a digital certificate with the names you'll use during the coexistence period and installing it on your Exchange 2010 Client Access server.
5. Associating your current host names, for example: mail.contoso.com, with your Exchange 2010 infrastructure.
6. Moving mailboxes from Exchange 2007 to Exchange 2010.
7. Decommissioning your Exchange 2007 infrastructure.

Note:
Throughout this topic, mail.contoso.com will be used as the primary namespace and

legacy.contoso.com will be used as the legacy namespace. When you perform your upgrade, you'll substitute the names of your own primary and legal namespaces.

Understanding Legacy Host Names

An important part of the upgrade process is configuring a legacy host name and associating that host name with your Exchange 2007 infrastructure. This is a necessary step if your organization has a significant number of mailboxes that can't all be moved from Exchange 2007 to Exchange 2010 during the downtime scheduled for the upgrade and if your organization supports Outlook Web Access for Internet users.

If your organization has a small number of mailboxes, and you're able to schedule downtime over an evening or a weekend, you can skip the step of configuring a legacy host name and move all mailboxes during this downtime. Doing this eliminates the need for Exchange 2007 and Exchange 2010 to coexist.

You'll have to configure a legacy host name to be published to the Internet and associated with the virtual directories of the various services you have on Exchange 2007, such as Microsoft Exchange ActiveSync, Microsoft Outlook Web Access, POP3, and IMAP4 if:

- You have a significant number of mailboxes to move from Exchange 2007 to Exchange 2010
  or
- You don't want to move all mailboxes at once
  and
- You have users who access Outlook Web Access from the Internet.

After a legacy host name has been configured and associated with your Exchange 2007 infrastructure, and your current host name has been associated with your Exchange 2010 infrastructure, users will experience a seamless transition. Exchange 2010 will redirect users from the Exchange 2010 Client Access server to the Exchange 2007 Client Access server. Users won't have to learn a new URL to access Outlook Web Access (called Outlook Web App in Exchange 2010) or reconfigure their Exchange ActiveSync devices. POP3, IMAP4, and Outlook Anywhere users can also continue to access their mailboxes without interruption.

How to create a legacy host name

The steps to perform this task will vary for each organization. That's because the exact steps depend on your Internet provider and firewall configuration. Example steps for GoDaddy are provided below to give you an idea of how things work. The steps you need to follow may vary. But, in general, you need to:

1. Create a DNS host (A) record in your internal and external DNS servers that points to the IP address of your legacy Internet-facing Exchange server (for example, your Exchange 2007 Client Access server or Exchange 2003 front-end server) in internal DNS or the public IP address on your reverse proxy or firewall solution (external DNS). The host name should be in the format of legacy.*domain*.com (for example, legacy.contoso.com).
2. Create a publishing rule for the legacy host name in your reverse proxy or firewall solution to point to your legacy Internet-facing Exchange server. Refer to your proxy/firewall solution's user manual for instructions for how to do this.
3. Configure the existing DNS host (A) record in your internal and external DNS servers for your original host name (for example, mail.contoso.com) to point to your Exchange 2010 organization. For example, point to the IP address of your Client Access server or array (internal DNS) or the public IP address on your reverse proxy or firewall solution (external DNS).
   So, for example, if your provider is GoDaddy.com, you can use the following steps to create a DNS host (A) record and associate it with your legacy Exchange infrastructure:
   3.a. From your GoDaddy account management home page, click **Domain Manager** under the **My Products** heading in the left sidebar.

3.b.If you're prompted to log in to your account, log in.
3.c.In the **Total DNS** section of the Domain Manager information screen, click **Total DNS Control**.
3.d.In the **A (Host)** section of the Total DNS Control screen, click **Add new A record**.
3.e.Enter the host name, for example legacy.contoso.com and enter the IP address of your legacy Exchange server in the **Points to IP address** box.
3.f.Choose a **TTL** (time to live) value. If you're performing this step well in advance of your Exchange 2010 installation, you can choose 1 day or 1 week from the drop-down list. Otherwise, choose the default of 1 hour or 1/2 hour.
3.g.Click **OK** to complete your changes.

How to verify the legacy host name can be accessed from the Internet
From outside your firewall, using your specific domain name instead of contoso, perform the following steps:

1. Navigate to https://mail.contoso.com/owa, and verify that you can access Outlook Web App for a user whose mailbox is on an Exchange 2010 server.
2. Navigate to https://legacy.contoso.com/exchange, and verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.
3. Navigate to https://mail.contoso.com/owa, and verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.

You can also use the Exchange Server Remote Connectivity Analyzer to verify connectivity for the legacy namespace.

You'll find ExRCA at: https://www.testexchangeconnectivity.com.

Certificate Planning for Upgrade

To support coexistence of Exchange 2003 and Exchange 2010, you'll likely have to obtain a new commercial certificate. We recommend that you obtain a certificate that supports Subject Alternative Names. However, a wildcard certificate is also supported. For more information about certificates, see Understanding Digital Certificates and SSL.

Installing Exchange 2010

After you've ensured that the prerequisites are met and you've obtained the correct certificates, you can begin your upgrade. Do this using the following steps:

Note:
In the following steps, replace <CAS2010> with the name of your Exchange 2010 Client Access server.

1. Install the Exchange 2010 Client Access server role.
2. During Setup, you can enter the primary external namespace for your virtual directories. This value should be the primary host name that your users use to connect to Exchange services from the Internet, for example: mail.contoso.com.
   - If you're upgrading through the graphical user interface Setup, you'll be prompted to configure a Client Access domain.
   - If you're upgrading from a command prompt, use the setup property /`ExternalCASServerDomain` and specify your domain, for example: mail.contoso.com.
3. If your organization requires Outlook Anywhere access, enable Outlook Anywhere.
   - This can be done using the following command: `Enable-OutlookAnywhere -Server:<CAS2010> -ExternalHostName:mail.contoso.com -SSLOffloading $false`
4. If you didn't configure a primary external namespace during setup, you'll have

to run the following commands to configure the virtual directories for the Offline Address Book, Exchange Web Services, Exchange ActiveSync, Outlook Web App, and Exchange Control Panel. You can do that with the following commands:

- Offline Address Book: `Set-OABVirtualDirectory <CAS2010>\OAB* -ExternalURL https://mail.contoso.com/OAB`
- Web Services: `Set-WebServicesVirtualDirectory <CAS2010>\EWS* -ExternalURL https://mail.contoso.com/ews/exchange.asmx`
- Exchange ActiveSync: `Set-ActiveSyncVirtualDirectory -Identity <CAS2010>\Microsoft-Server-ActiveSync -ExternalURL https://mail.contoso.com`
- Outlook Web App:`Set-OWAVirtualDirectory <CAS2010>\OWA* -ExternalURL https://mail.contoso.com/OWA`
- Exchange Control Panel: `Set-ECPVirtualDirectory <CAS2010>\ECP* -ExternalURL https://mail.contoso.com/ECP`

5. Configure your Outlook Web App settings to meet your organization's needs.
   - You can obtain the Outlook Web Access settings from your Exchange 2007 server using the cmdlet `Get-OWAVirtualDirectory`.
   - To configure the Outlook Web App settings in Exchange 2010, use the `Set-OWAVirtualDirectory` cmdlet.
6. Configure your Exchange ActiveSync authentication settings.
   - You can obtain the Exchange ActiveSync settings from your Exchange 2007 server using the `Get-ActiveSyncVirtualDirectory` cmdlet.
   - To configure the Exchange ActiveSync settings in Exchange 2010, use the `Set-ActiveSyncVirtualDirectory` cmdlet.
7. Install the Exchange 2010 Hub Transport server role and the Exchange 2010 Mailbox server role into the Internet-facing Active Directory site. For configuration steps for these server roles, see Upgrade from Exchange 2007 Transport and Upgrade from Exchange 2007 Mailbox.
8. Change the offline address book generation server and enable Web distribution on the Exchange 2010 Client Access server with the following steps:
   - Move the offline address book using the following command: Move-OfflineAddressBook "Default Offline Address List" –Server *<MBX2010>*
   - Add the Exchange 2010 Client Access server as a web distribution point using the following commands:

     ```
     $OABVDir=Get-OABVirtualDirectory –Server <CAS2010>
     $OAB=Get-OfflineAddressBook "Default Offline Address List"
     $OAB.VirtualDirectories += $OABVdir.DistinguishedName
     Set-OfflineAddressBook "Default Offline Address List" –VirtualDirectories $OAB.VirtualDirectories
     ```
9. Create a legacy host name in your external DNS infrastructure. You'll either need to associate this host name with your Exchange 2007 Client Access server or with your proxy infrastructure.
10. If you have Exchange 2003 mailboxes in your organization, enable Integrated Windows authentication on the Microsoft-Server-ActiveSync virtual directory on the Exchange 2003 back-end server. This allows the Exchange 2010 Client Access server and the Exchange 2003 back-end server to communicate using Kerberos authentication.
    - Install the hotfix located here, and then use Exchange System Manager to adjust the authentication settings of the Exchange ActiveSync virtual directory.
    - Or, set the **msExchAuthenticationFlags** attribute to a value of 6 on the **Microsoft-Server-ActiveSync** object within the configuration container on each Exchange 2003 mailbox server. An example script is provided here.

Important:

Don't use IIS Manager to change the authentication setting on the ActiveSync virtual directory, because the DS2MB process within the System Attendant will overwrite the settings that are

stored in Active Directory.

11. Reconfigure your External DNS settings or the publishing rules for your reverse proxy infrastructure to have your original namespace of mail.contoso.com point to your Exchange 2010 Client Access server or Client Access server array.
12. Test all client connections and re-enable Internet protocol client usage.

Return to top

1.2.2.4.3 Upgrade from Exchange 2007 Transport

Upgrade from Exchange 2007 Transport

Planning and Deployment > Deploying Exchange 2010 > Understanding Upgrade from Exchange 2007 to Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-09-26*

When you upgrade from Microsoft Exchange Server 2007 to Exchange Server 2010, there will be a period of time during which both versions coexist in production. You can plan an upgrade path from Exchange 2007 to Exchange 2010 by using the information in this topic, which includes overview information, technical information about message flow in a coexistence environment, and considerations when operating in a mixed version environment.

Important:

If you deploy Exchange 2010 as a new organization, you can't later install Exchange 2007 in the Exchange 2010 organization. This isn't a supported scenario. If you anticipate requiring Exchange 2007 functionality in your organization in the future, you must first install an Exchange 2007 organization and maintain at least one Exchange 2007 server.

The most important point in an Exchange 2010 and Exchange 2007 coexistence scenario is that every Mailbox server needs a Hub Transport server with a matching Exchange version in the same Active Directory site. Due to the changes made to the Exchange Server Object (XSO) model in Exchange 2010, Exchange 2010 Hub Transport servers can't pick up messages from and deliver messages to Exchange 2007 Mailbox servers. Similarly Exchange 2007 Hub Transport servers can't communicate with Exchange 2010 Mailbox servers. Therefore, you need to maintain your Exchange 2007 Hub Transport servers in a specific Active Directory site until all Exchange 2007 Mailbox servers are removed from that site. For more details about how messages are routed in a coexistence environment, see "Message Routing Across Versions" later in this topic.

Note:

In-place upgrades aren't supported in Exchange 2010. You need to install new Exchange 2010 servers into your environment, and then phase out the Exchange 2007 servers. For the scope of this document, the phrase *upgrade* refers to generally upgrading the version of your Exchange deployment and not a specific server.

Contents

Transport Rules and Journaling in a Coexistence Scenario

Maintaining DSN Settings in a Mixed Environment

Message Tracking Across Versions

Exchange 2010 Transport Features in a Coexistence Scenario

Transport Server Upgrade Path

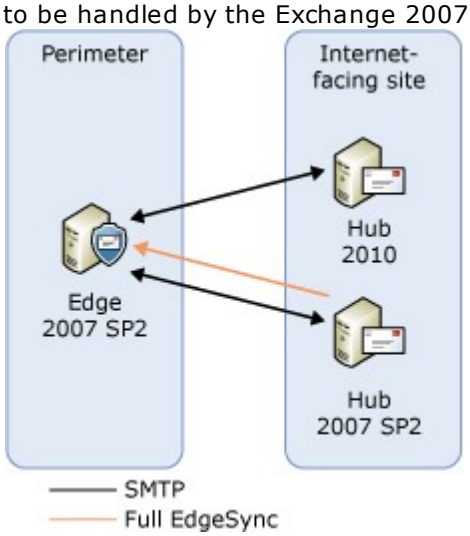
Upgrading your Exchange 2007 Hub Transport and Edge Transport servers should be part of your overall upgrade strategy. The recommended order is to upgrade your transport servers after your Client Access servers and before Unified Messaging and Mailbox servers. The Edge Transport servers need to be upgraded after the Hub Transport servers are upgraded. For more information about planning your upgrade, see Exchange 2007 - Planning Roadmap for Upgrade and Coexistence.

Before you introduce Exchange 2010 Hub Transport or Edge Transport servers, make sure that all of your Exchange 2007 servers in that site are upgraded to Exchange 2007 Service Pack 3 (SP3). Exchange 2007 SP3 is required for Exchange 2010 and Exchange 2007 Hub Transport servers to coexist in a single Active Directory site. Exchange 2007 SP3 is also required so that the Microsoft Exchange EdgeSync service works across versions.

If you have Exchange 2007 deployed in multiple sites, you must upgrade your Internet-facing sites first. The order of upgrade for the remaining sites depends on your particular topology and your organization's priorities.

The following process shows the recommended upgrade path for your transport servers in an Internet-facing site. (It is assumed that you are using Edge Transport servers with EdgeSync. If you are using a third-party smart host, you can omit steps 2-6.) The upgrade process is as follows:

1. Introduce your first Exchange 2010 Hub Transport server to your site. As soon as the Exchange 2010 Hub Transport server is introduced to the site, it will start using the Exchange 2007 Edge Transport server for message delivery to the Internet. The EdgeSync synchronization process will continue to be handled by the Exchange 2007 Hub Transport server.

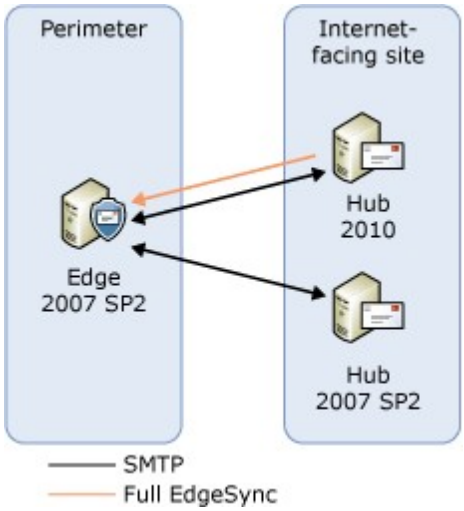


2. Subscribe your Exchange 2007 Edge Transport server to your site again. This action will add your Exchange 2010 Hub Transport server to the Edge Subscription as a source server. Exchange 2010 Hub Transport servers take

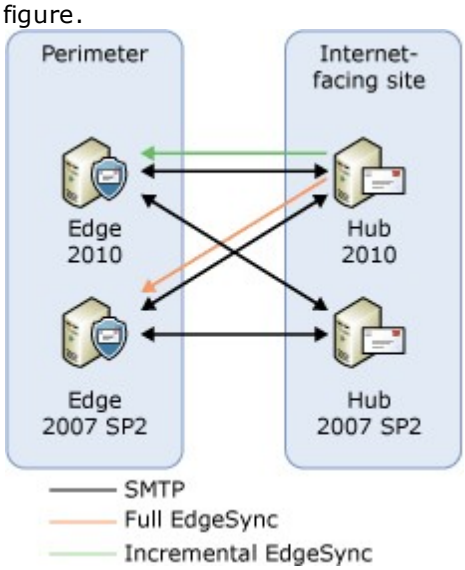
precedence over the Exchange 2007 Hub Transport server for the EdgeSync source server selection. Therefore, the Exchange 2010 Hub Transport server will take over Edge synchronization, as shown in the following figure. However, because the Edge Transport server is still running Exchange 2007 SP3, the Exchange 2010 Hub Transport server will still replicate full EdgeSync data.

Note:

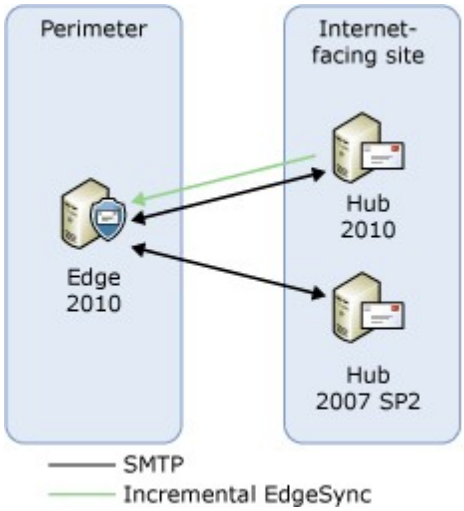
If you plan to add multiple Exchange 2010 Hub Transport servers to your Active Directory site, to save time, you can deploy all the new Hub Transport servers before subscribing your Edge Transport servers.



3. Introduce your first Exchange 2010 Edge Transport server to your perimeter network.
4. Subscribe your Exchange 2010 Edge Transport server to your site. At this point, the Exchange 2010 Hub Transport server will start incremental updates to the Exchange 2010 Edge Transport server, as shown in the following figure.



5. Remove the Exchange 2007 Edge Subscription.
6. Decommission your Exchange 2007 Edge Transport server, as shown in the following figure.

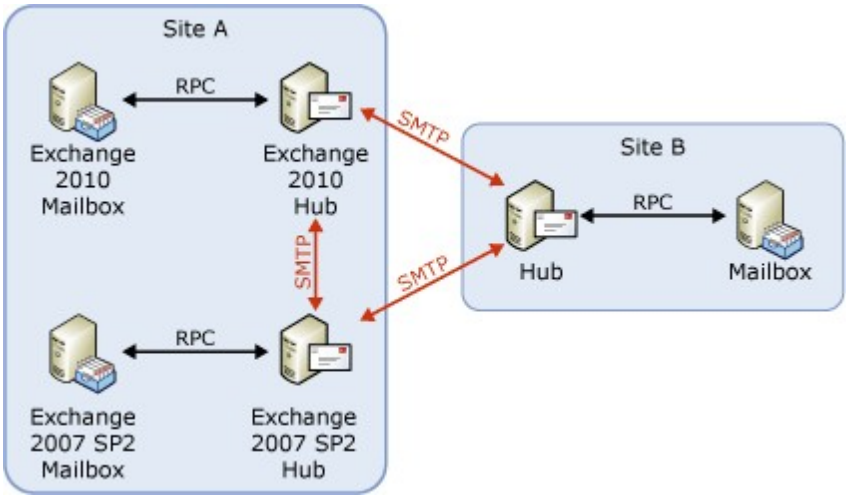


7. After all of your mailboxes are on Exchange 2010 Mailbox servers, decommission your Exchange 2007 Hub Transport servers.

Return to top

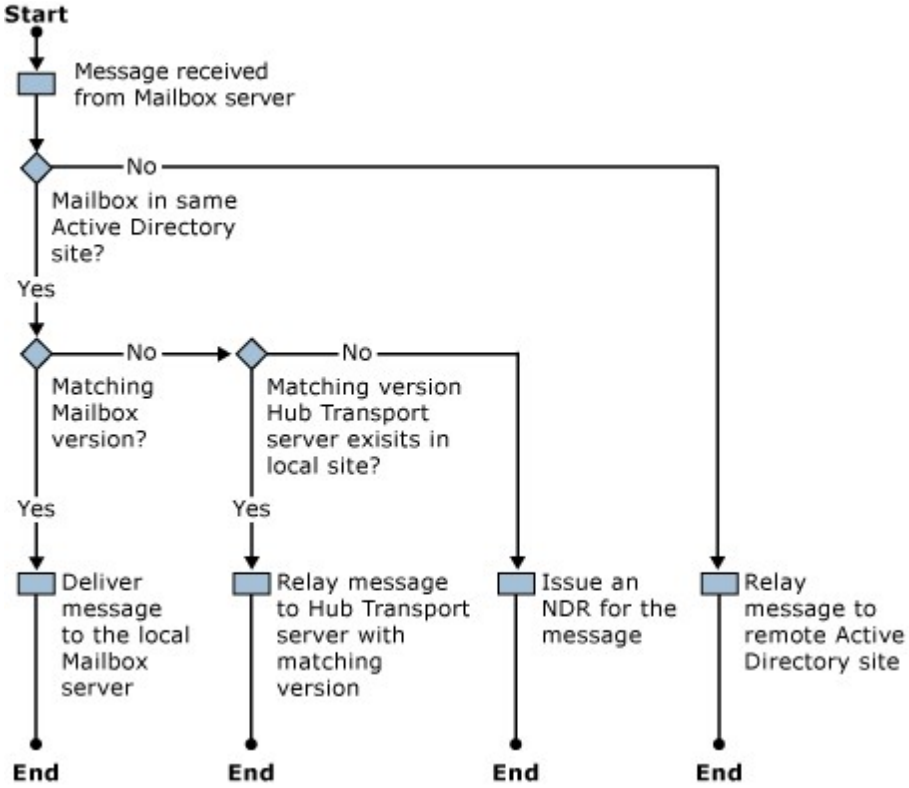
Message Routing Across Versions

Due to changes in the Exchange Server Object (XSO) model in Exchange 2010, Exchange 2010 Hub Transport servers can't pick up messages from and deliver messages to Exchange 2007 Mailbox servers. Similarly Exchange 2007 Hub Transport servers can't communicate with Exchange 2010 Mailbox servers. As a result, to have both Exchange 2010 and Exchange 2007 in the same Active Directory site, you must maintain both versions of Hub Transport servers in that site, as shown in the following figure. The versions of the servers in Site B aren't shown in the figure, because the handling of intersite SMTP traffic is the same as it is in Exchange 2007. The Hub Transport server relays the messages to the Hub Transport server in the remote site for delivery.



To enable message flow across versions, a feature called *versioned routing* is implemented in Exchange 2010. With versioned routing, the routing engine checks the version of a mailbox's home server, along with its Active Directory site. If the version doesn't match, the message is relayed to a Hub Transport server that has a matching version, as shown in the versioned routing workflow in the following figure. Routing is now dependent on

both Active Directory sites and Exchange versions.



When an Exchange 2010 mailbox user sends a message to an Exchange 2007 mailbox user in the same site, the following occurs:

1. The Exchange 2010 Mailbox server notifies the Exchange 2010 Hub Transport server of the new mail.
2. The Exchange 2010 Hub Transport server picks up the message.
3. The routing agent determines that the version of the Mailbox server that's the home server of the destination mailbox doesn't match its own version.
4. The routing agent locates an Exchange 2007 Hub Transport server in the local site.
5. The Exchange 2010 Hub Transport server relays the message to the Exchange 2007 Hub Transport server.
6. The routing agent on the Exchange 2007 Hub Transport server determines that the target mailbox is on an Exchange 2007 Mailbox server in the local site.
7. The Exchange 2007 Hub Transport server delivers the message to the Exchange 2007 Mailbox server.

Any messages sent from Exchange 2007 mailbox users to Exchange 2010 recipients follow a similar path.

Versioned routing was added to Exchange 2007 in SP2. To have both Exchange 2010 and Exchange 2007 coexist in the same Active Directory site, you must first upgrade your existing Exchange 2007 servers to SP3. When you have Exchange 2010 and Exchange 2007 SP3 in the same Active Directory site, each Hub Transport server handles messages for the Mailbox servers with matching versions. Versioned routing doesn't change the way intrasite messages are routed.

Consider the following when you have Exchange 2010 and Exchange 2007 in the same site:

- You can't specify an incompatible Hub Transport server as the submission server override for a Mailbox server.
- For a specific Mailbox server, if you don’t have a matching version Hub Transport server in the local site, any messages sent by users on that Mailbox server will remain on the Mailbox server.
- For a specific Mailbox server, if you don't have a matching version Hub Transport server in the local site, non-delivery reports (NDRs) will be issued for any messages sent to users on that Mailbox server.
- Messages sent to mail-enabled public folders are handled the same way messages sent to mailboxes.

Return to top

EdgeSync Differences

The edge synchronization process has been improved in Exchange 2010. In Exchange 2007, EdgeSync replicated all of the configuration and recipient information in its entirety. Especially in organizations with large number of recipients, this took a long time. Exchange 2010 introduces incremental updates for EdgeSync. When you first subscribe an Exchange 2010 Edge Transport server to a site, all the configuration information and recipient data is synchronized. In all subsequent updates, only the changes are replicated. Therefore, synchronization time and network utilization are substantially reduced.

Although Exchange 2007 Hub Transport servers can participate in EdgeSync with Exchange 2010 Edge Transport servers, incremental updates are only available between Exchange 2010 Hub Transport servers and Exchange 2010 Edge Transport servers. By default, when an Exchange 2010 Edge Transport server is subscribed to an Active Directory site that has Exchange 2010 Hub Transport servers, the Exchange 2010 Hub transport servers take over the EdgeSync process. You can fall back to Exchange 2007 Hub Transport servers by disabling the Microsoft Exchange EdgeSync service on the Exchange 2010 Hub Transport servers. However, when you do that, you go back to replicating all data with each EdgeSync update, instead of incremental updates.

For more information about EdgeSync, see Understanding Edge Subscriptions.

Return to top

Transport Rules and Journaling in a Coexistence Scenario

If you already use transport rules or journaling in your Exchange 2007 organization, make sure that these features continue to function during the coexistence period, regardless of which Hub Transport server processes a specific message.

The following significant changes were made to transport and journaling rules in Exchange 2010, which have an impact when managing these features in a mixed environment:

- **Format changes** Exchange 2010 transport rules support a series of new predicates and actions. To support these new predicates and actions, the format of how transport rules are stored in Active Directory has been modified. Exchange 2007 Hub Transport servers can't process these new predicates and actions. For a complete list of predicates and actions available in Exchange 2010, see Transport Rule Predicates and Transport Rule Actions.
- **Storage location in Active Directory** To prevent the Exchange 2007 Transport Rules agents from loading and attempting to process the rules created in Exchange 2010, the Exchange 2010 rules are stored in a separate

Active Directory container. The same situation applies to journaling rules.

Copying Existing Configuration to Exchange 2010

When installing Exchange 2010, if the Setup program detects the existence of Exchange 2007 transport rules, these legacy rules are automatically exported to a temporary location and subsequently imported to the Exchange 2010 transport rule container in Active Directory. This process happens automatically without any user interaction.

Note:
If there are any existing Exchange 2010 transport rules, Setup won't migrate Exchange 2007 rules because the migration overwrites all existing Exchange 2010 transport rules.

Similarly, all Exchange 2007 journal rules are converted and copied to Exchange 2010 journal rules during setup. For more information, see Export and Import Exchange 2007 Journal Rules.

Maintaining Transport Rules and Journaling in a Mixed Environment

The automatic import of rules to Exchange 2010 is only performed during initial setup. During the initial setup, the set of transport rules and journal rules for Exchange 2010 and Exchange 2007 will be synchronized. Going forward, if you make any changes to an existing rule, or create a rule, the rule will be changed in a single location based on the management tool you use. For example, in Exchange 2010, if you use the Exchange Management Shell to create a rule, only the Exchange 2010 rule container in Active Directory will be updated. Similarly if you use the Exchange Management Console (EMC) on an Exchange 2007 server to change an existing rule, only the Exchange 2007 version of that rule will be modified.

To ensure that your transport and journal rules remain consistent across versions, any changes you make must be made twice; once with Exchange 2010 management tools, and once with Exchange 2007 management tools.

Return to top

Maintaining DSN Settings in a Mixed Environment

In Exchange 2010, the internal and external DSN settings are configured for your entire Exchange organization. In Exchange 2007, these settings were configured on a per-server basis. As a result, these settings are stored in different configuration objects in Active Directory, and just like transport rules, need to be managed separately in a coexistence scenario.

Specifically, the following settings were moved from the **Set-TransportServer** cmdlet to the **Set-TransportConfig** cmdlet in Exchange 2010:

- ExternalDelayDsnEnabled
- ExternalDsnDefaultLanguage
- ExternalDsnLanguageDetectionEnabled
- ExternalDsnMaxMessageAttachSize
- ExternalDsnReportingAuthority
- ExternalDsnSendHtml
- ExternalPostmasterAddress
- InternalDelayDsnEnabled
- InternalDsnDefaultLanguage
- InternalDsnLanguageDetectionEnabled
- InternalDsnMaxMessageAttachSize
- InternalDsnReportingAuthority

- InternalDsnSendHtml

If you need to change any of these settings in your organization, you must make the change once for the organization using the **Set-TransportConfig** cmdlet in the Exchange 2010 Shell and once for each Exchange 2007 Hub Transport server in the organization using the **Set-TransportServer** cmdlet in the Exchange 2007 Shell.

Return to top

Message Tracking Across Versions

Exchange 2010 provides improved message tracking capabilities. End users, as well as administrators, can now track the messages they have sent using the Delivery Reports tool in the Exchange Control Panel.

Delivery Reports enable end-to-end message tracking from a single location, providing detailed delivery information including when a message was marked as read. In Exchange 2010, a new message tracking remote procedure call (RPC) and Web service interface was implemented to support Delivery Reports. These interfaces don't exist in Exchange 2007 and therefore the Delivery Reports feature doesn't extend to the Exchange 2007 infrastructure in a coexistence scenario. However, it's possible to use the message tracking tool in Exchange 2007 to track messages between versions.

The following table shows what to do when tracking messages in a mixed environment.

Tracking messages in a mixed environment

Sent from	Sent to	Tracking Tool
Exchange 2010 mailbox	Exchange 2010 mailbox	Use the Delivery Reports tool in Exchange Control Panel.
Exchange 2010 mailbox	Exchange 2007 mailbox	Use the Delivery Reports tool in Exchange Control Panel. The tool provides message tracking information to the point where the message is transferred to the Exchange 2007 server. No further tracking information will be available for that message. Alternatively, you can use Tracking Log Explorer in Exchange 2010 or message tracking in Exchange 2007.
Exchange 2007 mailbox	Exchange 2007 or Exchange 2010 mailbox	Use Tracking Log Explorer in Exchange 2010 or message tracking in Exchange 2007.

To learn more about message tracking in Exchange 2010, see Understanding Message Tracking.

Return to top

Exchange 2010 Transport Features in a

Coexistence Scenario

For the most part, new transport features in Exchange 2010 only function within the realm of Exchange 2010. When to start using the new features depends on the needs of your organization. You can wait until the upgrade is complete, or start as soon as you introduce Exchange 2010 to your environment. To decide when to use the new features in a mixed environment, consider the following information.

Moderated Recipients

Exchange 2010 introduces *moderated recipients*, so that messages sent to specific recipients can be subjected to an approval process. If you plan to use moderated recipients in a coexistence scenario, be aware of the following issues, which depend on the type of recipient:

- **Mailboxes** You can only enable mailboxes on Exchange 2010 Mailbox servers for moderation. After you enable a mailbox for moderation, you must make sure that it isn't moved back to an Exchange 2007 Mailbox server.
- **Distribution groups and dynamic distribution groups** The messages to a moderated distribution group go through the approval process only when that distribution group is expanded on an Exchange 2010 Hub Transport server. Because the distribution group can be expanded on any server, we recommend waiting until all your Hub Transport servers are upgraded to Exchange 2010 before using moderated distribution groups.
- **Mail contacts and mail users** Hub Transport servers route messages based on the external e-mail address specified for each mail user or mail contact. Because it isn't possible to force messages for these recipient types to go through an Exchange 2010 Hub Transport server, you may not want to enable these recipient types for moderation in a mixed environment.

If you enable a recipient for moderation, make sure that the designated moderators use a client that can display the "approve" and "reject" options for an approval request. We recommend that all moderators use Microsoft Office Outlook 2010 or Outlook Web App in Exchange 2010. Both of these clients have built-in user interfaces that allow moderators to make decisions on messages.

Note:

If your moderators are using Outlook 2007 or Outlook 2003, the moderation request will show up as voting buttons in the message that they receive. They will still be able to moderate messages using the voting buttons. However, for the best user experience, consider upgrading their clients to Outlook 2010 or later.

To learn more about moderated recipients, see Understanding Moderated Transport.

Shadow Redundancy

Exchange 2010 introduces *shadow redundancy* to provide redundancy for messages for the entire time they are in transit. The solution involves a technique similar to the transport dumpster. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all of the next hops for that message have completed delivery. If any of the next hops fail before reporting successful delivery, the message is resubmitted for delivery to that next hop.

Shadow redundancy is enabled by default on Exchange 2010, and it ensures that messages are redundant only while being transferred between Exchange 2010 servers. After that message is transferred to an Exchange 2007 server, it's no longer redundant. Therefore, to ensure that a message that originates on an Exchange 2010 server stays redundant until it's delivered, make sure that it doesn't get transferred to an Exchange 2007 server. For example, if you are using a hub site that has Exchange 2007 servers, messages between two spokes won't be redundant even if they both have Exchange 2010 servers.

To learn more about shadow redundancy, see Understanding Shadow Redundancy.

Return to top

1.2.2.4.4 Upgrade from Exchange 2007 Mailbox

Upgrade from Exchange 2007 Mailbox

Planning and Deployment > Deploying Exchange 2010 > Understanding Upgrade from Exchange 2007 to Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-29*

The Microsoft Exchange Server 2010 Mailbox server role can coexist with Exchange Server 2007. If you're upgrading from an Exchange 2007 organization to Exchange 2010, the first server role you will need to upgrade will be the Client Access server role.

Then, after Mailbox servers have been deployed, you can move mailboxes from Exchange 2007 to Exchange 2010. To move mailboxes to Exchange 2010, you can use either the move request cmdlets or the Exchange Management Console, depending on your Exchange version. For more information about how to move mailboxes, see the following topics:

Move Mailboxes from Exchange 2007 Servers to Exchange 2010 Servers

Move Mailboxes from Exchange 2010 Servers to Exchange 2007 Servers

Exchange 2007 and Exchange 2010 Coexistence

The following topics provide more details about Mailbox server role feature coexistence between Exchange 2007 and Exchange 2010:

Understanding Public Folders

Understanding Exchange Search

Understanding E-Mail Address Policies

For more information about upgrading from previous versions of Exchange, see the following topics:

Exchange 2007 - Planning Roadmap for Upgrade and Coexistence

Exchange 2003 - Planning Roadmap for Upgrade and Coexistence

1.2.2.4.5 Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging

Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging

Planning and Deployment > Deploying Exchange 2010 > Understanding Upgrade from Exchange

2007 to Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-07*

Unified Messaging (UM) was introduced in Microsoft Exchange Server 2007. In organizations that deployed Exchange 2007 Service Pack 3 (SP3) Unified Messaging and now want to upgrade to Microsoft Exchange Server 2010 Service Pack 1 (SP1) or later Unified Messaging with all its new features, there are tasks the Exchange administrator must perform to successfully upgrade their UM environment.

Note:
Exchange 2007 Service Pack 3 (SP3) contains Unified Messaging features. Versions of Microsoft Exchange earlier than Exchange 2007 can't be upgraded and require you to deploy a new Exchange 2010 Service Pack 1 (SP1) or later organization with all the server roles, including Unified Messaging.

Contents

Overview of Upgrading to Exchange 2010 SP1 or later Unified Messaging

Upgrading is the process of taking an existing Exchange 2007 Service Pack 3 (SP3) Unified Messaging environment, installing Exchange 2010 UM SP1 or later servers, and then removing and uninstalling the Exchange 2007 SP3 UM servers. However, during this process, there's the possibility at any time that an upgraded Exchange 2010 SP1 or later organization would contain both Exchange 2010 SP1 or later and Exchange 2007 SP3 UM servers. Such an organization would also contain both Exchange 2007 SP3 and Exchange 2010 SP1 or later Mailbox, Client Access, and Hub Transport servers. All the Exchange 2007 SP3 servers, including the UM server, must have Exchange Server 2007 SP3 installed. For more information, see Download Exchange Server 2007 Service Pack 3 (SP3).

UM-enabled users who have Exchange 2007 SP3 mailboxes will get the features with Exchange 2007 Service Pack 3 (SP3) Unified Messaging, and UM-enabled users who have Exchange 2010 SP1 or later mailboxes will get all the features included with Exchange 2010 SP1 or later Unified Messaging. The following table summarizes upgrade scenarios and the UM features that are available when Exchange 2007 SP3 and Exchange 2010 SP1 or later Unified Messaging coexist in the same Exchange organization.

Unified Messaging with Exchange 2007 SP 3 and Exchange 2010 SP1 or later mailboxes

	Exchange 2007 SP3 UM server	Exchange 2010 SP1 or later UM server
Exchange 2007 SP3 UM-enabled mailbox	UM-enabled users get the features included with Exchange 2007 SP3.	Incoming calls are redirected to an Exchange 2007 SP3 UM server in the same dial plan.

Exchange 2010 SP1 or later UM-enabled mailbox	Not supported. At least one Exchange 2010 SP1 or later.UM server is required.	UM-enabled users get the features included with Exchange 2010 SP1 or later.

When you install the first Exchange 2010 SP1 or later UM server and add it to an existing Exchange 2007 Service Pack 3 (SP3) organization, you must add the Exchange 2010 SP1 or later UM server to an existing UM dial plan that contains Exchange 2007 SP3 UM servers. Then you must configure each IP gateway or IP PBX to send all incoming calls to the Exchange 2010 SP1 or later UM servers within the same UM dial plan.

When an incoming call is received by an Exchange 2010 SP1 or later UM server, and the UM-enabled user's mailbox is located on an Exchange 2010 SP1 or later Mailbox server, the Exchange 2010 SP1 or later UM server will process the incoming call. If the user's mailbox is located on an Exchange 2007 SP3 Mailbox server, the incoming call will be routed to an Exchange 2007 SP3 UM server within the same UM dial plan, and the incoming call will be processed. If there are multiple Exchange 2007 SP3 UM servers in the same dial plan, the Exchange 2010 SP1 or later UM servers will send the incoming call to the Exchange 2007 SP3 UM servers using a round robin mechanism.

After all UM-enabled users' mailboxes are migrated to an Exchange 2010 SP1 or later Mailbox server, the Exchange 2007 Service Pack 3 (SP3) UM servers can be removed from the UM dial plan.

Upgrade Scenarios

When you're upgrading from Exchange 2007 SP3 Unified Messaging to Exchange 2010 SP1 or later Unified Messaging, there are two basic scenarios:

- **Full Upgrade** In a full upgrade, you replace all the Exchange 2007 SP3 UM servers with Exchange 2010 SP1 or later UM servers, and all existing Exchange 2007 SP3 UM-enabled mailboxes are moved to Exchange 2010 SP1 or later Unified Messaging. During this process, you'll most likely have both Exchange 2007 SP3 and Exchange 2010 SP1 or later UM servers coexisting in the same Exchange organization. At the end of the process, the Exchange 2010 SP1 or later UM server will answer all incoming calls and allow UM-enabled users to access their mailbox when they call in to an Outlook Voice Access number that's configured on a Exchange 2010 SP1 or later UM dial plan.

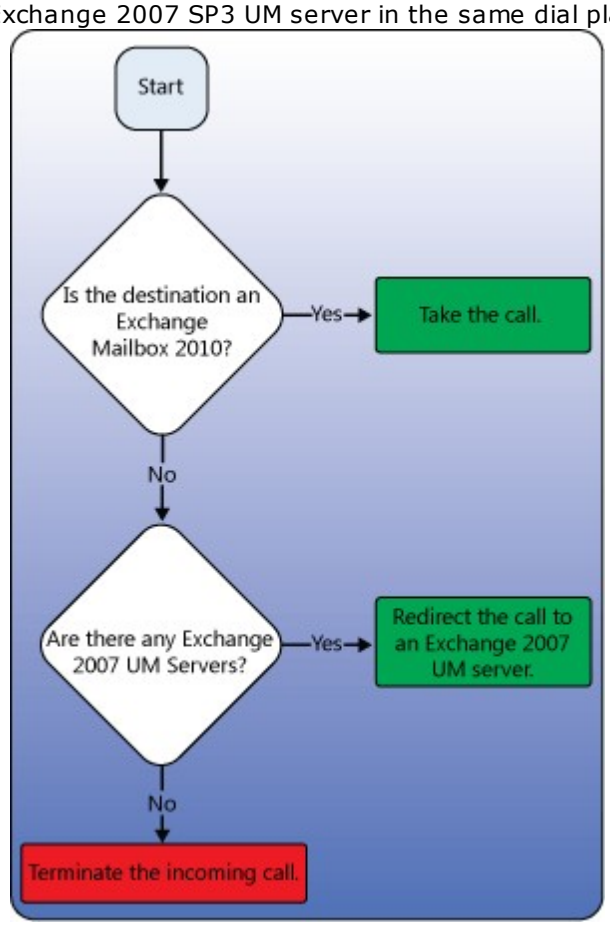
  Important:

  If you're uninstalling the last Exchange 2007 SP3 UM server in the Exchange 2010 SP1 or later organization, run the following command on an Exchange 2010 SP1 or later UM server within the same organization as the Exchange 2007 SP3 UM server: `Set-UMDialPlan -identity MyUMDialPlan -LegacyPromptPublishingPoint $null`. Running this command will force the Exchange 2007 SP3 UM server to unbind from the dial plan. You must run this command before you remove the last Exchange 2007 SP3 server from the Exchange 2010 SP1 or later organization.

- **Partial Upgrade** In a partial upgrade,a portion of the existing Exchange 2007 Service Pack 3 (SP3) UM-enabled mailboxes are moved to Exchange 2010 SP1 or later Unified Messaging. A partial upgrade is a term used to describe upgrading from an Exchange 2007 SP3 organization to an Exchange 2010 SP1 or later organization. In partial upgrades, Exchange 2010 SP1 or later UM servers will only process calls for UM-enabled mailboxes that are on Exchange 2010 SP1 or later Mailbox servers. If you're deploying Exchange 2010 SP1 or later Unified Messaging, and it will coexist with Exchange 2007 SP3 UM, you must keep at least one Exchange 2007 SP3 UM server deployed in your organization and it must be added to the same dial plan as the Exchange 2010 SP1 or later UM server or servers.

When you perform a partial upgrade from Exchange 2007 SP3 Unified Messaging to Exchange 2010 SP1 or later Unified Messaging, incoming calls will be handled differently from the way they're handled after a full upgrade, depending on the type of incoming call and whether UM is integrated with Microsoft Office Communications Server 2007. The following are some ways they're handled differently:

- **Call Answering** In call answering calls, the extension number of the destination mailbox is provided in the SIP INVITE header when the UM server answers the incoming call. Based on the information provided, it verifies the mailbox version, and the Exchange 2010 SP1 or later UM server immediately identifies the location of the destination UM-enabled mailbox. If the recipient mailbox is being hosted on an Exchange 2007 SP3 Mailbox server, the Exchange 2010 SP1 or later UM server will redirect the incoming call to an Exchange 2007 SP3 UM server in the same dial plan.

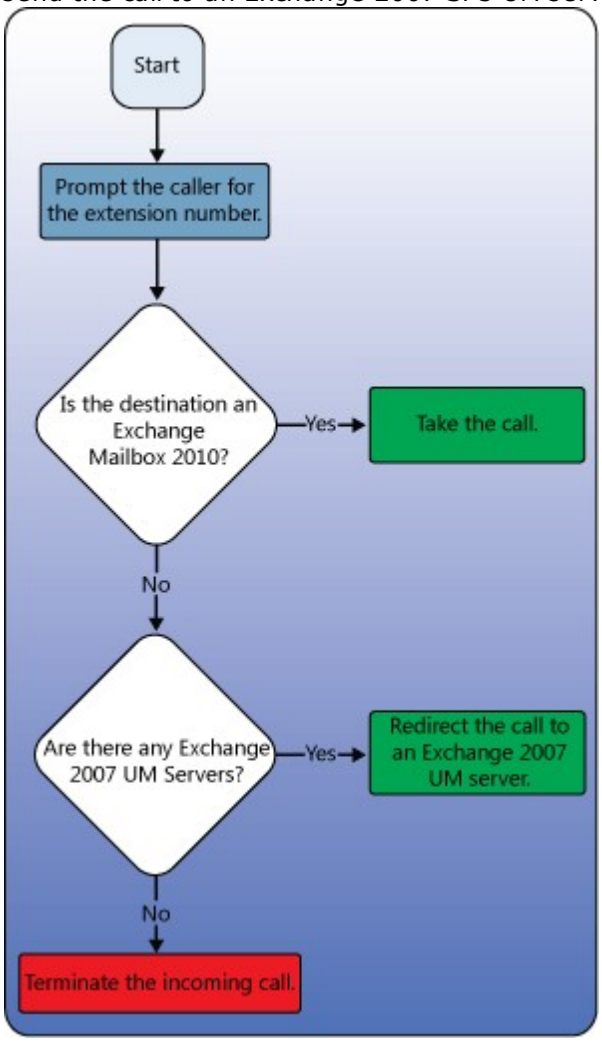


- **Subscriber Access** There are two subscriber access scenarios:

  Scenario 1: When a caller dials in to a subscriber access number configured on a dial plan from a phone number that isn't recognized by a UM server, and the incoming call contains no information about the destination user's mailbox in the SIP INVITE header, the Exchange 2010 SP1 or later UM server will take the call and then prompt the caller to provide the extension number by pressing the corresponding keys on the phone keypad. After the caller has provided the extension number, the Exchange 2010 SP1 or later UM server will identify the user, locate the UM-enabled mailbox, and check the version of the mailbox. If the mailbox is located on an Exchange 2007 SP3 Mailbox server, the Exchange 2010 SP1 or later UM server will do a SIP REFER request and send the call to an Exchange 2007 SP3

UM server.

Scenario 2: When a caller dials in to a subscriber access number configured on a dial plan, and the Exchange 2010 SP1 or later UM server identifies the calling number as an extension for a UM-enabled user with an Exchange 2007 SP3 mailbox, the call will be redirected to an Exchange 2007 SP3 UM server. The Exchange 2010 SP1 or later UM server will make a redirect request and send the call to an Exchange 2007 SP3 UM server.



- **Office Communications Server** If you're running the RTM version of Exchange 2010, Communications Server 2007 without R2 and without Cumulative Update 5 (CU5) or later can't determine the version of the mailbox for a UM-enabled user. So when a call is received by Communications Server 2007, and it redirects the call to another UM server in the same dial plan, either an Exchange 2007 SP3 UM server or an Exchange 2010 SP1 or later UM server might take the call. This causes a problem when you perform a partial upgrade, because the incoming call will fail if it's received by an Exchange 2007 SP3 UM server and the UM-enabled user's mailbox is on an Exchange 2010 SP1 or later Mailbox server. The call will fail because Exchange 2007 SP3 UM servers can't process calls for UM-enabled users who have Exchange 2010 SP1 or later mailboxes.

  The reason the incoming call will fail is that Communications Server 2007 can't tell whether the UM server that it redirected the call to is an Exchange 2007 SP3 UM server or an Exchange 2010 SP1 or later UM server.

If Communications Server 2007 is used as an IP gateway, and there are Exchange 2007 SP3 mailboxes that are enabled for UM, a new SIP URI dial plan will be required. The new SIP URI dial plan must contain only Exchange 2010 SP1 or later UM servers. The new dial plan is required to ensure that incoming calls are redirected only to Exchange 2010 SP1 or later UM servers.
If you're doing a partial upgrade that contains both Exchange 2010 SP1 or later and Exchange 2007 SP3 servers in the same SIP URI dial plan, you must install Communications Server R2 with Cumulative Update 5 (CU5) or later or install Microsoft Lync Server 2010. A separate SIP URI dial plan isn't required when you're running Communications Server R2 with CU5 or later or Lync Server 2010 with Exchange 2010 SP1 or later. The Exchange 2010 SP1 or later and Exchange 2007 SP3 UM servers can coexist in the same SIP URI dial plan. Both Office Communications Server 2007 R2 with CU5 or later and Lync Server 2010 have built-in logic that will direct all incoming calls to an Exchange 2010 SP1 or later UM server and not to an Exchange 2007 SP3 server in the same dial plan.

The following table contains information about the tasks that are required to perform a partial or full upgrade from earlier versions of Microsoft Exchange to Exchange 2010 SP1 or later Unified Messaging.

Upgrading to Exchange 2010 Unified Messaging

Version of Exchange that is currently deployed	Upgrade type	Existing UM dial plans	Actions required
Exchange Server 2003 or earlier versions	Not applicable	Not applicable	• Add Exchange 2010 SP1 or later UM servers to your Exchange 2010 SP1 or later organization. • Create the required UM dial plan(s). • Create the required UM IP gateways and UM hunt groups. • Add the UM servers to the appropriate dial plan. • Copy

			custom prompts to the custom prompts publishing location using the **Import-UMPrompt** cmdlet. • Move the Exchange mailboxes to Exchange 2010 SP1 or later Mailbox servers and UM-enable the mailboxes.
Exchange 2007 SP3	Full upgrade to Exchange 2010 SP1 or later	Telephone Extension, SIP URI and/or E.164	• Add Exchange 2010 SP1 or later UM servers to your Exchange 2010 SP1 or later organization. • Add the Exchange 2010 SP1 or later UM servers to the appropriate dial plan. • Copy custom prompts to the custom prompts publishing location using the **Import-UMPrompt** cmdlet. • From an Exchange

			2010 SP1 or later UM server in the same organization with the Exchange 2007 SP3 UM servers, run the following command: `Set-UMDial` • Move the Exchange 2007 SP3 UM-enabled mailboxes to Exchange 2010 SP1 or later Mailbox servers. • Uninstall the Exchange 2007 SP3 UM servers from the Exchange 2010 SP1 or later organization.
Exchange 2007 SP3	Partial upgrade to Exchange 2010 SP1 or later	Telephone Extension and/or E.164	• Add Exchange 2010 SP1 or later UM servers to the dial plan. • Don't remove the Exchange 2007 SP3 UM servers from the dial plan.

			• Configure the IP gateways or IP PBXs to send calls to an Exchange 2010 SP1 or later UM server. • Copy custom prompts to the custom prompt publishing locations using the **Copy-UMCustomPrompt** and **Import-UMPrompt** cmdlets.
Exchange 2007 SP3	Partial upgrade to Exchange 2010 SP1 or later	SIP URI	• Create a new SIP URI and/or E.164 dial plan. • Add Exchange 2010 SP1 or later servers to the SIP URI dial plan. • Move the Exchange 2007 SP3 UM-enabled mailboxes to Exchange 2010 SP1 or later Mailbox servers. • Create a new UM hunt group for the new SIP URI dial plan. • Disable

			the mailboxes of users who have Exchange 2007 SP3 UM-enabled mailboxes. • Enable the users for Unified Messaging using the new SIP URI dial plan. • Copy custom prompts to the custom prompt publishing locations using the **Copy-UMCustomPrompt** and **Import-UMPrompt** cmdlets.

Upgrading Custom Prompts from Exchange 2007 Unified Messaging

There are many custom greetings used by UM dial plans and auto attendants, including welcome greetings for dial plans and after hours welcome greetings and menus, business hours and non-business hours welcome greetings and menus, and key mappings for UM auto attendants. All these audio files that are used by Unified Messaging are known as custom prompts.

Exchange 2007 Service Pack 3 (SP3) Custom Prompts Overview

In Exchange 2007 SP3, the **Copy-UMCustomPrompt** cmdlet queries the appropriate dial plan object in Active Directory to determine the location of the prompt publishing point. There is only one prompt publishing point for each dial plan, and it's stored as a Windows file share (also known as UNC) path that identifies a file share available for dial plan and auto attendant custom prompts. After the location of the prompt publishing point is determined, the cmdlet validates the content in the custom prompt, and verifies that it's in the correct format and uses a supported audio codec. If the custom prompt passes the validation tests, the cmdlet copies the prompt content to the prompt publishing point.

After the custom prompt is copied to the prompt publishing point, any necessary directory updates are made and the prompt is copied to each UM server in the dial plan. After the custom prompt is added to the appropriate folder on the UM server that's configured as the prompt publishing point, the Microsoft Exchange File Distribution service that runs on

each UM server refers to the prompt publishing point and determines whether the files in the prompt publishing point have changed or additional files have been added. If files have been changed or additional files exist, the other UM servers pull the custom prompts from the prompt publishing point and copy them to the correct location in the *<Server name>*\ExchangeUM folder that exists on a local drive. After the custom prompt is copied to the prompt publishing point using the **Copy-UMCustomPrompt** cmdlet, use the **Set-UMDialPlan** or **Set-UMAutoAttendant** cmdlets to configure the dial plan or auto attendant to use the custom greeting file or prompts.

Exchange 2010 Service Pack 1 or later Custom Prompts

Custom prompts are also available in Exchange 2010 SP1 or later Unified Messaging for dial plans and auto attendants. The prompt publishing point that was available in Exchange 2007 SP3 Unified Messaging doesn't exist in Exchange 2010 SP1 or later. The system mailbox {e0dc1c29-89c3-4034-b678-e6c29d823ed9} is created when you install Exchange 2010 SP1 or later and is used to support features such as Message Approval and Multi-Mailbox Search. This system mailbox is also used in Exchange 2010 SP1 or later Unified Messaging to store dial plan and auto attendant custom prompts. If the system mailbox doesn't exist you can use **Setup /PrepareAD** and one will be created. System mailboxes aren't visible in the Exchange Management Console (EMC) or in Exchange address lists.

By using an Exchange 2010 SP1 or later system mailbox, custom prompts can be backed up and restored along with other mailboxes in a database. This reduces the amount of resources that are needed. Storing custom prompts in a system mailbox removes any possible inconsistencies that may have occurred between Active Directory and the Microsoft Exchange File Distribution service in Exchange 2007 SP3 Unified Messaging. For details about the system mailbox, see Overview of the Mailbox Server Role.

Before you upgrade from Exchange 2007 SP3 Unified Messaging to Exchange 2010 SP1 or later Unified Messaging, you must copy the custom prompts that existed for Exchange 2007 SP3 UM dial plans and auto attendants to a folder on an Exchange 2010 SP1 or later UM server using the **Copy-UMCustomPrompt cmdlet** and then import those custom prompt files to an Exchange 2010 SP1 or later UM server. Custom prompts can be imported to Exchange 2010 UM by using the **Import-UMPrompt** cmdlet. The Exchange 2007 SP3 Unified Messaging cmdlet **Copy-UMCustomPrompt** isn't supported in Exchange 2010 SP1 or later UM for copying custom prompts. For details, see Import and Export Custom Prompts for Unified Messaging.

Use the following syntax to import custom prompts for Exchange 2010 SP1 or later UM dial plans:

```
Import-UMPrompt -PromptFileData <Byte[]> -PromptFileName <String> -UMDialPlan <UM
```

Use the following syntax to import custom prompts for Exchange 2010 UM auto attendants:

```
Import-UMPrompt -PromptFileData <Byte[]> -PromptFileName <String> -UMAutoAttendan
```

The following table contains the steps that are required to ensure that custom prompts are available on the Exchange 2010 SP1 or later and Exchange 2007 SP3 UM servers.

Steps for Custom Prompts

Type of upgrade	Steps for upgrading custom prompts:
Full Upgrade	• Install Exchange 2007 SP3 on all Exchange servers in your organization. • Install the Exchange 2010 SP1 or later Unified Messaging server role and add the UM server to

	the Exchange 2007 SP3 ial plan. • Create the custom prompt if it's a new custom prompt. If the custom prompt was created in Exchange 2007 SP3, manually copy the prompt to a folder on an Exchange 2010 SP1 or later UM server using the **Copy-UMCustomPrompt** cmdlet. • Use the **Import-UMPrompt** cmdlet to import the custom prompt for a UM dial plan or auto attendant to an Exchange 2010 SP1 or later UM server. • From an Exchange 2010 SP1 or later UM server in the same organization with Exchange 2007 SP3 UM servers, run the following command: `Set-UMDialPlan -identity MyUMD` • Decommission your Exchange 2007 SP3 UM servers if there are no Exchange 2007 SP3 UM-enabled mailboxes in your organization.
Partial Upgrade	• Install Exchange 2007 SP3 on all Exchange servers in your organization. • Install the Exchange 2010 SP1 or later Unified Messaging server role and add the UM server to the Exchange 2007 SP3 dial plan. • Create new custom prompts, if needed. If the custom prompt was created in Exchange 2007 SP3, manually copy the prompt to a folder on an Exchange 2010 SP1 or later UM server. • Use the **Import-UMPrompt** cmdlet to import the custom prompt for a UM dial plan or auto attendant to an Exchange 2010 SP1 or later UM server. • If you update or create new custom prompts, you must use the **Import-UMPrompt** cmdlet to import the custom prompt to the Exchange 2010 SP1 or later UM servers and also use the **Copy-UMCustomPrompt** cmdlet to copy the same custom prompt file to the prompt publishing point for your Exchange 2007 SP3 UM servers. **Note:**

	During the upgrade process, Exchange 2007 SP3UM servers and Exchange 2010 SP1 or later UM servers may coexist in the same dial plan and both answer incoming calls. The Exchange 2007 SP3 UM servers will read custom prompts from the Exchange 2007 SP3 custom prompt publishing point and the Exchange 2010 SP1 or later UM servers will read custom prompts from the system mailbox. You must update both custom prompt publishing locations if you're adding or changing custom prompts for a dial plan or auto attendant that's associated with both Exchange 2007 SP3 UM servers and Exchange 2010 SP1 or later UM servers in the same dial plan. If an incoming call is answered by an Exchange 2007 SP3 UM server, the Exchange 2007 SP3 UM servers will play the default greetings if you add a custom prompt for Exchange 2010 SP1 or later UM servers using the **Import-UMPrompt** cmdlet but don't copy the custom prompt using the **Copy-UMCustomPrompt** cmdlet for the Exchange 2007 SP3 UM servers.

Important:

Exchange 2010 SP1 or later UM servers won't answer incoming calls for Exchange 2010 SP1 or later dial plans or auto attendants if the custom prompts are from Exchange 2007 SP3 Unified Messaging and weren't imported using the **Import-UMPrompt** cmdlet.

Autodiscover and Exchange Web Services in Unified Messaging

The Autodiscover service configures client computers running Microsoft Office Outlook 2007 or Outlook 2010 in addition to supported mobile phones. The Autodiscover service provides access to Exchange features for Outlook 2007 or Outlook 2010 clients connected to your Exchange messaging environment. The Autodiscover service must be deployed and configured correctly for these Outlook clients to automatically connect to Exchange features, for example, the offline address book, the Availability service, and Unified Messaging. For details, see Understanding the Autodiscover Service.

In an environment that contains both Exchange 2007 SP3 and Exchange 2010 SP1 or later servers, if the recipient has a mailbox that's hosted on an Exchange 2010 SP1 or later Mailbox server, the Autodiscover request must be directed to an Exchange 2010 SP1 or later Client Access server and not to an Exchange 2007 SP3 Client Access server. If Exchange 2007 SP3 isn't installed on the Exchange 2007 SP3 Client Access server, the Exchange 2007 SP3 Client Access server won't redirect correctly. When the Exchange

2007 SP3 Client Access server tries to generate an Autodiscover response, it isn't aware that there's an Exchange 2010 SP1 or later UM virtual directory and will create an incorrect value for the Unified Messaging URL that's used. You must install Exchange 2007 SP3 to ensure that the Exchange 2007 SP3 Client Access server redirects requests for Exchange 2010 SP1 or later UM-enabled users to the correct UM URL.

Outlook and Microsoft Office Outlook Web App use several URL properties, shown through Autodiscover, to enable UM features such as Play on Phone. When these URL properties are used, the values for the URL are returned but depend on both the version of Outlook and the Mailbox version for the user. The following table shows the versions of Outlook, the version of the user's Exchange mailbox, and which URL will be used.

Versions of Outlook and Exchange mailboxes

	User has an Exchange 2007 SP3 mailbox	**User has an Exchange 2010 SP1 or later mailbox**
Outlook 2007	• Https://<server name>/UnifiedMessaging/service.asmx is the value for the UM virtual directory that's returned to Outlook. • You must make sure that the UM virtual directory is configured correctly using the **Set-UMVirtualDirectory** cmdlet.	• Https://<server name>/EWS/UM2007Legacy.asmx is the value for the UM virtual directory that's returned to Outlook. • You must make sure that the EWS virtual directory is configured correctly using the **Set-WebServicesVirtualDirectory** cmdlet. If it isn't configured correctly, voice mail options and the Play on Phone feature won't work correctly.
Outlook 2010	• https://<server name>/UnifiedMessaging/service.asmx is the value for the UM virtual directory that's returned to Outlook. • You must make sure the UM virtual directory is configured correctly using the **Set-UMVirtualDirectory** cmdlet.	• Exchange Web Services (EWS) URL: https://<servername>/EWS/Exchange.asmx is the value for the EWS virtual directory that's returned to Outlook.You must make sure that the EWS virtual directory is configured correctly using the **Set-WebServicesVirtualDirectory** cmdlet. If it isn't configured correctly, voice mail options and the Play on Phone feature won't work correctly. • Exchange Control Panel (ECP) URL: https://<servername>/ecp/ecp-vdir is the value

		for the ECP virtual directory that's returned to Outlook. You must make sure that the ECP virtual directory is correctly configured using the **Set-WebServicesVirtualDirectory** cmdlet. If it isn't configured correctly, the **Voice Mail** option won't work. • ECP Unified Messaging URL <EcpUrl-um>: ?p=customize/voicemail.aspx&exsvurl=1.This is a hard-coded string, which is used together with the /EcpUrl property to locate the voice mail options page in the ECP. If this isn't configured correctly, the UM-enabled user won't be able to see the voice mail options page.

Service Packs for Exchange 2010

After you upgrade and install the RTM version of Exchange 2010 on UM servers in your organization, you should install Exchange 2010 Service Pack 2 (SP2). For details, see Install or Upgrade to Exchange 2010 SP2 Unified Messaging. If you're upgrading to Exchange 2010 SP2, you must remove all the Exchange 2010 RTM and SP1 UM language packs and install the Exchange 2010 SP2 UM language packs. For details, see:

- Upgrade Exchange 2010 UM Language Packs from RTM or SP1 to Exchange 2010 SP2
- Exchange Server 2010 SP2 UM Language Packs

1.2.2.5 Understanding Upgrade from Exchange 2003 and Exchange 2007 to Exchange 2010

Understanding Upgrade from Exchange 2003 and Exchange 2007 to Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-29*

When you're upgrading your mixed Microsoft Exchange Server 2003 and Exchange Server

2007 organization to Exchange Server 2010, there's a period of time when these earlier versions of Exchange and Exchange 2010 will coexist within your organization. This section discusses key points about both the upgrade process and coexistence as they apply to the Client Access, Transport, and Mailbox server roles.

For more information, see the following topics:

Checklist: Upgrading from Exchange 2003 and Exchange 2007

Upgrade from Exchange 2003 Client Access

Upgrade from Exchange 2003 Transport

Upgrade from Exchange 2003 Mailbox

Upgrade from Exchange 2007 Client Access

Upgrade from Exchange 2007 Transport

Upgrade from Exchange 2007 Mailbox

Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging

Managing Deployment of Exchange 2010

For more information about the upgrade process for the mixed Exchange 2003 and Exchange 2007 organization, see the "Exchange 2007 and Exchange 2003 Mixed Mode Coexistence" section in Exchange 2003 - Planning Roadmap for Upgrade and Coexistence.

Also, see Exchange Server Deployment Assistant for information about a Web-based tool that can help you with your deployment.

1.2.2.5.1 Checklist: Upgrading from Exchange 2003 and Exchange 2007

Checklist: Upgrading from Exchange 2003 and Exchange 2007

Planning and Deployment > Deploying Exchange 2010 > Understanding Upgrade from Exchange 2003 and Exchange 2007 to Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-30*

Use this checklist to upgrade from an environment in which you're running Microsoft Exchange Server 2003 and Exchange Server 2007 to Exchange Server 2010.

Before you start working with this checklist, make sure you're familiar with the concepts discussed in:

- Planning for Exchange 2010
- Deployment Security Checklist
- Exchange 2007 - Planning Roadmap for Upgrade and Coexistence

This checklist is generic in that it provides guidance for a typical upgrade scenario. For more customized step-by-step guidance about how to upgrade your mixed Exchange

2003 and Exchange 2007 organization, see the Exchange Server Deployment Assistant.

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Checklist for Upgrading from Exchange 2003 and Exchange 2007 to Exchange 2010

Done?	Task	Topic
	1. Verify system requirements	Exchange 2010 System Requirements
	2. Confirm prerequisite steps are done for Exchange 2003 and Exchange 2007	Exchange 2010 Prerequisites
	3. Configure disjoint namespace **Note:** This step is optional. It's only necessary if your organization is running a disjoint namespace.	Configure the DNS Suffix Search List for a Disjoint Namespace
	4. Install the Client Access server role	Install Exchange Server 2010
	5. Add digital certificates on the Client Access server	Create a New Exchange Certificate
	6. Enable Outlook Anywhere **Note:** This step is optional. It's only necessary if you want to use the Outlook Anywhere component of Exchange 2010.	Enable Outlook Anywhere
	7. Configure settings on virtual directories, including OAB, Web Services, ECP, Outlook Web App, and Exchange ActiveSync virtual directories **Note:** This step is necessary if you want to use Exchange Web Services, Outlook Anywhere, or the offline address book. It also may be required if you	Create an Offline Address Book Virtual Directory Configure ECP Virtual Directory Properties View or Configure Outlook Web App Virtual Directories View or Configure Exchange ActiveSync Virtual Directory Properties

	need to change any of the default settings for the Exchange Control Panel, Outlook Web App, or Exchange ActiveSync.	
	8. Install the Hub Transport server role	Install Exchange Server 2010
	9. Configure a legacy host name	Upgrade from Exchange 2007 Client Access
	10. Install the Unified Messaging server role **Note:** This step is optional. It's only necessary if you want to use Unified Messaging in your organization.	Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging Checklist: Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM UM Install the Exchange 2010 Unified Messaging Server Role
	11. Configure Unified Messaging **Note:** This step is optional. It's only necessary if you want to use Unified Messaging in your organization.	Checklist: Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM UM
	12. Install the Mailbox server role	Install Exchange Server 2010 Upgrade from Exchange 2007 Mailbox Upgrade from Exchange 2003 Mailbox
	13. Change the offline address book generation server	Move the Offline Address Book Generation Process to Another Server
	14. Install the Edge Transport server role **Note:** This step is optional. It's only necessary if you want to use the Edge server role in your organization.	Install Exchange Server 2010 Upgrade from Exchange 2007 Transport
	15. Subscribe the Edge Transport server **Note:** This step is optional. It's only necessary if you want to use the Edge server role in your organization.	Create an Edge Subscription File on an Edge Transport Server Import an Edge Subscription File to an Active Directory Site

	16. Move mailboxes from Exchange 2003 or Exchange 2007 to Exchange 2010	Create a Local Move Request
	17. Move public folder data to Exchange 2010	Configure Public Folder Replication
	18. Post-installation tasks	Exchange 2010 Post-Installation Tasks

Return to top

1.2.2.6 Understanding Unified Messaging Deployments

Understanding Unified Messaging Deployments

Exchange Server 2010 > Planning and Deployment > Deploying Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-28*

Microsoft Exchange Server 2010 Unified Messaging combines voice messaging and e-mail messaging into one store, accessible from a telephone and a computer. Unified Messaging integrates Microsoft Exchange with telephony networks and brings the UM features to the core of Microsoft Exchange. The following topics provide detailed information about deploying Exchange 2010 Unified Messaging:

Deploy a New Exchange 2010 RTM UM Environment

Checklist: Deploy a New Exchange 2010 RTM UM Environment

Checklist: Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM UM

Install or Upgrade to Exchange 2010 SP2 Unified Messaging

Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging

Deploy and Configure Incoming Faxing

Deploy Unified Messaging and Communications Server 2007 R2

Checklist: Deploy Office Communications Server 2007 R2 and Exchange 2010 Unified Messaging

1.2.2.6.1 Deploy a New Exchange 2010 RTM UM Environment

Deploy a New Exchange 2010 RTM UM Environment

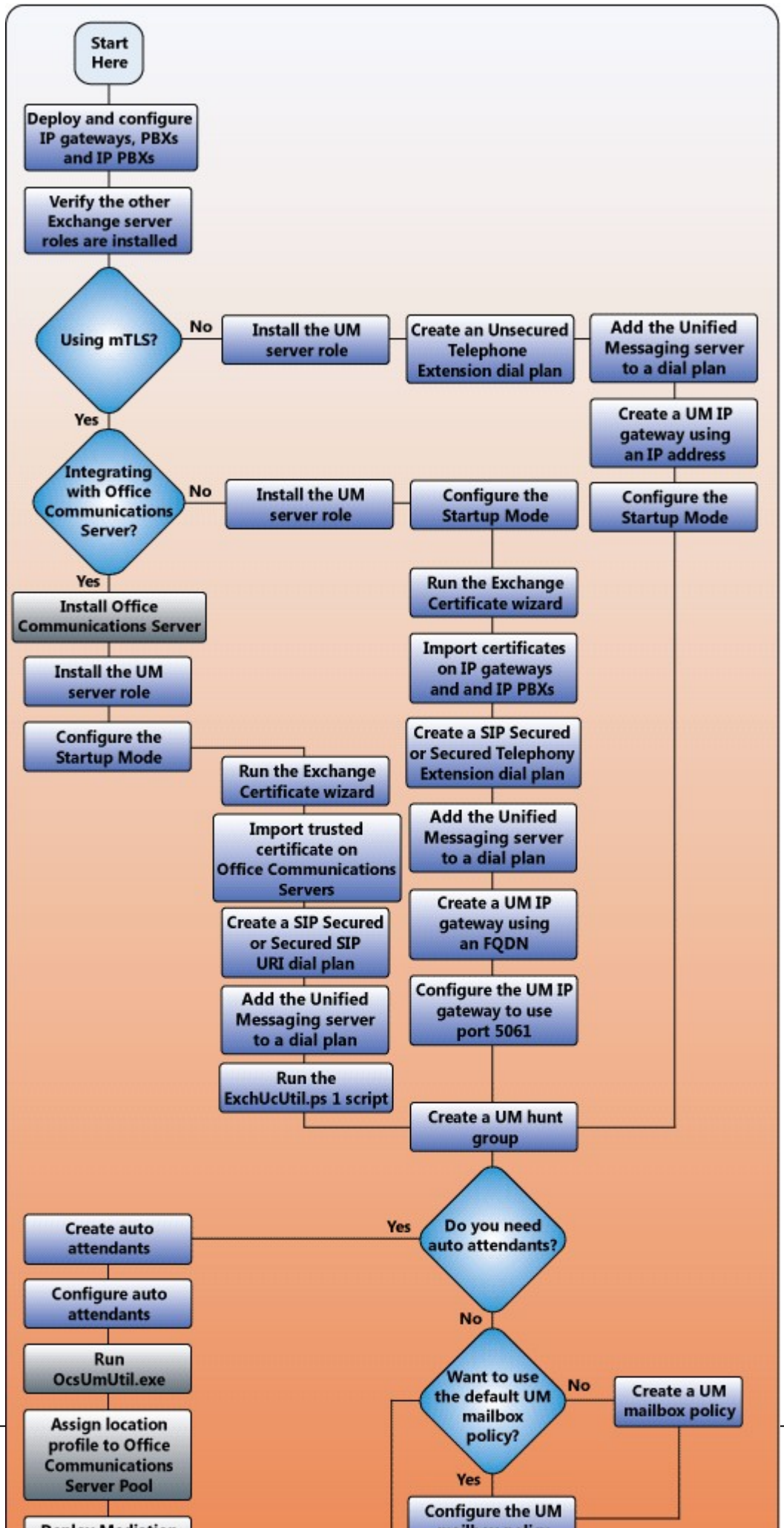
Planning and Deployment > Deploying Exchange 2010 > Understanding Unified Messaging Deployments >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Microsoft Exchange Server 2010 Unified Messaging (UM) provides an efficient and simple deployment model that's highly scalable but doesn't increase the complexity of the deployment. There are many deployment models for Unified Messaging in your organization. The recommended deployment model for Unified Messaging centralizes your Unified Messaging servers. Microsoft Exchange Server 2007 and or later versions contain Unified Messaging features. Versions that are earlier than Exchange 2007 can't be upgraded and require you to deploy an Exchange 2010 organization with all the Exchange server roles, including Unified Messaging, and then move the Microsoft Exchange Server 2003 (or earlier) mailboxes to an Exchange 2010 Mailbox server. For details, see Move Mailboxes from Exchange 2003 Servers to Exchange 2010 Servers.

The following illustration shows the steps that are required to successfully deploy a new Unified Messaging environment.


Start Here
Deploy and configure IP gateways, PBXs and IP PBXs
Verify the other Exchange server roles are installed
Using mTLS?
No
Install the UM server role
Create an Unsecured Telephone Extension dial plan
Add the Unified Messaging server to a dial plan
Create a UM IP gateway using an IP address
Configure the Startup Mode
Yes
Integrating with Office Communications Server?
No
Install the UM server role
Configure the Startup Mode
Run the Exchange Certificate wizard
Import certificates on IP gateways and and IP PBXs
Create a SIP Secured or Secured Telephony Extension dial plan
Add the Unified Messaging server to a dial plan
Create a UM IP gateway using an FQDN
Configure the UM IP gateway to use port 5061
Yes
Install Office Communications Server
Install the UM server role
Configure the Startup Mode
Run the Exchange Certificate wizard
Import trusted certificate on Office Communications Servers
Create a SIP Secured or Secured SIP URI dial plan
Add the Unified Messaging server to a dial plan
Run the ExchUcUtil.ps 1 script
Create a UM hunt group
Do you need auto attendants?
Yes
Create auto attendants
Configure auto attendants
Run OcsUmUtil.exe
Assign location profile to Office Communications Server Pool
No
Want to use the default UM mailbox policy?
No
Create a UM mailbox policy
Yes
Configure the UM

Contents

Before You Deploy

Before you deploy Exchange 2010 Unified Messaging, we recommend that you familiarize yourself with the concepts in the following topics:

- Overview of Unified Messaging
- Understanding Unified Messaging Dial Plans
- Understanding Unified Messaging Mailbox Policies
- Understanding Unified Messaging IP Gateways
- Understanding Unified Messaging Hunt Groups
- Understanding Unified Messaging Auto Attendants
- Understanding Unified Messaging Servers
- Understanding Unified Messaging Users

Return to top

Deploying Unified Messaging

All the available deployment options for Unified Messaging have several steps in common. These steps are required to create a scalable and highly available system to support large numbers of Unified Messaging users. These steps are as follows:

1. Deploy and configure your telephony components for Unified Messaging.
2. Verify that you've correctly installed the Exchange 2010 server roles that are required by Unified Messaging.
3. Install the Unified Messaging server role.
4. Create and configure the required Unified Messaging Active Directory components.
5. Perform post deployment tasks for Unified Messaging.

- If you're looking for a checklist of tasks that must be performed to deploy a new UM environment, see Checklist: Deploy a New Exchange 2010 RTM UM Environment.

Return to top

Deploy and Configure Telephony Components

To successfully deploy an Exchange 2010 Unified Messaging server in an Exchange organization, the Exchange administrator must become knowledgeable about data networking concepts and telephony terminology and concepts and be able to correctly configure the telephony components that are required by Unified Messaging. Performing a new deployment or upgrading a legacy voice mail system requires significant knowledge about PBXs and Exchange 2010 Unified Messaging. For more information, see the Microsoft Exchange Server 2007 Unified Messaging (UM) Specialists Web site.

Generally, there are three tasks that must be completed to successfully configure the telephony components that are required by Unified Messaging:

1. **Provision PBX lines** The first step in deploying a scalable UM solution is to provision PBX lines.
2. **Organize channels** After you provision PBX-based voice channels, you can

organize the channels as hunt groups.

3. **Deploy IP gateways** After you organize your voice channels as hunt groups, you must end these channels at IP gateways. IP gateways are used with a legacy PBX to convert the circuit-switched protocols found on a telephony network to IP-based packet-switched protocols.

When you integrate your organization's telephony and data networks during the deployment of Exchange 2010 Unified Messaging, you must configure the telephony and data networking components correctly. You must also configure the following components or interfaces to successfully deploy Unified Messaging:

- **Configure the connection from the PBXs in your organization to communicate with your IP gateways.** For details, see Configure an IP Gateway to Communicate with a PBX.
- **Configure the connection from the IP gateway interface to the PBX.** For more information about how to configure your PBX interface to communicate with your supported IP gateway, see the product documentation that's specific to your PBX. For details, see Configure an IP Gateway to Communicate with a PBX.
- **Configure the connection from the IP gateway interface to the Exchange Server 2010 Unified Messaging server.** For details, see Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server.
- **Configure the connection from the Unified Messaging server to the IP gateway interface.** For details, see Connect a Unified Messaging Server to a Supported IP Gateway.

For more information about telephony components, see Understanding Telephony Concepts and Components.

Return to top

Verify Installation of the Mailbox, Hub Transport, and Client Access Server Roles

Different deployment paths are available for organizations that plan to deploy Exchange 2010. Although these paths all lead to the same end—a successful deployment of Exchange 2010—each path is slightly different because each customer's needs and starting points are different. However, generally there are common starting points and paths that cover all supported deployment scenarios, including new installations and upgrades. Because Unified Messaging relies on the functionality of other server roles found in Exchange 2010, the Unified Messaging server role will most likely be the last server role that you install in your Exchange 2010 organization. You must follow these steps to install the server roles other than Unified Messaging before you can install the Unified Messaging server role:

1. Verify that your existing infrastructure meets certain prerequisites before you install Exchange 2010. For details, see Exchange 2010 Prerequisites.
2. Verify that you've correctly installed the Exchange 2010 server roles required by Unified Messaging. After you install Exchange 2010, we recommend that you verify the installation and review the server setup logs. For details, see Verify an Exchange 2010 Installation.

Return to top

Install the Unified Messaging Server Role

After you've completed the deployment of your IP gateways or IP PBXs on your network, you must install the Unified Messaging server role on one or more computers in your Exchange environment. Depending on the needs of your business, to provide a highly scalable and available Unified Messaging system, consider installing the Unified Messaging server role on more than one computer. For more information about how to plan and deploy a highly available and scalable Unified Messaging system, see Understanding Unified Messaging Availability or Understanding Unified Messaging Performance and Scalability.

Follow these steps to install the Unified Messaging server role:

1. **Review the Exchange 2010 system requirements before installation.**
   Before you install the Unified Messaging server role, we recommend that you make sure that your network, hardware, software, clients, and other elements meet the requirements for Exchange 2010. For details, see Exchange 2010 System Requirements.
2. **Install the Unified Messaging server role.**
   There's more than one way to install the Unified Messaging server role on a computer that's running Exchange 2010. The Unified Messaging server role can be installed on a single computer that has no other Exchange 2010 server roles installed, or on a computer that's running another Exchange 2010 server role. Before you install the Unified Messaging server role, you must install the Mailbox, Hub Transport, and the Client Access server roles. However, you can install the Mailbox, Hub Transport, Client Access and the Unified Messaging server roles on the same physical computer. For details, see Install the Exchange 2010 Unified Messaging Server Role.
3. **Verify your Exchange 2010 Unified Messaging installation.**
   After you install Exchange 2010, we recommend that you verify the installation and review the server setup logs. If the Setup process fails or errors occur during installation, you can use the setup logs to track down the source of the problem. For details, see Verify an Exchange 2010 Installation.
4. **Download and Install the Unified Messaging Language Packs.**
   After you install Exchange 2010, you may have to download and install the required Unified Messaging Service Pack 1 (SP1) language packs you need on the UM servers in your organization. Make sure to install each UM language pack on each UM server and to set the default language on all dial plans that the UM server is associated with.
   Exchange Unified Messaging language packs are version-specific and platform-specific. Since Exchange 2007, there have been separate releases for UM language packs, including Exchange 2007 RTM, Exchange 2007 SP1, Exchange 2010 RTM, and Exchange 2010 SP1. For some of these versions, both 32-bit and 64-bit downloads are available, but for other releases only 64-bit downloads are available. It's very important that you install the correct version and platform of the UM language packs on a UM server.
   For more information about how to install a UM language pack, see Install a Unified Messaging Language Pack on a UM Server. To download Unified Messaging language packs, see Exchange Server 2010 UM Language Packs.

Return to top

Create and Configure UM Components

There are several UM components in Active Directory that are required for the deployment and operation of Exchange 2010 Unified Messaging. Unified Messaging components in Active Directory connect the telephony infrastructure with the Unified Messaging Active Directory environment. After you've successfully installed the Unified Messaging server role on at least one computer, follow these steps.

Step 1: Create and configure UM dial plans

UM dial plans are integral to the operation of Exchange 2010 Unified Messaging and are required to successfully deploy Unified Messaging on your network. After you've successfully installed the Unified Messaging server role, a UM dial plan will be the first Active Directory component that you'll create.

By default, UM dial plans and the Unified Messaging servers that are associated with the dial plan send and receive data without using encryption. In Unsecured mode, the VoIP and SIP traffic won't be encrypted. When you create the dial plan or after you've created the dial plan, you can configure the dial plan to encrypt the VoIP and SIP traffic by using Mutual Transport Layer Security (mutual TLS). After you configure the VoIP security setting, you'll then have to configure the startup mode for the UM server. For details, see Configure the Startup Mode on a UM Server.

Perform one of the following procedures to create a new UM dial plan.

Use the EMC to create a UM dial plan
You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the action pane, click **New UM Dial Plan**.
3. In the New UM Dial Plan wizard, complete the following fields:
   - **Name** Type the name of the dial plan. A UM dial plan name is required and must be unique. However, the name you type is used only for display purposes in the EMC and the Shell. If you have to change the display name of the dial plan after it's been created, you must first delete the existing UM dial plan and then create another dial plan that has the appropriate name. If your organization uses multiple UM dial plans, we recommend that you use meaningful names for your UM dial plans. The maximum length of a UM dial plan name is 64 characters, and it can include spaces. However, it can't include any of the following characters: " / \ [ ] : ; | = , + * ? < >.

     Important:
     Although the field for the name of the dial plan can accept 64 characters, the name of the dial plan can't be longer than 49 characters. This is because, when you create a dial plan, a default UM mailbox policy is also created that has the name *<DialPlanName>* Default Policy. The *name* parameter for both the UM dial plan and UM mailbox policy can be 64 characters long.

   - **Number of digits in extension numbers** Enter the number of digits for extension numbers in the dial plan. The number of digits for extension numbers is based on the telephony dial plan created on a Private Branch eXchange (PBX). For example, if a user associated with a telephony dial plan dials a four-digit extension to call another user in the same telephony dial plan, you select 4 as the number of digits in the extension.

     This is a required field that has a value range from 1 through 20. The typical extension length is from 3 through 7. If your existing telephony environment includes extension numbers, you must specify a number of digits that matches the number of digits in those extensions.

     When you create a Session Initiation Protocol (SIP) dial plan or an E.164 dial plan and associate a UM-enabled user with the dial plan, you must still enter an extension number to be used by the user. This number is used by Outlook Voice Access users when they access their Exchange 2010 mailbox.

   - **URI Type** Use this drop-down list to select the URI type for the UM dial plan. A URI is a string of characters that identifies or names a resource. The main purpose of this identification is to enable VoIP devices to communicate with other devices over a network using specific protocols. URIs are defined in schemes that define a specific syntax, format, and the protocols for the call.

     You can select one of the following URI types for the dial plan:
     Telephone extension This is the most common URI type. The calling and called party information from the IP gateway or IP PBX will be listed in one of the following formats: Tel:512345 or 512345@*<IP address>*. This is the default URI type for dial plans.
     SIP URI Use this URI type if you need a SIP URI dial plan when an IP PBX supports SIP routing or if you're integrating Microsoft Office Communications Server 2007 and Exchange Unified Messaging. The calling and called party information from the IP gateway or IP PBX will be listed as a SIP address in the

following format: sip:<*username*>@<*domain* or *IP address*>:Port.
E.164 E.164 is an international numbering plan for public telephone systems in which each assigned number contains a country/region code, a national destination code, and a subscriber number. The calling and called party information sent from the IP gateway is listed in the following format: Tel:+14255550123.

Note:
After you create a dial plan, you will be unable to change the URI type without deleting the dial plan, and then re-creating the dial plan to include the correct URI type.

- **VoIP Security** Use this drop-down list to select the VoIP security setting for the UM dial plan. By default, when you create a UM dial plan, it communicates in unsecured mode. A Unified Messaging server can operate in any mode configured on a dial plan because the Unified Messaging server is configured to listen on TCP port 5060 for unsecured requests and on TCP port 5061 for secured requests at the same time.
  You can select one of the following security settings for the dial plan:
  Unsecured By default, when you create a UM dial plan, it communicates in unsecured mode, and the Unified Messaging servers associated with the UM dial plan send and receive data from IP gateways, IP PBXs, and other Exchange 2010 computers using no encryption. In unsecured mode, both the Realtime Transport Protocol (RTP) media channel and SIP signaling information aren't encrypted.
  SIP secured When you select **SIP secured**, only the SIP signaling traffic is encrypted, and the RTP media channels still use TCP, which isn't encrypted. Mutual Transport Layer Security (TLS) is used to encrypt the SIP signaling traffic.
  Secured When you select **Secured**, both the SIP signaling traffic and the RTP media channels are encrypted. An encrypted signaling media channel that uses Secure Realtime Transport Protocol (SRTP) also uses mutual TLS to encrypt the VoIP data.
- **Country/Region code** Use this field to type the country/region code number to be used for outgoing calls. This number will automatically be prepended to the telephone number that's dialed. This field accepts from 1 through 4 digits. For example, in the United States, the country/region code is 1. In the United Kingdom, it's 44.

4. On the **Set UM Servers** page, click **Add** and then on the **Select UM Server** page select the UM server that you want to add to the UM dial plan.
5. On the **Completion** page, confirm whether the dial plan was successfully created:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to complete the New UM Dial Plan wizard.

Use the Shell to create a UM dial plan
You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example creates a new UM dial plan named `MyUMDialPlan` that uses four-digit extension numbers.

```
New-UMDialplan -Name MyUMDialPlan -NumberofDigits 4
```

This example creates a new UM dial plan named MyUMDialPlan that uses five-digit extension numbers and supports SIP URIs:

```
New-UMDialplan -Name MyUMDialPlan -UriType SIPName -NumberofDigits 5
```

For more information about syntax and parameters, see Set-UMDialplan.

Return to top

Step 2: Create and configure your UM IP gateways

A UM IP gateway represents either an IP gateway hardware device or an IP PBX hardware device. The combination of the UM IP gateway object and a UM hunt group object establishes a logical link between an IP gateway or IP PBX and a UM dial plan.

If you've created or enabled VoIP security on a dial plan, the UM IP gateway that you will create by using one of the following procedures in this section will be associated with a UM dial plan that uses VoIP security. In that case, you must use a fully qualified domain name (FQDN) to create the UM IP gateway, and not an IP address. You must also configure the UM IP gateway to listen on TCP port 5061. To configure a UM IP gateway to listen on TCP port 5061, run the following command: **Set-UMIPGateway -identity MyUMIPGateway -Port 5061**. You must also verify that any IP gateways or IP PBXs have also been configured to listen on port 5061 for mutual TLS.

Perform one of the following procedures to create a new UM IP gateway.

Use the EMC to create a UM IP gateway

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the result pane, click the **UM IP Gateways** tab.
3. In the action pane, click **New UM IP Gateway**.
4. In the **New UM IP Gateway** wizard, in the **Name** section, type the name of the UM IP gateway. This is the display name for the UM IP gateway.
5. In the **IP Address** section, type the IP address for the UM IP gateway, and then click **New**.

   Note:

   Alternatively, you can enter an FQDN for the UM IP gateway. If you choose to use an FQDN, you must add the appropriate host records with the correct IP addresses to the DNS zone. If you're configuring a UM IP gateway that will be associated with a dial plan that's operating in Secured mode, you must create the UM IP gateway with an FQDN.

6. On the **New UM IP Gateway** page, click **New**.
7. On the **Completion** page, click **Finish**.

Use the Shell to create a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example creates a UM IP gateway named MyUMIPGateway that enables a Unified Messaging server to start accepting calls from an IP gateway that has an IP address of 10.10.10.1.

```
New-UMIPGateway -Name MyUMIPGateway -Address 10.10.10.1
```

This example creates a UM IP gateway named MyUMIPGateway that enables a Unified Messaging server to start accepting calls from an IP gateway that has an FQDN of MyUMIPGateway.contoso.com and listens on port 5061.

```
New-UMIPGateway -Name MyUMIPGateway -Address "MyUMIPGateway.contoso.com" -Port 50
```

For more information about syntax and parameters, see New-UMIPGateway.

Return to top

Step 3: Create and configure your UM hunt groups (optional)

Hunt group is a term that's used to describe a group of PBX or IP PBX resources or extension numbers that are shared by users. Hunt groups are used to efficiently distribute calls into or out of a given business unit.

If you've created a UM IP gateway and associated the UM IP gateway with a UM dial plan, a default UM hunt group is created. You can associate another UM hunt group with the same or a different UM IP gateway, depending on the number of UM IP gateways that you've created.

When you create a UM hunt group, you enable all Unified Messaging servers that are specified within the UM dial plan to communicate with an IP gateway. To learn more about UM hunt groups, see Understanding Unified Messaging Hunt Groups. To create a new UM hunt group, perform one of the following procedures.

Use the EMC to create a UM hunt group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM hunt groups" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. In the result pane, select a UM IP gateway.
4. In the action pane, click **New UM Hunt Group**.
5. In the New UM Hunt Group wizard, view or complete the following fields:
   - **Associated UM IP gateway** This display-only field shows the name of the UM IP gateway that will be associated with the UM hunt group.
   - **Name** Use this text box to create the display name for the UM hunt group. A UM hunt group name is required and must be unique, but it's used only for display purposes in the EMC and the Shell. If you have to change the display name of the hunt group after it's been created, you must first delete the existing hunt group and then create another hunt group that has the appropriate name.

     If your organization uses multiple hunt groups, we recommend that you use meaningful names for your hunt groups. The maximum length of a UM hunt group name is 64 characters, and it can include spaces. However, it can't include any of the following characters: " / \ [ ] : ; | = , + * ? < >.
   - **Dial plan** Click the **Browse** button to select the dial plan that will be associated with the UM hunt group. Associating a hunt group with a dial plan is required. A UM hunt group can be associated with only one UM IP gateway and one UM dial plan.
   - **Pilot identifier** Use this text box to specify a string that uniquely identifies the pilot identifier or pilot ID configured on the PBX or IP PBX.

     An extension number or a SIP URI can be used in this field. Alphanumeric characters are accepted in this field. For legacy PBXs, a numeric value is used as a pilot identifier. However, some IP PBXs can use SIP URIs.
6. On the **Completion** page, confirm whether the UM hunt group was successfully created:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

7. Click **Finish** to complete the New UM Hunt Group wizard.

Use the Shell to create a UM hunt group
You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM hunt groups" entry in the Unified Messaging Permissions topic.

This example creates a UM hunt group named `MyUMHuntGroup` that has a pilot identifier of 12345.

```
New-UMHuntGroup -Name MyUMHuntGroup -PilotIdentifier 12345  -UMDialplan MyUMDialP
```

This example creates a UM hunt group named `MyUMHuntGroup` that has multiple pilot identifiers.

```
New-UMHuntGroup -Name MyUMHuntGroup -PilotIdentifier 5551234,55555 -UMDialplan My
```

For more information about syntax and parameters, see New-UMHuntGroup.

Return to top

Step 4: Create and configure a UM mailbox policy

UM mailbox policies are required when you enable users for Exchange 2010 Unified Messaging. The mailbox of each UM-enabled user must be linked to a single UM mailbox policy. After you create a UM mailbox policy, you link one or more UM-enabled mailboxes to the UM mailbox policy. This lets you control PIN security settings such as the minimum number of digits in a PIN or the maximum number of failed sign-in attempts for the UM-enabled users who are associated with the UM mailbox policy.

Every time that you create a UM dial plan, a UM mailbox policy is also created. The UM mailbox policy will be named *<DialPlanName>* Default Policy. However, if you have to create a new UM mailbox policy, perform one of the following procedures.

Use the EMC to create a UM mailbox policy
You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Mailbox Policies** tab.
3. In the action pane, click **New UM Mailbox Policy**.
4. In the New UM Mailbox Policy wizard, complete the following fields:
   - **Name** Use this text box to specify a unique name for the UM mailbox policy. If you must change the display name of the UM mailbox policy after it's been created, you must first delete the existing UM mailbox policy, and then create another UM mailbox policy that has the appropriate name. To delete the UM mailbox policy, there must not be any UM-enabled users associated with the UM mailbox policy.
     The UM mailbox policy name is required, but it's used for display purposes only. Because your organization may use multiple UM mailbox policies, we recommend that you use meaningful names for your UM mailbox policies. The maximum length of a UM mailbox policy name is 64 characters, and it can include spaces. However, it cannot include any of the following characters: " / \ [ ] : ; | = , + * ? < >.
   - **Select associated dial plan** Click **Browse** to select the UM dial plan that will be associated with the UM mailbox policy. You must associate a UM mailbox policy with at least one UM dial plan. However, you can also associate multiple UM mailbox policies with a single dial plan.
5. On the **Completion** page, confirm whether the UM mailbox policy was successfully created:

- A status of **Completed** indicates that the wizard completed the task successfully.
- A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

6. Click **Finish** to complete the New UM Mailbox Policy wizard.

Use the Shell to create a UM mailbox policy
You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example creates a UM mailbox policy named `MyUMMailboxPolicy` associated with a UM dial plan named `MyUMDialPlan`.

```
New-UMMailboxPolicy -Name MyUMMailboxPolicy -UMDialPlan MyUMDialPlan
```

For more information about syntax and parameters, see New-UMMailboxPolicy.

Return to top

Step 5: Add a Unified Messaging server to dial plans

After you install the Unified Messaging server role, the UM server can't answer incoming calls until you add it to a UM dial plan. Although the status of the Exchange 2010 Unified Messaging server is set to enabled after installation, there's a parameter that's used to enable or disable the status of the Unified Messaging server.

A Unified Messaging server can be associated with a single or multiple UM dial plans. A single UM server can be added to a multiple dial plans that use mutual TLS (Secured), SIP secured, or TCP (Unsecured). To add a UM server to a dial plan, perform one of the following procedures.

Use the EMC to add a UM server to a dial plan
You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Server Configuration**.
2. In the result pane, select the Unified Messaging server you want to add to a dial plan.
3. In the action pane, click **Properties**.
4. On the **UM Settings** > **Associated Dial Plans**, click **Add**.
5. In the **Select Dial Plan** window, from the list of available dial plans, select the dial plan you want to add the UM server to, and then click **OK**.

Use the Shell to add a UM server to a dial plan
You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example adds a Unified Messaging server to a dial plan named `MyUMDialPlan` and prevents the UM server from accepting new calls. It also sets the startup mode to dual mode, which enables the UM server to accept TCP and TLS requests.

```
Set-UMServer -Identity MyUMServer -DialPlans MyUMDialPlan -Status Disabled -UMSta
```

This example adds the Unified Messaging server named `MyUMServer` to two UM dial plans, named `MyUMDialPlan` and `MyUMDialPlan2`, and also sets the maximum number of incoming voice and fax calls.

```
Set-UMServer -Identity MyUMServer -DialPlans MyUMDialPlan, MyUMDialPlan2 -MaxCall
```

For more information about syntax and parameters, see Set-UMServer.

Return to top

Step 6: Create and configure UM auto attendants (optional)

Exchange 2010 Unified Messaging enables you to create one or more UM auto attendants, depending on the needs of your organization. When you create a UM auto attendant, you create a voice menu system for your organization. Callers from outside or inside your organization can then move through the menu system to locate and place or transfer calls to users or departments in your organization.

Callers can move through the menu system by using dual tone multi-frequency (DTMF), also known as touchtone, or voice inputs. For automatic speech recognition (ASR) to work, so users can use voice inputs, you must speech-enable the UM auto attendant.

Creating and using auto attendants is optional in Exchange 2010 Unified Messaging. However, if you want to create a new UM auto attendant, perform one of the following procedures.

Use EMC to create a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. In the action pane, click **New UM Auto Attendant**.
4. In the New UM Auto Attendant wizard, complete the following fields:
   - **Name** Use this text box to create the display name for the UM auto attendant. A UM auto attendant name is required and must be unique. However, it's used only for display purposes in the EMC and the Shell.
     If you have to change the display name of the auto attendant after it's created, you must first delete the existing UM auto attendant and then create another UM auto attendant that has the appropriate name. If your organization uses multiple UM auto attendants, we recommend that you use meaningful names for your UM auto attendants. The maximum length of a UM auto attendant name is 64 characters, and it can include spaces.
   - **Select associated dial plan** Click **Browse** to select the UM dial plan to associate with this UM auto attendant. Selecting and associating a UM dial plan with the auto attendant is required. A UM auto attendant can be associated with only one UM dial plan.
   - **Extension numbers** Use this field to enter the extension number that callers will use to reach the auto attendant. Type an extension number in the box, and then click **Add** to add the number to the list. The number of digits in the extension number that you provide doesn't have to match the number of digits for an extension number configured on the associated UM dial plan. This is because direct calls are allowed to UM auto attendants.
     You can also create a new auto attendant without adding an extension number, because an extension number isn't required. You can edit or remove an existing extension number. To edit an existing extension number, click **Edit**. To remove an existing extension number from the list, click **Remove**.
   - **Create auto attendant as enabled** Select this option to enable the auto attendant to answer incoming calls when you complete the New UM Auto Attendant wizard. By default, a new auto attendant is created as disabled.
     If you decide to create the UM auto attendant as disabled, you can use the EMC or the Shell to enable the auto attendant after you finish the wizard.

- **Create auto attendant as speech-enabled** Select this check box to speech-enable the UM auto attendant. When you speech-enable the auto attendant, callers will be able to respond to the system or custom prompts used by the UM auto attendant using touchtone or voice inputs. By default, the auto attendant won't be speech-enabled when it's created.
  For callers to use a speech-enabled auto attendant, you must install the appropriate Unified Messaging language pack that contains Automatic Speech Recognition (ASR) support and configure the properties of the auto attendant to use this language.

5. On the **Completion** page, confirm whether the UM auto attendant was successfully created:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to complete the New UM Auto Attendant wizard.

Use the Shell to create a new UM auto attendant
You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example creates a UM auto attendant named `MyUMAutoAttendant` that can accept incoming calls but isn't speech-enabled.

```
New-UMAutoAttendant -Name MyUMAutoAttendant -UMDialPlan MyUMDialPlan -PilotIdenti
```

This example creates a speech-enabled UM auto attendant named `MyUMAutoAttendant`.

```
New-UMAutoAttendant -Name MyUMAutoAttendant -UMDialPlan MyUMDialPlan -PilotIdenti
```

For more information about syntax and parameters, see New-UMAutoAttendant.

After you've created a non-speech-enabled or a speech-enabled auto attendant, you must create and configure key mappings so that the auto attendant can function correctly. If you don't enable key mappings for either business or non-business hours, callers will hear the voice prompts but won't be able to interact with the auto attendant. To create key mappings for an auto attendant, see the following topics:

- Enable Business Hours Key Mappings on a UM Auto Attendant
- Enable Non-Business Hours Key Mappings on a UM Auto Attendant
- Configure Key Mapping Entries on a UM Auto Attendant

Return to top

Post Deployment Tasks for Unified Messaging

After you complete a new installation of the Unified Messaging server role and have successfully deployed Unified Messaging, you should complete the post-installation tasks. The post-deployment tasks will help you enable users for Unified Messaging, secure your UM deployment, and deploy incoming faxing for UM-enabled users.

Enabling Users for Unified Messaging

After you've deployed your IP gateways or IP PBXs, installed the Unified Messaging server role, and created the Active Directory components for Unified Messaging, you must enable your users for Unified Messaging. For details, Enable a User for Unified Messaging.

Secure Your UM Deployment

You can help increase the level of protection for your network if you correctly plan a UM security strategy and then correctly configure the security settings for UM servers and UM-enabled users.

Mutual TLS for UM

To use mutual TLS to encrypt SIP and Real-time Transport Protocol (RTP) traffic that's sent and received by your Unified Messaging servers, perform the following tasks:

- Run the Exchange Certificate wizard. For details, see Create a New Exchange Certificate.
- Associate the certificate with the UM server.
- Import the required certificates on the IP gateways and the IP PBX and Unified Messaging servers in your organization. To import an Exchange certificate, see Import an Exchange Certificate.
- Configure VoIP security on the UM dial plans. For details, see Configure VoIP Security on a UM Dial Plan.
- Configure the startup mode on the Unified Messaging server. For details, see Configure the Startup Mode on a UM Server.
- Configure the UM IP gateways to listen on port 5061. For details, see Configure the TCP Listening Port on a UM IP Gateway.

For more information about VoIP security with Unified Messaging, see Understanding Unified Messaging VoIP Security.

PIN Policies for UM-enabled Users

In Exchange 2010 Unified Messaging, PIN policies are defined and configured on a UM mailbox policy. Multiple UM mailbox policies can be created, depending on your requirements. When you enable a user for Exchange 2010 Unified Messaging, you associate the user with an existing UM mailbox policy. The UM PIN policies that are configured on the UM mailbox policy should be based on the security requirements of your organization. For more information about how to configure PIN settings for UM-enabled users, see Configuring Security for Unified Messaging Users.

Return to top

Deploying Faxing

Exchange 2010 UM forwards incoming fax calls to a dedicated fax partner solution, which then establishes the fax call with the fax sender and receives the fax on behalf of the UM-enabled user. However, to allow UM-enabled users to receive fax messages in their mailbox, you must first deploy Exchange 2010 Unified Messaging, set up and configure the fax partner server, and then configure the UM dial plans, UM mailbox policies, and UM-enabled users to receive faxes. For details, see Deploy and Configure Incoming Faxing.

Return to top

1.2.2.6.2 Checklist: Deploy a New Exchange 2010 RTM UM Environment

Checklist: Deploy a New Exchange 2010 RTM UM Environment

Planning and Deployment > Deploying Exchange 2010 > Understanding Unified Messaging Deployments >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-05*

Use this checklist to install and deploy Microsoft Exchange Server 2010 Unified Messaging (UM). Before you start working with this checklist, make sure you're familiar with the concepts in:

- Overview of Unified Messaging
- Deploy a New Exchange 2010 RTM UM Environment

For step-by-step guidance about how to upgrade from Microsoft Exchange Server 2007 to Exchange 2010, see Checklist: Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM UM.

Checklist for deploying Exchange 2010 Unified Messaging

Done?	Tasks	Topic
	Deploy and configure the IP gateways, IP PBXs, and PBXs in your organization.	Managing IP Gateways
	Verify that the Exchange server roles other than the Unified Messaging server role have been installed and configured.	Verify an Exchange 2010 Installation
	Install the Unified Messaging server role.	Install the Exchange 2010 Unified Messaging Server Role
	Optional: Install the Unified Messaging language packs you need on the UM servers in your organization.	Install a Unified Messaging Language Pack on a UM Server
	Create the required number of UM dial plans for your organization.	Create a UM Dial Plan
	Configure the UM dial plans in your organization.	View or Configure the Properties of a UM Dial Plan
	Create the required number of UM IP gateways.	Create a UM IP Gateway
	Create the required number of UM hunt groups.	Create a UM Hunt Group
	Add each UM server that has been installed to the appropriate dial plan.	Add a UM Server to a Dial Plan
	Optional: Configuring mutual TLS • Run the Exchange Certificate wizard. • Configure your UM dial plan security setting. • Configure the Startup Mode for each UM server.	• Create a New Exchange Certificate • Configure VoIP Security on a UM Dial Plan • Configure the Startup Mode on a UM Server • Configure a Fully

	• Configure your UM IP gateways to listen on port 5061. • Import your Exchange certificate on each IP gateway or IP PBX.	Qualified Domain Name for a UM IP Gateway • Configure the TCP Listening Port on a UM IP Gateway
	Create the required number of auto attendants.	Create a UM Auto Attendant
	Configure the auto attendants in your organization.	View or Configure the Properties of a UM Auto Attendant
	Create a UM mailbox policy or configure the default UM mailbox policy.	• Create a UM Mailbox Policy • View or Configure the Properties of a UM Mailbox Policy
	Enable users in your organization for Unified Messaging.	Enable a User for Unified Messaging
	Optional: Deploy and configure incoming faxing.	Deploy and Configure Incoming Faxing

Return to top

1.2.2.6.3 Checklist: Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM UM

Checklist: Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM UM

Planning and Deployment > Deploying Exchange 2010 > Understanding Unified Messaging Deployments >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-27*

Use this checklist to upgrade an existing Microsoft Exchange Server 2007 Unified Messaging (UM) environment. Before you start working with this checklist, make sure you're familiar with the concepts in:

- Overview of Unified Messaging
- Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging

Note:
For more information about how to perform the tasks that must be completed for Microsoft Office Communications Server 2007, see Office Communications Server and Client Documentation Rollup.

Checklist for upgrading to Exchange 2010 Unified Messaging

Done?	Tasks	Topic
	Verify that you have deployed or upgraded	Verify an Exchange 2010 Installation

	the Client Access, Mailbox, and Hub Transport servers in your organization to Exchange Server 2010.	
	Install Exchange 2007 Service Pack 3 (SP3) on all existing Exchange 2007 SP3 servers, including the Unified Messaging servers in your organization.	Download Exchange Server 2007 Service Pack 3 (SP3)
	Install the Exchange 2010 Unified Messaging server role.	Install the Exchange 2010 Unified Messaging Server Role
	Optional: Install the Unified Messaging language packs you need on the UM servers in your organization.	Install a Unified Messaging Language Pack on a UM Server
	Optional: If you're going to have Exchange 2007 SP3 Unified Messaging servers and users with UM-enabled mailboxes on Exchange 2007 SP3 in your Exchange 2010 organization, you'll need to create additional dial plans and UM hunt groups with new pilot numbers. If you're integrating with Communications Server 2007, a new UM SIP URI dial plan is required that has been configured with a new pilot identifier **Note:** You'll need to disable Unified Messaging your users and then re-enable them using the new SIP URI dial plan.	• Create a UM Dial Plan • Create a UM Hunt Group • Managing UM Hunt Groups • Enable a User for Unified Messaging • Disable Unified Messaging for a User
	Add the Exchange 2010 UM servers to the Exchange 2007 SP3 UM dial plan.	Add a UM Server to a Dial Plan
	Import any custom prompts that were created for Exchange 2007 SP3 UM dial plans or auto attendants to	Import-UMPrompt

	Exchange 2010 Unified Messaging.	
	Configure all IP gateways or IP PBXs to send incoming calls to the Exchange 2010 UM servers.	Managing IP Gateways
	Move the Exchange 2007 UM-enabled mailboxes to an Exchange 2010 Mailbox server.	Move Mailboxes from Exchange 2010 Servers to Exchange 2007 Servers
	Remove the Exchange 2007 SP3 Unified Messaging servers from the UM dial plan. **Important:** Only remove the Exchange 2007 SP3 UM servers from the dial plan if there aren't any Exchange 2007 SP3 UM-enabled mailboxes.	Remove a UM Server from a Dial Plan
	Remove the Exchange 2007 SP3 Unified Messaging servers from the Exchange organization. **Important:** Only remove the Exchange 2007 SP3 UM servers from the Exchange organization if there aren't any Exchange 2007 SP3 UM-enabled mailboxes in your organization.	Uninstall the Unified Messaging Server Role in Exchange 2010
	Optional: Deploy and configure incoming faxing.	Deploy and Configure Incoming Faxing

Note:
Exchange 2007 and later versions contain Unified Messaging features. Versions that are earlier than Exchange 2007 SP3 can't be upgraded and require you to deploy an Exchange 2010 organization with all the server roles, including Unified Messaging. For details, see Deploy a New Exchange 2010 RTM UM Environment.

1.2.2.6.4 Install or Upgrade to Exchange 2010 SP2 Unified Messaging

Install or Upgrade to Exchange 2010 SP2 Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-14*

You can deploy Exchange Server 2010 Service Pack 2 (SP2) on your Unified Messaging servers by performing a clean installation of Exchange 2010 SP2, by upgrading from Exchange Server 2007 SP3 to Exchange 2010 SP2, or by upgrading from the RTM or SP1 version of Exchange 2010 to Exchange 2010 SP2.

Upgrading Exchange Unified Messaging Servers to SP2

There are several steps that you must complete to correctly install or upgrade your Exchange Unified Messaging (UM) servers. However, different steps are required depending on the method you're using to deploy Exchange 2010 SP2 on your UM servers. These methods include:

- **A clean installation** You perform a clean installation of the operating system and then install Exchange 2010 SP2 on new hardware. For the steps to perform a clean installation, see Checklist: Install Exchange Server 2010 SP2 on a New UM Server.
- **Upgrading from Exchange 2007 SP3 Unified Messaging** You upgrade an existing Unified Messaging server running Exchange 2007 SP3 to Exchange 2010 SP2. For the steps to upgrade, see Checklist: Upgrade UM from Exchange 2007 SP3 to Exchange 2010 SP2.
- **Upgrading from Exchange 2010 Unified Messaging RTM or SP1** You upgrade an existing Unified Messaging server running the RTM or the SP1 version of Exchange 2010 to Exchange 2010 SP2 Unified Messaging. For the steps to upgrade, see Checklist: Upgrade UM from Exchange 2010 RTM or SP1 to Exchange 2010 SP2.

Performing a Clean Installation of Exchange 2010 SP2

The following steps are required to perform a clean installation of Exchange 2010 SP2 on a new Unified Messaging server.

Step 1: Prerequisites

Starting with Exchange 2010 SP1, the Unified Messaging server role relied on Unified Communications Managed API v. 2.0 (UCMA) for its underlying SIP signaling and speech processing. The UCMA platform, along with its prerequisites, must be installed on the UM server before you install or upgrade UM to Exchange 2010 SP2. If any of the prerequisites are missing from the server, Exchange 2010 SP2 Setup will inform you that the component is missing and provide you with a download link so you can download and install it. Then you can continue by restarting Setup for SP2.

The Unified Messaging server role in Exchange 2010 SP2 relies on the following components and requires that they be installed prior to installing SP2:

- Windows Server 2008 or Windows Server 2008 R2 - Installing Windows Server 2008 R2
- Microsoft .NET Framework 3.5 Service Pack 1 (SP1) - Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 updates - Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64
- Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu) - Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0)
- Microsoft Speech Platform - Server Runtime (Version 10.1) (SpeechPlatformRuntime.msi)
- Unified Communications Managed API 2.0, Core Runtime (64-bit) (UcmaRuntimeWebDownloadX64.msi)

Note:
If you've already installed a version of the Unified Communications Managed API v. 2.0 on a Client Access server in your Exchange organization, you must also install a hotfix. For information about how to install the required hotfix, see OCS 2007 R2 Web Service Provider Hotfix KB 981256.

For more information about UCMA, see UCMA 2.0 Core Architecture or Overview of Unified Messaging.

Step 2: Download and Install Exchange 2010 SP2

You can download and install Exchange 2010 SP2 on each server or install SP2 from the Exchange 2010 SP2 DVD. Either way, you use the Microsoft Exchange Server 2010 Service Pack 2 Setup wizard to install Exchange 2010 SP2.

- To download and install Exchange 2010 SP2 from the Web, see Exchange Server 2010 SP2.
- To install Exchange 2010 from the Exchange 2010 SP2 DVD, see Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3.

Step 3: Download and Install the Exchange 2010 SP2 UM Language Packs

Exchange Unified Messaging language packs are version-specific and platform-specific. Since Exchange 2007, there have been separate releases for UM language packs, including the RTM version of Exchange 2007, Exchange 2007 SP1, SP2, and SP3, the RTM version of Exchange 2010, and Exchange 2010 SP1 and SP2. For some of these versions, both 32-bit and 64-bit downloads are available, but for other releases only 64-bit downloads are available.

It's very important that you install the correct version and platform of the UM language packs on a UM server. Don't install UM language packs on a Unified Messaging server that's running an earlier version of Exchange or that's designed for a 32-bit platform.

The last task to perform when you upgrade is to download and install the required Unified Messaging SP2 language packs that you need on the UM servers in your organization. Make sure to install each UM language pack on each UM server and to set the default language on all dial plans that the UM server is associated with. Setting the default language makes that language available to users. Each UM language pack is bundled in a single .exe file. To download the SP2 UM language packs, see Exchange Server 2010 SP2 UM Language Packs.

Important:
To ensure that all Unified Messaging features are available in the UM language packs you install, you must install the Exchange 2010 Client and Server Language Pack on each UM server in the dial plan. If you don’t install the Client and Server Language Pack, some features may not work as expected. Some features, like Voice Mail Preview, will work in the language that's configured on the dial plan, but when only the UM language pack is installed. However, features like Outlook Voice Access and user interface text won’t work in the language chosen by the user without having both the UM language pack and the Client and Server Language Pack installed. The language pack bundle for Exchange Server 2010 Service Pack 2 (SP2) is integrated into the download for Exchange 2010 SP2. To download SP2 for Exchange 2010, see Microsoft Exchange Server 2010 Service Pack 2 (SP2). However, the language pack bundle for Exchange 2010 SP1 is still available. To download and install the additional Exchange 2010 SP1 client and server language packs on servers in your organization, see the Microsoft Exchange Server 2010 SP1 Language Pack Bundle.

Step 4: Add the UM Server to a UM Dial Plan

After you install the Unified Messaging server, it's in an enabled state. However, before the UM server can answer and process incoming calls, you must add the UM server to a UM dial plan. You can add an Exchange 2010 SP2 UM server to one or more UM dial plans that have different security settings at the same time. For more information, see Add a UM

Server to a Dial Plan.

Upgrading Unified Messaging from Exchange 2007 SP3

The following steps are required to perform an upgrade on a Unified Messaging server that has Exchange 2007 SP3 installed to an Exchange 2010 SP2 Unified Messaging server.

Step 1: Verify Installation of Exchange 2010 Servers

Verify that you've deployed or upgraded the Client Access, Mailbox, and Hub Transport servers in your organization to Exchange 2010. For details, see Verify an Exchange 2010 Installation.

Step 2: Disable Call Answering

While you're upgrading the UM server running Exchange 2007 SP3, you don't want it to be able to answering incoming calls. Perform one of the following two tasks to prevent the UM server from answering incoming calls:

- **Disable Unified Messaging** For information about how to do this, see How to Disable Unified Messaging on Exchange 2007.
- **Remove the UM server from a dial plan** For information about how to do this, see How to Remove a Unified Messaging Server from a Dial Plan.

Step 3: Remove Any UM Language Packs

Unified Messaging language packs make it possible for Exchange 2007 and Exchange 2010 UM servers to speak additional languages to callers and recognize languages other than US English (en-US) when callers use Automatic Speech Recognition (ASR) or when voice messages are transcribed. Several UM language packs are available for Exchange 2010 SP2.

After you install the Unified Messaging sever role, only the en-US UM language pack is available. If you've installed other UM language packs in addition to the en-US language pack on any UM server, you must first remove all Exchange 2007 UM language packs except the en-US language pack (because it can't be removed). You must do this because of the differences between the speech services platform included with Exchange 2007 and the platform used for speech services and SIP signaling in Exchange 2010 SP2. For more information about the new UM language packs that are available, see New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1.

To check which UM language packs are installed, run one of the following commands.

- To see a list of all the language packs that are installed on a specific UM dial plan, run:

```
Get-UMDialPlan identity MyUMDialPlan |FormatList
```

- To see a list of all the UM language packs installed on a single UM server, run:

```
Get-UMServer -identity MyUMServer |FormatList
```

For more information about how to remove a language pack from a UM server, see How to Remove a Unified Messaging Language Pack from a Unified Messaging Server.

After you've removed all the language packs, install the Exchange 2010 SP2 version. For details, see Upgrade Exchange 2010 UM Language Packs from RTM or SP1 to Exchange 2010 SP2.

Important:

If you have multiple UM dial plans in your organization, we recommend that you remove all UM language packs from each of the UM servers that are associated with a single dial plan. After you remove these language packs, you can install the prerequisites and Exchange 2010 SP2 and then install the SP2 UM language packs on each UM server.

Step 4: Prerequisites

Starting with Exchange 2010 SP1, the Unified Messaging server role relied on Unified Communications Managed API v. 2.0 (UCMA) for its underlying SIP signaling and speech processing. The UCMA platform, along with its prerequisites, must be installed on the UM server before you install or upgrade UM to Exchange 2010 SP2. If any prerequisite is missing from the server, Exchange 2010 Setup will inform you that the component is missing and provide you with a link so you can download and install it. Then you can continue by restarting Setup for Exchange 2010 SP2.

The Unified Messaging server role in Exchange 2010 SP2 relies on the following components, and requires that they be installed prior to installing SP2:

- Windows Server 2008 or Windows Server 2008 R2 - Installing Windows Server 2008 R2
- Microsoft .NET Framework 3.5 Service Pack 1 (SP1) - Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 updates - Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64
- Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu) - For more information, see Microsoft Knowledge Base article 968930, Windows Management Framework core package (Windows PowerShell 2.0 and WinRM 2.0).
- Microsoft Speech Platform - Server Runtime (Version 10.1) (SpeechPlatformRuntime.msi)
- Unified Communications Managed API 2.0, Core Runtime (64-bit) (UcmaRuntimeWebDownloadX64.msi)

Note:

If you've already installed a version of the Unified Communications Managed API v. 2.0 on a Client Access server in your Exchange organization, you must also install a hotfix. For information about how to install the required hotfix, see OCS 2007 R2 Web Service Provider Hotfix KB 981256.

For more information about UCMA, see UCMA 2.0 Core Architecture or Overview of Unified Messaging.

Step 5: Download and Install Exchange 2010 SP2

After you've removed the Exchange 2010 RTM UM language packs from the UM servers, you can download and install Exchange 2010 SP2 on each UM server. You use the Microsoft Exchange Server 2010 Service Pack 2 Setup wizard to install Exchange 2010 SP2.

- For more information about Exchange 2010 SP2 and to download it, see Exchange Server 2010 SP2.
- For more information about how to install Exchange 2010 SP2, see Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3.

Step 6: Download and Install the SP2 UM Language Packs

Exchange Unified Messaging language packs are version-specific and platform-specific. Since the original release of Exchange 2007, there have been separate releases for UM language packs, including Exchange 2007 RTM, Exchange 2007 SP1, SP2, and SP3, Exchange 2010 RTM, and Exchange 2010 SP1 and SP2. For some of these versions, both 32-bit and 64-bit downloads are available, but for other releases only 64-bit downloads are available.

It's very important that you install the correct version and platform of the UM language packs on a UM server. Don't install UM language packs on a Unified Messaging server that's running an earlier version of Exchange or that's designed for a 32-bit platform.

The last task to perform when you upgrade is to download and install the required Unified Messaging SP2 language packs that you need on the UM servers in your organization.

Make sure to install each UM language pack on each UM server and to set the default language on all dial plans that the UM server is associated with. Setting the default language makes that language available to users. Each UM language pack is bundled in a single .exe file. To download the Exchange 2010 SP2 UM language packs, see Exchange Server 2010 SP2 UM Language Packs.

To ensure that all Unified Messaging features are available in the UM language packs you install, you must install the Exchange 2010 Client and Server Language Pack on each UM server in the dial plan. If you don't install the Client and Server Language Pack, some features may not work as expected. Some features, like Voice Mail Preview, will work in the language that's configured on the dial plan but when only the UM language pack is installed. However, features like Outlook Voice Access and user interface text won't work in the language selected by the user without having both the UM language pack and the Client and Server Language Pack installed. The language pack bundle for Exchange Server 2010 Service Pack 2 (SP2) is integrated into the download for Exchange 2010 SP2. To download SP2 for Exchange 2010, see Microsoft Exchange Server 2010 Service Pack 2 (SP2). However, the language pack bundle for Exchange 2010 SP1 is still available. To download and install the additional Exchange 2010 SP1 client and server language packs on servers in your organization, see the Microsoft Exchange Server 2010 SP1 Language Pack Bundle.

Step 7: Add the UM Server to a UM Dial Plan

After you install the Unified Messaging (UM) server, it's in an enabled state. However, before the UM server can answer and process incoming calls, you must add the UM server to a UM dial plan. You can add an Exchange 2010 SP2 UM server to one or more UM dial plans that have different security settings at the same time. For more information, see Add a UM Server to a Dial Plan.

Upgrading from the RTM or SP1 version of Exchange 2010 to SP2

The following steps are required to upgrade a Unified Messaging server running the RTM or SP1 version of Exchange 2010 to Exchange 2010 SP2.

Step 1: Disable Call Answering

While you're upgrading the UM server running Exchange 2010 RTM or SP1, you don't want it to be able to answering incoming calls. Perform one of the following two tasks to prevent the UM server from answering incoming calls:

- **Disable Unified Messaging** For information about how to do this, see Disable Unified Messaging on Exchange 2010.
- **Remove the UM server from a dial plan** For information about how to do this, see Remove a UM Server from a Dial Plan.

Step 2: Prerequisites

Starting with Exchange 2010 SP1, the Unified Messaging server role relied on Unified Communications Managed API v. 2.0 (UCMA) for its underlying SIP signaling and speech processing. The UCMA platform, along with its prerequisites, must be installed on the UM server before you install or upgrade UM to Exchange 2010 SP2. If any prerequisite is missing from the server, Exchange 2010 Setup will inform you that the component is missing and provide you with a link so you can download and install it. Then you can continue by restarting Setup for Exchange 2010 SP2.

The Unified Messaging server role in Exchange 2010 SP2 relies on the following, and requires that they be installed prior to installing SP2:

- Windows Server 2008 or Windows Server 2008 R2 - Installing Windows Server 2008 R2
- Microsoft .NET Framework 3.5 Service Pack 1 (SP1) - Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 updates - Microsoft .NET Framework 3.5 Family

Update for Windows Vista x64, and Windows Server 2008 x64

- Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu) - For more information, see Microsoft Knowledge Base article 968930, Windows Management Framework core package (Windows PowerShell 2.0 and WinRM 2.0).
- Microsoft Speech Platform - Server Runtime (Version 10.1) (SpeechPlatformRuntime.msi)
- Unified Communications Managed API 2.0, Core Runtime (64-bit) (UcmaRuntimeWebDownloadX64.msi)

Note:
If you've already installed a version of the Unified Communications Managed API v. 2.0 on a Client Access server in your Exchange organization, you must also install a hotfix. For information about how to install the required hotfix, see OCS 2007 R2 Web Service Provider Hotfix KB 981256.

For more information about UCMA, see UCMA 2.0 Core Architecture or Overview of Unified Messaging.

Step 3: Remove any RTM or SP1 UM Language Packs

Unified Messaging language packs make it possible for Exchange 2007 and Exchange 2010 UM servers to speak additional languages to callers and recognize languages other than US English (en-US) when callers use Automatic Speech Recognition (ASR) or when voice messages are transcribed. Several UM language packs are available for Exchange 2010 SP2. For more information about the new UM language packs that are available, see New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1.

After you install the Unified Messaging sever role, only the en-US UM language pack is available. If you've installed other UM language packs in addition to the en-US language pack on any UM server, you must first remove all Exchange 2010 RTM or SP1 UM language packs except the en-US language pack (because it can't be removed). You must do this because of the differences between the speech services platform included with Exchange 2007 SP3 and Exchange 2010 RTM and SP1 and the platform used for speech services and SIP signaling in Exchange 2010 SP2.

To check which UM language packs are installed, run one of the following commands.

- To see a list of all the language packs that are installed on a specific UM dial plan, run:

```
Get-UMDialPlan identity MyUMDialPlan |FormatList
```

- To see a list of all the UM language packs installed on a single UM server, run:

```
Get-UMServer -identity MyUMServer |FormatList
```

For more information about how to remove a language pack from a UM server, see Remove a Unified Messaging Language Pack from a UM Server.

After you've removed all the language packs, install the Exchange 2010 SP2 version. For details, see Upgrade Exchange 2010 UM Language Packs from RTM or SP1 to Exchange 2010 SP2.

Important:
If you have multiple UM dial plans in your organization, we recommend that you remove all UM language packs from each of the UM servers that are associated with a single dial plan. After you remove these language packs, you can install the prerequisites and Exchange 2010 SP2 and then install the SP2 UM language packs on each UM server.

Step 4: Download and Install Service Pack 2

After you've removed the Exchange 2010 RTM UM language packs from the UM servers,

you can download and install Exchange 2010 SP2 on each UM server. You use the Microsoft Exchange Server 2010 Service Pack 2 Setup wizard to install Exchange 2010 SP2.

- For more information about Exchange 2010 SP2 and to download it, see Exchange Server 2010 SP2.
- For more information about how to install Exchange 2010 SP2, see Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3.

Step 5: Download and Install the SP2 UM Language Packs

Exchange Unified Messaging language packs are version-specific and platform-specific. Since Exchange 2007, there have been separate releases for UM language packs, including Exchange 2007 RTM, Exchange 2007 SP1, SP2, and SP3, Exchange 2010 RTM, and Exchange 2010 SP1 and SP2. For some of these versions, both 32-bit and 64-bit downloads are available, but for other releases only 64-bit downloads are available.

It's very important that you install the correct version and platform of the UM language packs on a UM server. Don't install UM language packs on a Unified Messaging server that's running an earlier version of Exchange or that's designed for a 32-bit platform.

The last task to perform when you upgrade is to download and install the required Unified Messaging SP2 language packs that you need on the UM servers in your organization. Make sure to install each UM language pack on each UM server and to set the default language on all dial plans that the UM server is associated with. Setting the default language makes that language available to users. Each UM language pack is bundled in a single .exe file. To download the Exchange 2010 SP2 UM language packs, see Exchange Server 2010 SP2 UM Language Packs.

Important:

To ensure that all Unified Messaging features are available in the UM language packs you install, you must install the Exchange 2010 Client and Server Language Pack on each UM server in the dial plan. If you don’t install the Client and Server Language Pack, some features may not work as expected. Some features, like Voice Mail Preview, will work in the language that’s configured on the dial plan but when only the UM language pack is installed. However, features like Outlook Voice Access and user interface text won’t work in the language selected by the user without having both the UM language pack and the Client and Server Language Pack installed. The language pack bundle for Service Pack 2 (SP2) is integrated into the download for Exchange Server 2010 SP2. To download SP2 for Exchange 2010, see Microsoft Exchange Server 2010 Service Pack 2 (SP2). However, the language pack bundle for Exchange 2010 SP1 is still available. To download and install the additional Exchange 2010 SP1 client and server language packs on servers in your organization, see the Microsoft Exchange Server 2010 SP1 Language Pack Bundle.

Step 6: Add the UM Server to a UM Dial Plan

When you install the Unified Messaging (UM) server, it's left in an enabled state. However, before the UM server can answer and process incoming calls, you must add the UM server to a UM dial plan. You can add a Microsoft Exchange Server 2010 SP2 UM server to one or more UM dial plans with different security settings at the same time. For details, see Add a UM Server to a Dial Plan.

1.2.2.6.4.1 Checklist: Install Exchange Server 2010 SP2 on a New UM Server

Checklist: Install Exchange Server 2010 SP2 on a New UM Server

Deploying Exchange 2010 > Understanding Unified Messaging Deployments > Install or Upgrade to Exchange 2010 SP2 Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-09*

Use this checklist to install Microsoft Exchange Server 2010 Service Pack 2 (SP2) on a new Exchange Unified Messaging (UM) server that you're deploying. Before you start to work with this checklist, make sure you're familiar with the concepts in the following topics:

- What's New in Exchange 2010 SP2
- New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1

Checklist for installing Exchange 2010 SP2 on a new UM server

Done?	Tasks	Topic
	Install Windows Server 2008 or a later version.	• Exchange 2010 Prerequisites • Installing Windows Server 2008 R2
	Prerequisites: • Install Microsoft .NET Framework 3.5 Service Pack 1 (SP1). • Install the Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 updates. • Install Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu). • Install the Microsoft Speech Platform - Server Runtime (Version 10.1) (SpeechPlatformRuntime.msi). • Do one of the following: • If you've installed a version of Communications Managed API 2.0 other than the UCMA Core Runtime on a Client Access server in your Exchange organization, you must also install the OCS 2007 R2 Web Service Provider Hotfix KB 981256. • If you haven't installed a version of Communications	• Microsoft .NET Framework 3.5 Service Pack 1 • Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 • Windows Management Framework Core package (Windows PowerShell 2.0 and WinRm 2.0) • Microsoft Speech Platform - Server Runtime (Version 10.1) • OCS 2007 R2 Web Service Provider Hotfix KB 981256 • Unified Communications Managed API 2.0, Core Runtime (64-bit)

	Managed API 2.0 on a Client Access server in your Exchange organization, you must install the Unified Communications Managed API 2.0, Core Runtime (64-bit).	
	Download Exchange 2010 Service Pack 2 (SP2).	Download SP2 for Exchange Server 2010
	Run Setup.exe to install SP2.	Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3
	Download and install the required Exchange 2010 SP2 Unified Messaging language packs on the UM server.	• Exchange Server 2010 SP2 UM Language Packs • Install a Unified Messaging Language Pack on a UM Server
	Add the Unified Messaging server that's running Exchange 2010 SP2 to a UM dial plan.	Add a UM Server to a Dial Plan

1.2.2.6.4.2 Checklist: Upgrade UM from Exchange 2007 SP3 to Exchange 2010 SP2

Checklist: Upgrade UM from Exchange 2007 SP3 to Exchange 2010 SP2

Deploying Exchange 2010 > Understanding Unified Messaging Deployments > Install or Upgrade to Exchange 2010 SP2 Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-27*

Use this checklist to upgrade an existing Unified Messaging (UM) server running Microsoft Exchange Server 2007 SP3 to Exchange Server 2010 Service Pack 2 (SP2). Before you start to work with this checklist, make sure you're familiar with the concepts in the following topics:

Checklist for upgrading a UM server running Exchange 2007 SP3 to Exchange 2010 SP2

Done?	Tasks	Topic
	Verify that you've deployed or upgraded the Client Access, Mailbox, and Hub Transport servers in your organization to Exchange 2010 SP2.	Verify an Exchange 2010 Installation

	Disable call answering on the Exchange 2007 SP3 UM server that's being upgraded.	How to Disable Unified Messaging on Exchange 2007
	Remove the Exchange 2007 SP3 UM server from all UM dial plans.	How to Remove a Unified Messaging Server from a Dial Plan
	Remove any UM language packs that are installed on the UM server that's being upgraded.	How to Remove a Unified Messaging Language Pack from a Unified Messaging Server
	Upgrade or install Windows Server 2008 or Windows Server 2008 R2.	• Exchange 2010 Prerequisites • Installing Windows Server 2008 R2
	Prerequisites: • Install Microsoft .NET Framework 3.5 Service Pack 1 (SP1). • Install the Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 updates. • Install Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu). • Install the Microsoft Speech Platform - Server Runtime (Version 10.1) (SpeechPlatformRuntime.msi). • Do one of the following: • If you have installed a version of Communications Managed API 2.0 other than the UCMA Core Runtime on an Exchange 2010 Client Access server in your Exchange organization, you must also install the OCS 2007 R2 Web Service Provider Hotfix KB 981256. • If you haven't installed a version of Communications Managed API 2.0 on an Exchange 2010 Client Access server in your	• Microsoft .NET Framework 3.5 Service Pack 1 • Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 • Windows Management Framework Core package (Windows PowerShell 2.0 - and WinRM 2.0) • Microsoft Speech Platform - Server Runtime (Version 10.1) • OCS 2007 R2 Web Service Provider Hotfix KB 981256 • Unified Communications Managed API 2.0, Core Runtime (64-bit)

	Exchange 2010 organization, you must install the Unified Communications Managed API 2.0, Core Runtime (64-bit).	
	Download Exchange 2010 SP2.	Download SP2 for Exchange Server 2010.
	Run Setup.exe to install Exchange 2010 SP2.	Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3
	Download and install the required Exchange 2010 SP2 Unified Messaging language packs on the UM server.	• Exchange Server 2010 SP2 UM Language Packs • Install a Unified Messaging Language Pack on a UM Server
	Add the Unified Messaging server that's running Exchange 2010 SP2 to a UM dial plan.	Add a UM Server to a Dial Plan

1.2.2.6.4.3 Checklist: Upgrade UM from Exchange 2010 RTM or SP1 to Exchange 2010 SP2

Checklist: Upgrade UM from Exchange 2010 RTM or SP1 to Exchange 2010 SP2

Deploying Exchange 2010 > Understanding Unified Messaging Deployments > Install or Upgrade to Exchange 2010 SP2 Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-09*

Use this checklist to upgrade an existing Microsoft Exchange Server 2010 Unified Messaging (UM) RTM environment to Exchange 2010 Service Pack 2 (SP2). Before you start to work with this checklist, make sure you're familiar with the concepts in the following topics:

- What's New in Exchange 2010 SP2
- New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1

Checklist for upgrading a UM server from the RTM or SP1 version of Exchange 2010 to SP2

Done?	Tasks	Topic
	Disable call answering on the UM server that's being upgraded.	• Disable Unified Messaging on Exchange 2010 • Remove a UM Server from a Dial Plan

	Prerequisites:
	• Install Microsoft .NET Framework 3.5 Service Pack 1 (SP1).
	• Install the Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 updates.
	• Install Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu).
	• Install the Microsoft Speech Platform - Server Runtime (Version 10.1) (SpeechPlatformRuntime.msi).
	• Do one of the following:
	  • If you've installed a version of Microsoft Unified Communications Managed API 2.0 other than the UCMA Core Runtime on an Exchange 2010 Client Access server in your Exchange organization, you must also install the OCS 2007 R2 Web Service Provider Hotfix KB 981256.
	  • If you haven't installed a version of Unified Communications Managed API 2.0 on an Exchange 2010 Client Access server in your Exchange organization, you must install the Unified Communications Managed API 2.0, Core Runtime (64-bit).
		• Microsoft .NET Framework 3.5 Service Pack 1
		• Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64
		• Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0)
		• Microsoft Speech Platform - Server Runtime (Version 10.1)
		• OCS 2007 R2 Web Service Provider Hotfix KB 981256
		• Unified Communications Managed API 2.0, Core Runtime (64-bit)

	Remove any Exchange 2010 RTM or SP1 UM language packs that are currently installed on UM servers in your organization.	Remove a Unified Messaging Language Pack from a UM Server

	Download Exchange 2010 SP2.	Download SP2 for Exchange Server 2010
	Run Setup.exe to install Exchange 2010 SP2.	Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3
	Download and install the required Exchange 2010 SP2 Unified Messaging language packs on the UM servers in your organization.	Exchange Server 2010 SP2 UM Language Packs Install a Unified Messaging Language Pack on a UM Server Upgrade Exchange 2010 UM Language Packs from RTM or SP1 to Exchange 2010 SP2
	Add the Unified Messaging server that's running Exchange 2010 SP2 to a UM dial plan.	Add a UM Server to a Dial Plan

1.2.2.6.4.4 Upgrade Exchange 2010 UM Language Packs from RTM or SP1 to Exchange 2010 SP2

Upgrade Exchange 2010 UM Language Packs from RTM or SP1 to Exchange 2010 SP2

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-09*

Unified Messaging (UM) language packs enable the Exchange 2010 UM server to speak additional languages to callers and recognize languages other than US English (en-US) when callers use Automatic Speech Recognition (ASR) or when voice messages are transcribed. For more information, see Client Language Support for Unified Messaging.

Upgrading RTM or SP1 UM Language Packs to SP2

When you upgrade an existing Unified Messaging server to Exchange 2010 SP2, there are specific steps you must follow to replace the Exchange 2010 RTM or SP1 UM language packs that are installed on the server with the Exchange 2010 SP2 version of the UM language packs.

To upgrade the UM servers to use UM language packs for Exchange 2010 SP2, follow these steps:

Step 1 Install the prerequisites on the UM servers that you'll be upgrading to SP1. For more information, see Install or Upgrade to Exchange 2010 SP2 Unified Messaging.

Step 2 Determine which RTM or SP1 UM language packs are installed on each UM server that you'll be upgrading. To see which languages are available or installed, use one of the following commands:

- For a list of all available languages per UM dial plan, run:

```
Get-UMDialPlan identity MyUMDialPlan |FormatList
```

- For a list of all available UM languages installed on a single UM server, run:

```
Get-UMServer -identity MyUMServer |FormatList
```

Step 3 Remove all RTM or SP1 UM language packs from the UM servers that you'll be upgrading. For more information, see Remove a Unified Messaging Language Pack from a UM Server.

Step 4 Download Exchange Server 2010 SP2. For more information, see Download SP2 for Exchange Server 2010.

Step 5 Install Exchange 2010 SP2 on the UM servers that you're upgrading. For more information, see Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3.

Step 6 Download Exchange 2010 SP2 UM language packs that you need. For more information, see Exchange Server 2010 UM Language Packs for SP2. You'll have to download the SP2 version of each RTM or SP1 UM language pack that was installed on the UM servers.

Step 7 Install the Exchange 2010 SP2 UM language packs that you downloaded. For more information, see Install a Unified Messaging Language Pack on a UM Server.

Important:

To ensure that all Unified Messaging features are available in the UM language packs you install, install the Exchange 2010 Client and Server Language Pack on each UM server in the dial plan. If you don't install the Client and Server Language Pack, some features may not work as expected. Some features, for example, Voice Mail Preview, will work in a specific language when only the UM language pack is installed. However, features such as Outlook Voice Access and user interface text won't work in a specific language without having both the UM language pack and the Client and Server Language Pack installed. The language pack bundle for Exchange Server 2010 Service Pack 2 (SP2) is integrated into the download for Exchange 2010 SP2. To download SP2 for Exchange 2010, see Microsoft Exchange Server 2010 Service Pack 2 (SP2). However, the language pack bundle for Exchange 2010 SP1 is still available. To download and install the additional Exchange 2010 SP1 client and server language packs on servers in your organization, see the Microsoft Exchange Server 2010 SP1 Language Pack Bundle.

1.2.2.6.5 Deploy and Configure Incoming Faxing

Deploy and Configure Incoming Faxing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-14*

Microsoft Exchange Server 2010 Unified Messaging (UM) relies on certified fax partner solutions for enhanced fax functionality such as outbound fax or fax routing. By default, when you install the Unified Messaging server role, the server isn't configured to allow incoming fax messages to be delivered to a UM-enabled user. Instead, the UM server redirects incoming fax calls to a certified fax partner solution. The fax partner's server receives the fax data and then sends it to the recipient's mailbox in an e-mail message

with the fax included as a .tif attachment.

The Unified Messaging server ensures that the final message delivered to the user is identical to the fax messages generated by Microsoft Exchange Server 2007 Unified Messaging. However, the fax partner solution must meet a set of requirements to interoperate with Exchange 2010 Unified Messaging. For details about the Fax Partner program, see Fax Advisor for Exchange 2010.

Deploying and Configuring Faxing

Exchange 2010 UM forwards incoming fax calls to a dedicated fax partner solution, which then establishes the fax call with the fax sender and receives the fax on behalf of the UM-enabled user. However, to allow UM-enabled users to receive fax messages in their mailbox, you must first run Exchange 2010 Unified Messaging setup and configure the Fax Partner server, and then configure the UM dial plans, UM mailbox policies, and enable UM-enabled users to receive faxes. For details, see Managing Unified Messaging Components.

Step 1: Deploy Unified Messaging

To correctly deploy faxing, you must first successfully deploy Unified Messaging servers in your organization and configure your supported IP gateways to allow faxing. For details about how to deploy UM, see Deploy a New Exchange 2010 RTM UM Environment. For details about how to deploy IP gateways, see Managing IP Gateways.

Important:

Sending and receiving faxes using T.38 or G.711 isn't supported in an environment where Unified Messaging and Microsoft Office Communications Server 2007 are integrated.

Step 2: Configure Fax Partner Servers

You must next install and configure the Fax Partner server or servers in your organization. There are specific steps that you must take to successfully integrate the fax partner server with Exchange 2010 Unified Messaging. For details, see Fax Advisor for Exchange 2010.

Note:

Microsoft Windows firewall ports on the fax partner server must be configured to allow the SIP signaling traffic using either TCP port 5060 or 5061, and also be configured to allow fax data that uses a UDP port range defined by the manufacturer.

Step 3: Enable Faxing on Unified Messaging

There are three components that must be configured correctly for users to be able to receive faxes by using Exchange 2010 Unified Messaging:

- UM dial plans
- UM mailbox policies
- UM mailboxes

Faxing can be enabled or disabled on UM dial plans, UM mailbox policies, or on the UM-enabled user's mailbox. By default, although the user's mailbox allows incoming faxes, you must first enable inbound faxing on the UM mailbox policy that's associated with the UM-enabled user and then enter the fax partner server's URI.

To enable UM-enabled users to receive faxes, you must do the following:

- Verify that each UM dial plan allows the users who are associated with the dial plan to receive faxes. By default, all users who are associated with a dial plan can receive faxes. For UM-enabled users to receive fax messages in their mailbox, each Unified Messaging server that's associated with the dial plan must be configured to accept incoming fax calls. You must also enable fax messages to be received by users who are associated with the dial plan. For more information about how to enable users associated with a dial plan to receive faxes or to prevent them from doing this, see Enable UM-Enabled Users to Receive Faxes on a UM Dial Plan.

Note:
If you prevent fax messages from being received on a dial plan, no users who are associated with the dial plan will be able to receive fax messages, even if you configure an individual user's properties to allow them to receive fax messages. Enabling or disabling faxing on a UM dial plan takes precedence over the settings for an individual UM-enabled user.

- Configure the UM mailbox policy that's associated with the UM-enabled user. The UM mailbox policy must be configured to allow incoming faxes, including the fax partner's URI and the name of the fax partner's server. The *FaxServerURI* must use the following form: sip:*<fax server URI>*:*<port>*;*<transport>*, where "Fax Server URI" is either an FQDN or an IP address of the fax partner server. The "port" is the port on which the fax server listens for incoming fax calls and "transport" is the transport protocol that's used for the incoming fax (UDP, TCP, or TLS). For example, you might configure fax as follows:

```
Set-UMMailboxPolicy MyUMMailboxPolicy -AllowFax $true -FaxServerURI "si
```

  For details, see Enable or Disable Inbound Faxing on a UM Mailbox Policy.
- Verify that the Exchange 2010 mailbox that's UM-enabled can receive fax messages. By default, all users who are associated with a dial plan can receive faxes. However, there may be situations when a user can't receive faxes because the ability to receive faxes has been disabled on their mailbox. For more information about how to enable a UM-enabled user to receive faxes, see Enable a UM-Enabled User to Receive Faxes.
  You can prevent a single user who's associated with a dial plan from receiving fax messages. To do this, configure the properties for the user by using the Exchange Management Console or by using the **Set-UMMailbox** cmdlet in the Exchange Management Shell. You can also use the **Set-UMMailbox** cmdlet to prevent multiple users from receiving fax messages. For more information about how to prevent a user or users from receiving fax messages, see Prevent a UM-Enabled User from Receiving Faxes.

Step 4: Configuring Authentication

In addition to configuring your UM dial plans, UM mailbox policies, and UM-enabled users, you have to configure authentication between the UM server and the fax partner server. The UM server must be able to authenticate the origin of the messages claiming to be coming from the fax partner's server.

Fax messages sent to a UM server from a fax partner server must be authenticated and any unauthenticated messages claiming to have come from a fax partner server will not be processed by the UM server. To authenticate the connection from the fax partner to a UM server, you can use:

- Mutual TLS
- Sender ID validation
- A dedicated receive connector

A receive connector should be sufficient for authenticating the fax partner servers deployed in your organization together with the UM server. The receive connector will ensure that the Exchange server treats all traffic coming from the fax partner server as authenticated.

The receive connector should be deployed on the Hub Transport server used by the fax partner server to submit SMTP fax messages, and must be configured with the following values:

- *AuthMechanism: ExternalAuthoritative*
- *PermissionGroups: ExchangeServers, PartnersFax*
- *RemoteIPRanges: {the fax server's IP address}*
- *RequireTLS: False*

- *EnableAuthGSSAPI: False*
- *LiveCredentialEnabled: False*

For details, see Managing Connectors.

If the fax partner server sends network traffic to a UM server over a public network, for example, a service-based fax partner server hosted in the cloud, we recommend that you authenticate the fax partner server using a sender ID check. This type of authentication ensures that the IP that the fax message came from is, in fact, authorized to send e-mail message on behalf of the fax partner domain that the message claims to have come from. DNS is used to store the sender ID records (or SPF records) and fax partners must publish their SPF records in the DNS forward lookup zone. Exchange 2010 will validate the IP addresses by querying DNS. However, the sender ID agent must be running on an Exchange 2010 Edge server to be able to perform the DNS query.

You can also use TLS to encrypt the network traffic, or mutual TLS for encryption and authentication between the fax partner server and an Exchange 2010 Unified Messaging server. For details, see Understanding Unified Messaging VoIP Security.

1.2.2.6.6 Deploy Unified Messaging and Communications Server 2007 R2

Deploy Unified Messaging and Communications Server 2007 R2

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-13*

Microsoft Exchange Server 2010 Unified Messaging (UM) and Microsoft Office Communications Server 2007 can be deployed together to provide voice messaging, instant messaging, enhanced user presence, audio/video conferencing, and an integrated e-mail and messaging experience for users in your organization. This topic discusses how to configure Exchange 2010 Unified Messaging and Communications Server 2007 to support these features.

Looking for more information about Communications Server 2007? See the reference and Help documentation for Communications Server 2007 in the Office Communications Server and Client Documentation Rollup.

Contents

Deploying Exchange Unified Messaging and Communications Server 2007

Exchange 2010 Unified Messaging combines voice messaging and e-mail messaging into a single messaging infrastructure. Communications Server 2007 Enterprise Voice takes advantage of the Unified Messaging infrastructure to provide voice mail, subscriber

access, call notification, and auto attendant services.

Before you can implement these services or features, you must do the following:

- Install Communications Server 2007 in the same Active Directory directory service topology as the Unified Messaging servers.
- Deploy the following Exchange 2010 server roles:
  - **Unified Messaging server role** The Unified Messaging server connects Exchange 2010 with Communications Server 2007.
  - **Hub Transport server role** The Hub Transport server routes e-mail messages from the Unified Messaging server to user mailboxes.
  - **Client Access server role** The Client Access server hosts client protocols, such as POP3, IMAP4, HTTPS, Outlook Anywhere (formerly known as RPC over HTTP), the Availability service, and the Autodiscover service. The Client Access server also hosts Exchange Web Services.
  - **Mailbox server role** The Mailbox server hosts user mailboxes.

    For more information about the server roles included in Exchange 2010, see Getting Started With Exchange 2010. For more information about how to install each server role included in Exchange 2010, see Understanding a New Installation of Exchange 2010.
- Install and configure Communications Server 2007 in your organization as follows:
  - Install Communications Server 2007 on servers in your organization.
  - Install a certificate that's valid and signed by a certification authority (CA) on the Communications Server 2007 servers.
  - Make sure that the certificate that you installed on the Communications Server 2007 servers is trusted by the Unified Messaging servers.
  - Confirm that at least one Communications Server 2007 pool object is created during installation.

Certificate Configuration Recommendations

You must have a certificate that's trusted by both the computers running Exchange and Communications Server 2007. In an environment that has Communications Server 2007 and Exchange 2010 Unified Messaging, use the following guidelines for deploying a trusted certificate:

- Import a certificate that's valid and signed by a CA. This should be a trusted third-party commercial certificate or a public key infrastructure (PKI) certificate and should be imported on the Communications Server 2007 computers and the Exchange servers that have the Unified Messaging and Client Access server roles installed.
- The most simple certificate deployment scenario is to import the same third-party commercial or PKI certificate to each Exchange 2010 server that has the following server roles installed: Unified Messaging, Client Access, and Hub Transport. Also, install this trusted certificate on each computer running Communications Server 2007. This will help simplify your certificate deployment and reduce the administrative overhead associated with deploying certificates. However, you must obtain a trusted certificate that supports subject alternative names.

  Note:

  If you use a SIP secured or Secured dial plan, a trusted certificate is required between the Unified Messaging servers and the IP gateways. A trusted certificate is also required if a direct Session Initiation Protocol (SIP) connection is used. If you use a SIP secured or Secured dial plan, you can use the same trusted certificate used between Communications Server 2007 computers and the Unified Messaging, Client Access, and Hub Transport servers.
- Although you can install the Unified Messaging server role and other Exchange 2010 server roles on the same computer, when you deploy Communications

Server 2007, we recommend that you install the Unified Messaging server role on a computer that won't be running other Exchange 2010 server roles. If another server role is installed on the same computer as the Unified Messaging server role, the Microsoft Exchange Unified Messaging service may select the incorrect certificate and be unable to use mutual Transport Layer Security (mutual TLS) to encrypt traffic. This occurs because of limitations with subject alternative names found in certificates.
For example, if you install the Unified Messaging server role first, and then later install the Client Access server role on the same server, the Microsoft Exchange Unified Messaging service will use the certificate created by the Client Access server role instead of the certificate created when the Unified Messaging server role was installed. This is because the Microsoft Exchange Unified Messaging service looks for the certificate in the trusted root store that has the most time left before it will expire.

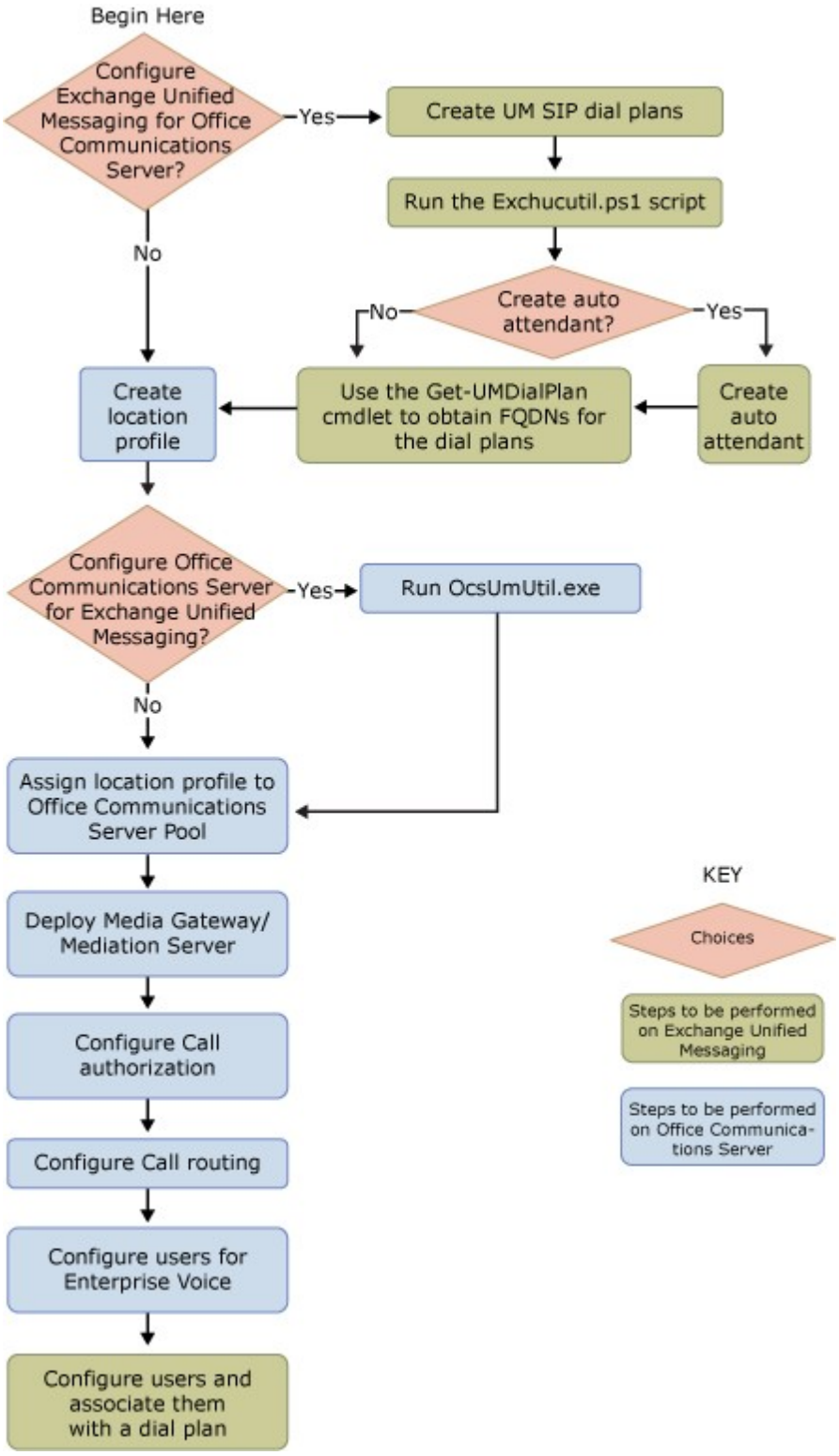
- Because the trusted certificate uses mutual TLS to establish an encrypted channel with Communications Server 2007 and with Client Access, Hub Transport, and Unified Messaging servers, the name on the certificate used during mutual TLS negotiation must match the fully qualified domain name (FQDN) of the server that presents the certificate.

Return to top

Deployment Path

After you install the required server roles in your Exchange 2010 organization, there's a recommended sequence of steps that you must perform on the Exchange Unified Messaging environment and in your Communications Server 2007 environment to correctly deploy Enterprise Voice and Exchange 2010 Unified Messaging. Exchange 2010 Unified Messaging is used to provide call answering, Outlook Voice Access, and auto attendant services. Communications Server 2007 enables more advanced features found in Enterprise Voice services. The following figure illustrates the recommended deployment path for implementing Enterprise Voice services found with Exchange 2010 Unified Messaging and Communications Server 2007.

Deploying Exchange 2010 Unified Messaging and Communications Server 2007



For more information about Communications Server 2007 and to download the reference and Help documentation for Communications Server 2007, see Office Communications Server and Client Documentation Rollup.

There are several steps that you must complete to configure Exchange 2010 Unified Messaging to work with Enterprise Voice in Communications Server 2007. You must do the following:

1. Create one or more Exchange 2010 Unified Messaging SIP Uniform Resource Identifier (URI) dial plans that each map to a corresponding Communications Server 2007 location profile. An Enterprise Voice location profile must be created for each Exchange UM dial plan. You can use the **Get-UMDialPlan** cmdlet to obtain the FQDN of a SIP URI dial plan. For more information about how to create a SIP URI dial plan, see Create a UM Dial Plan.

   Important:
   When you are integrating Exchange Unified Messaging and Office Communications Server, you'll probably find it unnecessary to configure dialing rules or dialing rule groups in Exchange Unified Messaging. Office Communications Server is designed to perform call routing and number translation for users in your organization, and will also do this when the calls are made by Exchange Unified Messaging on behalf of users.

2. Install a certificate on the Unified Messaging servers that's valid and signed by a CA, and then restart the Microsoft Exchange Unified Messaging service on each Unified Messaging server.
3. Encrypt the Voice over IP (VoIP) traffic by configuring the SIP URI dial plan as SIP secured or Secured. For more information about how to configure the security settings on a UM dial plan, see Configure VoIP Security on a UM Dial Plan. For more information about VoIP security and configuring mutual TLS, see Understanding Unified Messaging VoIP Security.
   Although a UM dial plan can be configured as SIP secured or Secured, we recommend that you configure the dial plan as Secured to enable Microsoft Office Communicator 2007 Phone Edition devices to work correctly. This is recommended because of the default encryption level settings configured in Communications Server 2007. A Communicator Phone Edition device will only work if the encryption settings are configured as shown in the following table. This table shows the relationship between the encryption settings for both Communications Server 2007 and UM dial plans.
   Encryption settings for Communicator Phone Edition

Communications Server 2007	UM dial plan
Encryption required (default)	Secured
Encryption optional	SIP secured/secured
No encryption	SIP secured

4. Add the servers running the Unified Messaging server role to the SIP dial plan. To enable the server to answer incoming calls, you must add the Unified Messaging server to a dial plan. For more information about how to add a Unified Messaging server to a dial plan, see Add a UM Server to a Dial Plan.
5. Create a SIP address for the users who will use Enterprise Voice. For more information about how to create a SIP address for a UM-enabled user, see Enable a User for Unified Messaging. Or if you want to change the SIP address for a UM-enabled user, see Modify a SIP Address for a UM-Enabled User.

   Important:
   Users who are associated with a SIP URI dial plan cannot receive incoming faxes. This is because incoming voice and fax calls are routed through a mediation server and faxing isn't supported when using a mediation server.

6. Open the Exchange Management Shell and run the exchucutil.ps1 script located in the <Exchange Installation folder>\Exchange Server\Script folder. The exchucutil.ps1 script does the following:
   - Grants Communications Server 2007 permission to read Exchange UM Active Directory objects, specifically, the SIP URI dial plan objects created in

the previous task. For more information about how to configure permissions on Active Directory objects, see How to Use ADSI Edit to Apply Permissions.

- Creates a UM IP gateway in Active Directory for each Communications Server 2007 pool or for each server running Communications Server 2007 Standard Edition that hosts users who are enabled for Enterprise Voice. For more information about how to create a UM IP gateway, see Create a UM IP Gateway.
- Creates an Exchange UM hunt group for each IP gateway. The hunt group pilot identifier will be the name of the dial plan associated with the corresponding gateway. The hunt group must specify the Exchange 2010 Unified Messaging SIP dial plan used with the UM IP gateway. For more information about how to create a UM hunt group, see Create a UM Hunt Group.

Return to top

You must also complete the following tasks to configure Communications Server 2007 to work with Exchange 2010 Unified Messaging:

- Create location profiles. The location profile name must match the FQDN of the corresponding UM dial plans.
- Assign location profiles to Communications Server 2007 pools.
- Deploy and configure media gateways and mediation servers.
- Define telephone usages, voice policies, and outbound call routes.
- Configure the users for Enterprise Voice services.
- Run the **ocsumutil.exe** command that creates the contact objects for subscriber access and for the auto attendant. It also validates that there's a location profile name that matches the FQDN of the Exchange UM dial plan.

Note:

When you install Communications Server 2007, the **msRTC-SIPLine** attribute is added to Active Directory. If you haven't installed Communications Server 2007 in your environment, this attribute isn't added to Active Directory, and caller ID name resolution across dial plans in a single forest and in cross-forest scenarios won't work correctly unless you configure Unified Messaging proxy addresses for users who aren't UM-enabled.

For more information about how to perform the tasks that must be completed for Communications Server 2007, see Office Communications Server and Client Documentation Rollup.

After you configure the Communications Server 2007 and the Unified Messaging servers, you must enable the user to use Communications Server 2007 and install Communicator on the user's client computer.

Important:

Sending and receiving faxes using T.38 or G.711 isn't supported in an environment when Unified Messaging and Office Communications Server are integrated.

Return to top

For More Information

Office Communications Server and Client Documentation Rollup

Checklist: Deploy Office Communications Server 2007 R2 and Exchange 2010 Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-30*

Use this checklist to install and deploy Microsoft Exchange Server 2010 Unified Messaging (UM) and Microsoft Office Communications Server 2007. Before you start working with this checklist, make sure you're familiar with the concepts in:

- Overview of Unified Messaging
- Deploy a New Exchange 2010 RTM UM Environment

For more information about how to perform the tasks that must be completed for Communications Server 2007, see Office Communications Server and Client Documentation Rollup.

For step-by-step guidance about how to upgrade from Microsoft Exchange Server 2007 to Exchange 2010, see Checklist: Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM UM.

Checklist for deploying Office Communications Server and Exchange 2010 Unified Messaging

Done?	Tasks	Topic
	Verify that the Exchange 2010 server roles other than the Unified Messaging server role have been installed and configured.	Verify an Exchange 2010 Installation
	Install Communications Server 2007.	Next Steps: Starting Deployment
	Install the Unified Messaging server role.	Install the Exchange 2010 Unified Messaging Server Role
	Optional: Install the Unified Messaging language packs you need on the UM servers in your organization.	Install a Unified Messaging Language Pack on a UM Server
	Configure the Startup Mode for each UM server.	Configure the Startup Mode on a UM Server
	Run the Exchange Certificate wizard.	Create a New Exchange Certificate
	Import a trusted certificate on each	Configuring Certificates on the Server Running Microsoft Exchange Server

	Communications Server 2007 server.	2007 Unified Messaging
	Create the number of SIP URI dial plans required for your organization.	Create a UM Dial Plan
	Configure the SIP URI dial plans in your organization.	View or Configure the Properties of a UM Dial Plan
	Add each UM server that has been installed to the appropriate dial plan.	Add a UM Server to a Dial Plan
	Configure your UM dial plan security setting.	Configure VoIP Security on a UM Dial Plan
	Create the required number of auto attendants.	Create a UM Auto Attendant
	Configure the auto attendants in your organization.	View or Configure the Properties of a UM Auto Attendant
	Run the ExchUcUtil.ps1 script.	Step 1. Configure Unified Messaging on Microsoft Exchange to Work with Office Communications Server **Note:** The ExchUcUtil.ps1 script is located in the *<Program Files>*\Microsoft\Exchange Server\V14\Scripts folder.
	Create and assign a location profile to the Communications Server 2007 pool.	Step 2. Create Location Profiles
	Run OcsUmUtil.exe.	Step 3. Configure Communications Server to Work with Unified Messaging on Microsoft Exchange Server
	Create and assign a location profile to the Communications Server pool.	Step 4. Assign Location Profile to Pool
	Deploy Mediation Server.	Step 5. Deploy a Mediation Server
	Configure call routing. **Important:** If you've integrated Exchange Unified Messaging and Office Communications Server, you'll probably find it unnecessary to configure dialing rules or dialing rule groups in Exchange	Step 7. Configure Outbound Call Routing

	Unified Messaging. Office Communications Server is designed to perform call routing and number translation for users in your organization, and will also do this when the calls are made by Exchange Unified Messaging on behalf of users.	
	Enable users for Enterprise Voice and assign a TEL URI.	Step 8. Enable Users for Enterprise Voice
	Configure users for Enterprise Voice.	Step 10. Configure Per-User Location Profiles
	Create a UM mailbox policy or configure the default UM mailbox policy.	• Create a UM Mailbox Policy • View or Configure the Properties of a UM Mailbox Policy
	Enable users with a SIP address for Unified Messaging in your organization.	Enable a User for Unified Messaging
	Optional: Deploy and configure incoming faxing	Deploy and Configure Incoming Faxing

Important:
Sending and receiving faxes using T.38 or G.711 isn't supported in an environment where Unified Messaging and Communications Server 2007 are integrated.

1.2.2.7 Managing Deployment of Exchange 2010

Managing Deployment of Exchange 2010

Exchange Server 2010 > Planning and Deployment > Deploying Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-28*

Configure Edge Transport Server Using Cloned Configuration

Create Additional Routing Group Connectors from Exchange 2010 to Exchange 2003

Deploy the Edge Transport Server Role in an Existing Exchange 2003 Organization Before Upgrading to Exchange 2010

Install Exchange Server 2010

Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3

Install Exchange 2010 in an Existing Exchange 2003 Organization

Install Exchange 2010 in an Existing Exchange 2007 Organization

Install Exchange 2010 in a Mixed Exchange 2003 and Exchange 2007 Organization

Install Exchange 2010 in Unattended Mode

Install the Exchange 2010 Management Tools

Install Exchange 2010 Using the Custom Installation Type

Move Internet Mail Flow from Exchange 2003 to Exchange 2010

Move Mailboxes from Exchange 2003 Servers to Exchange 2010 Servers

Move Mailboxes from Exchange 2007 Servers to Exchange 2010 Servers

Move Mailboxes from Exchange 2010 Servers to Exchange 2003 Servers

Move Mailboxes from Exchange 2010 Servers to Exchange 2007 Servers

Prepare Legacy Exchange 2003 Permissions

Provision Exchange 2010 Server and Delegate Setup

Suppress Link State Updates

Upgrade Custom LDAP Filters to OPATH Filters

1.2.2.7.1 Create Additional Routing Group Connectors from Exchange 2010 to Exchange 2003

Create Additional Routing Group Connectors from Exchange 2010 to Exchange 2003

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Exchange Management Shell to configure routing group connectors between the default routing group in Microsoft Exchange Server 2010 and Exchange Server 2003 routing groups.

The first routing group connector between Exchange 2010 and Exchange 2003 is created and configured during installation of the first Hub Transport server role in an existing Exchange organization. Perform this procedure if you have planned your routing topology and decided to create additional connectors between Exchange versions.

Important:

You can't use Exchange System Manager in Exchange 2003 to manage the Exchange 2010 routing group or any routing group connectors that include an Exchange 2010 Hub Transport server as either a source server or target server.

To learn more about routing group connectors between Exchange 2010 and Exchange 2003, see Upgrade from Exchange 2003 Transport.

Prerequisites

Suppress minor link state updates on all Exchange 2003 servers. For more information about how to suppress link state updates, see the "Link State Updates in a Coexistence Environment" section in Upgrade from Exchange 2003 Transport.

Use the Shell to create a routing group connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Routing group connectors" entry in the Transport Permissions topic.

Note:
You must use the Shell to create and manage routing group connectors. They aren't shown in the EMC.

This example creates reciprocal routing group connectors between the Exchange 2010 routing group and the routing group associated with the specified Exchange 2003 server, assigns a cost of 10 to that connector, and enables public folder referrals.

```
New-RoutingGroupConnector -Name "Interop RGC" -SourceTransportServers "Ex2010Hub1
```


1.2.2.7.2 Deploy the Edge Transport Server Role in an Existing Exchange 2003 Organization Before Upgrading to Exchange 2010

Deploy the Edge Transport Server Role in an Existing Exchange 2003 Organization Before Upgrading to Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Using an Edge Transport server, you can provide anti-spam, antivirus, and transport rules processing for your Exchange organization. You can deploy and configure an Edge Transport server to act as a smart host in the perimeter network of an existing Microsoft Exchange Server 2003 organization before you start upgrading your existing Exchange 2003 servers to Exchange Server 2010. Although it's a better practice to introduce Exchange 2010 into your Exchange 2003 organization and use Edge subscriptions, you may want to start using Edge servers before you start your upgrade. This deployment option may be desirable in the following scenarios:

- You want to start utilizing the benefits of Edge protection before beginning the upgrade of your internal Exchange organization.
- You have multiple sites that won't be upgraded all at the same time, and you want the servers in these sites to send mail directly to the perimeter before they're upgraded.
- You have an Exchange 2010 deployment and your organization merges with or acquires another organization that has Exchange 2003 deployed, and you want to centralize mail flow through your Edge servers.

Note:
In the scenario described in this topic, no computers running Microsoft Exchange Server 2010 have been deployed in the Exchange organization. This limits the available features

on the Edge Transport server because you can't use any of the features that rely on Edge Subscription. The features that rely on Edge Subscription are recipient lookup and safelist aggregation. If you want to create an Edge Subscription, you must deploy at least one Exchange 2010 Hub Transport server in the Exchange organization and configure the organization for coexistence. For more information, see Upgrade from Exchange 2003 Transport.

Looking for other management tasks related to Edge Transport servers? Check out Managing Transport Servers.

Prerequisites

- An Edge Transport server has been deployed in the perimeter network. For detailed steps, see Install Exchange 2010 Using the Custom Installation Type.
- An Edge Transport server has been configured to perform antivirus and anti-spam processing and to apply transport rules. For detailed steps, see Managing Anti-Spam and Antivirus Features and Managing Transport Rules.
- Accepted domains are configured on the Edge Transport server. You need to create an accepted domain entry for each SMTP domain for which the Exchange organization receives e-mail. For detailed steps, see Transport Server Post-Deployment Tasks.
- Verify the configuration of the Domain Name System (DNS) mail exchange (MX) resource record for those domains and make any changes that may be needed so that e-mail to your accepted domains is directed to the Edge Transport server.
- Determine the authentication method that will be used to help secure the connection between the Edge Transport server and the Exchange organization. We recommend that you use Basic authentication over Transport Layer Security (TLS). Alternatively, you can decide to use Externally Secured as your authentication mechanism. This authentication mechanism relies on network security, such as Internet Protocol security (IPsec), to help secure the connection. For more information about the authentication methods that are available, see Securing Transport Servers.

Deploy an Edge Transport server in an Exchange 2003 Organization

For all deployments, you must first create a Send connector from the Edge Transport server to the Internet. Then, configure mail flow as appropriate for your selected authentication method.

Create a Send connector from the Edge Transport server to the Internet

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

Use the New Send Connector wizard in the EMC to create a Send connector on the Edge Transport server with the following settings:

- **Introduction page** In **Select the intended use for this Send connector**, select **Internet**.
- **Address space page** Click **Add**, and in the **SMTP Address Space** dialog, type * (an asterisk).

For detailed steps, see Create an SMTP Send Connector.

Alternatively, you can use the **New-SendConnector** cmdlet to create the connector in the Shell. This example creates the Send connector To Internet, which uses DNS to route messages.

```
New-SendConnector -Name "To Internet" -AddressSpaces * -Usage Internet -DNSRoutin
```

If you use a smart host to route messages to the Internet, you need to use different parameters. This example creates the same Send connector but configures it to use the smart host 10.10.1.1 instead of DNS to route messages.

```
New-SendConnector -Name "To Internet" -AddressSpaces * -Usage Internet -DNSRoutin
```

For detailed syntax and parameter information, see New-SendConnector.

Note:

When you install the Edge Transport server role, a default Receive connector is created that's configured to receive mail from the Internet. Therefore, you don't need to create a Receive connector that corresponds to the Send connector you created in this section.

Configure mail flow between the Edge Transport server and the Exchange 2003 organization using Basic authentication over TLS

The procedures in this section help you configure secured mail flow between the Edge Transport server and the Exchange 2003 organization using Basic authentication over TLS.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

Configure credentials for authenticated mail flow

1. Create the credentials used by the Edge Transport server to authenticate to the Exchange 2003 server. Create a user account in Active Directory that services the Exchange organization. Add the user account to the Exchange Domain Servers security group.

   Important:

   This account is granted the permissions and rights assigned to Exchange servers. Make sure that you safeguard the account credentials to prevent misuse of the account. You can configure the account to enable logon to specific computers only.

2. On the Edge Transport server, create the credentials used by the Exchange 2003 server to authenticate to the Edge Transport server. Create a user account in the Users folder in the Local Users and Groups container on the Edge Transport server.

Configure Exchange 2003 to accept messages from the Edge Transport server

On the Exchange 2003 server or servers that will receive messages from the Edge Transport server, verify that the SMTP virtual server is configured to enable Basic authentication over TLS.

1. Open Exchange System Manager. Expand the **Servers** node. Expand the

desired server. Expand the **Protocols** node. Expand **SMTP**. Right-click **Default SMTP Virtual Server**, and select **Properties**.
2. Click the **Access** tab, and then click **Authentication**.
3. In the **Authentication** dialog box, select **Basic authentication (password is sent in clear text)** and **Requires TLS encryption**. Click **OK**.
4. Click **OK** to close **Default SMTP Virtual Server Properties**.

Create a Send connector from the Edge Transport server to the Exchange 2003 organization

Use the New Send Connector wizard in the EMC to create a Send connector on the Edge Transport server with the following settings:

- **Introduction page** In **Select the intended use for this Send connector**, select **Internal.**
- **Address Space page** Click Add to open the SMTP Address Space dialog. In this dialog, type – in the Address field. This character is a placeholder that represents all authoritative internal relay domains in your accepted domains configuration. Alternatively, you can list each domain as a separate entry. Leave the remaining fields with their default settings and click OK.
- **Network Settings page** In **Route mail through the following smart hosts**, enter the IP address or the fully qualified domain name (FQDN) of the Exchange 2003 bridgehead server that will receive messages from the Edge Transport server. If you configure more than one bridgehead server as a smart host, the connections from the Edge Transport server will be load-balanced between the smart hosts.
- **Configure smart host authentication settings page** Select **Basic Authentication** and **Basic Authentication over TLS**. In the **User name** and **Password** fields, enter the credentials for the user account that you created in the "Configure credentials for authenticated mail flow" section earlier in this topic.
  For detailed steps, see Create an SMTP Send Connector.

Alternatively, you can use the **New-SendConnector** cmdlet to create the connector in the Shell. This example creates the Send connector To Exchange Organization with the required settings and designates the servers 10.10.1.10 and 10.10.1.11 as the Exchange 2003 bridgehead servers that will receive mail from the Edge Transport server.

```
$mycred = get-credential
```

In the dialog box that appears, enter the credentials for the user account you created the "Configure credentials for authenticated mail flow" section. Use the *domain**user* format or user principal name (UPN) format to enter the user name, and then provide the user's password. Click **OK**.

```
New-SendConnector -Name "To Exchange Organization" -Usage Internal -AddressSpaces
```

For detailed syntax and parameter information, see New-SendConnector.

After you create the Send connector, you must grant the permissions required to enable transmission of XExch50 data from the Edge Transport server to the Exchange 2003 server by running this command in the Shell.

```
Add-AdPermission -Identity "To Exchange Organization" -User "NT Authority\Anonymo
```

Create a Receive connector on the Edge Transport server to accept messages from the Exchange 2003 organization

Use the New Receive Connector wizard in the EMC to create a Receive connector on the Edge Transport server with the following settings:

- **Introduction**page In **Select the intended use for this Receive connector**, select **Internal**.
- **Remote network settings page** Delete all network ranges and add the IP addresses of the Exchange 2003 bridgehead servers that will relay messages

to the Edge Transport server

After you create the connector, modify the authentication method by selecting **Basic Authentication** and **Offer Basic authentication only after starting TLS** on the **Authentication** tab of the connector's properties. For detailed steps, see Create an SMTP Receive Connector and Configure Receive Connector Properties.

Alternatively, you can use the **New-ReceiveConnector** cmdlet to create the connector in the Shell. This example creates the Receive connector From Exchange Organization with the required settings and designates that the servers 10.10.1.10 and 10.10.1.11 are the only ones from which the Receive connector will accept messages.

```
New-ReceiveConnector -Name "From Exchange Organization" -Usage Internal -RemoteIP
```

On the Edge Transport server, run this command in the Shell to grant permissions on the new Receive connector to the local user account you created in the "Configure credentials for authenticated mail flow" section.

```
Add-AdPermission -Identity "Receive Connector Name" -User Edge\Contoso -ExtendedR
```

Important:

This account is granted the permissions that enable it to relay messages through the Edge Transport server. Make sure that you safeguard the account credentials to prevent misuse of the account.

Configure Exchange 2003 to send messages to the Edge Transport server

On the Exchange 2003 server, follow these steps to create an SMTP connector configured to relay all Internet e-mail through the Edge Transport server and use Basic authentication over TLS to help secure the connection:

1. Open Exchange System Manager. Right-click the **Connectors** container that's located in the routing group where the server that will host this connector resides, select **New**, and then select **SMTP Connector**.

   Note:

   If no routing groups are displayed in Exchange System Manager, right-click the Exchange organization container, select **Properties**, and then select the **Display routing groups** check box.

2. Select the **General** tab. In the **Name** field, type a unique name for the connector.
3. Select **Forward all mail through this connector to the following smart hosts**, and type the IP address or FQDN of the Edge Transport server. If you enter an IP address, it must be enclosed in brackets, for example: [192.168.1.1].
4. Click **Add** to add a local bridgehead server. In the **Add Bridgehead** dialog box, select one or more Exchange 2003 servers.
5. Select the **Address Space** tab, and then click **Add** to create an address space. In the **Add Address Space** dialog box, select **SMTP**, and then click **OK**.
6. On the **Internet Address Space Properties** page, enter *, and then click **OK**.
7. Select the **Advanced** tab, and then click **Outbound Security**. In the **Outbound Security** dialog box, select **Basic Authentication**, and then click **Modify**.
8. In the **Outbound Connection Credentials** dialog box, enter the user name for the local user account that you created on the Edge Transport server, enter the password for the account, and then click **OK**.
9. On the **Outbound Security** dialog box, select **TLS encryption**. Click **OK** to close the **Outbound Security** dialog box. Click **OK**.

Configure mail flow between the Edge Transport server and the Exchange 2003

organization using anonymous access

The procedures in this section help you configure unauthenticated mail flow between the Edge Transport server and the Exchange 2003 organization using anonymous access.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

Configure Exchange 2003 to accept messages from the Edge Transport server

1. On the Exchange 2003 server or servers that will receive messages from the Edge Transport server, verify that the SMTP virtual server is configured to enable Anonymous access:
   a. Open Exchange System Manager. Expand the **Servers** node. Expand the desired server. Expand the **Protocols** node. Expand **SMTP**. Right-click **Default SMTP Virtual Server**, and then select **Properties**.
   b. Click the **Access** tab, and then click **Authentication**.
   c. In the **Authentication** dialog box, select **Anonymous access**. Click **OK**.
2. Configure the relay restriction for the Exchange 2003 server to enable only the Edge Transport server to relay through this virtual server:
   a. On the **Access** tab of **Default SMTP Virtual Server Properties**, click **Relay**.
   b. In the **Relay Restrictions** dialog box, select **Only the list below**, and then click **Add**.
   c. In the **Computer** dialog box, select **Single computer** to specify a single IP address, or select **Group of computers** to specify an IP address range. Click **OK**.
   d. In the **Relay Restrictions** dialog box, verify that the check box **Allow all computers which successfully authenticate to relay, regardless of the list above** is selected. Click **OK**.
   e. Click **OK** to close **Default SMTP Virtual Server Properties**.
3. Follow these steps to modify the registry settings on the Exchange 2003 bridgehead server to enable the Exchange 2003 server to send and receive XExch50 properties anonymously:

   Caution:
   Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

   a. Open Registry Editor.
   b. Locate **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SMTPSVC\XEXCH50**
   c. Right-click **XEXCH50** and select **New | DWORD Value**. Type **SuppressExternal** for the value name. By default, the value data is **0**. This indicates that the XEXCH50 properties are transmitted to the remote server anonymously.
   d. Right-click **XEXCH50** and select **New** | **Key**. Type the number of the SMTP virtual server instance as the key value. For example, the default virtual server instance is **1**, and the second SMTP virtual server created on a server is **2**.
   e. Right-click the key that you just created, point to **New**, and then click **DWORD Value**.
   f. In the details pane, type **Exch50AuthCheckEnabled** for the value name. By default, the value data is **0**. This indicates that the XEXCH50 properties are transmitted when e-mail is sent anonymously.

Create a Send connector from the Edge Transport server to the Exchange 2003 organization

Use the New Send Connector wizard in the EMC to create a Send connector on the Edge Transport server with the following settings:

- **Introduction page** In **Select the intended use for this Send connector**, select **Internal.**
- **Address space**page Type the **--** character, which is a placeholder that represents all authoritative and internal relay domains in your accepted domains configuration. Alternatively, you can list each domain as a separate entry.
- **Network settings**page In **Route mail through the following smart hosts**, enter the IP address or the FQDN of the Exchange 2003 bridgehead server that will receive messages from the Edge Transport server. If you configure more than one bridgehead server as a smart host, the connections from the Edge Transport server will be load-balanced between the smart hosts.
- **Configure smart host authentication settings**page Select **Externally Secured (for example with IPsec)**.
  For detailed steps, see Create an SMTP Send Connector.
  Alternatively, you can use the **New-SendConnector** cmdlet to create the connector in the Shell. This example creates the Send connector To Exchange Organization with the required settings and designates the servers 10.10.1.10 and 10.10.1.11 as the Exchange 2003 bridgehead servers that will receive mail from the Edge Transport server.

```
New-SendConnector -Name "To Exchange Organization" -Usage Internal -Add
```

1. After you create the Send connector, you must grant the permissions required to enable transmission of XExch50 data from the Edge Transport server to the Exchange 2003 server by running this command in the Shell.

```
Add-AdPermission -Identity "To Exchange Organization" -User "NT Author
```

Create a Receive connector on the Edge Transport server to accept messages from the Exchange 2003 organization

Use the New Receive Connector wizard in the EMC to create a Receive connector on the Edge Transport server with the following settings:

- **Introduction**page In **Select the intended use for this Receive connector**, select **Internal.**
- **Remote network settings**page Delete all network ranges and add the IP addresses of the Exchange 2003 bridgehead servers that will relay messages to the Edge Transport server.

After you create the connector, modify the authentication method by selecting **Externally Secured (for example with IPsec)** on the **Authentication** tab of the connector's properties. Clear all other authentication options. For detailed steps, see Create an SMTP Receive Connector and Configure Receive Connector Properties.

Alternatively, you can use the **New-ReceiveConnector** cmdlet to create the connector in the Shell. This example creates the Receive connector From Exchange Organization with the required settings and designates that the servers 10.10.1.10 and 10.10.1.11 are the only ones from which the Receive connector will accept messages.

```
New-ReceiveConnector -Name "From Exchange Organization" -Usage Internal -RemoteIP
```

Important:

If you specify an IP address range instead of specific IP addresses for this Receive connector, it will enable all connections from the specified remote IP address range to relay messages through the Edge Transport server. In this scenario, make sure that a trusted network connection exists between the Edge Transport server and the Exchange

organization.

Configure Exchange 2003 to send messages to the Edge Transport server

On the Exchange 2003 server, follow these steps to create an SMTP connector configured to relay all Internet e-mail through the Edge Transport server:

1. Open Exchange System Manager. Right-click the **Connectors** container located in the routing group where the server that will host this connector resides, select **New**, and then select **SMTP Connector**.

   Note:

   If no routing groups are displayed in Exchange System Manager, right-click the Exchange organization container, select **Properties**, and then select the **Display routing groups** check box.

2. Select the **General** tab. In the **Name** field, type a unique name for the connector.
3. Select **Forward all mail through this connector to the following smart hosts**, and type the IP address or FQDN of the Edge Transport server. If you enter an IP address, it must be enclosed in brackets, for example: [192.168.1.1].
4. Click **Add** to add a local bridgehead server. In the **Add Bridgehead** dialog box, select one or more Exchange 2003 servers.
5. Select the **Address Space** tab, and then click **Add** to create an address space. In the **Add Address Space** dialog box, select **SMTP**, and then click **OK**.
6. On the **Internet Address Space Properties** page, enter *, and then click **OK**.
7. Click **OK** to close the SMTP connector properties page.

1.2.2.7.3 Install Exchange Server 2010

Install Exchange Server 2010

Planning and Deployment > Deploying Exchange 2010 > Managing Deployment of Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-15*

This topic explains how to use the Microsoft Exchange Server 2010 Setup wizard to perform an installation of Exchange 2010. For more information about planning and deploying Exchange 2010, see the following topics:

- Planning for Exchange 2010
- Deploying Exchange 2010

Prerequisite

You must ensure that any server on which you plan to install Exchange 2010 meets the appropriate prerequisites and system requirements before you begin your installation. To understand the prerequisites for all server roles, see Exchange 2010 Prerequisites. For more information about system requirements, see Exchange 2010 System Requirements. For more information about server roles, see Overview of Exchange 2010 Server Roles.

Caution:

After you install Exchange 2010 on a server, you must not change the server name. Renaming a server after you have installed an Exchange 2010 server role is not

supported.

Install Exchange Server 2010

If you're installing the first Exchange 2010 server in the organization, and the Active Directory preparation steps have not been performed, the account you use must have membership in the Enterprise Administrators group. If you haven't previously prepared the Active Directory schema, the account must also be a member of the Schema Admins group. For more information about preparing Active Directory for Exchange 2010, see Prepare Active Directory and Domains. If you have already performed the schema and Active Directory preparation steps, the account you use must be a member of the Delegated Setup management role group or the Organization Management role group.

On the **Start** page, make sure that you've completed **Steps 1** through **3**. If you haven't already installed the components discussed in those steps, Setup will link you to the appropriate sites where you can download the components. For more information about Windows PowerShell installation, see Install Windows Management Framework.

Important:

If you're installing Exchange 2010 on Windows Server 2008 R2, don't use the downloadable .NET Framework package. Instead, use Server Manager in Windows Server 2008 R2 or run **ServerManagerCmd -i NET-Framework**.

For information about Exchange language options, see Exchange 2010 Language Support.

1. The **Introduction** page begins the process of installing Exchange into your organization. It will guide you through the installation. Click **Next** to continue.

2. On the License Agreement page, review the software license terms. If you agree to the terms, select "I accept the terms in the license agreement.", and then click **Next**.

3. On the Error Reporting page, select whether you want to enable or disable the Exchange Error Reporting feature, and then click **Next**.

4. On the **Installation Type** page, select whether you want a typical Exchange Server installation or a custom Exchange Server installation. For Exchange 2010 SP1, you can select to automatically install all required Windows roles and features for this server. You can also click **Browse** to change the specified installation path, and then click **Next**. Note that, if you choose the **Typical Exchange Server Installation** option, the Hub Transport, Client Access, and Mailbox server roles plus the Exchange Management Tools will be installed. You will not be able to install the Unified Messaging server role or Edge Transport server role. You can add additional server roles later if you choose not to install them during this installation. For more information about a custom Exchange installation, see Install Exchange 2010 Using the Custom Installation Type.

   Note:

   For e-mail messages to flow correctly, you must install both the Mailbox server role and the Hub Transport server role in the same Active Directory site. You can also install the Mailbox server role, the Hub Transport server role, the Client Access server role, and the Unified Messaging server role on the same computer or on separate computers.

5. On the **Server Role Selection** page, click **Next**. You can add additional server roles later if you choose not to install them during this installation. The Edge Transport server role can't coexist on the same computer with any other

server role. You must deploy the Edge Transport server role in the perimeter network and outside the Active Directory forest. Also, the Exchange management tools aren't installed by default. Therefore, select **Management Tools** to install the Exchange Management Console and the Exchange cmdlets for the Exchange Management Shell. The management tools are installed automatically if you install any other server role.

Note:
You will not see this page if you choose a typical Exchange installation.

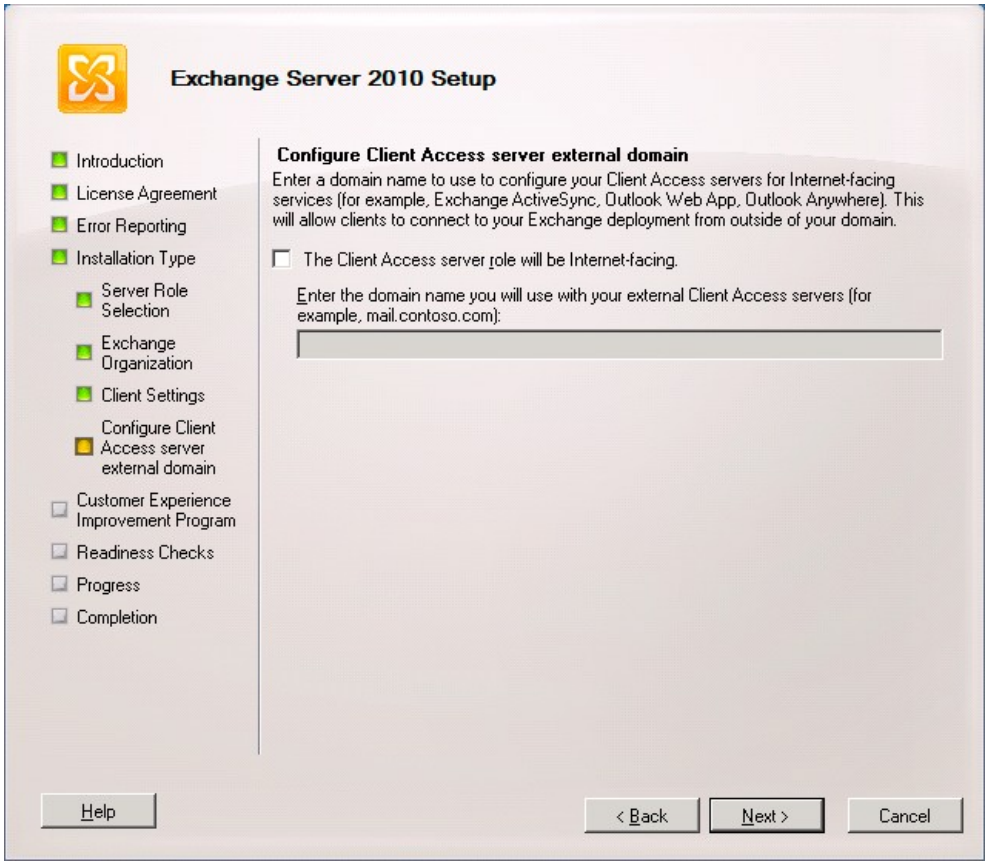
6. If this is the first Exchange server in your organization, on the **Exchange Organization** page, type a name for your Exchange organization. The Exchange organization name can contain only the following characters:
   - A through Z
   - a through z
   - 0 through 9
   - Space (not leading or trailing)
   - Hyphen or dash

   Note:
   The organization name can't contain more than 64 characters. The organization name can't be blank.

7. If this is the first Exchange server in your organization, on the **Client Settings** page, click the option that describes the client computers in your organization that are running Microsoft Office Outlook.
8. On the **Client Settings** page, if you have client computers that are running Outlook 2003 or earlier and you select **Yes**, Exchange 2010 will create a public folder database on the Mailbox server. If all your client computers are running Outlook 2010, public folders are optional in Exchange 2010. If you select **No**, Exchange 2010 will not create a public folder database on the Mailbox server. You can add a public folder database later. For example, if you add client computers that are running Outlook 2003 and you need a public folder database, you can create one on the Exchange 2010 Mailbox server. You must then configure the offline address book for public folder distribution, and then restart the Microsoft Exchange Information Store service before client computers that are running Outlook 2003 and earlier will be able to connect to the server.

9. On the **Configure Client Access Server external domain** page, enter a domain name to use to configure your Client Access servers.

   Note:
   If the Client Access server will not be Internet-facing, you can click **Next** without configuring a domain name. For more information about configuring Client Access servers, see Managing External Client Access. Click **Next**.



10. On the **Customer Experience Improvement** page, choose the appropriate selections for your organization, and then click **Next**.

11. On the Readiness Checks page, view the status to determine if the organization and server role prerequisite checks completed successfully. If they haven't completed successfully, you must resolve any reported errors before you can install Exchange 2010. You don't need to exit Setup when resolving some of the prerequisite errors. After resolving a reported error, click **Retry** to re-run the prerequisite check. Be sure to also review any warnings that are reported. If all readiness checks have completed successfully, click **Install** to install Exchange 2010.

12. On the **Completion** page, click **Finish**.

Important:

If you're installing Exchange 2010 into an existing Exchange 2003 or Exchange 2007 organization, see the "Configure the Client Access server" section in the following topics:
Install Exchange 2010 in an Existing Exchange 2003 Organization
Install Exchange 2010 in an Existing Exchange 2007 Organization
Install Exchange 2010 in a Mixed Exchange 2003 and Exchange 2007 Organization

1.2.2.7.4 Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3

Upgrade Exchange 2010 to Exchange 2010 SP1, SP2 or Exchange 2010 SP3

Planning and Deployment > Deploying Exchange 2010 > Managing Deployment of Exchange 2010

>

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-02-04*

You can use the Microsoft Exchange Server 2010 Service Pack Setup wizard to upgrade your current version of Exchange 2010. If you have the release-to-manufacturing (RTM) version of Exchange 2010 installed, you can upgrade to either Microsoft Exchange Server 2010 Service Pack 3 (SP3), Microsoft Exchange Server 2010 Service Pack 2 (SP2) or to Microsoft Exchange Server 2010 Service Pack 1 (SP1). If you have Exchange 2010 SP1 or Exchange 2010 SP2, installed, we strongly recommend that you upgrade to Exchange 2010 SP3. See Release Notes for Exchange Server 2010 SP3 for more information.

After you install a service pack, you must restart the computer so that changes can be made to the registry and operating system.

Caution:

After you upgrade Exchange 2010 to a newer service pack, you can't uninstall the service pack to revert to the previous version. If you uninstall the service pack, you remove Exchange from the server.

You should upgrade your Exchange 2010 server roles in the following order:

- Client Access
- Hub Transport
- Unified Messaging
- Mailbox

The Edge Transport server role can be upgraded at any time. However, we recommend that you upgrade the Edge Transport server role either before or after you upgrade all other server roles.

Prerequisites

- Make sure that any server on which you plan to install the service pack meets the system requirements. For more information about system requirements, see Exchange 2010 System Requirements.
- Understand the prerequisites for all server roles. For more information about prerequisites, see Exchange 2010 Prerequisites. For more information about server roles, see Overview of Exchange 2010 Server Roles.
- Understand the Unified Messaging server role improvements and new features that were added in Exchange 2010 SP1. These improvements and new features are also included in Exchange 2010 SP2. To use some of these new features, you must correctly deploy Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010 in your environment. For more information, see New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1 and Install or Upgrade to Exchange 2010 SP2 Unified Messaging.

Permissions

To perform the following procedures, the account you use must be a member of the Delegated Setup management role group or the Organization Management management role group.

To apply an Exchange 2010 service pack to an Exchange 2010 server that has the Edge Transport server role installed, the account you use must be a member of the local Administrators group on that computer.

To upgrade a computer that has only the Exchange management tools installed, you must log on by using an account that's a member of the local Administrators group on that computer.

If you haven't yet prepared the schema for Exchange 2010 SP1 or Exchange 2010 SP2, the account you use to upgrade the server must be a member of the Schema Admins group and the Enterprise Admins group. This requirement also applies if you're installing Exchange 2010 SP3, and if you haven't yet prepared the schema for it. For more information, see Prepare Active Directory and Domains.

Upgrade load balanced Client Access array members

If your organization uses a load balanced array of Client Access servers, see the following guidance about how to upgrade your Client Access servers from one version of Exchange 2010 to another, for example, from Exchange 2010 RTM to Exchange 2010 SP1. If you have an array of Client Access servers that you need to upgrade from one version to another, use the following steps.

Note:
Exchange 2010 RTM, Exchange 2010 SP1, Exchange 2010 SP2 and Exchange 2010 SP3 can't coexist within the same load balanced array.

Important:
Do not upgrade any Mailbox server from one version to another until all Client Access servers within the Active Directory site have been upgraded to the target version. The following guidance assumes that the Mailbox and Client Access server roles are not co-located. If your environment deploys multi-role servers, see Exchange Server Team Bog article Patching the Multi-Role Server DAG for the steps to patch the servers.

1. Determine the number of Client Access server array members that can be offline at one time without negatively affecting the service. For example, if you have six Client Access servers in a load balanced array, and you have designed your load-balancing solution to handle three simultaneous failures, you can have three Client Access server array members offline.
2. To continue with the example, disable new connections to the three servers, and let the existing connections terminate. After all connections have been terminated, remove those servers from your load-balancing pool.
3. Upgrade those three servers to the target version. Verify that the upgrade was successful.
4. Restore the upgraded servers to the load-balanced array.
5. Prepare to remove the servers that have not been upgraded from the load balanced array by disabling new connections.
6. Verify that all connections to the servers identified in step 5 have been terminated, and then remove those servers from the load-balanced array.
7. Upgrade the second batch of servers to the target version of the software. Verify that the upgrade was successful.
8. Restore the most recently upgraded servers to the array.

Upgrade database availability group members

When you apply an Exchange 2010 service pack to a database availability group (DAG) member, you need to consider and plan for some specific issues. Before applying an Exchange 2010 service pack to any DAG members, consider the following:

- **Upgrade only passive servers** Before applying the service pack to a DAG member, move all active mailbox database copies off the server to be

upgraded and configure the server to be blocked from activation. If the server to be upgraded currently holds the primary Active Manager role, move the role to another DAG member prior to performing the upgrade. You can determine which DAG member holds the primary Active Manager role by running `Get-DatabaseAvailabilityGroup <DAGName> -Status | Format-List PrimaryActiveManager`.

- **Place server in maintenance mode** Before applying the service pack to any DAG member, you may want to adjust monitoring applications that are in use so that the server doesn't generate alerts or alarms during the upgrade. For example, if you're using Microsoft System Center Operations Manager 2007 to monitor your DAG members, you should put the DAG member to be upgraded in maintenance mode prior to performing the upgrade. If you're not using System Center Operations Manager 2007, you can use `StartDagServerMaintenance.ps1` to put the DAG member in maintenance mode. After the upgrade is complete, you can use `StopDagServerMaintenance.ps1` to take the server out of maintenance mode.
- **Stop any processes that might interfere with the upgrade** Stop any scheduled tasks or other processes running on the DAG member or within that DAG that could adversely affect the DAG member being upgraded or the upgrade process.
- **Verify the DAG is healthy** Before you apply the service pack to any DAG member, we recommend that you verify the health of the DAG and its mailbox database copies. A healthy DAG will pass MAPI connectivity tests to all active databases in the DAG, will have mailbox database copies that have a copy queue length and replay queue length that's very low (if not zero), and will have a copy status and content index state of Healthy.
- **Be aware of other implications of the upgrade** A DAG member running Exchange 2010 RTM can move its active databases to a DAG member running Exchange 2010 SP1 or SP2. After a DAG member has been upgraded to a newer Exchange 2010 service pack, its active database copies cannot be moved to another DAG member that is running Exchange 2010 RTM. If you try to do this, an error will occur.
  When you update a DAG server from Exchange 2010 RTM to Exchange 2010 SP1, Event ID 1185 is recorded in the Application log if there is a database schema update that requires the Exchange mailbox database to change or be updated. If there is no database schema update, this event is not logged.
  When you update from Exchange 2010 SP1 to Exchange 2010 SP2, Event ID 1185 is not recorded in the Application log. This is because a database schema update is not required.

Note:

The database schema update is different from the AD schema update.

Caution:

We recommend that you do not move the active database from a DAG member that is running Exchange 2010 SP2 to a DAG member that is running Exchange 2010 SP1. We make this recommendation even though it is possible to move the database, and the move does not generate an error.

Run the following scripts and commands on the DAG member that is being upgraded in preparation for the service pack.

- Verify the health and status of the DAG by saving the following commands as a Windows PowerShell script (.ps1) file.

```
(Get-DatabaseAvailabilityGroup -Identity (Get-MailboxServer -Identity $
Get-MailboxDatabase | Sort Name | Get-MailboxDatabaseCopyStatus | Forma
function CopyCount
{
$DatabaseList = Get-MailboxDatabase | Sort Name
```

```
$DatabaseList | % {
$Results = $_ | Get-MailboxDatabaseCopyStatus
$Good = $Results | where { ($_.Status -eq "Mounted") -or ($_.Status -eq
$_ | add-member NoteProperty "CopiesTotal" $Results.Count
$_ | add-member NoteProperty "CopiesFailed" ($Results.Count-$Good.Count
}
$DatabaseList | sort copiesfailed -Descending | ft name,copiesTotal,cop
}
CopyCount
```

- Perform a server switchover by running the following command.

```
Move-ActiveMailboxDatabase -Server <DAGMemberName>
```

- Prevent the DAG member from becoming a failover target by running the following command.

```
Set-MailboxServer -DatabaseCopyAutoActivationPolicy:Blocked
```

- If necessary, move the primary Active Manager role to another DAG member by running the following command.

```
Cluster group "cluster group" /move
```

- Install the Exchange 2010 service pack. For details, see "Install the Exchange 2010 service pack" later in this topic.
- Enable the upgraded DAG member to become a failover target by running the following command.

```
Set-MailboxServer -DatabaseCopyAutoActivationPolicy:Value
```

  Where *Value* is either *IntrasiteOnly* or *Unrestricted*.
- Repeat steps 1–6 on each DAG member until the service pack has been applied to every DAG member.

For more information, see the following topics:

- Perform a Server Switchover
- Move-ActiveMailboxDatabase
- Set-MailboxServer
- Understanding Mailbox Database Copies

Install the Exchange 2010 service pack

When installing a new Exchange 2010 service pack on multiple Exchange 2010 servers within an organization, we recommend that you first upgrade your Client Access servers. In an organization that has multiple Active Directory sites that use multiple Client Access servers in a proxy situation, you must upgrade the Internet-facing Client Access servers before upgrading Client Access servers that aren't Internet-facing. Then, we recommend you install the Hub Transport, Unified Messaging, and Mailbox server roles.

The Edge Transport server role can be upgraded at any time. However, we recommend upgrading the Edge Transport server role either before or after all other server roles are upgraded.

1. Insert the Exchange 2010 SP1, SP2 or Exchange 2010 SP3 DVD into the DVD drive. When the **AutoPlay** dialog box appears, click **Run Setup.exe** under **Install or run program**. If the **AutoPlay** dialog box doesn't appear, navigate to the root of the DVD and double-click **Setup.exe**. Alternatively, browse to the location of your Exchange 2010 installation files and double-click **Setup.exe**.
2. On the **Start** page, click **Install Microsoft Exchange Server Upgrade** to

begin the installation.

Important:
Make sure that you've completed all the required steps described on the **Start** page before you begin your installation. If you haven't already installed the components discussed on the **Start** page, Setup provides links to the appropriate sites where you can download the components. For more information about Windows PowerShell installation, see Install Windows Management Framework.

Important:
If you're installing Exchange 2010 on Windows Server 2008 R2, don't use the downloadable .NET Framework package. Instead, use Server Manager in Windows Server 2008 R2 or run **ServerManagerCmd -i NET-Framework**.

3. The **Introduction** page begins the process of installing Exchange into your organization. It will guide you through the installation. Click **Next** to continue.
4. On the **License Agreement** page, review the software license terms. If you agree to the terms, select **I accept the terms in the license agreement**, and then click **Next**.
5. On the **Readiness Checks** page, view the status to determine if the organization and server role prerequisite checks completed successfully. If they haven't completed successfully, you must resolve any reported errors before you can install Exchange 2010. You don't need to exit Setup when you resolve some of the prerequisite errors. After you resolve a reported error, click **Retry** to run the prerequisite check. Make sure to also review any reported warnings. If all readiness checks have finished successfully, click **Upgrade** to install the service pack.
6. On the **Completion** page, click **Finish**.

Use unattended setup to install the Exchange 2010 service pack

1. Insert the Exchange 2010 SP1, SP3 or Exchange 2010 SP3 DVD into the DVD drive.
2. At the command prompt, navigate to the DVD drive or to the network location of the Exchange 2010 installation files.
3. At the command prompt, run the following command:

```
Setup.com /M:Upgrade /InstallWindowsComponents
```

For more information, see the following topics:

1. New Deployment Functionality in Exchange 2010 SP1
2. What's New in Exchange 2010 SP2
3. What's New in Exchange 2010 SP3

1.2.2.7.5 Install Exchange 2010 in an Existing Exchange 2003 Organization

Install Exchange 2010 in an Existing Exchange 2003 Organization

>

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-31*

You can use Microsoft Exchange Server 2010 Setup to install the first server running Exchange 2010 in an existing Exchange Server 2003 organization.

You can't perform an in-place upgrade from Exchange 2003 to Exchange 2010. However, you can install an Exchange 2010 server into the existing Exchange organization, and then move the Exchange resources, such as mailboxes, public folders, and connectors to Exchange 2010.

After you perform this procedure, your organization will be running in a coexistence mode. You can maintain this mode for an indefinite period of time, or you can immediately complete the upgrade to Exchange 2010 by moving all resources from Exchange 2003 to Exchange 2010, and then decommissioning the Exchange 2003 servers.

When you install Exchange 2010 in an existing Exchange 2003 organization, Setup performs the following coexistence-specific tasks:

- Creates the Active Directory universal security group ExchangeLegacyInterop. This group is granted the permissions that allow the Exchange 2003 servers to send e-mail messages to the Exchange 2010 servers.
- Creates a two-way routing group connector between Exchange 2010 and a selected Exchange 2003 bridgehead server. Exchange 2010 and Exchange 2003 use different routing topologies. You must configure a routing group connector to enable mail flow between the Exchange versions.

For information about performing a custom installation, see Install Exchange 2010 Using the Custom Installation Type. For information about installing Exchange 2010 in unattended mode, see Install Exchange 2010 in Unattended Mode.

Although it's a better practice to introduce Exchange 2010 into your Exchange 2003 organization and use Edge Subscriptions, you may want to start using Edge Transport servers before you start your upgrade. For more information, see Deploy the Edge Transport Server Role in an Existing Exchange 2003 Organization Before Upgrading to Exchange 2010.

Exchange Server 2010 Deployment Assistant

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Prerequisites

You must ensure that each of the servers meets the appropriate prerequisites and system requirements before you begin your installation. For more information, see the following topics:

- Overview of Exchange 2010 Server Roles
- Exchange 2010 Prerequisites
- Exchange 2010 System Requirements

Warning:
After you install Exchange 2010 on a server, you must not change the server name. Renaming a server after you have installed an Exchange 2010 server role is not supported.

Install Exchange 2010

If this is the first instance of Exchange 2010 that you're installing into your existing organization, make sure that you install the Client Access server role first, followed by the Hub Transport server role, followed by the Unified Messaging server role, and last, the Mailbox server role. For more information about the Client Access server role, see "Configure the Client Access server" later in this topic.

To perform the following procedure, the account you use must be delegated membership in the Schema Admins group if you haven't previously prepared the Active Directory schema. If you're installing the first Exchange 2010 server in the organization, the account you use must have membership in the Enterprise Admins group. If you've already prepared the schema and aren't installing the first Exchange 2010 server in the organization, the account you use must be delegated the Delegated Setup role group.

Note:
For information about preparing Active Directory for Exchange 2010, see Prepare Active Directory and Domains. For information about permissions in Exchange 2010, see Understanding Permissions and Understanding Role Based Access Control.

1. Insert the Exchange 2010 DVD into the DVD drive. When the **AutoPlay** dialog box appears, click **Run Setup.exe** under **Install or run program**. If the **AutoPlay** dialog box doesn't appear, navigate to the root of the DVD and double-click **Setup.exe**. Alternatively, browse to the location of your Exchange 2010 installation files and double-click **Setup.exe**.
2. The Exchange Server 2010 Setup welcome screen appears. In the **Plan** section, you can follow the links to read overview information regarding Exchange 2010, deploying languages, and the Exchange 2010 Deployment Assistant. In the **Enhance** section, you can read more information about Forefront Protection 2010, and install Microsoft Forefront Protection 2010. In the **Install** section, the software listed for **Step 1: Install .NET Framework 3.5 SP1** and **Step 2: Install Windows PowerShell v2** was installed with the Exchange 2010 prerequisites. However, if these prerequisites aren't already installed, click the appropriate step to install them.
   For more information about Windows PowerShell installation, see Install Windows Management Framework.

   Important:
   If you're installing Exchange 2010 on the Windows Server 2008 R2 operating system, don't use the downloadable .NET Framework package. Instead, use Server Manager in Windows Server 2008 R2 or run **ServerManagerCmd -i NET-Framework**.
3. When **Step 1** and **Step 2** are shown as **Installed**, click **Step 3: Choose Exchange language option** to expand the Exchange language options, and then choose the appropriate option:
   - **Install all languages from the language bundle** This option installs all the Exchange 2010 languages from an Exchange 2010 language bundle. You can connect to the Internet to download the latest applicable language bundle or to use a previously downloaded language bundle on a local drive or network share. Internet connectivity is required for Exchange Setup to download the language pack bundle.
   - **Install only languages from the DVD** This option installs only the languages included with the Setup DVD. The installation of additional language support requires installing the languages from the language bundle.

For more information about Exchange language options, see Exchange 2010 Language Support.

4. After language installation is complete, click **Step 4: Install Microsoft Exchange**. This option starts the Exchange Server 2010 Setup wizard.

   Note:
   After your installation is complete, you can return to **Step 5: Get critical updates for Microsoft Exchange**.

5. On the **License Agreement** page, review the software license terms. If you agree to the terms, select **I accept the terms in the license agreement**, and then click **Next**.
6. On the **Error Reporting** page, click **Yes**, and then click **Next**.
7. On the **Installation Type** page, click **Typical Exchange Server Installation**. If you want to change the path for the Exchange 2010 installation, click **Browse**, locate the appropriate folder in the folder tree, and then click **OK**. Click **Next**.

   Note:
   If you choose the **Typical Exchange Server Installation** option, you won't be able to install the Unified Messaging server role or Edge Transport server role during this installation. You can add additional server roles later if you don't install them during this installation.

8. On the **Configure Client Access Server** external domain page, enter a domain name to use to configure your Client Access servers. Click **Next**. For more information about configuring Client Access servers, see "Configure the Client Access Server" later in this topic.
9. On the **Customer Experience Improvement** page, choose the appropriate selection for your organization, and then click **Next**.
10. On the **Readiness Checks** page, view the status to determine whether the organization and server role prerequisite checks completed successfully. If they completed successfully, click **Install** to install Exchange 2010.
11. On the **Completion** page, click **Finish**.

Configure the Client Access Server

If this is the first Exchange 2010 server you've installed in your Exchange 2003 organization, you need to perform several additional steps to configure your Exchange 2010 Client Access server.

1. If your organization requires Outlook Anywhere access, enable Outlook Anywhere as shown in the following example.

   ```
   Enable-OutlookAnywhere -Server:<CAS2010> -ExternalHostName:mail.contos
   ```

2. If you didn't configure a primary external namespace during setup, configure the virtual directories for the offline address book (OAB), Exchange Web Services, Microsoft Exchange ActiveSync, Microsoft Office Outlook Web App, and Exchange Control Panel (ECP) as shown in the following examples. This example configures the virtual directories for the OAB.

   ```
   Set-OABVirtualDirectory <CAS2010>\OAB* -ExternalUrl "https://mail.cont
   ```

   This example configures the virtual directories for Exchange Web Services.

   ```
   Set-WebServicesVirtualDirectory <CAS2010>\EWS* -ExternalUrl https://ma
   ```

   This example configures the virtual directories for Exchange ActiveSync.

   ```
   Set-ActiveSyncVirtualDirectory -Identity <CAS2010>\Microsoft-Server-Ac
   ```

   This example configures the virtual directories for Outlook Web App.

   ```
   Set-OwaVirtualDirectory <CAS2010>\OWA* -ExternalUrl https://mail.conto
   ```

   This example configures the virtual directories for the ECP.

   ```
   Set-EcpVirtualDirectory <CAS2010>\ECP* -ExternalUrl https://mail.conto
   ```

3. Configure the Exchange 2003 URL property on the /owa virtual directory. This

is necessary for Exchange 2003 and Exchange 2010 to coexist. This example configures this property.

```
Set-OwaVirtualDirectory <CAS2010>\OWA*  -Exchange2003Url https://legac
```

Note:
You must enable forms-based authentication on the Exchange 2003 front-end server to allow your users to access their mailboxes through a single sign-on during the coexistence period.

4. Change the OAB generation server and enable Web distribution on the Exchange 2010 Client Access server using the following steps.
   4.a. Move the OAB as shown in this example.

```
Move-OfflineAddressBook "Default Offline Address List" -Ser
```

   4.b. Add the Exchange 2010 Client Access server as a Web distribution point as shown in these examples.

```
$OABVDir = Get-OABVirtualDirectory -Server
<CAS2010>
$OAB = Get-OfflineAddressBook "Default Offline
Address List"
$OAB.VirtualDirectories and $OABVdir.DistinguishedName =
Set-OfflineAddressBook "Default Offline Address
List" -VirtualDirectories $OAB.VirtualDirectories
```

5. Enable Integrated Windows authentication on the Microsoft-Server-ActiveSync virtual directory on the Exchange 2003 back-end server. This allows the Exchange 2010 Client Access server and the Exchange 2003 back-end server to communicate using Kerberos authentication. Do one of the following:
   5.a. Install a hotfix. To download the hotfix, see Event ID 1036 is logged on an Exchange 2007 server that is running the CAS role when mobile devices connect to the Exchange 2007 server to access mailboxes on an Exchange 2003 back-end server. Use Exchange System Manager to adjust the authentication settings of the Exchange ActiveSync virtual directory.
   5.b. Set the **msExchAuthenticationFlags** attribute to a value of 6 on the **Microsoft-Server-ActiveSync** object within the configuration container on each Exchange 2003 Mailbox server. For an example script, see Server Build DVD Visual Basic Script Examples.

Important:
Don't use IIS Manager to change the authentication setting on the Microsoft ActiveSync virtual directory, because the DS2MB process within the Microsoft Exchange System Attendant will overwrite the settings stored in Active Directory.

6. Create a legacy host name in your external Domain Name System (DNS) infrastructure and associate this host name with your Exchange 2003 front-end server or with your proxy infrastructure. See "Create a Legacy Host Name" later in this topic.
7. Reconfigure your external DNS settings or the publishing rules for your reverse proxy infrastructure to have your original namespace of mail.contoso.com point to your Exchange 2010 Client Access server or Client Access server array.

Create a Legacy Host Name

The exact steps for this procedure depend on your Internet service provider (ISP) and firewall configuration. Example steps for GoDaddy are provided to show you how this works. Your actual steps may vary. In general, you need to perform the following steps.

1. Create a DNS host (A) record in your internal and external DNS servers that points to the IP address of your legacy Internet-facing Exchange server (for example, Exchange Server 2007 Client Access server or Exchange 2003 front-end server) in internal DNS or the public IP address on your reverse proxy or

firewall solution (external DNS). The host name should be in the format of legacy.domain.com (for example, legacy.contoso.com).
2. Create a publishing rule for the legacy host name in your reverse proxy or firewall solution to point to your legacy Internet-facing Exchange server. Refer to your proxy or firewall solution's user manual for instructions about how to do this.
3. Configure the existing DNS host (A) record in your internal and external DNS servers for your original host name (for example, mail.contoso.com) to point to your Exchange 2010 organization, for example, the IP address of your Client Access server or array (internal DNS), or the public IP address on your reverse proxy or firewall solution (external DNS).
   For example, if your provider is GoDaddy.com, you can create a DNS host (A) record and associate it with your legacy Exchange infrastructure.
   3.a. From your GoDaddy account management home page, click **Domain Manager** under the **My Products** heading in the left sidebar.
   3.b. If prompted, log on to your account.
   3.c. In the **Total DNS** section of the **Domain Manager** information screen, click **Total DNS Control**.
   3.d. In the **A (Host)** section of the **Total DNS Control** screen, click **Add new A record**.
   3.e. Enter the host name, for example, legacy.contoso.com, and enter the IP address of your legacy Exchange server in the **Points to IP address** box.
   3.f. Choose a **TTL** (Time to Live) value. If you're performing this step well in advance of your Exchange 2010 installation, you can choose **1 day** or **1 week** from the drop-down list box. Otherwise, choose the default of **1 hour** or **1/2 hour**.
   3.g. Click **OK** to complete your changes.

Verify the legacy host name is accessible from the Internet

From outside your firewall, perform the following steps, using your specific domain name.

1. Navigate to https://mail.contoso.com/owa, and then verify that you can access Outlook Web App for a user whose mailbox is on Exchange 2010.
2. Navigate to https://legacy.contoso.com/exchange, and then verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.
3. Navigate to https://mail.contoso.com/owa, and then verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.

You can also use the Microsoft Exchange Server Remote Connectivity Analyzer to verify connectivity for the legacy namespace. To use the Remote Connectivity Analyzer, see Microsoft Exchange Remote Connectivity Analyzer.

Verify Installation and View Configuration Objects

To verify that Exchange 2010 installed correctly, see Verify an Exchange 2010 Installation. After installation is complete, you can view the Exchange 2010 configuration objects in the Exchange Management Console (EMC).

Note:

You can only view and manage the Exchange 2010 configuration objects using the EMC in Exchange 2010.

To verify that mail flow is working correctly, you can perform the following procedure:

1. Configure your Hub Transport server. For more information, see Transport Server Post-Deployment Tasks.
2. Create a mailbox on the Exchange 2010 Mailbox server. For more information,

see Create a Mailbox.

3. Send an e-mail message from the Exchange 2010 mailbox to a user who has a mailbox that is located on an Exchange 2007 server. Verify that the e-mail message is received.
4. Send an e-mail message from a user who has a mailbox that is located on an Exchange 2007 server to the new Exchange 2010 mailbox user. Verify that the e-mail message is received.

You can also use the Exchange Remote Connectivity Analyzer to test Exchange connectivity.

Finally, be sure to perform the tasks described in Finalize Deployment Tasks that are required for the server roles that you have installed.

Important:

Exchange 2010 now creates system address lists in a new container. Recipients created or modified using Exchange 2003 or Exchange 2007 management tools won't be stamped with these system address lists. As a result, they won't be seen by the Exchange 2010 **Get-Recipient** cmdlet.
To fix this issue, you must enable Active Directory virtual list view (VLV). After you have completed the upgrade of an existing Exchange 2003 organization to Exchange 2010 and have decommissioned your Exchange 2003 servers, you must enable Active Directory VLV. To enable VLV for Exchange 2010, run the **Enable-AddressListPaging** cmdlet. For more information, see Enable-AddressListPaging.

1.2.2.7.6 Install Exchange 2010 in an Existing Exchange 2007 Organization

Install Exchange 2010 in an Existing Exchange 2007 Organization

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-31*

You can use Microsoft Exchange Server 2010 Setup to install the first server running Exchange 2010 in an existing Exchange Server 2007 organization.

You can't perform an in-place upgrade from Exchange 2007 to Exchange 2010. However, you can install an Exchange 2010 server into the existing Exchange organization, and then move the Exchange resources, such as mailboxes, public folders, and connectors to Exchange 2010. After you perform this procedure, your organization will be running in a coexistence mode. You can maintain this mode for an indefinite period of time, or you can immediately complete the upgrade to Exchange 2010 by moving all resources from Exchange 2007 to Exchange 2010, and then decommissioning the Exchange 2007 servers.

Note:

You can install Exchange 2010 in a native mode Exchange organization. However, if you create a forest in which to install Exchange 2010, you can't later add earlier versions of Exchange.

For more information about performing a custom installation, see Install Exchange 2010 Using the Custom Installation Type. For information about installing Exchange 2010 in unattended mode, see Install Exchange 2010 in Unattended Mode.

Exchange Server 2010 Deployment Assistant

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Prerequisites

You must ensure that each of the servers meets the appropriate prerequisites and system requirements before you begin your installation. For more information, see the following topics:

- Overview of Exchange 2010 Server Roles
- Exchange 2010 Prerequisites
- Exchange 2010 System Requirements

Warning:

After you install Exchange 2010 on a server, you must not change the server name. Renaming a server after you have installed an Exchange 2010 server role is not supported.

Install Exchange 2010

If this is the first instance of Exchange 2010 that you're installing into your existing organization, make sure that you install the Client Access server role first, followed by the Hub Transport server role, followed by the Unified Messaging server role, and last, the Mailbox server role. For more information about the Client Access server role, see "Configure the Client Access server" later in this topic.

To perform the following procedure, the account you use must be delegated membership in the Schema Admins group if you haven't previously prepared the Active Directory schema. If you're installing the first Exchange 2010 server in the organization, the account you use must have membership in the Enterprise Admins group. If you've already prepared the schema and aren't installing the first Exchange 2010 server in the organization, the account you use must be delegated the Delegated Setup role group.

Note:

For information about preparing Active Directory for Exchange 2010, see Prepare Active Directory and Domains. For information about permissions in Exchange 2010, see Understanding Permissions and Understanding Role Based Access Control.

1. Insert the Exchange 2010 DVD into the DVD drive. When the **AutoPlay** dialog box appears, click **Run Setup.exe** under **Install or run program**. If the **AutoPlay** dialog box doesn't appear, navigate to the root of the DVD and double-click **Setup.exe**. Alternatively, browse to the location of your Exchange 2010 installation files and double-click **Setup.exe**.
2. The Exchange Server 2010 Setup welcome screen appears. In the **Plan** section, you can follow the links to read overview information regarding Exchange 2010, deploying languages, and the Exchange 2010 Deployment Assistant. In the **Enhance** section, you can read more information about Forefront Protection 2010, and install Microsoft Forefront Protection 2010. In the **Install** section, the software listed for **Step 1: Install .NET Framework 3.5 SP1** and **Step 2: Install Windows PowerShell v2** was installed with the Exchange 2010 prerequisites. However, if these prerequisites aren't already

installed, click the appropriate step to install them.
For more information about Windows PowerShell installation, see Install Windows Management Framework.

Important:
If you're installing Exchange 2010 on the Windows Server 2008 R2 operating system, don't use the downloadable .NET Framework package. Instead, use Server Manager in Windows Server 2008 R2 or run **ServerManagerCmd -i NET-Framework**.

3. When **Step 1** and **Step 2** are shown as **Installed**, click **Step 3: Choose Exchange language option** to expand the Exchange language options, and then choose the appropriate option:
   - **Install all languages from the language bundle** This option installs all the Exchange 2010 languages from an Exchange 2010 language bundle. You can connect to the Internet to download the latest applicable language bundle or to use a previously downloaded language bundle on a local drive or network share. Internet connectivity is required for Exchange Setup to download the language pack bundle.
   - **Install only languages from the DVD** This option installs only the languages included with the Setup DVD. The installation of additional language support requires installing the languages from the language bundle.

     For more information about Exchange language options, see Exchange 2010 Language Support.
4. After language installation is complete, click **Step 4: Install Microsoft Exchange**. This option starts the Exchange Server 2010 Setup wizard.

Note:
After your installation is complete, you can return to **Step 5: Get critical updates for Microsoft Exchange**.

5. On the **License Agreement** page, review the software license terms. If you agree to the terms, select **I accept the terms in the license agreement**, and then click **Next**.
6. On the **Error Reporting** page, click **Yes**, and then click **Next**.
7. On the **Installation Type** page, click **Typical Exchange Server Installation**. If you want to change the path for the Exchange 2010 installation, click **Browse**, locate the appropriate folder in the folder tree, and then click **OK**. Click **Next**.

Note:
If you choose the **Typical Exchange Server Installation** option, you won't be able to install the Unified Messaging server role or Edge Transport server role during this installation. You can add additional server roles later if you don't install them during this installation.

8. On the **Configure Client Access Server** external domain page, enter a domain name to use to configure your Client Access servers. Click **Next**. For more information about configuring Client Access servers, see "Configure the Client Access Server" later in this topic.
9. On the **Customer Experience Improvement** page, choose the appropriate selection for your organization, and then click **Next**.
10. On the **Readiness Checks** page, view the status to determine whether the organization and server role prerequisite checks completed successfully. If they completed successfully, click **Install** to install Exchange 2010.
11. On the **Completion** page, click **Finish**.

Configure the Client Access Server

If this is the first Exchange 2010 server you've installed in your Exchange 2007 organization, you need to perform several additional steps to configure your Exchange 2010 Client Access server.

1. If your organization requires Outlook Anywhere access, enable Outlook Anywhere as shown in the following example.

```
Enable-OutlookAnywhere -Server:<CAS2010> -ExternalHostName:mail.contos
```

2. If you didn't configure a primary external namespace during setup, configure the virtual directories for the offline address book (OAB), Exchange Web Services, Microsoft Exchange ActiveSync, Microsoft Office Outlook Web App, and Exchange Control Panel (ECP) as shown in the following examples.
   This example configures the virtual directories for the OAB.

```
Set-OABVirtualDirectory <CAS2010>\OAB* -ExternalUrl "https://mail.cont
```

   This example configures the virtual directories for Exchange Web Services.

```
Set-WebServicesVirtualDirectory <CAS2010>\EWS* -ExternalUrl https://ma
```

   This example configures the virtual directories for Exchange ActiveSync.

```
Set-ActiveSyncVirtualDirectory -Identity <CAS2010>\Microsoft-Server-Ac
```

   This example configures the virtual directories for Outlook Web App.

```
Set-OwaVirtualDirectory <CAS2010>\OWA* -ExternalUrl https://mail.conto
```

   This example configures the virtual directories for the ECP.

```
Set-EcpVirtualDirectory <CAS2010>\ECP* -ExternalUrl https://mail.conto
```

3. Configure your Outlook Web App settings to meet your organization's needs.
   - To obtain the Outlook Web Access settings from your Exchange 2007 server, run the **Get-OwaVirtualDirectory** cmdlet.
   - To configure the Outlook Web App settings in Exchange 2010, run the **Set-OwaVirtualDirectory** cmdlet.
4. Configure your Exchange ActiveSync authentication settings.
   - To obtain the Exchange ActiveSync settings from your Exchange 2007 server, run the **Get-ActiveSyncVirtualDirectory** cmdlet.
   - To configure the Exchange ActiveSync settings in Exchange 2010, run the **Set-ActiveSyncVirtualDirectory** cmdlet.
5. Install the Exchange 2010 Hub Transport server role and the Exchange 2010 Mailbox server role into the Internet-facing Active Directory site. For configuration steps for these server roles, see Upgrade from Exchange 2007 Transport and Upgrade from Exchange 2007 Mailbox.
6. Change the OAB generation server and enable Web distribution on the Exchange 2010 Client Access server using the following steps.
   - Move the OAB as shown in this example.

```
Move-OfflineAddressBook "Default Offline Address List" -Ser
```

   - Add the Exchange 2010 Client Access server as a Web distribution point as shown in these examples.

```
$OABVDir = Get-OABVirtualDirectory -Server <CAS2010>
$OAB = Get-OfflineAddressBook "Default Offline
Address List"
$OAB.VirtualDirectories += $OABVdir.DistinguishedName
```

```
Set-OfflineAddressBook "Default Offline Address List" -Virt
```

7. Create a legacy host name in your external Domain Name System (DNS) infrastructure and associate this host name with your Exchange 2007 Client Access server or with your proxy infrastructure. See "Create a Legacy Host Name" later in this topic.
8. Reconfigure your external DNS settings or the publishing rules for your reverse proxy infrastructure to have your original namespace of mail.contoso.com point to your Exchange 2010 Client Access server or Client Access server array.

Create a Legacy Host Name

The exact steps for this procedure depend on your Internet service provider (ISP) and firewall configuration. Example steps for GoDaddy are provided to show you how this works. Your actual steps may vary. In general, you need to perform the following steps.

1. Create a DNS host (A) record in your internal and external DNS servers that points to the IP address of your legacy Internet-facing Exchange server (for example, Exchange 2007 Client Access server or Exchange 2003 front-end server) in internal DNS or the public IP address on your reverse proxy or firewall solution (external DNS). The host name should be in the format of legacy.domain.com (for example, legacy.contoso.com).
2. Create a publishing rule for the legacy host name in your reverse proxy or firewall solution to point to your legacy Internet-facing Exchange server. Refer to your proxy or firewall solution's user manual for instructions about how to do this.
3. Configure the existing DNS host (A) record in your internal and external DNS servers for your original host name (for example, mail.contoso.com) to point to your Exchange 2010 organization, for example, the IP address of your Client Access server or array (internal DNS), or the public IP address on your reverse proxy or firewall solution (external DNS).
   For example, if your provider is GoDaddy.com, you can create a DNS host (A) record and associate it with your legacy Exchange infrastructure.
   3.a. From your GoDaddy account management home page, click **Domain Manager** under the **My Products** heading in the left sidebar.
   3.b. If prompted, log on to your account.
   3.c. In the **Total DNS** section of the **Domain Manager** information screen, click **Total DNS Control**.
   3.d. In the **A (Host)** section of the **Total DNS Control** screen, click **Add new A record**.
   3.e. Enter the **host name**, for example, legacy.contoso.com, and enter the IP address of your legacy Exchange server in the **Points to IP address** box.
   3.f. Choose a **TTL** (Time to Live) value. If you're performing this step well in advance of your Exchange 2010 installation, you can choose **1 day** or **1 week** from the drop-down list box. Otherwise, choose the default of **1 hour** or **1/2 hour**.
   3.g. Click **OK** to complete your changes.

Verify the legacy host name is accessible from the Internet

From outside your firewall, perform the following steps, using your specific domain name.

1. Navigate to https://mail.contoso.com/owa, and then verify that you can access Outlook Web App for a user whose mailbox is on Exchange 2010.
2. Navigate to https://legacy.contoso.com/exchange, and then verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.
3. Navigate to https://mail.contoso.com/owa, and then verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.

You can also use the Microsoft Exchange Server Remote Connectivity Analyzer to verify connectivity for the legacy namespace. To use the Remote Connectivity Analyzer, see Microsoft Exchange Remote Connectivity Analyzer.

Verify Installation and View Configuration Objects

To verify that Exchange 2010 installed correctly, see Verify an Exchange 2010 Installation. After installation is complete, you can view the Exchange 2010 configuration objects in the Exchange Management Console (EMC).

Note:
You can only view and manage the Exchange 2010 configuration objects using the EMC in Exchange 2010.

To verify that mail flow is working correctly, you can perform the following procedure:

1. Configure your Hub Transport server. For more information, see Transport Server Post-Deployment Tasks.
2. Create a mailbox on the Exchange 2010 Mailbox server. For more information, see Create a Mailbox.
3. Send an e-mail message from the Exchange 2010 mailbox to a user who has a mailbox that is located on an Exchange 2007 server. Verify that the e-mail message is received.
4. Send an e-mail message from a user who has a mailbox that is located on an Exchange 2007 server to the new Exchange 2010 mailbox user. Verify that the e-mail message is received.

You can also use the Exchange Remote Connectivity Analyzer to test Exchange connectivity.

Finally, be sure to perform the tasks described in Finalize Deployment Tasks that are required for the server roles that you have installed.

Important:
Exchange 2010 now creates system address lists in a new container. Recipients created or modified using Exchange 2003 or Exchange 2007 management tools won't be stamped with these system address lists. As a result, they won't be seen by the Exchange 2010 **Get-Recipient** cmdlet.
To fix this issue, you must enable Active Directory virtual list view (VLV). After you have completed the upgrade of an existing Exchange 2003 organization to Exchange 2010 and have decommissioned your Exchange 2003 servers, you must enable Active Directory VLV. To enable VLV for Exchange 2010, run the **Enable-AddressListPaging** cmdlet. For more information, see Enable-AddressListPaging.

1.2.2.7.7 Install Exchange 2010 in a Mixed Exchange 2003 and Exchange 2007 Organization

Install Exchange 2010 in a Mixed Exchange 2003 and Exchange 2007 Organization

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-31*

You can use Microsoft Exchange Server 2010 Setup to install the first server running Exchange 2010 in an existing Exchange organization where both Exchange Server 2003 and Exchange Server 2007 are present.

You can't perform an in-place upgrade from Exchange 2003 or Exchange 2007 to Exchange 2010. However, you can install an Exchange 2010 server into the existing Exchange organization, and then move the Exchange resources, such as mailboxes, public folders, and connectors to Exchange 2010.

After you perform this procedure, your organization will be running in a coexistence mode. You can maintain this mode for an indefinite period of time, or you can immediately complete the upgrade to Exchange 2010 by moving all resources from Exchange 2003 and Exchange 2007 to Exchange 2010, and then decommissioning the Exchange 2003 and

Exchange 2007 servers. For more information about removing your Exchange 2003 and Exchange 2007 servers, see the following topics:

- How to Remove the Last Legacy Exchange Server from an Organization
- How to Completely Remove Exchange 2007 from a Server

To learn more about upgrading your organization, see the following topics:

- Understanding Upgrade to Exchange 2010
- Exchange 2003 - Planning Roadmap for Upgrade and Coexistence
- Exchange 2007 - Planning Roadmap for Upgrade and Coexistence

For more information about performing a custom installation, see Install Exchange 2010 Using the Custom Installation Type. For information about installing Exchange 2010 in unattended mode, see Install Exchange 2010 in Unattended Mode.

Exchange Server 2010 Deployment Assistant

Exchange Server 2010 introduces the Exchange Server Deployment Assistant, or ExDeploy, a new Web-based tool that can help you with your Exchange deployment. ExDeploy asks you a few questions about your current environment and then generates a custom checklist and procedures that help simplify your deployment.

For more information, see Exchange Server Deployment Assistant.

Prerequisites

You must ensure that each of the servers meets the appropriate prerequisites and system requirements before you begin your installation. For more information, see the following topics:

- Overview of Exchange 2010 Server Roles
- Exchange 2010 Prerequisites
- Exchange 2010 System Requirements

Warning:

After you install Exchange 2010 on a server, you must not change the server name. Renaming a server after you have installed an Exchange 2010 server role is not supported.

Install Exchange 2010

If this is the first instance of Exchange 2010 that you're installing into your existing organization, make sure that you install the Client Access server role first, followed by the Hub Transport server role, followed by the Unified Messaging server role, and last, the Mailbox server role. For more information about the Client Access server role, see "Configure the Client Access server" later in this topic.

To perform the following procedure, the account you use must be delegated membership in the Schema Admins group if you haven't previously prepared the Active Directory schema. If you're installing the first Exchange 2010 server in the organization, the account you use must have membership in the Enterprise Admins group. If you've already prepared the schema and aren't installing the first Exchange 2010 server in the organization, the account you use must be delegated the Delegated Setup role group.

Note:

For information about preparing Active Directory for Exchange 2010, see Prepare Active Directory and Domains. For information about permissions in Exchange 2010, see

Understanding Permissions and Understanding Role Based Access Control.

1. Insert the Exchange 2010 DVD into the DVD drive. When the **AutoPlay** dialog box appears, click **Run Setup.exe** under **Install or run program**. If the **AutoPlay** dialog box doesn't appear, navigate to the root of the DVD and double-click **Setup.exe**. Alternatively, browse to the location of your Exchange 2010 installation files and double-click **Setup.exe**.
2. The Exchange Server 2010 Setup welcome screen appears. In the **Plan** section, you can follow the links to read overview information regarding Exchange 2010, deploying languages, and the Exchange 2010 Deployment Assistant. In the **Enhance** section, you can read more information about Forefront Protection 2010, and install Microsoft Forefront Protection 2010. In the **Install** section, the software listed for **Step 1: Install .NET Framework 3.5 SP1** and **Step 2: Install Windows PowerShell v2** was installed with the Exchange 2010 prerequisites. However, if these prerequisites aren't already installed, click the appropriate step to install them.
   For more information about Windows PowerShell installation, see Install Windows Management Framework.

   Important:
   If you're installing Exchange 2010 on the Windows Server 2008 R2 operating system, don't use the downloadable .NET Framework package. Instead, use Server Manager in Windows Server 2008 R2 or run **ServerManagerCmd -i NET-Framework**.
3. When **Step 1** and **Step 2** are shown as **Installed**, click **Step 3: Choose Exchange language option** to expand the Exchange language options, and then choose the appropriate option:
   - **Install all languages from the language bundle** This option installs all the Exchange 2010 languages from an Exchange 2010 language bundle. You can connect to the Internet to download the latest applicable language bundle or to use a previously downloaded language bundle on a local drive or network share. Internet connectivity is required for Exchange Setup to download the language pack bundle.
   - **Install only languages from the DVD** This option installs only the languages included with the Setup DVD. The installation of additional language support requires installing the languages from the language bundle.

   For more information about Exchange language options, see Exchange 2010 Language Support.
4. After language installation is complete, click **Step 4: Install Microsoft Exchange**. This option starts the Exchange Server 2010 Setup wizard.

   Note:
   After your installation is complete, you can return to **Step 5: Get critical updates for Microsoft Exchange**.
5. On the **License Agreement** page, review the software license terms. If you agree to the terms, select **I accept the terms in the license agreement**, and then click **Next**.
6. On the **Error Reporting** page, click **Yes**, and then click **Next**.
7. On the **Installation Type** page, click **Typical Exchange Server Installation**. If you want to change the path for the Exchange 2010 installation, click **Browse**, locate the appropriate folder in the folder tree, and then click **OK**. Click **Next**.

   Note:
   If you choose the **Typical Exchange Server Installation** option, you won't be able to install the Unified Messaging server role or Edge Transport server role during this installation. You can add additional server roles later if you don't install them during this installation.
8. On the **Configure Client Access Server** external domain page, enter a domain name to use to configure your Client Access servers. Click **Next**. For

more information about configuring Client Access servers, see "Configure the Client Access Server" later in this topic.

9. On the **Customer Experience Improvement** page, choose the appropriate selection for your organization, and then click **Next**.
10. On the **Readiness Checks** page, view the status to determine whether the organization and server role prerequisite checks completed successfully. If they completed successfully, click **Install** to install Exchange 2010.
11. On the **Completion** page, click **Finish**.

Configure the Client Access Server

If this is the first Exchange 2010 server you've installed in your mixed Exchange 2003 and Exchange 2007 organization, you need to perform several additional steps to configure your Exchange 2010 Client Access server.

1. If your organization requires Outlook Anywhere access, enable Outlook Anywhere as shown in the following example.

```
Enable-OutlookAnywhere -Server:<CAS2010> -ExternalHostName:mail.contos
```

2. If you didn't configure a primary external namespace during setup, configure the virtual directories for the offline address book (OAB), Exchange Web Services, Microsoft Exchange ActiveSync, Microsoft Office Outlook Web App, and Exchange Control Panel (ECP) as shown in the following examples. This example configures the virtual directories for the OAB.

```
Set-OABVirtualDirectory <CAS2010>\OAB* -ExternalUrl "https://mail.cont
```

This example configures the virtual directories for Exchange Web Services.

```
Set-WebServicesVirtualDirectory <CAS2010>\EWS* -ExternalUrl https://ma
```

This example configures the virtual directories for Exchange ActiveSync.

```
Set-ActiveSyncVirtualDirectory -Identity <CAS2010>\Microsoft-Server-Ac
```

This example configures the virtual directories for Outlook Web App.

```
Set-OwaVirtualDirectory <CAS2010>\OWA* -ExternalUrl https://mail.conto
```

This example configures the virtual directories for the ECP.

```
Set-EcpVirtualDirectory <CAS2010>\ECP* -ExternalUrl https://mail.conto
```

3. Configure your Outlook Web App settings to meet your organization's needs.
   - To obtain the Outlook Web Access settings from your Exchange 2007 server, run the **Get-OwaVirtualDirectory** cmdlet.
   - To configure the Outlook Web App settings in Exchange 2010, run the **Set-OwaVirtualDirectory** cmdlet.
4. Configure your Exchange ActiveSync authentication settings.
   - To obtain the Exchange ActiveSync settings from your Exchange 2007 server, run the **Get-ActiveSyncVirtualDirectory** cmdlet.
   - To configure the Exchange ActiveSync settings in Exchange 2010, run the **Set-ActiveSyncVirtualDirectory** cmdlet.
5. Install the Exchange 2010 Hub Transport server role and the Exchange 2010 Mailbox server role into the Internet-facing Active Directory site. For configuration steps for these server roles, see Upgrade from Exchange 2007 Transport and Upgrade from Exchange 2007 Mailbox.
6. Change the OAB generation server and enable Web distribution on the Exchange 2010 Client Access server using the following steps.
   - Move the OAB as shown in this example.

```
Move-OfflineAddressBook "Default Offline Address List" -Ser
```

   - Add the Exchange 2010 Client Access server as a Web distribution point as shown in these examples.

```
$OABVDir = Get-OABVirtualDirectory -Server <CAS2010>
$OAB = Get-OfflineAddressBook "Default Offline
```

```
Address List"
$OAB.VirtualDirectories += $OABVdir.DistinguishedName
Set-OfflineAddressBook "Default Offline Address List" -Virt
```

7. If you have Exchange 2003 mailboxes in your organization, enable Integrated Windows authentication on the Microsoft-Server-ActiveSync virtual directory on the Exchange 2003 back-end server. This allows the Exchange 2010 Client Access server and the Exchange 2003 back-end server to communicate using Kerberos authentication. Do one of the following:
   - Install a hotfix. To download the hotfix, see Event ID 1036 is logged on an Exchange 2007 server that is running the CAS role when mobile devices connect to the Exchange 2007 server to access mailboxes on an Exchange 2003 back-end server. Use Exchange System Manager to adjust the authentication settings of the Exchange ActiveSync virtual directory.
   - Set the **msExchAuthenticationFlags** attribute to a value of 6 on the **Microsoft-Server-ActiveSync** object within the configuration container on each Exchange 2003 Mailbox server. For an example script, see Server Build DVD Visual Basic Script Examples.

   Important:
   Don't use IIS Manager to change the authentication setting on the Microsoft ActiveSync virtual directory, because the DS2MB process within the Microsoft Exchange System Attendant will overwrite the settings stored in Active Directory.
8. Create a legacy host name in your external Domain Name System (DNS) infrastructure and associate this host name with your Exchange 2007 Client Access server or with your proxy infrastructure. See "Create a Legacy Host Name" later in this topic.
9. Reconfigure your external DNS settings or the publishing rules for your reverse proxy infrastructure to have your original namespace of mail.contoso.com point to your Exchange 2010 Client Access server or Client Access server array.

Create a Legacy Host Name

The exact steps for this procedure depend on your Internet service provider (ISP) and firewall configuration. Example steps for GoDaddy are provided to show you how this works. Your actual steps may vary. In general, you need to perform the following steps.

1. Create a DNS host (A) record in your internal and external DNS servers that points to the IP address of your legacy Internet-facing Exchange server (for example, Exchange 2007 Client Access server or Exchange 2003 front-end server) in internal DNS or the public IP address on your reverse proxy or firewall solution (external DNS). The host name should be in the format of legacy.domain.com (for example, legacy.contoso.com).
2. Create a publishing rule for the legacy host name in your reverse proxy or firewall solution to point to your legacy Internet-facing Exchange server. Refer to your proxy or firewall solution's user manual for instructions about how to do this.
3. Configure the existing DNS host (A) record in your internal and external DNS servers for your original host name (for example, mail.contoso.com) to point to your Exchange 2010 organization, for example, the IP address of your Client Access server or array (internal DNS), or the public IP address on your reverse proxy or firewall solution (external DNS).
   For example, if your provider is GoDaddy.com, you can create a DNS host (A) record and associate it with your legacy Exchange infrastructure.
   3.a. From your GoDaddy account management home page, click **Domain Manager** under the **My Products** heading in the left sidebar.
   3.b. If prompted, log on to your account.
   3.c. In the **Total DNS** section of the **Domain Manager** information screen, click **Total DNS Control**.

3.d.In the **A (Host)** section of the **Total DNS Control** screen click **Add new A record**.
3.e.Enter the **host name**, for example, legacy.contoso.com, and enter the IP address of your legacy Exchange server in the **Points to IP address** box.
3.f.Choose a **TTL** (Time to Live) value. If you're performing this step well in advance of your Exchange 2010 installation, you can choose **1 day** or **1 week** from the drop-down list box. Otherwise, choose the default of **1 hour** or **1/2 hour**.
3.g.Click **OK** to complete your changes.

Verify the legacy host name is accessible from the Internet

From outside your firewall, perform the following steps, using your specific domain name.

1. Navigate to https://mail.contoso.com/owa, and then verify that you can access Outlook Web App for a user whose mailbox is on Exchange 2010.
2. Navigate to https://legacy.contoso.com/exchange, and then verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.
3. Navigate to https://mail.contoso.com/owa, and then verify that you can access Outlook Web App for a user whose mailbox is on a legacy Exchange server.

You can also use the Microsoft Exchange Server Remote Connectivity Analyzer to verify connectivity for the legacy namespace. To use the Remote Connectivity Analyzer, see Microsoft Exchange Remote Connectivity Analyzer.

Verify Installation and View Configuration Objects

To verify that Exchange 2010 installed correctly, see Verify an Exchange 2010 Installation. After installation is complete, you can view the Exchange 2010 configuration objects in the Exchange Management Console (EMC).

Note:
You can only view and manage the Exchange 2010 configuration objects by using the EMC in Exchange 2010.

To verify that mail flow is working correctly, you can perform the following procedure:

1. Configure your Hub Transport server. For more information, see Transport Server Post-Deployment Tasks.
2. Create a mailbox on the Exchange 2010 Mailbox server. For more information, see Create a Mailbox.
3. Send an e-mail message from the Exchange 2010 mailbox to a user who has a mailbox that is located on an Exchange 2007 server. Verify that the e-mail message is received.
4. Send an e-mail message from a user who has a mailbox that is located on an Exchange 2007 server to the new Exchange 2010 mailbox user. Verify that the e-mail message is received.

You can also use the Exchange Remote Connectivity Analyzer to test Exchange connectivity.

Finally, be sure to perform the tasks described in Finalize Deployment Tasks that are required for the server roles that you have installed.

Important:
Exchange 2010 now creates system address lists in a new container. Recipients created or modified using Exchange 2003 or Exchange 2007 management tools won't be stamped with these system address lists. As a result, they won't be seen by the Exchange 2010

Get-Recipient cmdlet.
To fix this issue, you must enable Active Directory virtual list view (VLV). After you have completed the upgrade of an existing Exchange 2003 organization to Exchange 2010 and have decommissioned your Exchange 2003 servers, you must enable Active Directory VLV. To enable VLV for Exchange 2010, run the **Enable-AddressListPaging** cmdlet. For more information, see Enable-AddressListPaging.

1.2.2.7.8 Install Exchange 2010 in Unattended Mode

Install Exchange 2010 in Unattended Mode

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Setup from a Command Prompt window to install Microsoft Exchange Server 2010 in unattended mode. To perform an unattended setup, you must install Exchange 2010 from the command prompt.

Note:
After you install any server roles on a computer running Exchange 2010, you can't use the Exchange 2010 Setup wizard to add any additional server roles to this computer. If you want to add more server roles to a computer, you must either use Add or Remove Programs from Control Panel or use Setup.com from a Command Prompt window.

For information about tasks to complete after installation, see Exchange 2010 Post-Installation Tasks.

Prerequisites

- You must install both the Mailbox server role and the Hub Transport server role in each Active Directory site for e-mail messages to flow correctly.
- You must install a Client Access server in each Active Directory site that has a Mailbox server role for client access to work correctly.
- You can install the Mailbox server role, the Hub Transport server role, the Client Access server role, and the Unified Messaging (UM) server role on the same computer or on separate computers. You must install the Edge Transport server role on a separate computer in your organization's perimeter network.
- You must ensure that each of the server roles meets the appropriate prerequisites and system requirements before you begin your installation:
  - For more information about server roles, see Overview of Exchange 2010 Server Roles.
  - To understand the prerequisites for all server roles, see Exchange 2010 Prerequisites.
  - For more information about system requirements, see Exchange 2010 System Requirements.
- You must ensure the account you use is delegated membership in the Schema Admins group if you haven't previously prepared the Active Directory schema. If you're installing the first Exchange 2010 server in the organization, the account you use must have membership in the Enterprise Admins group. If you've already prepared the schema and aren't installing the first Exchange 2010 server in the organization, the account you use must be a member of the Exchange 2010 Organization Management role group.
  Administrators who are members of the Delegated Setup role group can

deploy Exchange 2010 servers that have been previously provisioned by a member of the Organization Management role group. For more information about delegated setup, see Provision Exchange 2010 Server and Delegate Setup. For more information about permissions, delegating roles, and the rights that are required to administer Exchange 2010, see Understanding Permissions.

Note:
During Exchange 2010 installation, when preparing Active Directory, system mailboxes are created in the root domain that users and administrators can't log on to. These system mailboxes are created for Exchange 2010 features such as Message Approval and E-discovery.

Warning:
After you install Exchange 2010 on a server, you must not change the server name. Renaming a server after you have installed an Exchange 2010 server role is not supported.

Use Setup.com to install Exchange 2010 in unattended mode

1. Log on to the server on which you want to install Exchange 2010.
2. Insert the Exchange 2010 DVD into the DVD drive, and then, at the command prompt, navigate to the DVD drive, or navigate to the network location of the Exchange 2010 installation files.
3. At the command prompt, run the applicable command for your organization.

```
Setup.com [/mode:<setup mode>] [/role:<server roles to install>] [/Ins
```

- *[/mode: <setup mode>*, or */m:<setup mode>]*
  You must use the */mode* parameter to specify the setup mode. If you don't specify a mode, Setup uses the default Install mode. Select one of the following modes:
  Install Use this mode when you're installing a new role or adding a role to an existing installation (maintenance mode). You can use this mode from both the Exchange Setup wizard and the unattended install.
  Uninstall Use this mode when you're removing the Exchange installation or removing a single server role from an existing installation (maintenance). You can use this mode from both the Exchange Setup wizard and the unattended install.
  Upgrade Select this mode used when you have an existing installation of Exchange and you're installing the new version. This mode is used for a Service Pack installation. You can use this mode from both the Exchange Setup wizard and the unattended install.
  RecoverServer Use this mode when there has been a catastrophic failure of a server, and you need to recover data. You must install a server using the same fully qualified domain name (FQDN) as the failed server, and then run Setup with the **/m:RecoverServer** switch. Don't specify the roles to restore. Setup detects the Exchange Server object in Active Directory and installs the corresponding files and configuration automatically. After you recover the server, you can restore databases and reconfigure any additional settings.
  To run in RecoverServer mode, you can't have Exchange installed on the server. The Exchange server object must exist in Active Directory. You can only use this mode during an unattended installation.
- *[/roles: <server roles>*, */role:<server roles>*, or */r:<server roles>]*

You must use the */roles* parameter to specify which server roles to install or uninstall. Select from one or more of the following roles, in a comma-separated list:
ClientAccess (or CA, or C)
EdgeTransport (or ET, or E)

Note:
The Edge Transport server role can't coexist on the same computer with any other server role. You must deploy the Edge Transport server role in the perimeter network and outside the Active Directory forest.

HubTransport (or HT, or H)
Mailbox (or MB, or M)
UnifiedMessaging (or UM, or U)
ManagementTools (or MT, or T)

Note:
If you select ManagementTools, you'll install the EMC and the Exchange cmdlets for the Exchange Management Shell. The management tools will be installed automatically if you install any other server role.

For example, to specify the Client Access and Mailbox server roles, specify the following: **Setup.com /roles:ClientAccess,Mailbox** or alternatively, specify the following: **Setup.com /r:C,M**.

- [*/InstallWindowsComponents*]
  During an Exchange 2010 SP1 installation, you can install the required Windows roles and features for each selected Exchange 2010 SP1 server role. If a reboot is required, Setup will resume where the installation ended. For example, to specify /InstallWindowsComponents, specify the following: **Setup.com /roles:ClientAccess,Mailbox /InstallWindowsComponents**
- [*/OrganizationName:<organization name>*, or */on:<organization name>*]
  Use the */OrganizationName* parameter to specify the name to give the new Exchange organization. This parameter is required if you're installing the first server in an organization, and you haven't run **Setup /PrepareAD**. If you're installing a server in an existing Exchange organization or if you've already run **Setup /PrepareAD**, you can't use this parameter.

  Note:
  In the Exchange 2010 Setup wizard, the default value is **First Organization**. In the command-line version of Setup, there is no default value.

  The Exchange organization name can contain only the following characters:
  A through Z
  a through z
  0 through 9
  Space (not leading or trailing)
  Hyphen or dash
  The organization name can't contain more than 64 characters. The organization name can't be blank. If the organization name contains spaces, you must enclose it in quotation marks (").
- [*/TargetDir:<destination folder>*, or */t:<destination folder>*]
  Use the */TargetDir* parameter to specify the location to install Exchange 2010 files. The default location is Program Files \Microsoft\Exchange Server. You can't install Exchange 2010 to a root directory such as C:\. You can't install Exchange 2010 on

a ROM drive, RAM disk, network drive, removable disk, or unknown drive type. You can't change the installation directory if Exchange is already installed on the server (for example, if you're adding a server role). If the destination folder contains spaces, you must enclose it in quotation marks (").

- [*/SourceDir:<source folder>*, or */s:<source folder>*]
  Use the */SourceDir* parameter to specify the location from which to install Exchange 2010 files when you're adding a server role to an existing Exchange 2010 server and if the source folder isn't the folder from which you're running Setup. The default value is the current directory from which you're running Setup. If the source folder contains spaces, you must enclose it in quotation marks (").
- [*/UpdatesDir:<updates folder>*, or */u:<updates folder>*]
  Use the */UpdatesDir* parameter to specify the directory from which updates will be installed. If the updates folder contains spaces, you must enclose it in quotation marks ("). Files in the Updates directory must be either an Updates.exe file, or one or more *.msp files. Setup will install the updates before installing the Exchange server roles specified.
  By default, Setup uses the Updates folder that's in the root folder of the installation media. If you want Setup to search for updates in a different folder instead of in the default Updates folder, use this parameter. You can specify only one folder for updates.
- [*/DomainController:<FQDN of domain controller>*, or */dc:<FQDN of domain controller>*]
  Use the */DomainController* parameter to specify the domain controller to use to read from and write to Active Directory during setup. You can use NetBIOS or fully qualified domain name (FQDN) format. The domain controller that you specify must be in the same Active Directory site as the server on which you run Setup and must meet the following requirements: Windows Server 2003 Standard Edition with SP1 or later (32-bit or 64-bit), or Windows Server 2003 Enterprise Edition with SP1 or later (32-bit or 64-bit), or Windows Server 2008 Standard or Enterprise (32-bit or 64-bit), or Windows Server 2008 R2 Standard or Enterprise, or Windows Server 2008 Datacenter or R2 Datacenter. If you don't use this parameter, Setup will select a domain controller to use.
  To run **Setup /PrepareSchema** or **Setup /PrepareAD**, or to install the first Exchange 2010 server in an organization if you haven't run **Setup /PrepareAD**, Setup must use the schema master domain controller to read from and write to Active Directory. If you specify a domain controller that isn't the schema master, Setup will stop and return an error message.
- [*/AnswerFile:<filename>*, or */a:<filename>*]
  Use the */AnswerFile* parameter to specify the location of a file that contains parameters for Setup. You can use this file to install Exchange 2010 on multiple computers with the same parameters. You can use the following parameters in the answer file: *EnableLegacyOutlook*, *LegacyRoutingServer*, *OrganizationName*, *DoNotStartTransport*, *UpdatesDir*, *EnableErrorReporting*, *NoSelfSignedCertificates*, *AdamLdapPort*, and *AdamSslPort*.

  Note:
  Don't include the slash mark (/) with the parameters in the answer file.

  The following is an example of the contents in the answer file

AnswerFile01.txt.

```
EnableErrorReporting
UpdatesDir=C:\Exchange2010_Updates
```

The following is an example of the Setup command to use this answer file.

```
Setup.com /Mode:Install /Roles:Mailbox /AnswerFile:C:\Answer
```

- [*/DoNotStartTransport*]
  Use the */DoNotStartTransport* parameter to specify that the Microsoft Exchange Transport service won't start when Setup completes. By default, Setup starts the Microsoft Exchange Transport service after installing either the Hub Transport or Edge Transport server role. If you need to do additional configuration before the Edge Transport or Hub Transport server accepts e-mail messages, for example, configuring anti-spam agents, you should use this parameter. We recommend that you use this parameter when you use the */RecoverServer* parameter to recover a Hub Transport or Edge Transport server so that you can move the queue database from the failed server to the correct location on the new server before starting the Microsoft Exchange Transport service.

  Note:
  The Microsoft Exchange Transport service runs only on the Hub Transport and Edge Transport server roles.

- [*/EnableLegacyOutlook*]
  Use the */EnableLegacyOutlook* parameter to specify that you have client computers that are running Microsoft Outlook 2003 or earlier. Exchange 2010 will create a public folder database on the Mailbox server. If all of your client computers are running Office Outlook 2007, public folders are optional in Exchange 2010. If you don't use this parameter, Exchange 2010 won't create a public folder database on the Mailbox server. You can add a public folder database later.
  You can only use this parameter if you're installing the first Mailbox server in an organization.
  When you install the first Mailbox server in an existing Exchange Server 2003 organization, by default, Setup will create the public folder database on the Exchange 2010 server. You don't need to specify this parameter. Setup won't create a public folder database on subsequent Mailbox server installations in this organization.
- [*/LegacyRoutingServer*]
  Use the */LegacyRoutingServer* parameter to specify an Exchange 2003 bridgehead server that's located in the routing group to which you'll create the initial routing group connector. A routing group connector is required for mail flow between Exchange 2010 and Exchange 2003 when these Exchange server versions coexist in the same organization.
  You can use this parameter only if you're installing the first Hub Transport server in the organization and if you have Exchange 2003 servers in the existing organization. In this scenario, this parameter is required to establish mail flow between Exchange 2010 and Exchange 2003.
- [*/EnableErrorReporting*]
  Use the */EnableErrorReporting* parameter to enable error reporting during Setup. If you decide to enable error reporting,

the Microsoft Error Reporting Service collects information about how you use Exchange 2010 and about any issues you may encounter. This information is used to help Microsoft diagnose problems and provide solutions.
You can use this parameter only if you're running Setup in Install mode.
If you enable error reporting, Setup sets the following registry key to 0:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\E14\DisableErrorReporting
By default, this registry key is set to 1 and error reporting is disabled.

- [*/NoSelfSignedCertificates*]
  Use the */NoSelfSignedCertificates* parameter if you don't want Setup to create self-signed certificates in the case where no other valid certificate is found for Secure Sockets Layer (SSL) or Transport Layer Security (TLS) sessions. If you don't have a certificate, communication between clients and the Client Access or Unified Messaging server will be unencrypted.
  You can only use this parameter if you're installing either the Client Access server role or the Unified Messaging server role.
- [*/AdamLdapPort:<port>*]
  Use the */AdamLdapPort* parameter to specify the LDAP port to use for the Edge Transport server role Active Directory Lightweight Directory Services (AD LDS) instance. The default value is 50389. Exchange stores the ADAM LDAP port in the following registry key:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v14\EdgeTransportRole\AdamSettings\MSExchangeAdam\LdapPort
  You can use this parameter only if you're installing the Edge Transport server role.
- [*/AdamSslPort:<port>*]
  Use the */AdamSslPort* parameter to specify the SSL port to use for the Edge Transport server role AD LDS instance. You can specify any valid unused port number. The default value is 50636. Exchange stores the Active Directory Lightweight Directory Services (AD LDS) SSL port in the following registry key:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v14\EdgeTransportRole\AdamSettings\MsExchangeAdam\SslPort
  You can use this parameter only if you're installing the Edge Transport server role.
- [*/LanguagePack:<path to language pack bundle> or /lp:<path to language pack bundle>*]
  Use the */LanguagePack* parameter to specify an Exchange language pack that you want to add. For more information, see Exchange 2010 Language Support.
- [*/AddUmLanguagePack:<UM language pack name>*]
  Use the */AddUmLanguagePack* parameter to specify a UM language pack that you want to add. If you add a UM language pack, callers and Outlook Voice Access users can interact with the UM system in another language. For a list of Unified Messaging languages, see Client Language Support for Unified Messaging.
  To install a UM language pack, the Unified Messaging server role must already be installed.
  When you add a language pack, by default, Setup expects the language pack .msi file to be in the ServerRoles

\UnifiedMessaging directory of the installation directory. To specify a different location, use the */SourceDir* parameter.

Note:
Don't include "umlang-" or the .msi extension in the language pack name. For example, the German language pack is umlang-de-DE.msi. To install this language pack, run the following command: **Setup.com /AddUmLanguagePack:de-DE**

Note:
You can't install a language pack by running the language pack .msi file. You must use Setup.com to install the language pack.

- [*/RemoveUmLanguagePack:<UM language pack name>*]
  Use the */RemoveUmLanguagePack* parameter to specify a Unified Messaging language pack that you want to remove.

  Note:
  Don't include "umlang-" or the .msi extension in the language pack name. For example, the German language pack is umlang-de-DE.msi. To remove this language pack, run the following command: **Setup.com /RemoveUmLanguagePack:de-DE**

  Note:
  You can't remove a language pack by running the language pack .msi file. You must use Setup.com to remove the language pack.

- [*/NewProvisionedServer:<server name>*, or */nprs:<server name>*]
  Use the */NewProvisionedServer* parameter to create a placeholder server object in Active Directory so that you can delegate the setup of a server. If you provide permissions to this server object for a user who has Exchange Server Administrators role permissions, that user can install Exchange 2010 on the server. During Setup, additional attributes on this server object will be added. If you don't specify a server name, Setup.com will create a placeholder server object in Active Directory for the local server.
  To run Setup.com with the */NewProvisionedServer* parameter, you must be a member of the Exchange 2010 Organization Management role group, you must have an existing Exchange organization in Active Directory, and you must have at least one Exchange 2010 server installed in the organization. The server that you specify must have a machine account in Active Directory.
  After you provision a server with the */NewProvisionedServer* parameter, you can view the server in the EMC or in the results of the **Get-ExchangeServer** cmdlet.
- [*/RemoveProvisionedServer:<server name>*, or */rprs:<server name>*]
  Use the */RemoveProvisionedServer* parameter to remove a placeholder server object that was created using the *NewProvisionedServer* parameter. You can remove the server object at any time before you install Exchange 2010 on that server. After you install Exchange 2010, you can't use this parameter to remove the server object. You can use this parameter only to remove a provisioned server object. If you run Setup.com with the */RemoveProvisionedServer* parameter on a server that has Exchange 2010 installed, Setup.com will complete successfully, but the server object won't be removed. If you don't specify a server name, Setup.com will remove the placeholder server object in Active Directory that has the same name as the local server.
  To run Setup.com with the */RemoveProvisionedServer* parameter,

you must be a member of the Exchange Organization Management role group.

- [*/ExternalCASServerDomain:<domain>*]
  Use this parameter to specify the external domain for the Client Access server to configure the external URL for the OWA/ ActiveSync/Web Services/OAB virtual directory. For example, to specify the ExternalCASServerDomain, specify the following: **Setup.com /roles:ClientAccess,Mailbox / ExternalCASServerDomain:Mail.Contoso.com**. For more information, see Configure External Client Access Namespaces.
- [*/MdbName:<mailbox database name>*]
  Use this parameter to enter the default database name that is created when installing the Mailbox server role. This name must be unique within the organization. If you don't use this parameter during your Mailbox server role installation, you can create a new database that aligns with your naming conventions, and then move mailboxes if necessary and delete the default database that's created. For example, to specify the MdbName, specify the following: **Setup.com /roles: Mailbox / MdbName: MailboxDatabase01**.
- [*/DbFilePath:<Edb file path>*]
  Use this parameter to enter the full path to the .edb file when installing the Mailbox server role. For example, to specify the Dbfilepath, specify the following: **Setup.com /roles: Mailbox / Dbfilepath:D:\DatabaseFiles\MailboxDatabase01.edb**.
- [*/LogFolderPath:<log folder path>*]
  Use this parameter to enter the folder path to the directory where the database logs should be placed when installing the Mailbox server role. For example, to specify the log folder path, specify the following: **Setup.com /roles: Mailbox / Logfolderpath:D:\DatabaseFiles\LogFolder**.
- [*Upgrade*]
  Use this parameter when you have an existing installation of Exchange and you're installing a new version. This mode is used for service pack installations.
- [*/Hosting*]
  Use this parameter to install and enable hosting functionality and features. For example, to specify hosting mode, specify the following: **Setup.com /roles: Mailbox /Hosting**.
  This parameter is available for multi-tenant deployments. It isn't available for on-premises deployments. For more information about multi-tenant deployments, see Multi-Tenant Support.
- [*/?*]
  Use the */?* parameter to display Help for the Setup.com command.

4. Setup copies the setup files locally to the computer on which you're installing Exchange 2010.
5. Setup checks the prerequisites, including all prerequisites specific to the server roles that you're installing. If you haven't met all the prerequisites, Setup fails and returns an error message that explains the reason for the failure. If you've met all the prerequisites, Setup installs Exchange 2010.
6. Verify that the installation completed successfully. For more information, see Verify an Exchange 2010 Installation.

Examples

The following are examples of using Setup.com:

- **Setup.com /mode:Install /role:Mailbox,HubTransport / TargetDir:"C:\Exchange 2010"**

This command installs the Mailbox server role, the Hub Transport server role, and the management tools to the C:\Exchange 2010 directory.

- **Setup.com /r:M,C,U**
  This command installs the Mailbox server role, Client Access server role, Unified Messaging server role, and the management tools.
- **Setup.com /mode:Uninstall /role:HT**
  This command removes the Hub Transport server role from the server.
- **Setup.com /mode:Uninstall**
  This command completely removes Exchange 2010 from the server and removes this server's Exchange configuration from Active Directory.
- **Setup.com /mode:Install /role:Mailbox,HubTransport /OrganizationName:MyOrg**
  This command creates an Exchange organization in Active Directory called MyOrg and also installs the Mailbox server role, Hub Transport server role, and the management tools.
- **Setup.com /mode:Upgrade**
  This command upgrades an existing version of Exchange. The upgrade parameter is used for service pack installations.
- **Setup.com /PrepareAD /on:"My Org"**
  This command creates an Exchange organization called My Org and prepares Active Directory for Exchange 2010.
- **C:\Exchange2010\bin\Setup.com /m:Install /r:C /SourceDir:d:\amd64**
  This command adds the Client Access server role to an existing Exchange 2010 server using D:\amd64 as the source directory.
- **Setup.com /role:Mailbox,HubTransport /UpdatesDir:"C:\Exchange2010\New Patches"**
  This command updates ExchangeServer.msi with patches from the specified directory, and then installs the Mailbox server role, Hub Transport server role, and the management tools.
- **Setup.com /mode:Install /role:Mailbox,HubTransport /DomainController:DC01**
  This command uses the domain controller DC01 to query and make changes to Active Directory while installing the Mailbox server role, Hub Transport server role, and the management tools.
- **Setup.com /mode:Install /role:Mailbox /AnswerFile:c:\ExchangeConfig.txt**
  This command installs the Mailbox server role by using the settings in the ExchangeConfig.txt file.
- **Setup.com /mode:Install /role:EdgeTranport /DoNotStartTransport**
  This command installs the Edge Transport server role and the management tools. After installation, Exchange doesn't start the Microsoft Exchange Transport service.
- **Setup.com /mode:Install /role:Mailbox,HubTransport /TargetDir:"C:\Exchange2010" /EnableLegacyOutlook**
  This command installs the Mailbox server role, Hub Transport server role, and the management tools into the C:\Exchange2010 directory. This command also creates a public folder database on the Mailbox server.
- **Setup.com /mode:Install /role:Mailbox,HubTransport /TargetDir:"C:\Exchange2010" /LegacyRoutingServer:Ex2003.contoso.com**
  This command installs the Mailbox server role, Hub Transport server role, and the management tools into the C:\Exchange2010 directory. This command also creates a routing group connector from the Hub Transport server to the specified legacy Exchange server, and creates a routing group connector from the legacy Exchange server to the Hub Transport server.
- **Setup.com /mode:Install /role:Mailbox,HubTransport /EnableErrorReporting**
  This command installs the Mailbox server role, Hub Transport server role, and the management tools. This command also enables error reporting.
- **Setup.com /mode:Install /role:ClientAccess /NoSelfSignedCertificates**

This command installs the Client Access server role and the management tools and doesn't create a self-signed certificate.

- **Setup.com /r:ET /AdamLdapPort:50390 /AdamSslPort:50640**
  This command installs the Edge Transport server role and the management tools and configures the Active Directory Lightweight Directory Services (AD LDS) instance to use port 50390 for LDAP and port 50640 for SSL.
- **Setup.com /rprs:Exchange03**
  This command removes the object Exchange03 from Active Directory.
- **Setup.com /mode:Install /languagepack:<"C:ExchangeLanguagePack"> /role:Mailbox,HubTransport**
  This command installs the language pack bundle and the Mailbox and Hub Transport server roles.
- **Setup.com /AddUmLanguagePack:ko-KR**
  This command installs the Korean Unified Messaging language pack from the %ExchangeSourceDir%\ServerRoles\UnifiedMessaging directory.

1.2.2.7.9 Install Exchange 2010 Using the Custom Installation Type

Install Exchange 2010 Using the Custom Installation Type

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-31*

You can install Microsoft Exchange Server 2010 using the **Custom** installation type. A custom installation enables you to select which specific server role or roles you want installed. Custom installation differs from the Exchange 2010 **Typical** installation type in which the Hub Transport, Client Access, and Mailbox server roles plus the Exchange management tools are installed by default. For detailed steps about how to perform an installation of Exchange 2010 with the **Typical** installation type, see Install Exchange Server 2010.

After you've completed a custom installation of Exchange 2010, be aware of the following important points:

- **Potential for simultaneous OAB download requests** After you install the first Exchange 2010 server in an organization, if you create a recipient object (such as a mailbox, contact, distribution list, mailbox agent, or mail-enabled public folder), it will have a LegacyExchangeDN that corresponds to the new administrative group for the Exchange 2010 server. Because of this LegacyExchangeDN, Microsoft Outlook will request a full offline address book (OAB) download from the Exchange 2010 server for each user in this organization that logs on to a mailbox using Outlook and using OAB versions 2 or 3. This could result in many simultaneous OAB download requests, which causes high network utilization.
- **System restart required with the UM server role** After installing the Unified Messaging (UM) server role, you must restart the system to allow the Microsoft Exchange Unified Messaging service to reserve the required TCP ports.

Prerequisites

- Before you can install Exchange 2010, make sure that the server has the necessary prerequisites installed. You must ensure that the appropriate

software and operating system prerequisites are installed on the server before you begin your Exchange 2010 installation. To install the prerequisites for all server roles, see Exchange 2010 Prerequisites. For more information about system requirements, see Exchange 2010 System Requirements.

- For e-mail messages to flow correctly, you must install both the Mailbox server role and the Hub Transport server role in the same Active Directory site.
- You can install the Mailbox server role, Hub Transport server role, Client Access server role, and Unified Messaging server role on the same computer or on separate computers. The Edge Transport server role must always be installed on dedicated hardware; it can't coexist with other server roles.

Warning:

After you install Exchange 2010 on a server, you must not change the server name. Renaming a server after you have installed an Exchange 2010 server role is not supported.

Perform a custom installation of Exchange 2010

To perform the following procedure, the account you use must be delegated membership in the Schema Admins group if you haven't previously prepared the Active Directory schema.

If you're installing the first Exchange 2010 server in the organization, the account you use must have membership in the Enterprise Admins group.

If you've already prepared the schema and aren't installing the first Exchange 2010 server in the organization, the account you use must be delegated the Organization Management management role.

Note:

For information about preparing Active Directory for Exchange 2010, see Prepare Active Directory and Domains. For more information about permissions in Exchange 2010, see Understanding Role Based Access Control.

1. Log on to the server on which you want to install Exchange 2010.

   Important:

   Be sure that you've completed the prerequisite tasks discussed both in this topic and the Exchange 2010 Prerequisites topic before you install Exchange 2010.

2. Insert the Exchange 2010 DVD into the DVD drive (or browse to your install location). If Setup.exe doesn't start automatically, navigate to the DVD drive and double-click **Setup.exe**.
3. On the **Start** page, ensure that you've completed Steps 1 and 2. If you haven't already installed these components, Setup will provide you with links to Microsoft Web sites where you can download the necessary prerequisites. For more information about Windows PowerShell installation, see Install Windows Management Framework.

   Important:

   If you're installing Exchange 2010 on Windows Server 2008 R2, don't use the downloadable .NET Framework package. Instead, use Server Manager in Windows Server 2008 R2 or run **ServerManagerCmd -i NET-Framework**.

4. On the **Start** page, click **Step 3: Choose Exchange language option**. The language options will appear below Step 3. Choose either:
   4.a. **Install all languages from the language bundle** If you choose this option, all supported languages in the bundle are installed. Setup can download the necessary language bundles automatically, or you can browse to the location (hard drive or a network share) of previously

downloaded language bundles and install those.

4.b. **Install only languages from the DVD** If you choose this option, only English (U.S.) language support is installed. Language bundles can be installed at a later time to provide support for additional languages if needed.

5. After the language installation is complete, on the **Start** page, click **Step 4: Install Microsoft Exchange**. Setup copies the setup files locally to the computer on which you're installing Exchange 2010.
6. In the Exchange Server 2010 Setup wizard, on the **Introduction** page, click **Next**.
7. On the **License Agreement** page, review the software license terms. If you agree to the terms, select **I accept the terms in the license agreement**, and then click **Next**.
8. On the **Error Reporting** page, select **Yes**, and then click **Next**.
9. On the **Installation Type** page, click **Custom Exchange Server Installation**. For Exchange Server 2010 Service Pack 1 (SP1), you can select to automatically install all required Windows roles and features for this server. If you want to change the path for the Exchange 2010 installation, click **Browse**, locate the appropriate folder in the folder tree, and then click **OK**. Click **Next**.

10. On the **Server Role Selection** page, select the server roles that you want to install on the computer and click **Next**.

Note:

The Edge Transport server role can't coexist on the same computer with any other server role. You must deploy the Edge Transport server role in a perimeter network and outside your internal Active Directory forest.

11. If you selected **Mailbox Role**, **Client Access Role**, **Hub Transport Role**, and/or **Unified Messaging Role**, and if this is the first Exchange 2010 server in your organization, on the **Exchange Organization** page, type a name for

your Exchange 2010 organization. The Exchange organization name can contain only the following characters:
11.a.A through Z
11.b.a through z
11.c.0 through 9
11.d.Space (not leading or trailing)
11.e.Hyphen or dash

Note:
The organization name can't contain more than 64 characters. The organization name can't be blank. If the organization name contains spaces, you must enclose it in quotation marks.

12. If this is the first Exchange 2010 server in your organization, on the **Client Settings** page, click the appropriate option based on the client computers.
13. On the **Client Settings** page, if you have client computers running Office Outlook 2003 or earlier and you select **Yes**, Exchange 2010 will create a public folder database on the Mailbox server. If all your client computers are running Outlook 2010, public folders are optional in Exchange 2010. If you select **No**, Exchange 2010 won't create a public folder database on the Mailbox server. You can add a public folder database later. For example, if you add client computers running Outlook 2003 and you need a public folder database, you can create one on the Exchange 2010 Mailbox server. You must then configure the OAB for public folder distribution, and then restart the Microsoft Exchange Information Store service before client computers running Outlook 2003 and earlier will be able to connect to the server.
14. On the **Configure Client Access Server external domain** page, enter a domain name to use to configure your Client Access servers.

Note:
If the Client Access server won't be Internet-facing, you can click **Next** without configuring a domain name. For more information about configuring Client Access servers, see Managing External Client Access. Click **Next**.

15. On the **Customer Experience Improvement Program** page, choose the appropriate selection for your organization, and then click **Next**.
16. On the **Readiness Checks** page, view the status to determine if the organization and server role prerequisite checks completed successfully. If they haven't completed successfully, you must resolve any reported errors before you can install Exchange 2010. You don't need to exit Setup when resolving some of the prerequisite errors. After resolving a reported error, click **Retry** to rerun the prerequisite check. Be sure to also review any warnings that are reported. If all readiness checks have completed successfully, click **Install** to install Exchange 2010.
17. On the **Completion** page, click **Finish**.

1.2.2.7.10 Install the Exchange 2010 Management Tools

Install the Exchange 2010 Management Tools

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-21*

With the Microsoft Exchange Server 2010 management tools, you can configure and

manage your Exchange organization remotely. This topic explains how you can either use Setup.exe or unattended setup mode to install the Exchange 2010 management tools.

You can install the Exchange 2010 management tools on the following Windows operating systems:

- Windows 7
- Windows Vista with Service Pack 2 (SP2)
- Windows Server 2008 SP2
- Windows Server 2008 R2

For more information about managing Exchange 2010, see Exchange Management Console and Exchange Management Shell.

Prerequisites

You must ensure that each of your servers meets the appropriate prerequisites and system requirements before you begin your installation. For more information, see Exchange 2010 Prerequisites and Exchange 2010 System Requirements.

Warning:

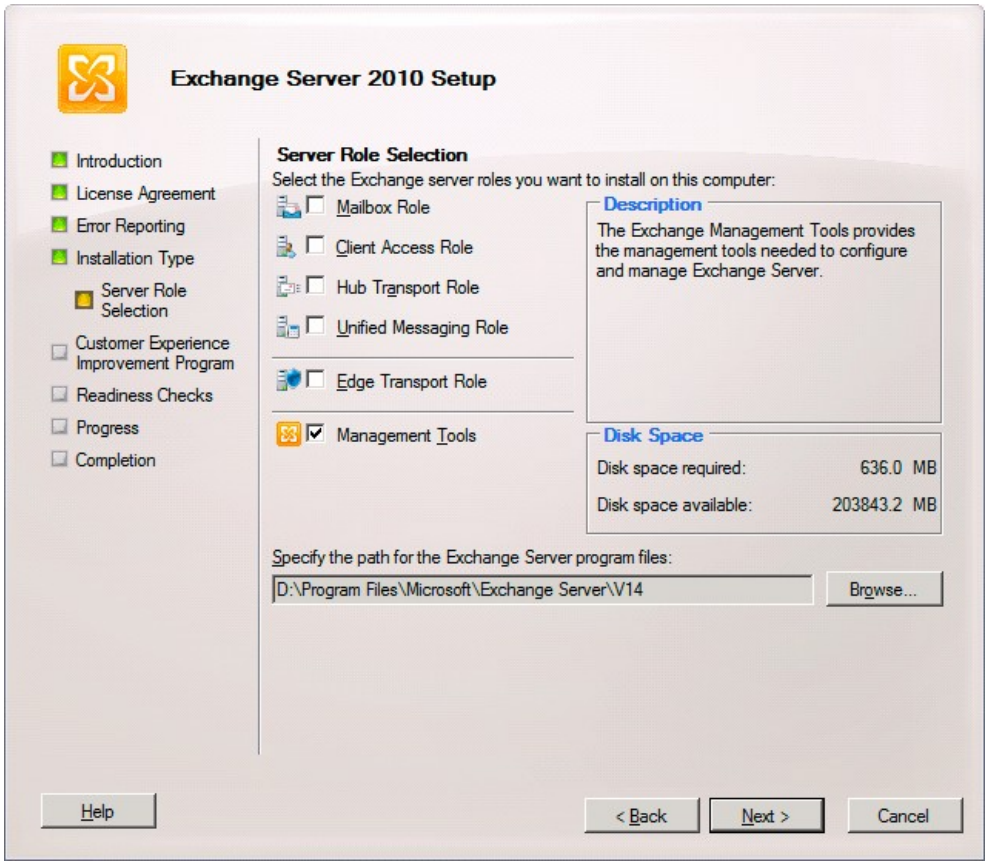
After you install Exchange 2010 on a server, you must not change the server name. Renaming a server after you have installed an Exchange 2010 server role is not supported.

Use Setup to install the Exchange 2010 management tools

1. Log on to the server on which you want to install the Exchange 2010 management tools on, using a domain account that has local administrative privileges.
2. Insert the Exchange 2010 DVD into the DVD drive. When the AutoPlay dialog appears, click **Run Setup.exe** under **Install or run program**. If the AutoPlay dialog doesn't appear, navigate to the root of the DVD and double-click Setup.exe. Alternatively, browse to the location of your Exchange 2010 installation files and double-click Setup.exe.
3. The Exchange Server 2010 Setup welcome screen appears. In the **Install** section, the software listed for **Step 1: Install .NET Framework 3.5 SP1** and **Step 2: Install Windows PowerShell v2** was installed with the Exchange 2010 prerequisites. If these prerequisites aren't already installed, click the appropriate step to install them.
4. When **Step 1**, **Step 2**, and **Step 3** are listed as **Installed**, click **Step 4: Install Microsoft Exchange**.

   Note:

   After your installation is complete, you can return to complete **Step 5: Get critical updates for Microsoft Exchange**.
5. In the Exchange 2010 Setup wizard, on the **Introduction** page, click **Next**.
6. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
7. On the **Error Reporting** page, select whether you want to enable or disable Exchange Error Reporting feature, and then click **Next**.
8. On the **Installation Type** page, click **Custom Exchange Server Installation**. If you want to change the path for the Exchange 2010 installation, click **Browse**, locate the appropriate folder in the folder tree, and then click **OK**. Click **Next**.
9. On the **Server Role Selection** page, select **Management Tools**.



10. If this is the first Exchange 2010 server in your organization, on the **Exchange Organization** page, type a name for your Exchange organization. The Exchange organization name can contain only the following characters:
    - A through Z
    - a through z
    - 0 through 9
    - Space (not leading or trailing)
    - Hyphen or dash

    Note:
    The organization name can't contain more than 64 characters. The organization name can't be blank. If the organization name contains spaces, you must enclose it in quotation marks.
11. On the **Readiness Checks** page, view the status to determine if the organization and other prerequisite checks completed successfully. If they have not completed successfully, you must resolve any reported errors before you can install Exchange 2010. You don't need to exit Setup when resolving some of the prerequisite errors. After resolving a reported error, click **Retry** to re-run the prerequisite check. Be sure to also review any warnings that are reported. If all readiness checks have completed successfully, click **Install** to install the Exchange 2010 management tools.
12. On the **Completion** page, click **Finish**.

Use unattended Setup mode to install the Exchange 2010 management tools

1. Insert the Exchange 2010 DVD into the DVD drive, and then at the command prompt navigate to the DVD drive, or navigate to the network location of the

Exchange 2010 installation files.
2. At the command prompt, run the following command.

```
Setup.com /R:MT
```

For more information, see Install Exchange 2010 in Unattended Mode.

1.2.2.7.11 Move Internet Mail Flow from Exchange 2003 to Exchange 2010

Move Internet Mail Flow from Exchange 2003 to Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you upgrade your organization from Microsoft Exchange Server 2003 to Exchange Server 2010, one of the steps you need to complete is moving the handling of Internet mail from your existing servers to Exchange 2010 servers. In Exchange 2010, the preferred method of handling Internet mail is by using Edge Transport servers subscribed to the Active Directory site where your Hub Transport servers reside. However, you can also configure Internet mail flow through a third-party SMTP host or directly through your Hub Transport servers. This topic provides instructions for both of these approaches to moving Internet mail flow from Exchange 2003 to Exchange 2010 servers:

Move Internet Mail Flow to Exchange 2010 Using Edge Transport Servers

Move Internet Mail Flow to Exchange 2010 without Edge Transport Servers

To learn more about upgrading from Exchange 2003 to Exchange 2010, see the following topics:

- Understanding Upgrade from Exchange 2003 to Exchange 2010
- Understanding Upgrade from Exchange 2003 and Exchange 2007 to Exchange 2010

Prerequisites

- Exchange 2010 Client Access, Hub Transport, and Mailbox servers have been deployed into your existing Exchange organization.
- Mail flow between your existing Exchange organization and Exchange 2010 deployment is functioning correctly.
- Exchange 2010 Edge Transport servers have been deployed in your perimeter network (if you will be using Edge Transport servers for Internet mail).

Move Internet Mail Flow to Exchange 2010 Using Edge Transport Servers

1. Subscribe the Edge Transport servers to your Exchange organization. This will enable Internet message flow through your Exchange 2010 Hub and Edge Transport servers.
   1.a. Create an Edge Subscription File on an Edge Transport Server
   1.b. Import an Edge Subscription File to an Active Directory Site
2. Remove the SMTP connector in Exchange 2003 that is used to handle Internet mail. Your account needs to be a member of the local administrators

group and a member of a group that has had the Exchange Administrators role applied at the administrative group level.
2.a.In Exchange System Manager, expand the **Organization** node, expand **Administrative Groups**, expand *<AdministrativeGroupName>*, expand **Routing Groups**, expand *<RoutingGroupName>*, and then select **Connector**.
2.b.In the right-hand pane, right-click the connector you want to delete and select **Delete**.
2.c.Click **OK** to confirm the deletion.

For more information about Edge subscriptions, see Understanding Edge Subscriptions.

Move Internet Mail Flow to Exchange 2010 without Edge Transport Servers

1. Configure mail flow by using one of the methods listed below depending on the needs of your organization. This will enable Internet message flow through your Exchange 2010 Hub Transport servers.
   - Configure Internet Mail Flow Through Exchange Hosted Services or an External SMTP Gateway
   - Configure Internet Mail Flow Directly Through a Hub Transport Server
2. Remove the SMTP connector in Exchange 2003 that is used to handle Internet mail. Your account needs to be a member of the local administrators group and a member of a group that has had the Exchange Administrators role applied at the administrative group level.
   - In Exchange System Manager, expand the **Organization** node, expand **Administrative Groups**, expand *<AdministrativeGroupName>*, expand **Routing Groups**, expand *<RoutingGroupName>*, and then select **Connector**.
   - In the right-hand pane, right-click the connector you want to delete and select **Delete**.
   - Click **OK** to confirm the deletion.

1.2.2.7.12 Move Mailboxes from Exchange 2003 Servers to Exchange 2010 Servers

Move Mailboxes from Exchange 2003 Servers to Exchange 2010 Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

Moving mailboxes from Microsoft Exchange Server 2003 Service Pack 2 (SP2) or later to Exchange Server 2010? Consider the following:

- The move process is performed offline, and end-users won't be able to access their mailboxes during the move.
- Perform the move from a server running Exchange 2010 by using the move request cmdlets in the Exchange Management Shell. You can't use Exchange System Manager on an Exchange 2003 server to move the mailboxes.
- You can't move mailboxes from Exchange 2003 Service Pack 1 (SP1) or earlier.
- Exchange 2003 doesn't have resource mailboxes. Instead, you must use shared mailboxes to represent resources. If you move a shared mailbox from

Exchange 2003 to Exchange 2010, the move request creates the mailbox as a shared Exchange 2010 mailbox. After you move the mailbox to Exchange 2010, you can convert it to a resource mailbox. For more information, see Convert a Mailbox.

For detailed instructions about how to move mailboxes, see Managing Move Requests.

To learn more about moving mailboxes, see Understanding Move Requests.

1.2.2.7.13 Move Mailboxes from Exchange 2007 Servers to Exchange 2010 Servers

Move Mailboxes from Exchange 2007 Servers to Exchange 2010 Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-28*

Moving mailboxes from Microsoft Exchange Server 2007 Service Pack 3 (SP3) to Exchange Server 2010? Consider the following:

- The move process is performed online, and end-users will be able to access their mailboxes during the move.
- You can't move mailboxes from Exchange 2007 SP1 or earlier. The source Mailbox server must be running Exchange 2007 SP3.
- Perform the move from a server running Exchange 2010 by using the Exchange Management Console or the move request cmdlets in the Exchange Management Shell. You can't use the **Move-Mailbox** cmdlets in Exchange 2007 to move mailboxes to Exchange 2010 servers.

For detailed instructions about how to move mailboxes, see Managing Move Requests.

To learn more about moving mailboxes, see Understanding Move Requests.

1.2.2.7.14 Move Mailboxes from Exchange 2010 Servers to Exchange 2003 Servers

Move Mailboxes from Exchange 2010 Servers to Exchange 2003 Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-14*

Moving mailboxes from Microsoft Exchange Server 2010 to Exchange Server 2003? Consider the following:

- The move process is performed offline, and end-users won't be able to access their mailboxes during the move.
- Perform the move from the server running Exchange 2010 by using the move request cmdlets in the Exchange Management Shell. You can't use Exchange System Manager on an Exchange 2003 server to move the mailboxes.

- If you're moving a mailbox that has a personal archive associated with it, you must disable the archive before moving the mailbox. For details, see Disable a Personal (On-Premises) or Cloud-Based Archive for a Mailbox.
- If you're moving a mailbox to Exchange 2003, you must disable single-item recovery and purge the Recoverable Items folder. For details, see Clean Up the Recoverable Items Folder.

For detailed instructions about how to move mailboxes, see Managing Move Requests.

To learn more about moving mailboxes, see Understanding Move Requests.

1.2.2.7.15 Move Mailboxes from Exchange 2010 Servers to Exchange 2007 Servers

Move Mailboxes from Exchange 2010 Servers to Exchange 2007 Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-28*

Moving mailboxes from Microsoft Exchange Server 2010 to Exchange Server 2007? Consider the following:

- The move process is performed offline, and end-users won't be able to access their mailboxes during the move.
- You can't move mailboxes to or from servers running Exchange 2007 Service Pack 1 (SP1) or earlier. The target database must be on a server running Exchange 2007 SP3.
- Perform the move from an Exchange 2010 server by using the move request cmdlets in the Exchange Management Shell. You can't use the **Move-Mailbox** cmdlets in Exchange 2007 to move the mailboxes.
- If the mailbox that you're moving has an archive mailbox associated with it, you must disable the archive before moving the mailbox.
- If you're moving a mailbox to Exchange 2007, you must disable single-item recovery and purge the Recoverable Items folder. For details, see Clean Up the Recoverable Items Folder.

For detailed instructions about how to move mailboxes, see Managing Move Requests.

To learn more about moving mailboxes, see Understanding Move Requests.

1.2.2.7.16 Prepare Legacy Exchange 2003 Permissions

Prepare Legacy Exchange 2003 Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

When upgrading from Exchange Server 2003 to Exchange Server 2010, you must first grant specific Exchange permissions in each domain in which you have run Exchange 2003

DomainPrep. To do this, you run the `setup /PrepareLegacyExchangePermissions` command. Granting these permissions is part of preparing Active Directory and your domains for installing Exchange Server 2010. For detailed instructions, see Prepare Active Directory and Domains.

This topic explains why you must run the `setup /PrepareLegacyExchangePermissions` command, when you run it, and what permissions are set by the command in your Exchange Server 2010 organization.

Why Run Setup /PrepareLegacyExchangePermissions

Essentially, you must run the `setup /PrepareLegacyExchangePermissions` command so that the Exchange 2003 Recipient Update Service functions correctly after you update the Active Directory schema for Exchange Server 2010. This section explains the main issue and how running the command resolves this issue.

Issue

In Exchange Server 2003, the Recipient Update Service updates some mailbox attributes, such as the proxy address, on mail-enabled user objects. The Recipient Update Service has permission to modify these attributes because the computer account (named *<ServerName>*) for the server on which the Recipient Update Service runs is in the Exchange Enterprise Servers (EES) group. The EES group is created when you run Exchange Server 2003 DomainPrep. Instead of granting the EES group permissions to each individual mailbox attribute that the Recipient Update Service must modify, the mailbox attributes are grouped together in property sets. When you run Exchange Server 2003 DomainPrep, Exchange provides the EES group with permissions to modify the property sets through access control entries (ACEs) that Exchange sets on the domain container in Active Directory.

Exchange Server 2010 has a management role called Recipient Management. This role contains permissions to manage the e-mail attributes of all users. Exchange administrators who are members of the Exchange Recipient Management role can manage only users' e-mail properties.

To enable this functionality, Exchange Server 2010 must move some e-mail attributes of users into a property set called the "Exchange-Information property set." Exchange does this by redefining the attribute schemas in Active Directory when importing the new Exchange Server 2010 schema. However, the legacy EES group doesn't have permissions to the Exchange-Information property set. Therefore, when you import the new Exchange Server 2010 schema, the Recipient Update Service will no longer have permissions to the users' e-mail attributes and will stop functioning correctly. (For example, it will not be able to set proxy addresses for newly created Exchange Server 2003 users.)

Resolution

Running the `setup /PrepareLegacyExchangePermissions` command enables the legacy Recipient Update Service to function correctly. Before importing the new Exchange Server 2010 schema, Exchange Server 2010 must grant new permissions in each domain in which you have run Exchange Server 2003 DomainPrep. The `setup /PrepareLegacyExchangePermissions` command grants these new permissions. Before you run `setup /PrepareSchema`, you must run `setup /PrepareLegacyExchangePermissions` and allow the permissions to replicate across your Exchange organization.

The server where you run `setup /PrepareLegacyExchangePermissions` contacts the local global catalog to locate the domains in which you have run Exchange Server 2003 DomainPrep by checking for the EES and Exchange Domain Servers (EDS) groups. The

server must be able to communicate with every domain in the forest in which you ran Exchange Server 2003 DomainPrep. Also, the account that you use to run `setup /PrepareLegacyExchangePermissions` must have the permissions assigned to the Enterprise Admins universal security group (USG) so that it can set the ACEs in each domain and in the Exchange organization.

Permissions Set By Setup /PrepareLegacyExchangePermissions

Running `setup /PrepareLegacyExchangePermissions` finds every domain in the forest that has the EES group and the Exchange Domain Servers (EDS) group. For each domain that has these groups, `setup /PrepareLegacyExchangePermissions` does the following:

- Adds an ACE to the domain root access control list (ACL) to provide the EES group with WRITE_PROP permissions on the Exchange-Information property set.
- Adds an ACE to the domain root ACL to provide authenticated users with READ_PROP permissions on the Exchange-Information property set.
- Adds an ACE to the AdminSDHolder container of the domain to provide the EES group with WRITE_PROP and READ_PROP permissions on the Exchange-Information property set.
- Adds an ACE to the Exchange organization container ACL to provide the EDS group with WRITE_PROP permissions on the Exchange-Information property set.

Running Setup /PrepareLegacyExchangePermissions Again

There are some cases in which you will need to run `setup /PrepareLegacyExchangePermissions` again:

- You have a domain that contains Exchange Server 2003 servers, and you have not run DomainPrep.
- In an existing domain, you have mailbox-enabled users who will log on to mailboxes on Exchange Server 2003 servers in domains in which you have not run DomainPrep.

In these cases, you must run `setup /PrepareLegacyExchangePermissions` again after you run Exchange Server 2003 DomainPrep. This allows the Exchange Server 2003 Recipient Update Service to function correctly in this domain.

Exchange 2010 Deployment Permissions Reference

Exchange 2010 needs permissions to deploy and function properly in your organization. These permissions are stamped on the access control lists (ACL) of the objects used by Exchange 2010 during setup. For more information, see Exchange 2010 Deployment Permissions Reference.

Provision Exchange 2010 Server and Delegate Setup

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-06*

This topic explains how to provision a server and delegate the setup and installation of Exchange. After the initial installation of the first instance of Exchange Server, you can provision a server for delegated setup of subsequent installations. This procedure allows a delegated account to install single instances of Exchange in your domain, without being a member of the Organization Management management role group.

However, be aware that you must install the *first* Exchange server in the domain by using an account that *is* a member of the Organization Management role group and local Administrators group. You can then install subsequent instances of Exchange using a member of the Delegated Setup management role group. (You just can't install the first instance of an Exchange server using a member of the Delegated Setup role group.)

Important:

A delegated user can't uninstall an Exchange server. Uninstalling or removing Exchange servers requires an account that is a member of the Organization Management role group and local Administrators group.

For more information about permissions, delegating roles, and the rights that are required to administer Exchange 2010, see Understanding Permissions, Understanding Role Based Access Control, and Delegated Setup.

Note:

Exchange 2010 needs permissions to deploy and function correctly in your organization. These permissions are stamped on the access control lists (ACL) of the objects used by Exchange 2010 during setup. For more information, see Exchange 2010 Deployment Permissions Reference.

You can use **Setup.com /NewProvisionedServer** to provision your server. The **Setup.com /NewProvisionedServer** command performs the following tasks:

- Creates the server object within the configuration partition: **CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Organization Name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Root Domain>**
- Adds the following access control entries (ACE) to the server object within the configuration partition for the Delegated Setup role group:
  - Full Control on the server object and its children
  - Deny access control entry for the Send As extended right
  - Deny access control entry for the Receive As extended right
  - Deny CreateChild and DeleteChild permissions for Exchange Public Folder Store objects

  Note:

  Public folders are administered at an organizational level; therefore, the creation and deletion of public folder stores is restricted to Exchange Organization Administrators.
- Adds the computer account to the Exchange Servers group.
- Adds the server as a provisioned server in the Exchange Management Console.

Provision an Exchange 2010 Server

If Exchange Server is installed on the computer you're provisioning, you can run the Setup.com command with associated arguments from the Run line or a command prompt. If the computer that you are running the Setup.com command from doesn't have Exchange installed, you must insert the Exchange 2010 DVD into the computer, and then run the Setup.com command from the root directory of the DVD.

Provision the local server

To run **Setup.com /NewProvisionedServer**, the account you use must be a member of the Organization Management role group.

To provision the local server, run the following command:

```
Setup.com /NewProvisionedServer
```

Note:
Running this command provisions the local server, but it doesn't delegate a user.

Provision a remote server

To run **Setup.com /NewProvisionedServer**, the account you use must be a member of the Delegated Setup role group.

To provision a remote server, run the following command:

```
Setup.com /NewProvisionedServer:ServerName
```


1.2.2.7.18 Upgrade Custom LDAP Filters to OPATH Filters

Upgrade Custom LDAP Filters to OPATH Filters

Planning and Deployment > Deploying Exchange 2010 > Managing Deployment of Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-21*

In Microsoft Exchange Server 2003 and earlier versions, LDAP filtering syntax is used to create custom address lists, global address lists (GALs), e-mail address policies, and distribution groups. In Exchange Server 2010 and Exchange Server 2007, the OPATH filtering syntax replaces the LDAP filtering syntax. Using the OPATH filtering syntax allows you to create filters directly in Exchange Management Shell commands by using the *-RecipientFilter* parameter.

Note:
LDAP syntax filters are supported in Exchange 2010 and will exist only on objects that have been migrated from Exchange 2003 or earlier versions. If you want to edit the LDAP filter from an Exchange 2010 server, you must upgrade these LDAP filters to the OPATH syntax. For example, if you have Exchange 2003 servers in your organization, you can manage the LDAP syntax filter from an Exchange 2003 server. However, you can't manage or create LDAP syntax filters in Exchange 2010.

For information about how you can use a script to convert your LDAP filters to the OPATH syntax, see the Exchange Server Team blog article Need help converting your LDAP filters to OPATH?

Note:
The content of each blog and its URL are subject to change without notice. The content

within each blog is provided "AS IS" with no warranties, and confers no rights. Use of included script samples or code is subject to the terms specified in the Microsoft Terms of Use.

Important:
In Exchange 2003, you can create custom Active Directory extension attributes. However, in Exchange 2010, you can't use custom extension attributes as a filterable property. If your organization has custom extension attributes, we recommend that you use the 15 custom attributes provided by Exchange 2010 for each recipient. However, if the custom attributes don't meet the needs of your organization, we recommend that you don't upgrade objects that use custom extension attributes.

For more information about creating filters in recipient commands, see Creating Filters in Recipient Commands.

Contents

Determining Which Objects Require Upgrading

Before you upgrade the Exchange objects, you must first determine which objects require upgrading. There are two types of filters that you may need to upgrade:

- **Default objects** Default objects are the default e-mail address policies and address lists created when Exchange is installed.
- **Custom objects** Custom objects are custom LDAP filters created by an Exchange administrator in Exchange 2003 or an earlier version.

To determine which objects require upgrading, you can use the Exchange Management Console or the Exchange Management Shell.

Using the Exchange Management Console

To use the Exchange Management Console to determine which objects require upgrading, you must edit the object by using the Edit wizard for that object.

For example, if you want to determine whether an e-mail address policy has been upgraded, you select the e-mail address policy from the result pane, and then in the action pane, click **Edit** to open the Edit E-Mail Address Policy wizard.

If the e-mail address policy was created in Exchange 2003 and the filtering syntax hasn't yet been upgraded to OPATH, an error is displayed. This error signifies that the filtering syntax of the e-mail address policy was created in Exchange 2003 or an earlier version and may require upgrading. For information about how to upgrade the filtering syntax, see "Upgrading Default Objects" and "Upgrading Custom Objects" later in this topic.

Using the Exchange Management Shell

To use the Exchange Management Shell to determine which objects require upgrading, you can use the associated **Get-** cmdlet and format the list to view the recipient filters and the version of Exchange.

This example determines which e-mail address policies require upgrading.

```
Get-EmailAddressPolicy | Format-List Name, *RecipientFilter*, ExchangeVersion
```

After you run this command, the following information is displayed in the Exchange Management Shell.

In this example, two e-mail address policies were returned by the **Get-EmailAddressPolicy** cmdlet. **Default Policy**, which is highlighted in blue, is an Exchange 2003 object that requires upgrading. **Resource Mailboxes**, which is highlighted in red, was either created in Exchange 2010 or has already been upgraded.

If you can answer "Yes" to any of the following questions, the object hasn't been upgraded:

- Is the *RecipientFilter* attribute empty?
- Does the value of the *RecipientFilterType* attribute equal "Legacy"?
- Does the value of the *ExchangeVersion* attribute equal "0.0 (6.5.6200.0)"?

Return to top

Upgrading Default Objects

When you install Exchange 2003, a default e-mail address policy and multiple default address lists are created. The following list includes the default objects that will need to be upgraded if the filter must be changed in Exchange 2010, or if you need to administer the object in Exchange 2010:

- **E-mail Address Policies:** Default Policy
- **Address Lists:** All Contacts, All Groups, All Rooms, All Users, Default Global Address List, Public Folders

Because default objects have known filters, you can easily upgrade these default objects. For detailed instructions about how to upgrade default objects, see the following topics:

- Upgrade Default Address Lists from LDAP Filters to OPATH Filters
- Upgrade the Default E-Mail Address Policy from LDAP Filters to OPATH Filters

Note:

The *-ForceUpgrade* parameter doesn't construct the replacement recipient filter for the object, nor does it upgrade the object. The *-ForceUpgrade* parameter suppresses the confirmation question so that you can upgrade by using an unattended script.

Return to top

Upgrading Custom Objects

Upgrading custom objects is more difficult because it requires you to determine what the custom LDAP filter is filtering for, and then translate the filter into OPATH syntax. Custom LDAP filters can be created for the following Exchange objects:

- Address lists
- E-mail address policies
- Dynamic distribution groups

There are two methods you can use to upgrade custom objects:

- Use a script provided by the Microsoft Exchange Team. For information about this script, see the Exchange Server Team blog article Need help converting your LDAP filters to OPATH?

  Note:

  The content of each blog and its URL are subject to change without notice. The content within each blog is provided "AS IS" with no warranties, and

confers no rights. Use of included script samples or code is subject to the terms specified in the Microsoft Terms of Use.

- Manually upgrade the LDAP filter to OPATH as described in the following sections.

Step 1: Determine What the Custom LDAP Filter Does

To upgrade an Exchange 2003 LDAP filter to the OPATH syntax, you must first determine what the LDAP filter is filtering. Perform the following steps:

1. Copy an existing filter into a text editing application, such as Notepad.

Important:

Before you begin, document your existing LDAP filter.

This example is an LDAP filter for an e-mail address policy.

```
(&(&(|(&(&(objectCategory=user)(msExchangeHomeServerName=/o=ORG/ou=SIT
```

2. In Notepad, indent the lines of the filter to see the logical flow.
3. Write a statement that explains what the filter does. In this example, the e-mail address policy's filter includes the following objects:
   - All user category objects that have a home server in a particular administrative group
   - All groups or dynamic distribution lists that begin with a specific display name

Step 2: Translate the LDAP Filter into OPATH Syntax

After you determine the function of the LDAP filter, you must translate the LDAP filter into the OPATH syntax.

Note:

The names for many properties have changed. For example, the LDAP property **mailNickname** is called **Alias** in Exchange 2010. To view a complete list of the property names, see Filterable Properties for the -RecipientFilter Parameter.

1. Create the recipient filter based on the statements you recorded in Step 3 of the section "Determine What the Custom LDAP Filter Does" earlier in this topic.

```
(ServerLegacyDN -like "/o=ORG/ou=SITE/cn=Configuration/cn=Servers/cn=*
 ((RecipientType -eq "<group recipient type>" -or RecipientType -eq "D
```

2. Construct the command by using the appropriate **Set** cmdlet, and then run the command in the Exchange Management Shell.

```
Set-EmailAddressPolicy eap1 -RecipientFilter {(ServerLegacyDN -like "/
```

Note:

Many of the properties for the *-RecipientFilter* parameter accept wildcard characters. If you use a wildcard character, don't use the *-eq* operator. Instead, use the *-like* operator. The *-like* operator is used to find pattern matches in strings, whereas the *-eq* operator is used to find an exact match.

Return to top

1.2.2.7.18.1 Upgrade the Default E-Mail Address Policy from LDAP Filters to OPATH Filters

Upgrade the Default E-Mail Address Policy from LDAP Filters to OPATH Filters

Deploying Exchange 2010 > Managing Deployment of Exchange 2010 > Upgrade Custom LDAP Filters to OPATH Filters >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Microsoft Exchange Server 2003 and earlier versions, LDAP filtering syntax is used when customizing the default e-mail address policy. However, in Exchange Server 2010, the OPATH filtering syntax replaces the LDAP filtering syntax. This topic explains how to use the Exchange Management Shell to upgrade the filtering syntax from LDAP to OPATH for the legacy default e-mail address policy.

There is only one default e-mail address policy (named **Default Policy**) in your organization. The default e-mail address policy can be identified by having the priority value of "lowest".

Note:
LDAP syntax filters are supported in Exchange 2010 and will exist only on objects that have been migrated from Exchange 2003 or earlier versions. You must upgrade these LDAP filters to the OPATH syntax only if you want to edit the filter from an Exchange 2010 server. For example, if you have Exchange 2003 and Exchange 2010 servers in your organization, you can manage the LDAP syntax filter from an Exchange 2003 server. You can't manage or create LDAP syntax filters in Exchange 2010.

For more information about how to determine if the default e-mail address policy requires upgrading, see "Determining Which Objects Require Upgrading" in Upgrade Custom LDAP Filters to OPATH Filters.

Use the Shell to upgrade the default e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to upgrade the default e-mail address policy.

This example upgrades the default e-mail address policy.

```
Set-EmailAddressPolicy "Default Policy" -IncludedRecipients AllRecipients
```

A warning appears asking if you're sure you want to perform this action. Type **Y** to confirm.

For detailed syntax and parameter information, see Set-EmailAddressPolicy.

1.2.2.7.18.2 Upgrade Default Address Lists from LDAP Filters to OPATH Filters

Upgrade Default Address Lists from LDAP Filters to OPATH Filters

Deploying Exchange 2010 > Managing Deployment of Exchange 2010 > Upgrade Custom LDAP Filters to OPATH Filters >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-06-16*

In Microsoft Exchange Server 2003 and earlier versions, LDAP filtering syntax is used when customizing default address lists (which are created during an Exchange installation). However, in Exchange Server 2010, the OPATH filtering syntax replaces the LDAP filtering syntax. This topic explains how to use the Exchange Management Shell to upgrade the filtering syntax for any legacy default address lists from LDAP to OPATH.

Note:
LDAP syntax filters are supported in Exchange 2010 and will exist only on objects that have been migrated from Exchange 2003 or earlier versions. You must upgrade these LDAP filters to the OPATH syntax only if you want to edit the filter from an Exchange 2010 server. For example, if you have Exchange 2003 servers in your organization, you can manage the LDAP syntax filter from an Exchange 2003 server. You can't manage or create LDAP syntax filters in Exchange 2010.

The following default address lists may need to be upgraded:

- All Users
- All Groups
- All Contacts
- Public Folders
- Default Global Address List

Note:
The All Rooms address list is an Exchange 2010 default address list and doesn't require upgrading.

For more information about how to determine if your address lists require upgrading, see "Determining Which Objects Require Upgrading" in Upgrade Custom LDAP Filters to OPATH Filters.

Use the Shell to upgrade default recipient filters

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" and "Global address lists" entries in the Mailbox Permissions topic.

Note:
You can't use the EMC to upgrade default recipient filters.

This example upgrades the All Users default address list.

```
Set-AddressList "All Users" -IncludedRecipients MailboxUsers
```

This example upgrades the All Groups default address list.

```
Set-AddressList "All Groups" -IncludedRecipients MailGroups
```

This example upgrades the All Contacts default address list.

```
Set-AddressList "All Contacts" -IncludedRecipients MailContacts
```

This example upgrades the Public Folders default address list.

```
Set-AddressList "Public Folders" -RecipientFilter { RecipientType -eq 'PublicFold
```

This example upgrades the Default Global Address List.

```
Set-GlobalAddressList "Default Global Address List" -RecipientFilter {(Alias -ne
```

A warning appears asking if you're sure you want to perform this action. Type **Y** to confirm.

For detailed syntax and parameter information, see Set-AddressList or Set-GlobalAddressList

1.2.2.7.19 Suppress Link State Updates

Suppress Link State Updates

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

This topic explains how to use Registry Editor to suppress propagation of minor link state updates between routing groups in Microsoft Exchange Server 2010 and Exchange Server 2003.

We recommend that you perform this procedure if the following conditions are true:

- You have installed the Exchange 2010 Hub Transport server role in an existing Exchange 2003 organization. For more information about this step, see Install Exchange 2010 in an Existing Exchange 2003 Organization.
- The existing Exchange organization includes more than one Exchange 2003 routing group.
- You will configure more than one routing group connector between Exchange 2003 routing groups and Exchange 2010.

The first routing group connector is created when the first Hub Transport server role is installed on a computer in the Exchange organization. Before you create additional routing group connectors, perform this procedure on every Exchange 2003 server in the organization. When you suppress minor link state updates, the servers running Exchange 2003 don't mark connectors as unavailable. This procedure makes sure that earlier versions of Exchange only use least cost routing and don't try to calculate an alternative route.

The purpose of this procedure is to make sure that routing loops can't occur. Exchange 2010 doesn't use a link state routing table and doesn't support relay of link state information. If you don't suppress minor link state updates, routing loops may occur. For more information about how routing occurs in an Exchange organization that includes Exchange 2010 servers and Exchange 2003 servers, see Upgrade from Exchange 2003 Transport.

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Suppress Link State Updates on Exchange 2003

To perform this procedure, you must log on to the Exchange 2003 server by using an account that is delegated membership in the local Administrators group.

1. Open Registry Editor.
2. Locate **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RESvc\Parameters**.
3. Right-click **Parameters** and select **New | DWORD value**. Name the new DWORD value **SuppressStateChanges**.
4. Double-click **SuppressStateChanges**.
5. In the **Value** data field, enter **1**.
6. Close Registry Editor, and then restart the SMTP service, the Microsoft Exchange Routing Engine service, and the Microsoft Exchange MTA Stacks services for the change to take effect.

1.2.2.8 Deploy Multiple Forest Topologies

Deploy Multiple Forest Topologies

Exchange Server 2010 > Planning and Deployment > Deploying Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-05-11*

This topic provides an overview of deploying Microsoft Exchange Server 2010 in multiple forest topologies. You'll find information about the following subjects:

- **Supported Multiple Forest Topologies** Exchange 2010 supports two types of multiple forest topologies: cross-forest and resource forest.
- **GAL Synchronization** If you have a cross-forest environment, you need to ensure that the GAL in any given forest contains mail recipients from other forests.
- **Moving Mailboxes Across Forests** The **New-MoveRequest** cmdlet in the Exchange Management Shell can help move mailboxes from one forest to another.
- **Understanding Multiple Forest Administration** Learn about the permissions model to configure and manage the permissions between your forests.

Supported Multiple Forest Topologies

Exchange 2010 supports two types of multiple forest topologies:

- **Cross-forest** A cross-forest topology is one with multiple Exchange forests. Here is an overview of what you need to do to deploy Exchange 2010 in a topology with a multiple forest:
  .1. You must first install Exchange 2010 in each forest. For more information, see Understanding a New Installation of Exchange 2010.
  .2. Next, you must synchronize the recipients in each of the forests, so that the Global Address List (GAL) in each forest contains users from all the synchronized forests. See the "GAL Synchronization" section below for more details.
  .3. Finally, you must configure the Availability service so that users in one forest can view availability data for users in another forest. For more information, see Configure the Availability Service for Cross-Forest Topologies.
  For details about deploying Exchange 2010 in a cross-forest topology, see Deploy Exchange 2010 in a Cross-Forest Topology.
- **Resource forest** A resource forest topology is one with an Exchange forest and one or more user accounts forests. Here is an overview of what you need to do to deploy Exchange 2010 in a topology with a resource forest:
  .1. You must have a forest with Exchange installed. In the Exchange forest, you

must have disabled the user accounts that have Exchange mailboxes.
.2.You must have at least one forest that contains user accounts. This forest should *not* have Exchange installed.
.3.Then, you must associate the disabled user accounts in the Exchange forest with the user accounts in the accounts forest.

For details about deploying Exchange 2010 in a resource forest topology, see Deploy Exchange 2010 in an Exchange Resource Forest Topology.

GAL Synchronization

By default, a GAL contains mail recipients from a single forest. If you have a cross-forest environment, we recommend using Microsoft Identity Lifecycle Manager (ILM) 2007 Feature Pack 1 (FP1) to ensure that the GAL in any given forest contains mail recipients from other forests. ILM 2007 FP1 creates mail users that represent recipients from other forests, thereby allowing users to view them in the GAL and send mail. For example, users in Forest A appear as a mail user in Forest B and vice versa. Users in the target forest can then select the mail user object that represents a recipient in another forest to send mail.

To enable GAL synchronization, you create management agents that import mail-enabled users, contacts, and groups from designated Active Directory services into a centralized metadirectory. In the metadirectory, mail-enabled objects are represented as mail users. Groups are represented as contacts without any associated membership. The management agents then export these mail users to an organizational unit in the specified target forest.

For more information about Microsoft Identity Lifecycle Manager 2007 FP1, see Microsoft Identity Lifecycle Manager 2007 Feature Pack 1 Evaluation Edition.

Moving Mailboxes across Forests

In a cross-forest topology, you may want to move mailboxes from one forest to another. To do this you must use the **New-MoveRequest** cmdlet in the Exchange Management Shell. This is the same command that you use to move mailboxes within a single forest. For more information about moving mailboxes across forests, see the following topics:

- Prepare Mailboxes for Cross-Forest Move Requests
- Create a Remote Move Request That has Exchange 2010 in Both Forests
- Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010

Understanding Multiple Forest Administration

Microsoft Exchange Server 2010 uses new permissions functionality to manage your multiple forest environments.

Exchange 2010 uses a Role Based Access Control (RBAC) permissions model. The management role groups that administrators are members of, and the management role assignment policies that end-users are assigned, determine what each administrator and end-user can do. To understand multiple forest permissions, you need to be familiar with RBAC. For more information about RBAC and role groups and role assignment policies in particular, see Understanding Role Based Access Control.

You can use the RBAC permissions model to configure and manage the permissions between your forests. For more information about multiple forest permissions, see the following topics:

- Understanding Multiple-Forest Permissions
- Create Linked Role Groups that Mirror Built-in Role Groups

- Create a Linked Role Group

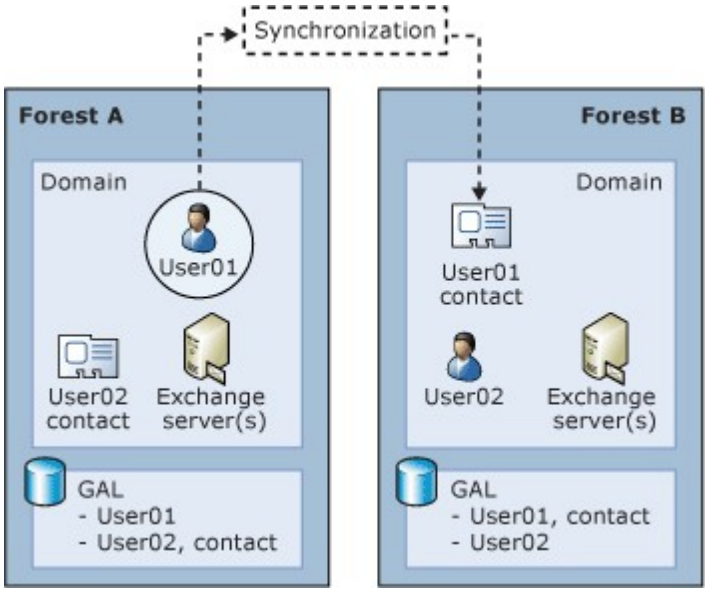
1.2.2.8.1 Deploy Exchange 2010 in a Cross-Forest Topology

Deploy Exchange 2010 in a Cross-Forest Topology

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-27*

This topic explains how to deploy Exchange 2010 in a cross-forest topology using Service Pack 1 (SP1) for ILM 2007 Feature Pack 1 (FP1). To deploy Exchange 2010 in a cross-forest topology, you must first install Exchange 2010 in each forest, and then connect the forests so that users can see address and availability data across the forests.



This topic does not describe how to deploy Exchange 2010 in a dedicated Exchange forest (or resource forest) topology. For more information about how to deploy Exchange 2010 in a resource forest topology, see Deploy Exchange 2010 in an Exchange Resource Forest Topology.

To synchronize the GALs in Exchange 2010, we recommend that you use Service Pack 1 (SP1) for ILM 2007 Feature Pack 1 (FP1). To download the feature pack, see Microsoft Knowledge Base article 977791, Service Pack 1 (build 3.3.1139.2) is available for Identity Lifecycle Manager 2007 Feature Pack 1.

Prerequisites

To perform the following procedure in Exchange 2010, confirm the following:

- You have correctly configured Domain Name System (DNS) for name resolution across forests in your organization. To verify that DNS is configured correctly, use the Ping tool to test connectivity to each forest from the other forests in your organization and from the server on which you will run the GALSync

agent.

- The GALSync management agent (MA) communicates with the Exchange 2010 forest using Windows PowerShell V2.0 RTM. Make sure Windows PowerShell v1.0 isn't installed on this computer by going to Control Panel, and then clicking Programs and Features.
- Ensure that Windows Remote Management has not been installed by Windows Update.
- Install Windows PowerShell and Windows Remote Management. For details, see Microsoft Knowledge Base article 968930, Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0).

Deploy Exchange 2010 in a cross-forest topology with SP1 for ILM 2007 FP1

1. In each forest, install Exchange 2010 separately. To install Exchange 2010, perform the same steps that you would if you were installing Exchange 2010 in a single forest topology. For detailed steps, see one of the following topics:
   - Install Exchange Server 2010
   - Install Exchange 2010 Using the Custom Installation Type

   Note:
   This topic assumes that you don't have an existing Exchange 2007 or Exchange Server 2003 topology. If you do have an existing Exchange topology and you want to upgrade, see Understanding Upgrade to Exchange 2010.
2. In each forest, use Active Directory Users and Computers to create a container in which ILM will create contacts for each mailbox from the other forest. We recommend that you name this container **FromILM**. To create the container, select the domain in which you want to create the container, right-click the domain, select **New**, and then select **Organizational Unit**. In **New Object - Organizational Unit**, type **FromILM**, and then click **OK**.
3. Create a GALSync management agent for each forest by using ILM 2007 Feature Pack 1. This allows you to synchronize the users in each forest and create a common GAL. For detailed steps, see the procedure "Configure a GAL Synchronization management agent with SP1 for ILM 2007 FP1" later in this topic.
4. Enable GALSync. To do this, in the main ILM Identity Manager window, click **Tools**, click **Options**, and then select the **Enable Provisioning Rules Extension** check box. Click **OK**.
5. Create an SMTP Send connector in each of the forests. For detailed steps, see Configure Cross-Forest Connectors.
6. In each forest, enable the Availability service so that users in each forest can view free/busy data about users in the other forest. For more information, see Managing the Availability Service.

   Note:
   The Availability service is supported only for Office Outlook 2007 clients.
7. If you require that mail can be relayed through any forest in your organization, you must configure a domain in that forest as an authoritative domain. For detailed steps, see Configure Exchange 2010 to Accept E-Mail for More Than One Authoritative Domain.
8. Move mailboxes from your existing Exchange 2003 or Exchange 2007 servers to the new Exchange 2010 Mailbox servers in each forest. For detailed steps, see Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010.

Configure a GAL Synchronization management agent with SP1

for ILM 2007 FP1

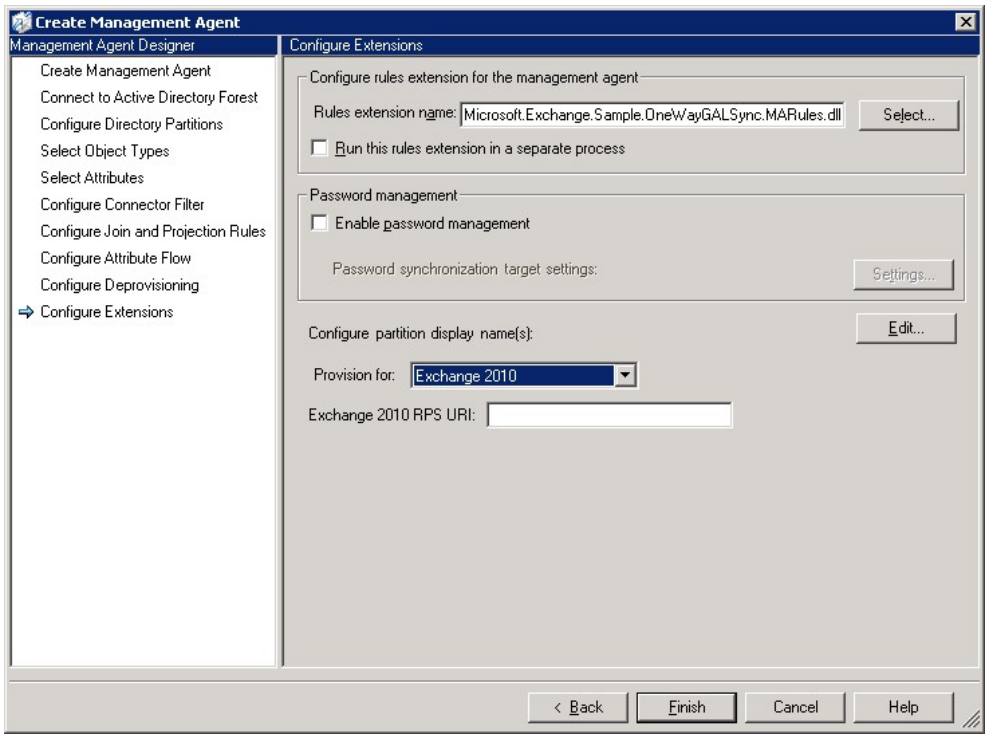
This procedure is necessary for deployment of Exchange 2010 in a cross-forest topology using Service Pack 1 (SP1) for ILM 2007 Feature Pack 1 (FP1). See step 3 in "Deploy Exchange 2010 in a cross-forest topology with SP1 for ILM 2007 FP1" earlier in this topic.

1. In SP1 for ILM 2007 FP1, select **Management Agents** from the toolbar, and then under **Actions**, click **Create**.
2. On the **Create Management Agent** page, under **Management agent for**, select **Active Directory global address list (GAL)**.
3. In the **Name** box, type a name for this management agent. When creating the name, we recommend that you include the name of the source forest from which this management agent will gather recipient information.
4. In the **Description** box, type a description for this management agent, and then click **Next**.
5. On the **Connect to Active Directory Forest** page, complete the following fields:
   - **Forest name** Name of the source forest.
   - **User name** and **Password** User name and password of an account that has permission to read schema information from the source forest.
   - **Domain** Domain for the specified account.

   Note:
   You can also enter the user name as *<user>*@*<domain>* and leave the domain field blank.
6. Click **Next**.
7. On the **Configure Directory Partitions** page, select the directory partitions on the source forest from which you want to project data to a destination forest.
8. On the **Configure Directory Partitions** page, click **Containers**.
9. On the **Select Containers** page, clear the top-level check box for the directory partition, select the containers for which this management agent will gather and store information, and then click **OK**. Be sure to select the container in which ILM will create contacts for each mailbox from the other forest, such as the FromILM container.
10. On the **Configure Directory Partitions** page, click **Next**.
11. On the **Configure GAL** page, click **Target**, and then select the container in which the contacts from other forests will reside in the target forest.
12. On the **Configure GAL** page, click **Source**, and then select the container in which other forests' objects that are synchronized to the target forest will reside.
13. Under **Exchange configuration**, click **Edit** to specify at least one Simple Mail Transfer Protocol (SMTP) e-mail suffix that is managed in the source forest. Click **Next**.
14. On the **Select Object Types** page, click **Next**.
15. On the **Select Attributes** page, click **Next**.
16. On the **Configure Connector Filter** page, click **Next**.
17. On the **Configure Join and Projection Rules** page, click **Next**.
18. On the **Configure Attributes Flow** page, click **Next**.
19. On the **Configure Deprovisioning** page, click **Next**.
20. On the **Configure Extensions** page, under **Configure partition display name(s)**: section, next to **Provision for:**, select **Exchange 2010**. If you select Exchange 2010, you will see the **Exchange 2010 RPS URI** field. Enter the URI of an Exchange 2010 Client Access server to make sure the Remote Powershell connection is functioning. The **Exchange 2010 RPS URI** should be in the following format: http://CAS_Server_FQDN/Powershell. Click **OK**.

    Note:
    Make sure that the administrator credentials used to connect to the Exchange 2010 forest can also make remote PowerShell connections to that forest.

The following figure shows how to select provisioning for Exchange 2010.



Testing Remote PowerShell Connection

This example tests whether you can make a remote PowerShell call to an Exchange 2010 Client Access server to verify that remote PowerShell is functioning correctly. From your ILM 2007 computer, first run this command:

```
$rs = new-pssession -conf microsoft.exchange -conn http://CAS_SERVER_NAME/powersh
```

Then run this command:

```
Invoke-Command $rs {get-recipient -ResultSize 1}
```


1.2.2.8.2 Deploy Exchange 2010 in an Exchange Resource Forest Topology

Deploy Exchange 2010 in an Exchange Resource Forest Topology

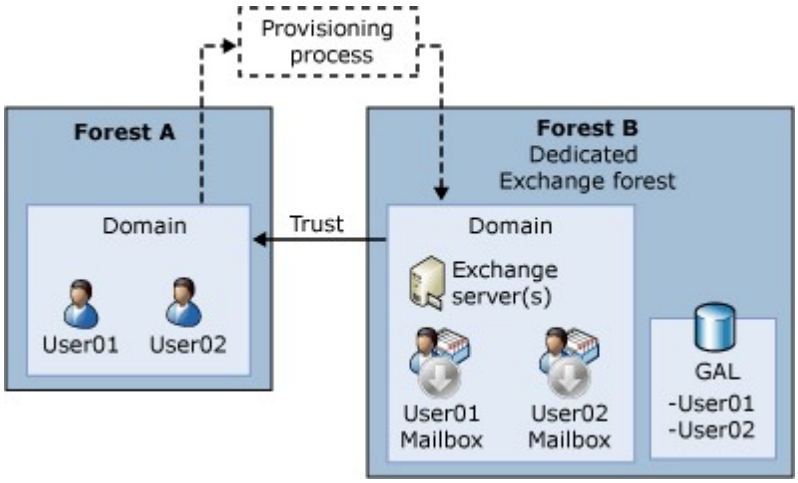
Planning and Deployment > Deploying Exchange 2010 > Deploy Multiple Forest Topologies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

This topic explains how to deploy Microsoft Exchange 2010 in an Exchange resource forest topology. An Exchange resource forest is also called a dedicated Exchange forest. This topic assumes that you don't have an existing Exchange 2010 topology.

The following figure shows an Exchange organization with a resource forest.



Prerequisites

Before you begin, confirm the following:

- You have the following two Active Directory forests:
  - One forest contains the user accounts for your organization. In this procedure, this forest is called the *accounts forest*.
  - One forest does not contain user accounts and does not yet have Exchange installed. In this procedure, this forest is called the *Exchange forest*. You will use the procedure to install Exchange 2010 in this forest.
- You have correctly configured Domain Name System (DNS) for name resolution across forests in your organization. To check that you have DNS configured correctly, ping each forest from the other forest or forests in your organization. For more information about configuring DNS, see the DNS Operations Guide.

Deploy Exchange 2010 in an Exchange resource forest topology

1. From a domain controller in the Exchange forest, create a one-way outgoing trust so that the Exchange forest trusts the accounts forest. For detailed steps, see Create a one-way, outgoing, forest trust for both sides of the trust.

   Note:

   Although we recommend that you create a forest trust, you can create either a forest trust or an external trust. If you create an external trust, when you create linked mailboxes in Step 3, on the **Master Account** page of the New Mailbox wizard, you must specify a user account that can access the domain controller in the trusted forest. You can't use the credentials with which you are currently logged on. If you create linked mailboxes by using the **New-Mailbox** cmdlet, you must specify a user account that can access the domain controller in the trusted forest by using the *LinkedCredential* parameter.

2. In the Exchange forest, install Exchange 2010. Install Exchange the same way that you would in a single forest scenario. For detailed steps about how to install Exchange 2010, see one of the following topics:
   - Install Exchange Server 2010
   - Install Exchange 2010 in Unattended Mode
3. In the Exchange forest, for each user in the accounts forest that will have a mailbox in the Exchange forest, create a mailbox that is associated with an external account. For detailed steps, see Create a Linked Mailbox.

1.2.2.8.3 Configure Cross-Forest Connectors

Configure Cross-Forest Connectors

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure Send connectors and Receive connectors to enable cross-forest communication. To establish direct mail flow between servers that are running Microsoft Exchange in different Active Directory forests, you must configure Send connectors and Receive connectors.

This topic explains how to configure cross-forest connectors for the following scenarios:

- Exchange Server 2010 to Exchange Server 2010
- Exchange 2010 to Exchange Server 2003

Configure cross-forest connectors between Exchange 2010 forests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" and "Receive connectors" entries in the Transport Permissions topic.

In this scenario, you create the cross-forest connectors between the Hub Transport servers in two Exchange 2010 organizations that are located in separate Active Directory forests. Basic authentication or external authentication mechanisms provide authentication and authorization between the servers in different forests. If you use Basic authentication, you can select from the following two methods to also use Transport Layer Security (TLS):

- Set the smart host authentication method to Basic authentication over TLS. This method provides both confidentiality and authentication of the receiving server. If you select this smart host authentication method, the sending server will validate the certificate of the receiving server as a requirement for mail flow.
- Set the *RequireTLS* parameter to `$true`. This method provides confidentiality, but doesn't authenticate the receiving server.

To configure a cross-forest connector between the Hub Transport servers in two Exchange 2010 organizations, you must meet the following prerequisites:

- Each forest must have an Exchange organization with Exchange 2010 servers.
- If you use Basic authentication, a domain account must exist in each forest to use for Basic authentication. For example, provide a user account that has the user principal name (UPN) FourthCoffee@Contoso.com as the credentials that must be used for authentication by the Exchange servers in the Fourth Coffee domain when mail is sent to the Exchange servers in the Contoso domain.
- If you use Basic authentication over TLS, the target server must be configured to use an X.509 certificate that contains a fully qualified domain name (FQDN) that's the same as the FQDN of the Receive connector.
- If you use external authentication, a trusted network connection must exist between the Hub Transport servers. This connection may be an IPsec

association or VPN. Alternatively, the servers may reside in a trusted physically controlled network.

To establish mail flow between the forests, follow these steps:

1. Create a user account in each forest to use for authentication to the receiving server in the second forest.
2. Create a Send connector.
3. Set permissions on the Send connector.
4. For externally secured connectors, create a new Receive connector.

Note:
If you're using Basic authentication over TLS, you must provide the FQDN of the remote Hub Transport server in the smart host settings. You can't use an IP address.

The following procedures establish cross-forest mail flow between the Exchange 2010 Hub Transport servers in the Contoso.com and FourthCoffee.com forests by using either Basic authentication or external authentication. You must perform the reciprocal procedure in each forest.

Configure cross-forest connectors between Exchange 2010 servers by using Basic authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" and "Receive connectors" entries in the Transport Permissions topic.

Step 1: Create a user account in each forest

- Create the user account in each forest and then add the account to the Exchange Servers universal security group. This account is used by the Send connector to authenticate to the receiving server in the second forest.

Important:
This account is granted the permissions that are associated with Exchange servers. Be sure to safeguard the account credentials to prevent misuse of the account. You can configure the account to allow logon to specific computers only.

Step 2: Create a Send connector in the Contoso forest

Use the EMC to create a Send connector

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**, and then in the action pane, click **New Send connector**.
2. On the New SMTP Send connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector.
3. From the **Select the intended use for this Send connector** drop-down list, select **Internal**, and then click **Next**.
4. On the **Address Space** page, click **Add**. In the **SMTP Address Space** dialog box, type the name of the remote SMTP domain, and then click **Next**.
5. On the **Network settings** page, only the **Route mail through the following smart hosts** setting can be selected. Click **Add**.
6. In the **Add Smart Host** dialog box, in the **IP address** or **Fully qualified domain name (FQDN)** field, type the FQDN of a Hub Transport server in the remote forest, and then click **OK**. To specify more than one Hub Transport server as a smart host, click **Add** and enter additional FQDNs, and then click **Next**.
7. On the Configure **smart host authentication settings** page, select **Basic Authentication** or **Basic Authentication over TLS**, type the user name and password that will be used to authenticate the connection, and then click **Next**.
8. On the **Source Server** page, click **Add**. In the **Select Hub Transport or Subscribed Edge Transport Server** dialog box, select one or more Hub

Transport servers in your organization, click **OK**, and then click **Next**.

9. On the **New Connector** page, click **New**.
10. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a Send connector

This example creates the Send connector from Contoso.com to FourthCoffee.com and uses Basic authentication over TLS to provide both confidentiality and authentication to the receiving server.

1. This command stores the credentials for use in authentication.

```
$mycred = Get-Credential
```

2. In the dialog box that appears, enter the credentials for the user account in the Fourth Coffee domain. Use the *domain**user* format or UPN format to enter the user name and provide the user's password.
3. Click **OK**.
4. This command creates the Send connector.

```
New-SendConnector -Name "Cross-Forest" -Usage Internal -AddressSpaces
```

This example creates the Send connector from Contoso.com to FourthCoffee.com and uses Basic authentication over TLS to provide only confidentiality.

1. This command stores the credentials for use in authentication.

```
$mycred = Get-Credential
```

2. In the dialog box that appears, enter the credentials for the user account in the Fourth Coffee domain. Use the *domain**user* format or UPN format to enter the user name and provide the user's password.
3. Click **OK**.
4. This command creates the Send connector.

```
New-SendConnector -Name "Cross-Forest" -Usage Internal -AddressSpaces
```

For detailed syntax and parameter information, see New-SendConnector.

Step 3: Use the Shell to set permissions on the Send connector

Note:

You can't use the EMC to set permissions on the Send connector.

This example uses the **Enable-CrossForestConnector.ps1** script in the Shell to set permissions on the Send connector.

```
.\Enable-CrossForestConnector.ps1 -Connector "Cross-Forest" -user "ANONYMOUS LOGO
```

Configure cross-forest connectors between Exchange 2010 servers by using external authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" and "Receive connectors" entries in the Transport Permissions topic.

Step 1: Create a Send connector

Use the EMC to create a Send connector

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**, and then in the action pane, click **New Send connector**.
2. On the New SMTP Send connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector. From the **Select the intended**

use for this Send connector drop-down list, select **Internal**, and then click **Next**.

3. On the **Address space** page, click **Add**. In the **SMTP Address Space** dialog box, type the name of the remote SMTP domain, and then click **Next**.
4. On the **Network settings** page, only the **Route mail through the following smart hosts** setting can be selected. Click **Add**.
5. In the **Add Smart Host** dialog box, in the **IP address** or **Fully qualified domain name (FQDN)** field, type the IP address or FQDN of a Hub Transport server in the remote forest, and then click **OK**. To specify more than one Hub Transport server as a smart host, click **Add** and enter additional IP addresses or FQDNs, and then click **Next**.
6. On the Configure **smart host authentication settings** page, select **Externally Secured (for example, with IPsec)**, and then click **Next**.
7. On the **Source Server** page, click **Add**. In the **Select Hub Transport or Subscribed Edge Transport Server** dialog box, select one or more Hub Transport servers in your organization, click **OK**, and then click **Next**.
8. On the **New Connector** page, click **New**.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a Send connector

This example creates the Send connector from Contoso.com to FourthCoffee.com.

```
New-SendConnector -Name "Cross-Forest" -Usage Internal -AddressSpaces FourthCoffe
```

For detailed syntax and parameter information, see New-SendConnector.

Step 2: Create a Receive connector

Use the EMC to create a Receive connector

1. In the console tree, navigate to **Server Configuration** > **Hub Transport**, and then in the action pane, click **New Receive Connector**.
2. On the New SMTP Receive Connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector.
3. From the **Select the intended use for this Receive connector** drop-down list, select **Internal**, and then click **Next**.
4. On the **Remote Network settings** page, remove the all network ranges entry, and then click **Add**.
5. In the **Add IP Address(es) of Remote Servers** dialog box, type the IP address of the remote Hub Transport server, click **OK**, and then click **Next**.
6. On the New Connector page, click **New**.
7. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a Receive connector

This example creates the Receive connector for Contoso.com to receive mail from FourthCoffee.com.

```
New-ReceiveConnector -Name "Cross-Forest" -Server HubA -PermissionGroups Exchange
```

For detailed syntax and parameter information, see New-ReceiveConnector.

Step 3: Modify the authentication method used for this connector

Note:
This step isn't necessary if you used the Shell to create the Receive connector in step 2. It's required if you used the EMC in step 2.

1. In the console tree, navigate to **Server Configuration** > **Hub Transport**.
2. In the result pane, select the Receive connector that you want to modify, and then in the action pane, click **Properties**.
3. Click the **Authentication** tab.
4. Clear the check boxes for **Transport Layer Security (TLS)** and **Exchange Server authentication**, and then select **Externally Secured (for example with IPsec)**.
5. Click **OK**.

Configure cross-forest connectors between Exchange 2010 and Exchange 2003

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" and "Receive connectors" entries in the Transport Permissions topic.

In this scenario, you create the cross-forest connectors between an Active Directory forest with an Exchange organization that's running Exchange 2010 and a second Active Directory forest with an Exchange organization that's running Exchange 2003. You can create the Send connectors and Receive connectors between the Exchange 2010 Edge Transport server and the Exchange 2003 bridgehead server or between the Exchange 2010 Hub Transport server and the Exchange 2003 bridgehead server.

To establish mail flow between the forests, follow these steps:

1. Create user accounts in each forest for authenticating the sending server. This step isn't required if you use external authentication.
2. Create a Send connector and select **Internal** as the usage for this connector on either the Exchange 2010 Edge Transport server or Hub Transport server.
3. Modify the authentication for the new Send connector.
4. Create an SMTP connector on Exchange 2003.
5. If you're using external authentication, modify the registry on the Exchange 2003 server to allow the Exchange 2003 server to send and receive XEXCH50 properties anonymously.

The following procedures establish cross-forest mail flow between the Exchange 2010 transport servers in the Contoso.com forest and the Exchange 2003 bridgehead servers in the FourthCoffee.com forest by using either Basic authentication or external authentication. After you perform one of the following procedures, we recommend that you test mail flow by sending a message between the two organizations. You should also examine the protocol logs to verify that XEXCH50 data is propagated to Exchange 2003.

Configure cross-forest connectors between Exchange 2010 and Exchange 2003 servers in separate forests and use Basic authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" and "Receive connectors" entries in the Transport Permissions topic.

Step 1: Create a user account in each forest

In the Exchange 2003 forest, create a user account. Add the user account to the Exchange Domain Servers security group in the domain where the Exchange 2003 server

that will act as smart host for this connector resides.

Important:

This account is granted the permissions that are associated with Exchange servers. Be sure to safeguard the account credentials to prevent misuse of the account. You can configure the account to allow logon to specific computers only.

In the Exchange 2010 forest, create a user account. Add the user account to the ExchangeLegacyInterop security group in the domain where the Exchange 2010 server that will act as the smart host for receiving messages from Exchange 2003 resides.

Step 2: Create a Send connector from Exchange 2010 to Exchange 2003

Use the EMC to create a Send connector

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**, and then in the action pane, click **New Send connector**.
2. On the New SMTP Send connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector. From the **Select the intended use for this Send connector** drop-down list, select **Internal**, and then click **Next**.
3. On the **Address Space** page, click **Add**. In the **SMTP Address Space** dialog box, type the name of the remote SMTP domain, and then click **Next**.
4. On the **Network settings** page, only the **Route mail through the following smart hosts** setting can be selected. Click **Add**.
5. In the **Add Smart Host** dialog box, in the **IP address** or **Fully qualified domain name (FQDN)** field, type the IP address or FQDN of the Exchange 2003 bridgehead server in the remote forest, and then click **OK**. To specify more than one bridgehead server as a smart host, click **Add** and enter additional IP addresses or FQDNs, and then click **Next**.
6. On the Configure **smart host authentication settings** page, in either **Basic Authentication** or **Basic Authentication over TLS**, type the user name and password that will be used to authenticate the connection, and then click **Next**.
7. On the **Source Server** page, click **Add**. In the **Select Hub Transport or Subscribed Edge Transport Server** dialog box, select one or more Hub Transport servers in your organization, click **OK**, and then click **Next**.
8. On the **New Connector** page, click **New**.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a Send connector

If the Exchange 2010 Send connector is configured to use Basic authentication over TLS or to use Basic authentication with the *RequiredTLS* parameter set to `$true`, the Exchange 2003 server must advertise the correct certificate before authentication can occur. You can verify that a certificate has been imported to the Exchange 2003 SMTP virtual server by viewing the properties of the virtual server. To view or import a server certificate, select the **Access** tab and click **Certificate**.

1. This command stores the credentials for use in authentication. In the Exchange 2010 forest, open the Shell on the Edge Transport server or the Hub Transport server, and run the following command.

   ```
   $mycred = Get-Credential
   ```

   In the dialog box that appears, enter the credentials for the user account that you created in the Exchange 2003 forest. Use the *domain**user* format or the UPN format to enter the user name and provide the user's password. Click **OK**.
2. In the Shell, use one of the following commands to create the Send

connector.

- This example creates a Send connector to use Basic authentication over TLS to provide both confidentiality and authentication to the receiving server.

```
New-SendConnector -Name "Legacy Forest" -SmartHostAuthMechar
```

- This example creates a Send connector to use Basic authentication with TLS to provide only confidentiality.

```
New-SendConnector -Name "Legacy Forest" -SmartHostAuthMechar
```

For detailed syntax and parameter information, see New-SendConnector.

Step 3: Use the Shell to set permissions on the Send connector

Note:
You can't use the EMC to set permissions on the Send connector.

This example uses the **Enable-CrossForestConnector.ps1** script in the Shell to set permissions on the Send connector.

```
.\Enable-CrossForestConnector.ps1 -Connector "Legacy Forest" -user "ANONYMOUS LOG
```

Step 4: Use Exchange System Manager to create an SMTP connector on an Exchange 2003 bridgehead server in the remote forest

1. In the Exchange 2010 forest, create a user account. Add the user account to the ExchangeLegacyInterop security group.

   Important:
   This account is granted the permissions that are associated with Exchange servers. Be sure to safeguard the account credentials to prevent misuse of the account. You can configure the account to allow logon to specific computers only.

2. In the Exchange 2003 forest, open Exchange System Manager. Right-click the **Connectors** container that's located in the routing group where the server that will host this connector resides, select **New**, and then select **SMTP Connector**.
3. Select the **General** tab. In the **Name** field, type a unique name for the connector.
4. Select **Forward all mail through this connector to the following smart hosts**, and then type the IP address or FQDN of the Exchange 2010 Edge Transport server or Hub Transport server. If you enter an IP address, it must be enclosed in brackets, for example, [192.168.1.1].
5. Click **Add** to add a local bridgehead server. In the **Add Bridgehead** dialog box, select one or more Exchange 2003 servers.
6. Select the **Address Space** tab, and then click **Add** to create an address space. In the **Add Address Space** dialog box, select **SMTP**, and then click **OK**.
7. On the **Internet Address Space Properties** page, enter the SMTP domain name of the Exchange 2010 forest, and then click **OK**.
8. Select the **Advanced** tab, and then click **Outbound Security**. In the **Outbound Security** dialog box, select **Basic Authentication**, and then click **Modify**.
9. In the **Outbound Connection Credentials** dialog box, enter the user name for the account that you created in the Exchange 2010 forest, enter the password for the account, and then click **OK**.
10. Click **OK** to close the **Outbound Security** dialog box. Click **OK**.

Configure cross-forest connectors between Exchange 2010 and Exchange 2003 servers without a trust relationship by using

external authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" and "Receive connectors" entries in the Transport Permissions topic.

Step 1: Create a Send connector

Use the EMC to create a Send connector

1. In the console tree navigate to **Organization Configuration** > **Hub Transport**.
2. In the action pane, click **New Send connector**.
3. On the New SMTP Send connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector. From the **Select the intended use for this Send connector** drop-down list, select **Internal**, and then click **Next**.
4. On the **Address Space** page, click **Add**. In the **SMTP Address Space** dialog box, type the name of the remote SMTP domain, and then click **Next**.
5. On the **Network settings** page, only the **Route mail through the following smart hosts** setting can be selected. Click **Add**.
6. In the **Add Smart Host** dialog box, in the **IP address** or **Fully qualified domain name (FQDN)** field, type the IP address or FQDN of the bridgehead server in the Exchange 2003 forest, and then click **OK**. To specify more than one bridgehead server as a smart host, click **Add** and enter additional IP addresses or FQDNs, and then click **Next**.
7. On the **Configure smart host authentication settings** page, select **Externally Secured (for example with IPsec)**, and then click **Next**.
8. On the **Source Server** page, click **Add**. In the **Select Hub Transport or Subscribed Edge Transport Server** dialog box, select one or more Hub Transport servers in your organization, click **OK**, and then click **Next**.
9. On the **New Connector** page, click **New**.
10. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a Send connector

This example creates the Send connector from Contoso.com to FourthCoffee.com.

```
New-SendConnector -Name "Legacy Forest" -Usage Internal -AddressSpaces FourthCoff
```

For detailed syntax and parameter information, see New-SendConnector.

Step 2: Create a Receive connector

Use the EMC to create a Receive connector

1. In the console tree, navigate to **Server Configuration** > **Hub Transport**, and then in the action pane, click **New Receive Connector**.
2. On the New SMTP Receive Connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector.
3. From the **Select the intended use for this Receiver connector** drop-down list, select **Internal**, and then click **Next**.
4. On the **Remote Network settings** page, remove the all network ranges entry, and then click **Add**.
5. In the **Add IP address(es) of Remote Servers** dialog box, type the IP address of the bridgehead server in the Exchange 2003 organization, click **OK**, and then click **Next**.
6. On the New Connector page, click **New**.
7. On the **Completion** page, review the following, and then click **Finish** to close

the wizard:

- A status of **Completed** indicates that the wizard completed the task successfully.
- A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a Receive connector

This example creates the Receive connector for Contoso.com to receive mail from FourthCoffee.com.

```
New-ReceiveConnector -Name "Legacy Forest" -Usage Internal -Server HubA -Permissi
```

For detailed syntax and parameter information, see New-ReceiveConnector.

Step 3: Modify the authentication method used for this connector

Note:

This step isn't necessary if you used the Shell to create the Receive connector in step 2. It's required if you used the EMC in step 2.

1. In the console tree, navigate to **Server Configuration** > **Hub Transport**.
2. In the result pane, select the Receive connector that you want to modify, and then in the action pane, click **Properties**.
3. Click the **Authentication** tab.
4. Clear the check boxes for **Transport Layer Security (TLS)** and **Exchange Server authentication**, select **Externally Secured (for example with IPsec)**, and then click **OK**.

Step 4: Modify the registry settings on the Exchange 2003 bridgehead server to allow the Exchange 2003 server to send and receive XEXCH50 properties anonymously

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

1. Open Registry Editor.
2. Locate **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SMTPSVC\XEXCH50**
3. Right-click **XEXCH50** and select **New | DWORD Value**. Type **SuppressExternal** for the value name. By default, the value data is **0**, which indicates that the XEXCH50 properties are transmitted to the remote server anonymously.
4. Right-click **XEXCH50** and select **New** | **Key**. Type the number of the SMTP virtual server instance as the key value. For example, the default virtual server instance is **1**, and the second SMTP virtual server created on a server is **2**.
5. Right-click the key that you just created, point to **New**, and then click **DWORD Value**.
6. In the details pane, type **Exch50AuthCheckEnabled** for the value name. By default, the value data is **0**, which indicates that the XEXCH50 properties are transmitted when e-mail is sent anonymously.

1.2.2.9 Exchange 2010 Post-Installation Tasks

Exchange 2010 Post-Installation Tasks

Exchange Server 2010 > Planning and Deployment > Deploying Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

After you complete a new installation of Microsoft Exchange Server 2010 or after you add an additional Exchange 2010 server role to an existing Exchange 2010 server, you should complete the post-installation tasks. The post-installation tasks will help you verify the installation and configure the components that you have just installed. Because each server role offers several features that you can configure for your organization, make sure that you complete the post-installation tasks for each server role that you install.

In the Exchange Management Console, when you select the **Microsoft Exchange** node, the result pane displays the **Post-Installation Tasks** tab. From that tab, you can find more information via links to several topics that describe, by server role, the various post-installation tasks:

Finalize Deployment Tasks This topic describes tasks that are required to complete the deployment of your Exchange 2010 organization. The tasks apply to features that are enabled by default but require additional configuration.

End-to-End Scenario Tasks This topic provides a checklist of the recommended actions to take to configure specific end-to-end scenarios. For example, how to configure monitoring for your Exchange servers.

Additional Post-Installation Tasks This topic provides you with information about optional tasks that you may want to perform after you install Exchange Server 2010.

In addition to the preceding topics, the following topics also provide information related to post-installation tasks:

Verify an Exchange 2010 Installation

Enter Product Key

Register Filter Pack IFilters with Exchange 2010

Transport Server Post-Deployment Tasks

And, if you're upgrading from an Exchange 2003 or a mixed Exchange 2003 and Exchange 2007 organization, see Upgrade Custom LDAP Filters to OPATH Filters.

1.2.2.9.1 Finalize Deployment Tasks

Finalize Deployment Tasks

Planning and Deployment > Deploying Exchange 2010 > Exchange 2010 Post-Installation Tasks >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-20*

Use this checklist to help you perform tasks to finalize your deployment after you install Exchange Server 2010. The tasks in this topic are required to complete the deployment of your Exchange organization. The tasks apply to features that are enabled by default but require additional configuration.

For guidance about optional tasks that you may want to perform after installing Exchange 2010, see Additional Post-Installation Tasks and End-to-End Scenario Tasks.

All Server Roles

Done?	Task
	Enter the product key for Exchange 2010. For more information, see Enter Product Key. You can also enter the product key by using the Set-ExchangeServer cmdlet.
	We recommend that you protect your Exchange servers from viruses, worms, and other malicious software. For more information, see Forefront Protection 2010 for Exchange Server.

Mailbox Server Role

Done?	Task
	Configure offline address book (OAB) distribution for Microsoft Office Outlook clients. For more information, see Create an Offline Address Book and Configure Offline Address Book Properties.
	Configure high availability, backup, and disaster recovery. For more information, see High Availability and Site Resilience.

Client Access Server Role

Done?	Task
	Configure secure access for your Client Access server. For more information, see Understanding Client Access Security.
	Configure Microsoft Exchange ActiveSync. By default, when you install the Client Access server role on a computer that is running Exchange 2010, Exchange ActiveSync is enabled. However, we recommend that you configure security, authentication, and policy settings if you plan to use ActiveSync in your environment. For more information, see Managing Exchange ActiveSync.

Hub Transport Server Role

Done?	Task
	Configure domains for which you will accept e-mail messages. For more information, see Transport Server Post-Deployment Tasks.
	Configure Internet mail flow. By default, a Hub Transport server isn't configured for Internet mail flow. If you don't subscribe an Edge Transport server to your Exchange organization, you must use one of the following methods to configure Internet mail flow to and from your Exchange organization: • Deploy an Edge Transport server and manually configure the Send connectors and Receive connectors that are required for Internet mail flow. This method doesn't establish any replication of recipient and configuration information from Active Directory Domain Services to the Edge Transport server. For more information, see Configure Mail Flow Between an Edge Transport Server and Hub Transport Servers Without Using EdgeSync. • Manually configure Internet mail flow between your Exchange 2010 organization and Microsoft Exchange Hosted Services or other external SMTP gateway servers. This method requires you to create the Send connectors and Receive connectors on one or more Hub Transport servers in your organization that are assigned to communicate with Exchange Hosted Services or the external SMTP gateway servers. For more information see Configure Internet Mail Flow Through Exchange Hosted Services or an External SMTP Gateway. • Configure the Hub Transport server for direct mail flow with the Internet. This method requires you to create the Send connectors and Receive connectors on one or more Hub Transport servers in your organization that are assigned to connect to the Internet. For more information, see Configure Internet Mail Flow Through Exchange Hosted Services or an External SMTP Gateway.
	Configure an external postmaster recipient to receive e-mail messages. The external postmaster address is used as the sender for system-

	generated messages and notifications that are sent to message senders that exist outside the Exchange 2010 organization. According to RFC 2821, every domain must be able to receive mail that is sent to the postmaster address. By default, no mailbox or other recipient object is configured to receive messages that are sent to the postmaster address for any accepted domains that are defined in the Exchange organization. For more information, see Configure the External Postmaster Address.

Unified Messaging Server Role

Done?	Task
	Configure Unified Messaging (UM). For more information see the following topics: • Create a UM Dial Plan • Create a UM IP Gateway • Add a UM Server to a Dial Plan • Enable a User for Unified Messaging **Note** These tasks are required to configure the first UM server in your organization or the first UM server in a new dial plan. To configure an additional UM server for an existing dial plan, you only need to complete the steps in Add a UM Server to a Dial Plan.
	Configure UM and Office Communications Server integration. For more information, see Deploy Unified Messaging and Communications Server 2007 R2.

Edge Transport Server Role

Done?	Task
	Subscribe the Edge Transport server. For more information, see Configure Internet Mail Flow Through a Subscribed Edge Transport Server. **Note** To subscribe the Edge Transport server manually instead of using the Edge Subscription process, see Configure Mail Flow Between an Edge Transport Server and Hub Transport Servers Without Using EdgeSync.
	Configure an external postmaster recipient to receive e-mail messages. The external postmaster address is used as the sender for system-generated messages and notifications that are sent to message senders that exist outside the Exchange

	2010 organization. According to RFC 2821, every domain must be able to receive mail that is sent to the postmaster address. By default, no mailbox or other recipient object is configured to receive messages that are sent to the postmaster address for any accepted domains that are defined in the Exchange organization. If you haven't subscribed this Edge Transport server to your Exchange organization, the value of the external postmaster address is postmaster@[Edge Transport server FQDN]. After you subscribe the Edge Transport server to the Exchange organization, the value of the external postmaster address is postmaster@[default accepted domain]. If you specify a custom value for the external postmaster address on the Hub Transport servers in your Exchange organization, you must manually configure the external postmaster address on the Edge Transport server. For more information, see Configure the External Postmaster Address.
	Configure Domain Name System (DNS). The Edge Transport server must be configured for internal DNS lookups within the Exchange organization and external DNS lookups for external recipients. Public DNS records must also be configured for this server to send or receive mail from the Internet. For more information, see Configure Edge Transport Server Properties.

1.2.2.9.2 End-to-End Scenario Tasks

End-to-End Scenario Tasks

Planning and Deployment > Deploying Exchange 2010 > Exchange 2010 Post-Installation Tasks >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Use this checklist to track your work to configure specific end-to-end scenarios after you install Exchange Server 2010. The tasks in this topic are optional for configuring features.

For information about other optional post-installation configuration tasks that aren't listed in this topic, but are recommended after you install Exchange 2010, see Additional Post-Installation Tasks.

For guidance about required tasks that you must perform after installing Exchange 2010, see Finalize Deployment Tasks.

All Server Roles

Done?	Task
	Configure monitoring for your Exchange servers. For more information, see Performance and Scalability.

Mailbox Server Role

Done?	Task
	Configure messaging records management (MRM). For more information, see Messaging Records Management.

Client Access Server Role

Done?	Task
	Configure Microsoft Outlook Anywhere to provide access to Exchange using Office Outlook 2007 or Outlook 2010 clients from outside the corporate network. For more information, see Managing Outlook Anywhere.
	Verify that AutoDiscover is enabled and configured correctly. For more information, see Managing the Autodiscover Service.

Hub Transport Server Role

Done?	Task
	Replicate safelist aggregation data. For more information, see Configure Safelist Aggregation.

Unified Messaging Server Role

Done?	Task
	Enable outdialing. For more information, see Understanding Outdialing.
	Enable mutual-TLS between IP gateways or IP PBXs and an Exchange Unified Messaging (UM) server. For more information, see Understanding Unified Messaging VoIP Security.
	Create and configure a UM auto attendant. For more information, see Create a UM Auto

	Attendant.

Edge Transport Server Role

Done?	Task
	Configure the list of internal SMTP servers. For more information, see Set-TransportConfig.
	Replicate safelist aggregation data. For more information, see Configure Safelist Aggregation.

1.2.2.9.3 Additional Post-Installation Tasks

Additional Post-Installation Tasks

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-08-21*

Use this checklist to keep track of the tasks you may want to perform after you install Exchange Server 2010. The tasks in this checklist are optional, depending on the features you want to enable in your organization.

For information about other optional post-installation configuration tasks that aren't listed in this topic, but are recommended after you install Exchange 2010, see End-to-End Scenario Tasks.

For guidance about required tasks that you must perform after installing Exchange 2010, see Finalize Deployment Tasks.

All Server Roles

Done?	Task
	Verify your Exchange Server 2010 installation: • Review the setup logs. • Verify the folder structure of Exchange files. • Verify the tools installed. • Verify the required Exchange services are started. For more information, see Verify an Exchange 2010 Installation.

Mailbox Server Role

Done?	Task
	Verify your Mailbox Server role installation. For more information, see Verify an Exchange 2010 Installation.
	Configure permissions using the Exchange administrator roles. For more information, see Permissions to Manage Mailbox Servers.
	Configure your Mailbox server role. For more information, see Configure Mailbox Server Properties.
	Create and manage databases. For more information, see Managing Mailbox Databases.
	Create mailboxes for users in your organization. For more information, see Create a Mailbox Database.
	Move mailboxes from an existing Exchange server. For more information, see Managing Move Requests.
	Configure high availability, backup, and disaster recovery. For more information, see High Availability and Site Resilience.

Client Access Server Role

Done?	Task
	Enable the Client Access server for POP3 and IMAP4 if you plan to let clients use POP3 or IMAP4. For more information, see Enabling POP3 and IMAP4 on a Client Access Server.
	Increase security for communications between clients and the Client Access server and between the Client Access server and other servers. For more information about how to help secure the Client Access server messaging environment, see Understanding Client Access Security.

Hub Transport Server Role

Done?	Task
	Verify your Hub Transport Server role installation. For more information, see Transport Server Post-Deployment Tasks.

Unified Messaging Server Role

Done?	Task
	Add additional Unified Messaging (UM) servers. For more information, see Add a UM Server to a Dial Plan.
	Add additional UM languages to UM servers. For more information, see Install a Unified Messaging Language Pack on a UM Server.
	Enable UM users to receive incoming faxes. For more information, see Fax Advisor for Exchange 2010.
	Configure UM dial plans and auto attendants with customized greetings. For more information, see Enable a Custom Welcome Greeting on a UM Dial Plan or Enable a Custom Business Hours Main Menu Prompt Greeting on a UM Auto Attendant.
	Configure UM auto attendants with key mappings. For more information, see Configure Key Mapping Entries on a UM Auto Attendant.

Edge Transport Server Role

Done?	Task
	Verify your Edge Transport Server role installation. For more information, see Transport Server Post-Deployment Tasks.

1.2.2.9.4 Verify an Exchange 2010 Installation

Verify an Exchange 2010 Installation

Planning and Deployment > Deploying Exchange 2010 > Exchange 2010 Post-Installation Tasks >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

After you install Microsoft Exchange Server 2010, we recommend that you verify the installation by running the **Get-ExchangeServer** cmdlet and by reviewing the setup log file. If the setup process fails or errors occur during installation, you can use the setup log file to track down the source of the problem.

Note:
For information about the Exchange services that are installed and their status after you install Exchange 2010, see Overview of Services Installed by Exchange Setup.

Run Get-ExchangeServer

To verify that Exchange 2010 installed successfully, run the **Get-ExchangeServer** cmdlet in the Exchange Management Shell. A list is displayed of all Exchange 2010 server roles that are installed on the specified server when this cmdlet is run.

Note:

The Edge Transport server role can't share hardware with another Exchange 2010 server role.

For detailed syntax and parameter information, see Get-ExchangeServer.

Review the Setup Log

You can also learn more about the installation and configuration of Exchange 2010 by reviewing the setup log created during the setup process.

During installation, Exchange Setup logs events in the Application log of Event Viewer on computers that are running Windows Server 2008 and Windows Server 2008 R2. Review the Application log, and make sure that there are no warning or error messages related to Exchange setup. These log files contain a history of each action that the system takes during Exchange 2010 setup and any errors that may have occurred. By default, the logging method is set to verbose. Information is available for each installed server role.

You can find the setup log at *<system drive>*\ExchangeSetupLogs\ExchangeSetup.log. The *<system drive>* variable represents the root directory of the drive where the operating system is installed.

The setup log file tracks the progress of every task that is performed during the Exchange 2010 installation and configuration. The file contains information about the status of the prerequisite and system readiness checks that are performed before installation starts, the application installation progress, and the configuration changes that are made to the system. Check this log file to verify that the server roles were installed as expected.

We recommend that you start to review the setup log file by searching for any errors. If you find an entry that indicates that an error occurred, read the associated text to determine the cause of the error.

1.2.2.9.5 Enter Product Key

Enter Product Key

Planning and Deployment > Deploying Exchange 2010 > Exchange 2010 Post-Installation Tasks >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Use the Enter Product Key wizard to enter a product key for a server running Microsoft Exchange Server 2010 that doesn't already have a product key configured.

When you install Exchange 2010, it's unlicensed. This is also known as a trial edition. The trial edition expires 120 days after the date of installation. A server that is unlicensed functions as an Exchange Standard Edition server, but it isn't eligible for support from Microsoft support services. When you start the Exchange Management Console, if you have Exchange 2010 servers in your organization that are unlicensed, Exchange displays

a list of all unlicensed Exchange 2010 servers and the number of days that are remaining until the trial edition expires. If you have Exchange 2010 servers for which the trial edition has expired, Exchange also displays a separate warning for each expired server.

After you complete the Enter Product Key wizard, you must restart the Microsoft Exchange Information Store service so that the change is applied. Depending on the product key that you enter, Exchange will determine if the server is running the Standard Edition or Enterprise Edition of Exchange 2010 and will update any necessary settings.

What Do You Want to Do?

- Use the EMC to enter the product key
- Use the Shell to enter the product key

Use the EMC to enter the product key

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Product key" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In the console tree, navigate to **Server Configuration**.
2. In the action pane, click **Enter Product Key Group**.
3. On the **Enter Product Key** page, enter the product key, and then click **Enter**.
4. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to enter the product key

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Product key" entry in the Exchange and Shell Infrastructure Permissions topic.

This example uses the **set-ExchangeServer** cmdlet to enter the product key.

```
Set-ExchangeServer -Identity ExServer01 -ProductKey aaaaa-aaaaa-aaaaa-aaaaa-aaaaa
```

For detailed syntax and parameter information, see Set-ExchangeServer.

1.2.2.9.6 Register Filter Pack IFilters with Exchange 2010

Register Filter Pack IFilters with Exchange 2010

Planning and Deployment > Deploying Exchange 2010 > Exchange 2010 Post-Installation Tasks >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-29*

Exchange Search uses IFilters to index text content in different file formats. Microsoft Office 2010 Filter Packs includes filters for Microsoft Office 2010 and Office 2007 file formats. Installation of the Filter Pack is a pre-requisite for Exchange 2010 Mailbox and Hub Transport servers. For details, see Exchange 2010 Prerequisites. The following file

name extensions are supported by the filter pack: .docm, .docx, .one, .pptm, .pptx, .vdx, .vsd, .vss, .vst, .vsx, .vtx, .xlsb, .xlsm, .xlsx, .zip. For more information and to download the Filter Pack, see Microsoft Office 2010 Filter Packs.

After you install the Filter Pack, the included IFilters are registered with Windows Search. To allow Exchange 2010 to index Office 2010 file formats, the IFilters must also be registered with Exchange Search. This is done by modifying the registry.

In Exchange 2010 SP1, Exchange Setup registers the IFilters from Office 2010 Filter Packs with Exchange Search.

In the release to manufacturing (RTM) version of Exchange 2010, you must register the IFilters with Exchange 2010 by modifying the registry. You must perform this step after you have installed Exchange 2010 RTM on the server.

Note:

In Exchange 2010 RTM, you can meet the prerequisite by installing 2007 Office System Converter: Microsoft Filter Pack. We recommend that you upgrade to the Office 2010 version of the Filter Pack.

What Do You Want to Do?

- Register Microsoft Filter Pack IFilters manually
- Register Microsoft Filter Pack IFilters automatically

Register Microsoft Filter Pack IFilters manually

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

1. Start Registry Editor (regedit).
2. Locate the following registry subkey: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v14\MSSearch\CLSID**
   Add the subkeys and values that are listed in the following table to this subkey.

Subkey	Value
{5A98B233-3C59-4B31-944C-0E560D85E6C3}	drive:\Program Files\Common Files\Microsoft Shared\Filters\offfiltx.dll
{DDFE337F-4987-4EC8-BDE3-133FA63D5D85}	drive:\Program Files\Common Files\Microsoft Shared\Filters\offfiltx.dll
{F90DFE0C-CBDF-41FF-8598-EDD8F222A2C8}	drive:\Program Files\Common Files\Microsoft Shared\Filters\offfiltx.dll
{20E823C2-62F3-4638-96BD-90F4F6784EBC}	drive:\Program Files\Common Files\Microsoft Shared\Filters\offfiltx.dll
{312AB530-ECC9-496E-AE0E-C9E6C5392499}	drive:\Program Files\Common Files\Microsoft Shared\Filters\offfiltx.dll
{B8D12492-CE0F-40AD-83EA-099A03D493F1}	drive:\Program Files\Common Files\Microsoft Shared\Filters\ONIFilter.dll
{FAEA5B46-761B-400E-B53E-	drive:\Program Files\Common Files

E805A97A543E}	\Microsoft Shared\Filters\VISFilt.DLL

3. In each of the subkeys you created in Step 2, create the following string value.

Value Name	Type	Value Data
ThreadingModel	String (REG_SZ)	Both

4. Locate the following registry subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v14\MSSearch\Filters
Add the subkeys and values that are listed in the following table to this subkey.

Subkey	Value
.docm	{5A98B233-3C59-4B31-944C-0E560D85E6C3}
.docx	{5A98B233-3C59-4B31-944C-0E560D85E6C3}
.pptm	{DDFE337F-4987-4EC8-BDE3-133FA63D5D85}
.pptx	{DDFE337F-4987-4EC8-BDE3-133FA63D5D85}
.xlsm	{F90DFE0C-CBDF-41FF-8598-EDD8F222A2C8}
.xlsx	{F90DFE0C-CBDF-41FF-8598-EDD8F222A2C8}
.xlsb	{312AB530-ECC9-496E-AE0E-C9E6C5392499}
.zip	{20E823C2-62F3-4638-96BD-90F4F6784EBC}
.one	{B8D12492-CE0F-40AD-83EA-099A03D493F1}
.vsd	{FAEA5B46-761B-400E-B53E-E805A97A543E}
.vss	{FAEA5B46-761B-400E-B53E-E805A97A543E}
.vst	{FAEA5B46-761B-400E-B53E-E805A97A543E}
.vdx	{FAEA5B46-761B-400E-B53E-E805A97A543E}
.vsx	{FAEA5B46-761B-400E-B53E-E805A97A543E}
.vtx	{FAEA5B46-761B-400E-B53E-E805A97A543E}

5. Restart the **Microsoft Search (Exchange)** service using the Services console or by typing the following command in the Exchange Management Shell.

```
Stop-Service msftesql-Exchange -Force; Start-Service MSExchangeSearch
```

Register Microsoft Filter Pack IFilters automatically

1. Paste the following text into a Notepad file.

```
# Copyright (c) 2009 Microsoft Corporation. All rights reserved.
# THIS CODE IS MADE AVAILABLE AS IS, WITHOUT WARRANTY OF ANY KIND. THE
# This is a filter registration script to configure Exchange Server 20
$DLLPath = $env:CommonProgramFiles + "\Microsoft Shared\Filters"
$CLSIDKey = "HKLM:\SOFTWARE\Microsoft\ExchangeServer\V14\MSSearch\CLSI
$FiltersKey = "HKLM:\SOFTWARE\Microsoft\ExchangeServer\v14\MSSearch\Fi
# Filter DLL Locations
$officeFilterLocation = $DLLPath + "\offfiltx.dll"
$onenoteFilterLocation = $DLLPath + "\ONIFilter.dll"
$visioFilterLocation = $DLLPath + "\VISFilt.DLL"
# Filter GUIDs
$docxGuid    ="{5A98B233-3C59-4B31-944C-0E560D85E6C3}"
$pptxGuid    ="{DDFE337F-4987-4EC8-BDE3-133FA63D5D85}"
$xlsxGuid    ="{F90DFE0C-CBDF-41FF-8598-EDD8F222A2C8}"
$zipGuid     ="{20E823C2-62F3-4638-96BD-90F4F6784EBC}"
$xlsbGuid    ="{312AB530-ECC9-496E-AE0E-C9E6C5392499}"
$onenoteGuid ="{B8D12492-CE0F-40AD-83EA-099A03D493F1}"
$vsdGuid     ="{FAEA5B46-761B-400E-B53E-E805A97A543E}"
# Create CLSIDs
Write-Host "Creating CLSIDs..."
New-Item -Path $CLSIDKey -Name $docxGuid -Value $officeFilterLocation
New-Item -Path $CLSIDKey -Name $pptxGuid  -Value $officeFilterLocation
New-Item -Path $CLSIDKey -Name $xlsxGuid  -Value $officeFilterLocation
New-Item -Path $CLSIDKey -Name $zipGuid  -Value $officeFilterLocation
New-Item -Path $CLSIDKey -Name $xlsbGuid -Value $officeFilterLocation
New-Item -Path $CLSIDKey -Name $onenoteGuid -Value $onenoteFilterLocat
New-Item -Path $CLSIDKey -Name $vsdGuid  -Value $visioFilterLocation -
# Set Threading model
Write-Host "Setting threading model..."
New-ItemProperty -Path "$CLSIDKey\$docxGuid" -Name "ThreadingModel" -V
New-ItemProperty -Path "$CLSIDKey\$pptxGuid" -Name "ThreadingModel" -V
New-ItemProperty -Path "$CLSIDKey\$xlsxGuid" -Name "ThreadingModel" -V
New-ItemProperty -Path "$CLSIDKey\$zipGuid" -Name "ThreadingModel" -Va
New-ItemProperty -Path "$CLSIDKey\$xlsbGuid" -Name "ThreadingModel" -V
New-ItemProperty -Path "$CLSIDKey\$onenoteGuid" -Name "ThreadingModel"
New-ItemProperty -Path "$CLSIDKey\$vsdGuid" -Name "ThreadingModel" -Va
# Create Filter Entries
Write-Host "Creating Filter Entries..."
# Uncomment these if you wish to index these uncommonly exchanged form
#New-Item -Path $FiltersKey -Name ".docm" -Value $docxGuid -Type Strin
#New-Item -Path $FiltersKey -Name ".pptm" -Value $pptxGuid -Type Strin
#New-Item -Path $FiltersKey -Name ".xlsm" -Value $xlsxGuid -Type Strin
#New-Item -Path $FiltersKey -Name ".vss" -Value $vsdGuid   -Type Strin
#New-Item -Path $FiltersKey -Name ".vst" -Value $vsdGuid   -Type Strin
#New-Item -Path $FiltersKey -Name ".vsx" -Value $vsdGuid   -Type Strin
#New-Item -Path $FiltersKey -Name ".vtx" -Value $vsdGuid   -Type Strin
# These are the entries for commonly exchange formats
New-Item -Path $FiltersKey -Name ".docx" -Value $docxGuid -Type String
New-Item -Path $FiltersKey -Name ".pptx" -Value $pptxGuid -Type String
New-Item -Path $FiltersKey -Name ".xlsx" -Value $xlsxGuid -Type String
New-Item -Path $FiltersKey -Name ".xlsb" -Value $xlsbGuid -Type String
New-Item -Path $FiltersKey -Name ".zip" -Value $zipGuid  -Type String
New-Item -Path $FiltersKey -Name ".one" -Value $onenoteGuid -Type Stri
New-Item -Path $FiltersKey -Name ".vsd" -Value $vsdGuid   -Type String
Write-Host "Registry subkeys created."
Write-Host "Please restart Microsoft Search  (Exchange) service from t
```

2. Name the file RegisterMicrosoftFilterPack.ps1, and then save it.
3. Start Windows PowerShell or the Exchange Management Shell.
4. Run the script RegisterMicrosoftFilterPack.ps1.

Important:

Whether Windows PowerShell or Exchange Management Shell allow you to run scripts is determined by the execution policy. For more details, see Script Security.

5. Restart the **Microsoft Search (Exchange)** service using the Services console or by typing the following command in the Exchange Management Shell.

```
Stop-Service msftesql-Exchange -Force; Start-Service MSExchangeSearch
```


1.2.2.9.7 Transport Server Post-Deployment Tasks

Transport Server Post-Deployment Tasks

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-04*

After you install Hub Transport server and Edge Transport server roles, you need to perform specific, additional tasks to have full message flow functionality. Tasks include configuring accepted domains and configuring Internet mail flow. These tasks, and recommendations for how to accomplish them, are described in this topic.

Configure Accepted Domains

Accepted domains are SMTP namespaces for which an Exchange organization sends and receives e-mail. An Exchange organization is considered authoritative for a specific accepted domain if it handles all mail delivery for recipients in that domain. Typically, the accepted domains that you use in a new installation are all authoritative. However, there are other types of accepted domains, which you may want to use depending on your needs.

To learn more about accepted domains, see Understanding Accepted Domains.

Accepted Domains in the Exchange Organization

By default, one accepted domain exists and is configured as authoritative for the Exchange organization during installation. The default authoritative domain is the fully qualified domain name (FQDN) of your Active Directory forest root domain. In many organizations, the internal domain name differs from the external domain name.

For example, your internal domain name may be contoso.local, and your external domain name may be contoso.com. The public Domain Name System (DNS) MX resource record for your organization will reference contoso.com. To send and receive e-mail across the Internet, you must configure contoso.com as an accepted domain. Also, if your Exchange organization is handling mail for more than one domain, you must specify these additional domains as accepted domains.

Accepted domains need to be configured only once for the Exchange organization after you deploy your first Hub Transport server.

For step-by-step instructions about creating accepted domains, see Create an Accepted Domain.

Note:

If you configure additional accepted domains for your organization, you need to update your e-mail address policies to assign these domain names to your recipients. To learn more about e-mail address policies, see Understanding E-Mail Address Policies.

Accepted Domains on Edge Transport Servers

You need to configure your accepted domains on each Edge Transport server you deploy. However, we recommend that you configure accepted domains only on the Hub Transport

server role, and then create an Edge Subscription for the Edge Transport server. The accepted domain configuration will be replicated to the Edge Transport servers when the Microsoft Exchange EdgeSync service runs. For more information, see Understanding Edge Subscriptions.

Configure Internet Mail Flow

After you install your first Hub Transport server, you must create additional connectors to begin sending and receiving messages from the Internet. The following connectors are created when you install your first Hub Transport server:

- **Intra-organization Send connector** This implicit Send connector isn't visible in the management tools and is computed based on your Active Directory site topology. This Send connector enables your Hub Transport servers to communicate with each other. For more information about internal message routing, see Understanding Message Routing.
- **Receive connector configured to accept messages from all remote IP addresses through port 25** This connector typically accepts connections from all IP address ranges. The usage type for this connector is Internal. This connector only accepts mail from other Exchange servers that are part of the same Exchange organization. By default, this connector doesn't accept anonymous submissions.
- **Receive connector configured to receive messages from all remote IP addresses through port 587** This connector is used to accept SMTP connections from POP3 or IMAP4 clients. This connector typically accepts connections from all IP address ranges. The usage type for this connector is Internal.

When you install an Edge Transport server, only the following connector is created during setup:

- **Receive connector configured to receive messages from all remote IP addresses through port 25** This connector is used for both incoming Internet e-mail and incoming e-mail from the Hub Transport servers. The permissions on the connector are automatically determined by how sessions are authenticated.

To learn more about connectors, see Understanding Send Connectors and Understanding Receive Connectors.

After a default installation:

- Your Hub Transport servers can communicate with each other.
- Your Hub Transport servers can receive message submissions from your Mailbox servers and non-MAPI clients (such as POP3 or IMAP4).
- Your Edge Transport server can receive messages from the Internet and your Hub Transport servers.

To complete deployment, you need to:

- Configure your Hub Transport servers to forward Internet messages to your Edge Transport servers.
- Configure your Edge Transport servers to send Internet messages to the Internet.
- Configure your Edge Transport servers to forward inbound messages to your Hub Transport servers.

You have two options to accomplish the additional tasks. For best results, we recommend that you subscribe your Edge Transport servers to your organization. The options are described in the following topics:

- Configure Internet Mail Flow Through a Subscribed Edge Transport Server
- Configure Mail Flow Between an Edge Transport Server and Hub Transport

Servers Without Using EdgeSync

If you don't use Edge Transport servers in your organization, you have two options for configuring Internet mail flow. Keep in mind that configuring Internet mail flow directly through your Hub Transport servers isn't recommended. The options are described in the following topics:

- Configure Internet Mail Flow Through Exchange Hosted Services or an External SMTP Gateway
- Configure Internet Mail Flow Directly Through a Hub Transport Server

1.2.2.10 Modify an Exchange 2010 Installation

Modify an Exchange 2010 Installation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-20*

The following topics provides information about modifying an installation of Microsoft Exchange Server 2010:

Modify or Remove Exchange 2010

Remove the Last Legacy Exchange Server from an Exchange 2010 Organization

Install an Exchange 2010 Language Pack

1.2.2.10.1 Modify or Remove Exchange 2010

Modify or Remove Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-03*

This topic explains how to use the Exchange Server 2010 Setup wizard to modify or remove Exchange 2010.

Prerequisite

You must ensure that each of the server roles meets the appropriate prerequisites and system requirements before you begin the modification or uninstall process. For more information about server roles, see Overview of Exchange 2010 Server Roles. To understand the prerequisites for all server roles, see Exchange 2010 Prerequisites. For more information about system requirements, see Exchange 2010 System Requirements.

Modify or Remove Exchange Server 2010

You can either run Exchange 2010 Setup.exe or navigate to Control Panel to modify or remove Exchange 2010 (either server roles or an entire installation).

1. The **Maintenance Mode** page of the Exchange Server 2010 Setup wizard begins the process of changing or removing your Exchange installation. Click **Next** to continue.

2. On the **Server Role Selection** page, select the Exchange server roles that you want to add (if you're changing an installation) or remove (if you're removing one or more server roles or an entire installation). Click **Next** to continue.

3. On the **Readiness Checks** page, view the status to determine if the organization and server role prerequisite checks completed successfully. If the prerequisites check doesn't complete successfully, review the **Summary** page to help troubleshoot and fix any issues that are preventing Setup from completing. If the checks have completed successfully, click **Install** if you want to add a server role or **Uninstall** to remove the specified server role(s) or the entire installation of Exchange 2010.

4. On the **Completion** page, click **Finish**.

1.2.2.10.2 Remove the Last Legacy Exchange Server from an Exchange 2010 Organization

Remove the Last Legacy Exchange Server from an Exchange 2010 Organization

Planning and Deployment > Deploying Exchange 2010 > Modify an Exchange 2010 Installation >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove the last computer running Microsoft Exchange Server 2007 or Exchange Server 2003 from an organization that also has Exchange Server 2010 servers. First, you prepare your Exchange organization for removal of the last Exchange 2007 or Exchange 2003 server. Next, you remove the last Exchange 2007 or Exchange 2003 server. To successfully remove the Exchange 2007 or Exchange 2003 server from your organization, you must complete both steps.

Looking for other management tasks related to installing Exchange 2010? Check out Managing Deployment of Exchange 2010.

Remove the last Exchange 2003 server

Removal of the last Exchange 2003 server requires that you satisfy some prerequisites and then complete a two-step process.

Prerequisites for removing the last Exchange 2003 server

- You installed one or more Exchange 2010 servers in the organization.
- If you're removing the last Exchange 2003 server, confirm that you don't plan to use any of the Exchange 2003 features that have been removed in Exchange 2010. The following are some of the features that aren't supported in Exchange 2010:
  - Novell GroupWise connector

- Network News Transfer Protocol (NNTP)
- Routing groups
- Lotus Notes connector

For a complete list of the features discontinued in Exchange 2010, see Discontinued Features.

Step 1: Prepare the Exchange 2003 organization to remove legacy Exchange servers

To perform the following procedure, the account you use must be delegated membership in the Exchange Full Administrator role on Exchange 2003 servers.

1. Move all mailboxes to an Exchange 2010 server in the organization. For more information, see Create a Local Move Request.
2. Move all content from the public folder database on the legacy Exchange 2003 server to a public folder database on an Exchange 2010 server in the organization. For detailed steps, see Move Public Folder Content from One Public Folder Database to Another Public Folder Database.
3. On Exchange 2003 servers, for each offline address book (OAB), move the generation process to an Exchange 2010 server. For detailed steps, see Move the Offline Address Book Generation Process to Another Server.
4. To remove the public folder mailbox and stores on the Exchange 2003 server, see How to Dismount and Delete the Mailbox and Public Folder Stores.
5. Verify that Internet mail flow is configured to route through your Exchange 2010 transport servers. For more information, see the following topics:
   - Configure Internet Mail Flow Directly Through a Hub Transport Server
   - Configure Internet Mail Flow Through a Subscribed Edge Transport Server
6. To verify that all inbound protocol services (Microsoft Exchange ActiveSync, Microsoft Office Outlook Web App, Outlook Anywhere, POP3, IMAP4, Autodiscover service, and any other Exchange Web service) are configured for Exchange 2010, see Managing Client Access Servers.
7. Delete the routing group connectors that connect the Exchange 2003 routing groups. You can do this from Exchange 2003 System Manager, or you can use the Remove-RoutingGroupConnector cmdlet in the Exchange Management Shell.
8. If you have Exchange 2003 recipient policies that are only Mailbox Manager policies and don't define e-mail addresses (they don't have an **E-mail Addresses (Policy)** tab), perform the following steps to delete the policies:
   - In Exchange System Manager, expand **Recipients**, and then select **Recipient Policies**.
   - To verify that a policy is only a Mailbox Manager policy, right-click the policy, and then select **Properties**. The **Properties** page must not have an **E-Mail Addresses (Policy)** tab.
   - To delete the policy, right-click the policy, and then select **Delete**. Click **OK**, and then click **Yes**.
9. If you have Exchange 2003 policies that are both E-mail Addresses and Mailbox Manager policies (they have both the **Mailbox Manager Settings (Policy)** tab and the **E-mail Addresses (Policy)** tab), perform the following steps to remove the mailbox manager portion of the policy:
   - In Exchange System Manager, expand **Recipients**, and then select **Recipient Policies**.
   - Right-click the policy, and then select **Change property pages**.
   - Clear the **Mailbox Manager Settings** check box, and then click **OK**.

Note:

Don't delete any e-mail address recipient policies that have e-mail addresses that you still want defined in your organization. Exchange 2010 will use those policies when provisioning new recipients.

Step 2: Remove the last Exchange 2003 server from an

Exchange 2010 organization

To perform the following procedure, the account you use must be delegated membership in the Exchange Full Administrator role on Exchange 2003 servers.

1. Perform the following steps to delete the domain Recipient Update Service:
   1.a. In Exchange 2003 System Manager, expand **Recipients**, and then select **Recipient Update Service**.
   1.b. Right-click each domain Recipient Update Service, and then select **Delete**.
   1.c. Click **Yes**.
2. You won't be able to delete the Enterprise **Recipient Update Service** by using Exchange 2003 System Manager. Instead, perform the following steps to delete the **Recipient Update Service** by using Active Directory Service Interfaces Editor (ADSI Edit or AdsiEdit.msc). AdsiEdit.msc is included on the Windows Server 2003 CD in Support\Tools. For more information about ADSI Edit, see ADSI Edit (adsiedit.msc).
   2.a. In ADSI Edit, navigate to **Configuration** > **CN=Configuration,CN=**<*domain*> > **CN=Services** > **CN=Microsoft Exchange** > **CN=**<*Exchange organization name*> > **CN=Address Lists Container** > **CN=Recipient Update Services**.
   2.b. In the result pane, right-click **Recipient Update Service (Enterprise Configuration)**, click **Delete**, and then click **Yes** to confirm the deletion.
3. Uninstall Exchange 2003 by using **Add or Remove Programs** from **Control Panel**. For more information, see How to Uninstall Exchange Server 2003.

   Caution:

   Before you remove any Exchange 2003 administrative groups that contained mailboxes, verify that the public folder hierarchy has been moved to another administrative group. Also, verify that the Free/Busy public folder has replicated to the servers in other administrative groups.
   The general process to create public folder replicas on servers in other administrative groups is to update the replica list for each public folder to specify the destination server. After you allow sufficient time for the data to be replicated to the destination server, verify that the public folder database is empty. To do this, use the Exchange System Manager **Public Folder Instances** node or use the **Get-PublicFolderStatistics** cmdlet. If the results are blank, the public folder database is empty. When you remove the public folder database, you may be prompted to select another public folder database to act as the site folder for administrative groups and OABs. You may also be prompted to select another public folder database to act as the default public folder database for some messaging databases. For these prompts, the site folder server represents the public folder database responsible for making sure that administrative group and OAB site folders exist. The site folder server may be any public folder database server in the organization. The site folder server doesn't delete site folders for missing administrative groups. However, the site folder server does remove site folders for missing OABs.

4. After the last Exchange 2003 server has been removed from the Exchange 2010 organization, you can also remove the legacy Exchange Domain Servers and Exchange Enterprise Servers security groups. For more information, see Delete a group.

   Caution:

   Before you delete either of these security groups, verify that each group is empty and isn't being used for any other purpose or process. If one or both of these groups has members, but if all members are shown as security identifiers (SIDs), the groups can be safely removed. If at least one group has members, and if the members are resolved to computer names, you should verify that the computers aren't functioning Exchange servers before you delete the groups.

Remove the last Exchange 2007 server

Removal of the last Exchange 2007 server requires that you satisfy some prerequisites and then complete a two-step process.

Prerequisites for removing the last Exchange 2007 server

- You installed one or more Exchange 2010 servers in the organization.
- If you're removing the last Exchange 2007 server, confirm that you don't plan to use any of the Exchange 2007 features that have been removed in Exchange 2010. The following are some of the features that aren't supported in Exchange 2010:
  - Storage groups
  - DSProxy
  - Cluster continuous replication
  - Single copy cluster

For a complete list of the Exchange 2007 features discontinued in Exchange 2010, see Discontinued Features.

Step 1: Prepare the Exchange 2007 organization to remove legacy Exchange servers

To perform the following procedure, the account you use must be delegated membership in the Exchange Organization Administrator role on Exchange 2007 servers.

1. Move all mailboxes to an Exchange 2010 server in the organization. For more information, see Create a Local Move Request.
2. Move all content from the public folder database on the legacy Exchange 2007 server to a public folder database on an Exchange 2010 server in the organization. For detailed steps, see Move Public Folder Content from One Public Folder Database to Another Public Folder Database.
3. On Exchange 2007 servers, for each offline address book (OAB), move the generation process to an Exchange 2010 server. For detailed steps, see Move the Offline Address Book Generation Process to Another Server.
4. To remove the public folder mailbox and stores on the Exchange 2007 server, see the following topics:
   - How to Remove a Public Folder Database
   - How to Remove a Mailbox Database
5. Verify that Internet mail flow is configured to route through your Exchange 2010 transport servers. For more information, see the following topics:
   - Configure Internet Mail Flow Directly Through a Hub Transport Server
   - Configure Internet Mail Flow Through a Subscribed Edge Transport Server
6. To verify that all inbound protocol services (Microsoft Exchange ActiveSync, Microsoft Office Outlook Web App, Outlook Anywhere, POP3, IMAP4, Autodiscover service, and any other Exchange Web service) are configured for Exchange 2010, see Managing Client Access Servers.

Step 2: Remove the last Exchange 2007 server from an Exchange 2010 organization

Uninstall Exchange 2007 by using **Add or Remove Programs** from **Control Panel**. For more information, see the following topics:

- How to Completely Remove Exchange 2007 from a Server
- How to Remove an Exchange 2007 Organization

Install an Exchange 2010 Language Pack

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-14*

You can use the Microsoft Exchange 2010 Language Pack wizard to install a language pack on your Microsoft Exchange Server 2010 server. An Exchange 2010 language pack contains the necessary resources for a supported Exchange language. Client and server language packs are grouped into a single bundle containing both client and server resource and support files. For more information about language packs, see Exchange 2010 Language Support.

Install the Exchange 2010 language pack

1. Download the language pack. For Exchange 2010 Service Pack 1 (SP1), download the latest language pack from Microsoft Exchange 2010 SP1 Language Pack Bundle.
2. Double-click the language pack file that you downloaded to start language pack setup.
3. On the **License Agreement** page, review the software license terms. If you agree to the terms, select **I accept the terms in the license agreement**, and then click **Next**.
4. On the **Readiness Checks** page, view the status to determine if the prerequisite checks completed successfully. If they haven't completed successfully, you must resolve any reported errors before you can install the language pack. You don't need to exit Setup when resolving some of the prerequisite errors. After resolving a reported error, click **Retry** to run the prerequisite check. Be sure to also review any warnings reported. If all readiness checks have completed successfully, click **Install** to install the language pack.
5. On the **Completion** page, click **Finish**.

Use unattended setup to install the Exchange 2010 language pack

1. Download the language pack. For Exchange 2010 SP1, download the latest language pack from Microsoft Exchange 2010 SP1 Language Pack Bundle.
2. Insert the Exchange 2010 SP1 DVD into the DVD drive. At the command prompt, navigate to the DVD drive or navigate to the network location of the Exchange 2010 installation files.
3. At a command prompt, run the following command. Include the path to the location where you saved the language pack and the filename of the language pack. For example, C:\Exchange\LanguagePackBundle.exe.

```
Setup.com /LanguagePack:<path to language pack bundle>
```

1.2.2.11 Installation Guide Templates

Installation Guide Templates

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-02*

This section provides the following document templates you can use to create customized installation guides for your organization's Microsoft Exchange Server 2010 server role installations:

Installation Guide Template - Client Access Server

Installation Guide Template - Hub Transport Server

Installation Guide Template - Mailbox Server

Installation Guide Template - DAG Member

You can use the Exchange 2010 templates as a starting point for formalizing your server build procedures. These guides are generic, so you'll need to modify them to meet the specific needs of your organization. Also, you can download these templates as a download package in .zip file format at Microsoft Exchange Server 2010 Install Guide Templates (http://go.microsoft.com/fwlink/?LinkID=187961).

We recommend that every procedure described in the guides that you perform be tested and validated in a lab environment before you use the procedure in a production environment.

1.2.2.11.1 Installation Guide Template - Client Access Server

Installation Guide Template - Client Access Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-21*

This topic provides you with an installation guide template that you can use as a starting point for formally documenting your organization's server build procedures for Microsoft Exchange Server 2010 servers that will have the Client Access server role installed.

The template includes the following key sections:

- Executive Summary
- Server Configuration
- Load Balancing Configuration
- Verification Steps
- Exchange Server Role Installation
- Exchange Server Role Configuration

For purposes of providing an example, the template uses the fictitious company name of Contoso. Also, you can download this template, along with templates for other server roles, as a download package in .zip file format at Microsoft Exchange Server 2010 Install

Guide Templates (http://go.microsoft.com/fwlink/?LinkID=187961).

Executive Summary

The purpose of this document is to explain the installation and configurations necessary to install the Exchange 2010 Client Access server role on the Windows Server 2008 platform.

Business Justification

By having an installation guide, Contoso will be able to ensure standardization across the enterprise, reducing total cost of ownership (TCO), and easing troubleshooting steps.

Scope

The scope of this document is limited to installation of an Exchange 2010 Client Access server for Contoso on the x64 version of the Windows Server 2008 (SP2 or R2) operating system.

Prerequisites

The administrator should have working knowledge of Windows Server 2008 concepts, Exchange 2010 concepts, the Exchange Management Console and Exchange Management Shell, the command line, and various system utilities. This document does not elaborate on the details of any system utility except as necessary to complete the tasks within.

In addition, before implementing the server role, the administrator should review the Understanding Client Access topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187352).

Assumptions

This document assumes that Windows Server 2008 x64 Edition is installed on the intended Client Access server per company baseline regulations which include the latest approved service pack and hotfixes. In addition, the following system prerequisites have been installed:

- Microsoft .NET Framework 3.5 SP1 and the update for .NET Framework 3.5 SP1 For more information, see Microsoft Knowledge Base article 959209, An update for the .NET Framework 3.5 Service Pack 1 is available (http://go.microsoft.com/fwlink/?linkid=3052&kbid=959209).
- Windows Management Framework (Windows Remote Management 2.0 and Windows PowerShell 2.0).

This document assumes that forest and domain preparation steps have been performed as described in the Prepare Active Directory and Domains topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187262).

This document assumes that the account you will be using for the Exchange tasks has been delegated the Server Management management role, as described in the Server Management topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187265).

This document also assumes that both Exchange 2010 Windows Server 2008 and Windows Server 2008 will be secured following the best practices found in the Windows Server 2008 Security Guide (http://go.microsoft.com/fwlink/?LinkId=122593).

Important:

The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Server Configuration

The following media are required for this section:

- Windows Server 2008 installation files

The following procedures are in this section:

1. Additional Software Verification
2. Network Interfaces Configuration
3. Drive Configuration
4. Windows Server 2008 Hotfix Installation
5. Domain Membership Configuration
6. Local Administrators Verification
7. Local Administrator Account Password Reset
8. Debugging Tools Installation
9. Page File Modifications
10. Drive Permissions
11. Windows Network Load Balancing Installation and Configuration
12. DNS Entry Creation

Additional Software Verification

1. Verify that Remote Desktop is enabled.
2. As an optional process, install Microsoft Network Monitor (http://go.microsoft.com/fwlink/?LinkId=86611).

Network Interfaces Configuration

1. Log on to the server with an account that has been delegated at least local administrative access.
2. Click **Start > Control Panel**, and then double-click **Network and Sharing Center**.
3. Click **Manage Network Connections**.
4. Locate the connection for the internal network and rename it according to your organization's naming standards.
5. Right-click the connection and then select **Properties**.
6. For Internet Protocol Version 4 (TCP/IPv4), add the following:
   6.a. **Static IP Address**, **Subnet Mask**, and **Gateway**
   6.b. DNS Server IP Addresses
   6.c. Select the check box to **Append parent suffixes of the primary DNS suffix**.
   6.d. WINS IP Addresses (if using WINS)
7. If you are using Internet Protocol Version 6 (TCP/IPv6), configure the IPv6 settings according to your organization's network standards.

Drive Configuration

1. Connect to the server through Remote Desktop and then log on with an account that has been delegated local administrative access.
2. Click **Start > Administrative Tools**, and then select **Computer Management**.
3. Expand **Storage** and then click **Disk Management**.
4. Using the Disk Management snap-in of the Microsoft Management Console (MMC), format, rename, and assign the appropriate **Drive Letters** so that the volumes and DVD drive match the appropriate server configuration.

Drive configuration

LUN	Drive letter	Usage
1	C	Operating system and Exchange binaries
2	Z	DVD drive

Windows Server 2008 Hotfix Installation

1. Connect to the server via Remote Desktop and log on with an account that has local administrative access.
2. Obtain the latest hotfixes approved by your company for your version of Windows Server 2008 x64 (SP2 or R2) and copy them to the server.
3. Launch the hotfix setup via one of two ways:
   3.a. Double-click the file and follow the GUI instructions.
   3.b. Perform a silent installation using the following command from an administrative command prompt:

```
<hotfix>.msu /quiet /norestart
```

4. Click **Yes** for any **Digital Signature not Found** dialog boxes that may appear.

> **Note:**
> These dialog boxes will not appear in environments that have not deployed the Windows Security templates.

5. Wait for all file copies to complete, and then restart the server. You can use the **Processes** tab in Windows Task Manager to monitor the hotfix installation progress. When the wusa.exe process has exited, the hotfix installation is complete.

Domain Membership Configuration

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start,** right-click **My Computer**, and then select **Properties**.
3. Under the **Computer Name, domain, and workgroup** settings, click **Change Settings**.
4. Click **Change**.
5. Choose the **Domain** option button, and then enter the appropriate domain name.
6. Enter the appropriate credentials.
7. Click **OK** and **OK**.
8. Click **OK** to close **System Properties**.
9. Restart the server.

Local Administrators Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Verify (or add if not already there) that the Domain Admins account and the user account that will perform the Exchange installation are members of the local Administrators group on this server.
3. Verify that your user account is a member of a group which is a member of the local Administrators group on the Windows Server 2008 server. If it is not, use an account that is a member of the local Administrators group before continuing.

Local Administrator Account Password Reset

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Manage**.
3. Expand the nodes to find **Configuration\Local Users and Groups\Users**.
4. Right-click **Administrator**, and then select **Set Password**. Change the password so that it meets strong complexity requirements.

Debugging Tools Installation

This section describes several useful tools that aid administrators in Exchange administration and in troubleshooting support issues.

Debugging Tools for Windows allow administrators to debug processes that are affecting service and determine root cause.

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Download and install the latest 64-bit Debugging Tools from Install Debugging Tools for Windows 64-bit Version (http://go.microsoft.com/fwlink/?LinkID=123594).

Page File Modifications

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Properties**.
3. Select the **Advanced System Settings**.
4. Under **Startup and Recovery**, click **Settings**.
   4.a. Under **Write Debugging Information**, select **Kernel Memory Dump** from the memory dump drop-down list.
   4.b. Click **OK**.
5. Under **Performance**, click **Settings**.
6. Click the **Advanced** tab.
7. Under **Virtual Memory**, click **Change**.
8. On servers that have a dedicated page file drive, follow these steps:
   8.a. In the **Drive** list, click **C:**, and then click **Custom size**.
   8.b. For the C: drive, set the **Initial Size (MB)** value to a minimum of 200 MB. (Windows requires between 150 MB and 2 GB page file space, depending on server load and the amount of physical RAM that is available for page file space on the boot volume when Windows is configured for a kernel memory dump. Therefore, you may be required to increase the size.)
   8.c. For the C: drive, set the **Maximum Size (MB)** value to that of the **Initial Size**.
   8.d. In the **Drive** list, select the page file drive (for example, the P: drive), and then click **Custom size**.
   8.e. In the **Initial Size (MB)** box, type the result of one of the following calculations:
      If the server has less than 8 GB of RAM, multiply the amount of RAM times 1.5.
      If the server has 8 GB of RAM or more, add the amount of RAM plus 10 MB.
   8.f. In the **Maximum Size (MB)** box, type the same amount that you typed in the **Initial Size** box.
   8.g. Delete all other page files.
   8.h. Click **OK**.
9. On servers that do not have a dedicated page file drive, follow these steps:
   9.a. In the **Drive** list, click **C:**, and then click **Custom size**.
   9.b. For the C: drive, in the **Initial Size (MB)** box, type the result of one of the following calculations:
      If the server has less than 8 GB of RAM, multiply the amount of RAM times 1.5.
      If the server has 8 GB of RAM or more, add the amount of RAM plus 10 MB.
   9.c. Delete all other page files.
   9.d. Click **OK**.
10. Click **OK** two times to close the **System Properties** dialog box.
11. Click **No** if prompted to restart the system.

Note:

For more information about page file recommendations, see the following Microsoft Knowledge Base articles: How to determine the appropriate page file size for 64-bit versions of Windows Server 2003 or Windows XP (http://go.microsoft.com/fwlink/?linkid=3052&kbid=889654); and Overview of

memory dump file options for Windows Vista, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 2000 (http://go.microsoft.com/fwlink/?linkid=3052&kbid=254649).

Drive Permissions

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, and then select **Computer**.
3. Right-click **D Drive**, and then select **Properties**.
4. Click the **Security** tab.
5. Click **Edit**.
6. Click **Add**, and then select the local server from **Locations**.
7. Grant the following rights as outlined in the following table.

Drive permissions

Account	Permissions
Administrators	Full Control
SYSTEM	Full Control
Authenticated Users	Read and Execute, List, Read
CREATOR OWNER	Full Control

8. Click the **Advanced** button.
9. Select the **CREATOR OWNER** permission entry, and then click **View/Edit**.
10. Select **Subfolders and Files Only** from the drop-down list.
11. Click **OK** two times.
12. Click **OK** to close the drive properties.
13. Repeat steps 3-12 for each additional drive (other than the C drive).

Load Balancing Configuration

Procedures in this section only need to be performed on Client Access servers that will be used in a load-balanced array. In particular, this section focuses on Windows Network Load Balancing (NLB). For more information about NLB, see Network Load Balancing (http://go.microsoft.com/fwlink/?LinkId=187482) and Network Load Balancing Clusters (http://go.microsoft.com/fwlink/?LinkId=49315) and Implementing a Network Load Balancing Cluster (http://go.microsoft.com/fwlink/?LinkId=187483).

If you are deploying a hardware load balancing array, review your vendor's documentation and follow their guidance for configuration.

For more information about load balancing in Exchange 2010, see the topics Understanding Load Balancing in Exchange 2010 (http://go.microsoft.com/fwlink/?LinkId=196447) and Load Balancing Requirements of Exchange Protocols (http://go.microsoft.com/fwlink/?LinkId=196448) in the Exchange Server 2010 Library.

Windows Network Load Balancing Installation and Configuration

The values used in NLB must be the same across all nodes in the NLB cluster. The values specified in the following table will ensure that the Windows Network Load Balancing array can load-balance the appropriate protocols (HTTPS, IMAP4, POP3, RPC Endpoint Mapper, the Address Book service, and the RPC Client Access service). For more information, see Understanding Load Balancing in Exchange 2010.

Load-balanced protocols and ports

Protocol	TCP port numbers
HTTPS	443

IMAP4	143 and 993
POP3	110 and 995
RPC Endpoint Mapper	135
Address Book service	59595
RPC Client Access service	59596

Note:
This document uses TCP59595 for the Address Book service and TCP59596 for the RPC Client Access service, but you can use any TCP high ports that are available within the environment between ports 59530 and 60554.

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Install Network Load Balancing for your operating system:
   2.a. **Windows Server 2008 SP2** Open an administrative command prompt window and run the following command:

```
ServerManagerCmd.exe -i NLB
```

   2.b. **Windows Server 2008 R2** Open an elevated Windows PowerShell console, and run the following commands:

```
Import-Module ServerManager
Add-WindowsFeature NLB
```

3. Click **Start > Administrative Tools**, and then right-click **Network Load Balancing Manager**.
4. Click **Cluster-New**.
5. In the **New Cluster wizard**, enter the local server's computer name, click **Connect** and then select the appropriate network connection.
6. Click **Next**.
7. In the **Host Parameters** section, verify the host's IP address and subnet mask.
8. Click **Next**.
9. In the **Cluster IP Address** section, click **Add** and enter:
   9.a. **IP Address**
   9.b. **Subnet Mask**
10. Click **Next**.
11. In the **Cluster Parameters** section, enter in the **Full Internet Name** (for example, mail.contoso.com) that will be used by the cluster and make sure **Unicast** is selected.
12. Click **Next**.
13. In the **Port Rules** section, select the default rule and click **Edit**.
14. Under **Port Range**, change the **From** value to **80** and the **To** value to **80**.
15. Under **Protocols**, select **TCP**.
16. Click **OK**.
17. Click **Add** to create a new port rule.
    17.a. Under **Port Range**, change the **From** value to **443** and the **To** value to **443**.
    17.b. Under Protocols, select **TCP**.
    17.c. Click **OK**.

Note:
If you are using IMAP or POP in the environment, be sure to create the appropriate rules.

18. Click **Add** to create a new port rule.
    18.a. Under **Port Range**, change the **From** value to **143** and the **To** value to

143.
18.b.Under **Protocols**, select **TCP**.
18.c.Click **OK**.
19.Click **Add** to create a new port rule.
19.a.Under **Port Range**, change the **From** value to **110** and the **To** value to **110**.
19.b.Under **Protocols**, select **TCP**.
19.c.Click **OK**.
20.Click **Add** to create a new port rule.
20.a.Under **Port Range**, change the **From** value to **993** and the **To** value to **993**.
20.b.Under **Protocols**, select **TCP**.
20.c.Click **OK**.
21.Click **Add** to create a new port rule.
21.a.Under **Port Range**, change the **From** value to **500** and the **To** value to **500**.
21.b.Under **Protocols**, select **UDP**.
21.c.Click **OK**.

Note:
The above rule for UDP 500 should be created if you are using IPSec in the environment.

22.Click **Add** to create a new port rule.
22.a.Under **Port Range**, change the **From** value to **995** and the **To** value to **995**.
22.b.Under **Protocols**, select **TCP**.
22.c.Click **OK**.
23.Click **Add** to create a new port rule.
23.a.Under **Port Range**, change the **From** value to **135** and the **To** value to **135**.
23.b.Under **Protocols**, select **TCP**.
23.c.Click **OK**.
24.Click **Add** to create a new port rule.
24.a.Under **Port Range**, change the **From** value to **59595** and the **To** value to **59596**.
24.b.Under **Protocols**, select **TCP**.
24.c.Click **OK**.
25.Click **OK**.
26.Click **OK** to acknowledge the resulting dialog box.
27.While still in the internal network connection properties, click **Internet Protocol (TCP/IP)** and select **Properties**.
28.Click **Advanced**.
29.Under **IP Addresses**, click **Add**.
29.a.Enter the **virtual IP Address** and **Subnet Mask** and click **OK**.
29.b.Click **OK**.
30.Click **Finish** to complete the New Cluster wizard.

DNS Entry Creation

Submit a change request to the appropriate operations group to have the domain name that was specified in the previous "Network Load Balancing Installation and Configuration" section for the NLB cluster (for example, mail.contoso.com) created as a host record associated to the NLB cluster's IP address.

Verification Steps

The following procedures are in this section:

1.Organizational Unit Verification
2.Active Directory Site Verification
3.Domain Controller Diagnostics Verification

4. Exchange Best Practices Analyzer Verification

Important:
The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Organizational Unit Verification

Submit a change request to the appropriate operations group and have the computer object moved to the appropriate organizational unit (OU).

Active Directory Site Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open a Command Prompt window.
3. Verify that the server is in the correct domain and Active Directory site. At the command line, type the following:

```
NLTEST /server:%COMPUTERNAME% /dsgetsite
```

4. The name of the Active Directory site to which the server belongs will be displayed. If the server is not in the correct Active Directory site, submit a change request to the appropriate operations group and have the server moved to the appropriate Active Directory site.

Domain Controller Diagnostics Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open a Command Prompt window, and then change paths to the C drive.
3. Run the following command:

```
dcdiag /s:<Domain Controller> /f:c:\dcdiag.log
```

Note:
Change **<domain Controller>** to a domain controller contained within the same Active Directory site as the Exchange server.

4. Review the output of **C:\dcdiag.log** file, and verify that there are no connectivity issues with the local domain controller.
5. Repeat steps 3 and 4 for each domain controller in the local Active Directory site.

Note:
Domain Controller Diagnostics (DCDiag) is a Windows support tool that tests network connectivity and DNS resolution for domain controllers. If the account being used does not have administrative privileges, several tests under the **Doing primary tests** heading may not pass. These tests can be ignored if the connectivity tests pass. In addition, the log file may report that some service validation tests did not pass. These messages can be ignored if the services do not exist on the domain controller.

Exchange Best Practices Analyzer Verification

The Microsoft Exchange Analyzers help administrators troubleshoot various operational support issues. Connect to a server in the environment that either has the Exchange 2010 SP1 (or later) Management tools installed through Remote Desktop and log on with an account that has local administrative access.

1. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010** and then select **Exchange Management Console**.
2. Open the **Toolbox** node.
3. Double-click **Best Practices Analyzer**.
4. Check and apply any updates for the Best Practices Analyzer engine.
5. Provide the appropriate information to connect to Active Directory and then click **Connect to the Active Directory server**.
6. In **Start a New Best Practices Scan**, select **Health Check**, and then click

Start Scanning.

7. Review the report, and take action on any errors or warnings that are reported by following the resolution articles that are provided within the Best Practices Analyzer.

Exchange Server Role Installation

The following media are required for this section:

- Microsoft Exchange Server 2010 installation files

The following procedures are in this section:

1. Exchange 2010 Prerequisites Installation for:
   - Windows Server 2008 SP2

     -or-
   - Windows Server 2008 R2
2. Exchange 2010 Installation
3. Exchange 2010 Update Rollup Installation
4. Product Key Configuration
5. System Performance Verification

Important:

The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Exchange 2010 Prerequisites Installation for Windows Server 2008 SP2

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open an elevated command prompt, navigate to the \Setup\ServerRoles \Common folder on the Exchange 2010 installation media, and then use the following commands to configure the Net.Tcp Port Sharing Service for automatic startup and to install the necessary operating system components:

```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-CAS.xml -Restart
```

Exchange 2010 Prerequisites Installation for Windows Server 2008 R2

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. On the Start Menu, navigate to **All Programs** > **Accessories** > **Windows PowerShell**. Open an elevated Windows PowerShell console, and run the following commands:

```
Import-Module ServerManager
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,W
```

3. After the system has restarted, log on as an administrator, open an elevated Windows PowerShell console, and configure the Net.Tcp Port Sharing Service for automatic startup by running the following command:

```
Set-Service NetTcpPortSharing -StartupType Automatic
```

Exchange 2010 Installation

This document uses the command-line method for installing the Exchange 2010 server roles; however, you can also use a GUI called the Setup Wizard. For more information about how to use the Setup Wizard to install an Exchange 2010 server role, see the Perform a Custom Exchange 2010 Installation topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187220).

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access. If the Exchange server

has been provisioned for delegated setup, the account must be delegated the Delegated Setup management role (or higher).
2. Follow the procedure detailed in the Install Exchange 2010 in Unattended Mode topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187229). For example, this command installs the Client Access server role:

```
setup.com /r:C
```

3. If this is the first Exchange 2010 server role being installed into an environment that does not contain any version of Microsoft Exchange, you must also specify the */OrganizationName* setup parameter. Do not restart the server, even if required.
4. To prevent the use of the server role before it is fully configured, open an administrative command prompt and stop the IIS services by running the following command:

```
net stop iisadmin /y
```

Exchange Server 2010 Update Rollup Installation

1. Connect to the server through Remote Desktop, and then log on with an account that has local administrative access.
2. Obtain the latest company approved rollup, and then copy it to the server.
3. Launch the Windows Installer patch (the MSP file) setup via one of two ways:
   3.a. Double-click the MSP file, and then follow the GUI instructions.
   3.b. Perform a silent installation using the following command from an administrative command prompt:

```
msiexec /i <Path and filename of MSP file> /q
```

4. Click **Yes** for any **Digital Signature not Found** dialog boxes that may appear.

Note:
These dialog boxes will appear only in environments that have deployed the Windows Security templates.

Product Key Configuration

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Follow the procedure documented in the Enter Product Key topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187234).

System Performance Verification

By default, Exchange 2010 optimizes the server's processor scheduling management for background services.

1. Connect to the server through Remote Desktop, and then log on with an account that has local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Properties**.
3. Select the **Advanced System Settings**.
4. Under **Performance**, click **Settings**.
   4.a. Click the **Advanced** tab.
   4.b. Verify that **Processor Scheduling** is set to **Background Services**.
5. Click **OK**.

Exchange Server Role Configuration

The following procedures are in this section:

1. Commercial Certificate Configuration
2. RPC Client Access Array Configuration
3. RPC Client Access and Address Book Services Configuration

4. Autodiscover Configuration
5. Outlook Anywhere Configuration
6. Offline Address Book Configuration
7. IMAP4 Configuration
8. POP3 Configuration
9. Outlook Web App Configuration (Internet Scenario) or Outlook Web App Configuration (Proxy Scenario)
10. Legacy ActiveSync Configuration
11. Handoff Test

Important:

The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Commercial Certificate Configuration

A commercial certificate is only needed if the Client Access server will service client requests from the Internet, or if you need to facilitate un-trusted cross-forest communication between Client Access servers.

Note:

For more information about using the certificate tasks, see the Understanding TLS Certificates topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187237).

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.

   Note:

   If generating a certificate that will use Subject Alternative Names, be sure that the certificate's principal name will be the one that the clients will use to connect (for example, mail.contoso.com). Do not list the Autodiscover namespace as the principal name in the certificate.

2. Generate the certificate request by using the following Exchange Management Shell command. The *DomainName* parameter includes the principal URL and the Autodiscover FQDN; be sure to define other FQDNs that clients may utilize. The *FriendlyName* parameter matches the principal URL that is used by Microsoft Office Outlook Web App and Outlook Anywhere.

   ```
   $Data = New-ExchangeCertificate -GenerateRequest -SubjectName [Full Su
   Set-Content -Path "c:\cert.req" -Value $Data.FileData -Encoding Byte
   ```

   An example of [Full Subject Path] is "c=US, o=Company, cn=CAS01.contoso.com".

   Note:

   The Windows RPC/HTTP client-side component in Windows Vista requires that the Subject Name (Common Name) on the certificate match the "Certificate Principal Name" configured for the Outlook Anywhere connection in the Outlook profile. This behavior was changed in Windows Vista Service Pack 1 (SP1). Therefore, as a best practice, make sure that mail.contoso.com is listed as the Subject Name in your certificate unless you plan to change the configuration. You can use the **Set-OutlookProvider** cmdlet to change the configuration. For more information about how to change the configuration, see the Exchange Team Blog article, When, if and how do you modify Outlook Providers? (http://go.microsoft.com/fwlink/?LinkId=160947)

3. Submit the request file to the Certificate Authority (CA) and have the CA generate the certificate.
4. After receiving the certificate, import and enable the certificate by running the following Exchange Management Shell command where [services] can be POP, IMAP, IIS, or a combination:

   ```
   Import-ExchangeCertificate -FileData ([Byte[]]$(Get-Content -Path C:\N
   ```

5. To mandate SSL on the default Web site, do the following:
   5.a. Open **Internet Information Services (IIS) Manager**.

5.b.Expand the **Server Node** object and the **Sites** node.
5.c.Click the **Default Web Site**.
5.d.In the middle pane, double-click **SSL Settings**.
5.e.Verify **Require secure channel (SSL)** is enabled.

Note:
If you require 128-bit encryption, also verify that **Require 128-bit encryption** is enabled.

RPC Client Access Array Configuration

If this is the first Client Access server being installed in the Active Directory site, and the Client Access server infrastructure will participate in a load-balanced array, then you also need to create the RPC Client Access array object. The fully-qualified domain name (FQDN) you specify for the RPC Client Access array should map to the FQDN or virtual IP address that is used for the load-balanced array that was previously created.

Note:
If the RPC Client Access array object already exists for this Active Directory site, you can skip this section.

- Launch the Exchange Management Shell with an account that has been delegated the Server Management role and then run the following command:

```
New-ClientAccessArray -Fqdn <FQDN of CAS load balanced array> -Site <Ac
```

RPC Client Access and Address Book Services Configuration

If the Client Access server is configured to participate in a load-balanced array, follow these steps to configure the RPC Client Access and Address Book services to use a specific TCP port for client connections. The procedure uses TCP59595 and TCP59596, but you can utilize any TCP high ports that are available within the environment between ports 59531 and 60554 (adjust load-balanced array rules accordingly).

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Start Registry Editor.

Important:
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

2.a.Navigate to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeRPC**
2.b.Right-click **MSExchangeRPC**, point to **New**, and then click **Key**.
2.c.Type **ParametersSystem** to name the new key.
2.d.Right-click **ParametersSystem**, point to **New**, and then click **DWORD (32-bit) Value**.
2.e.Type **TCP/IP Port** to name the new value.
2.f.Double-click **TCP/IP Port**.
2.g.In the **Value data** box, type **59595**, and then click **OK**.

Configure a static port for the Microsoft Exchange Address Book service by performing the steps below for your version of Exchange 2010.

In the Release to Manufacturing (RTM) version of Exchange 2010:

1. Navigate to *<Exchange Install Path>*\bin.
2. Open the MicrosoftExchange.AddressBook.Service.exe.config file in Notepad and add the following entry to the <appSettings> section of the file:

```
<add key="RpcTcpPort" value="59596" />
```

3. Close and save the file.

In Exchange 2010 Service Pack 1 (SP1):

1. Start Registry Editor.

Important:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

   1.a. Navigate to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeAB**
   1.b. Right-click **MSExchangeAB**, point to **New**, and then click **Key**.
   1.c. Type **Parameters** to name the new key.
   1.d. Right-click **Parameters**, point to **New**, and then click **String Value**.
   1.e. Type **RpcTcpPort** to name the new value.
   1.f. Double-click **RpcTcpPort**.
   1.g. In the **Value data** box, type **59596**, and then click **OK**.
2. Close Registry Editor and then restart the Microsoft Exchange Address Book service.

Autodiscover Configuration

Exchange 2010 includes a service named the Autodiscover service. The Autodiscover service makes it easier to configure Outlook 2007 or Outlook 2010 and some mobile phones. For more information, see the Understanding the Autodiscover Service topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=194169).

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Configure the internal Autodiscover URL by running the following command within the Exchange Management Shell. In the following example, CAS01 is the name of the Client Access server and internal.domain.fqdn is the internal namespace used for Autodiscover:

```
Set-ClientAccessServer -Identity CAS01 -AutoDiscoverServiceInternalUri
```

3. Optional: Follow the procedure outlined in the Configure the Exchange Services for the Autodiscover Service topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187243) to configure the Autodiscover service for use by Internet clients. This will enable Outlook Anywhere and set the offline address book (OAB), Web Services, and Unified Messaging virtual directories external URL parameter.
4. Optional: Follow the procedure outlined in the Configure Exchange ActiveSync Autodiscover Settings topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187244) for usage by mobile clients.
5. Optional: Enable site affinity by following the procedure outlined in the Configure the Autodiscover Service to Use Site Affinity topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187245).
6. Verify that Autodiscover functions correctly by following the procedure outlined in the Test Outlook Autodiscover Connectivity topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187247).

Outlook Anywhere Configuration

If you completed step 3 from the previous "Autodiscover Configuration" section, you can skip this section. Otherwise, complete this procedure.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. To enable Outlook Anywhere, follow the procedure outlined in the Enable Outlook Anywhere topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187249).
3. If the server will be servicing Outlook Anywhere clients on the Internet, follow the procedure outlined in the Configure an External Host Name for Outlook Anywhere topic in the Exchange Server 2010 Library (http://go.microsoft.com/

fwlink/?LinkId=187253).

Offline Address Book Configuration

If the Client Access server will not be a distribution point for the OAB, you can skip this section.

By default, the OAB virtual directory does not require SSL. By default, Client Access servers use self-signed certificates for providing HTTP and RPC encryption. Clients that use the BITS service to download files (such as OAB) cannot use self-signed certificates. If a commercial certificate is going to be used and ISA 2006 is not going to be used to enforce SSL, you should enable SSL on the OAB virtual directory.

Note:

To use OAB Web distribution, the OAB must be generated on an Exchange 2010 Mailbox server. If the OAB is not generated on an Exchange 2010 Mailbox server, you can skip step 1.

1. Launch the Exchange Management Shell with an account that has been delegated the Organization Management role and then run the following commands. In the following example, CAS01 is the name of the Client Access server and mail.contoso.com is the name of the external URL.

```
$a=get-oabvirtualdirectory -Server CAS01
Set-oabvirtualdirectory $a -ExternalURL https://mail.contoso.com/OAB
Set-OfflineAddressBook "default offline address book" -VirtualDirector
iisreset /noforce
```

2. If the server has a commercial certificate and will be servicing requests from the Internet and either Microsoft Internet Security and Acceleration (ISA) Server 2006, Microsoft Forefront Unified Access Gateway (UAG) or Microsoft Forefront Threat Management Gateway (TMG) 2010 will not be in use to enforce SSL for Internet requests, follow the procedure outlined in the Require SSL for Offline Address Book Distribution topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187254).

IMAP4 Configuration

If the Client Access server will not allow IMAP4 connections, you can skip this section.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
   1.a. To configure the IMAP4 bindings, run the following command. In the following example, CAS01 is the Client Access server and 0.0.0.0 implies any IP address.

```
Set-ImapSettings -server CAS01 -UnencryptedOrTLSBindings "(
```

   1.b. To disable plain text authentication and enable custom calendar item retrieval option for IMAP4, run the following command. In the following example, mail.contoso.com is the certificate name and external URL.

```
Set-ImapSettings -server CAS01 -X509CertificateName "mail.c
```

   1.c. To enable the Exchange IMAP4 service for automatic startup, run the following command:

```
Set-Service MSExchangeIMAP4 -ComputerName CAS01 -StartupTyp
```

POP3 Configuration

If the Client Access server will not allow POP3 connections, you can skip this section.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
   1.a. To configure the POP3 bindings, run the following command. In the

following example, CAS01 is the Client Access server and 0.0.0.0 implies any IP address.

```
Set-PopSettings -server CAS01 -UnencryptedOrTLSBindings "0.
```

1.b.To disable plain text authentication and enable custom calendar item retrieval option for POP3, run the following command. In the following example, mail.contoso.com is the certificate name and external URL.

```
Set-PopSettings -server CAS01 -X509CertificateName "mail.co
```

1.c.To enable the Exchange POP3 service for automatic startup, run the following command:

```
Set-Service MSExchangePOP3 -ComputerName CAS01 -StartupType
```

Outlook Web App Configuration (Internet Scenario)

Follow the steps in this section only if the Client Access server will service directly from the Internet and either ISA 2006 or UAG or TMG pre-authentication mechanisms are not in use. If either is not true, then skip this section and follow the steps outlined in the Outlook Web App Configuration (Proxy Scenario) section below.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. By default, when the Client Access server role is installed, forms-based authentication is enabled. Ensure that forms-based authentication is enabled by following the procedure outlined in the Configure Forms-based Authentication for Outlook Web App topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187486).
3. Configure the public and private cookie timeouts by following the procedures outlined in the Set the Forms-Based Authentication Public Computer Cookie Time-Out Value topic (http://go.microsoft.com/fwlink/?LinkId=187334) and the Set the Forms-Based Authentication Private Computer Cookie Time-Out Value topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187336).
4. Optional: Configure GZip compression by following the procedure outlined in the Configure Gzip Compression Settings topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187343).
5. Configure WebReady Document Viewing by following the procedure outlined in the Configure WebReady Document Viewing topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187344).
6. Configure private and public computer file access by following the procedure outlined in Configure Public and Private Computer File Access topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187346).
7. Optional: If redirection is to be used, run the following command from the Exchange Management Shell. In the following example, CAS01 is the name of the Client Access server and mail.contoso.com is the name of the external URL.

```
Set-OwaVirtualDirectory -identity "CAS01\owa (Default Web Site)" -Exte
Set-OwaVirtualDirectory -identity "CAS01\ecp (Default Web Site)" -Exte
```

8. Optional: To simplify the Outlook Web App URL and redirect users to HTTPS, follow the procedure outlined in the Simplify the Outlook Web App URL topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187347).
9. Restart the Client Access server.

Outlook Web App Configuration (Proxy Scenario)

Follow the steps in this section only if the Client Access server will not service requests

directly from the Internet, but it will receive requests from other Client Access servers that are located in other Active Directory sites, or the Client Access server will be using ISA or UAG or TMG to pre-authenticate Internet requests.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Configure Windows Integrated Authentication by following the procedure outlined in the Configure Forms-based Authentication for Outlook Web App topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187486).
3. Optional: Configure GZip compression by following the procedure outlined in the Configure Gzip Compression Settings topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187343).
4. Configure WebReady Document Viewing by following the procedure outlined in the Configure WebReady Document Viewing topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187344).
5. Configure private and public computer file access by following the procedure outlined in Configure Public and Private Computer File Access topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187346).
6. Optional: To simplify the Outlook Web App URL and redirect users to HTTPS, follow the procedure outlined in the Simplify the Outlook Web App URL topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187347).
7. Restart the Client Access server.

Legacy ActiveSync Configuration

In order for mobile devices to synchronize using Client Access servers when the mailbox resides on Exchange Server 2003, the Microsoft-Server-ActiveSync virtual directory must be configured to use Windows Integrated Authentication.

If there are no legacy Exchange Mailbox servers or no legacy mailboxes that are accessed via Exchange ActiveSync, you can skip this section.

Note:

You can manually configure the Microsoft-Server-ActiveSync virtual directory to use Windows Integrated Authentication by installing the hotfix described in Microsoft Knowledge Base article 937031 on a workstation running the Exchange 2003 System Manager (http://go.microsoft.com/fwlink/?linkid=3052&kbid=937031).

1. Connect to the server via Remote Desktop and log on with an account that has been delegated both local administrative access and the Exchange Full Administrator role within the Exchange 2003 environment.
2. Create the legacyEAS.vbs script by copying the code from the Server Build DVD Visual Basic Script Examples topic in the Exchange Server 2007 Library (http://go.microsoft.com/fwlink/?LinkId=167205).
3. Open a command prompt and navigate to the directory containing the script file and run the following command:

```
legacyEAS.vbs -d:DomainController -a:AdminGroup
```

Note:

Replace `Domain Controller` with a domain controller that is in the same Active Directory site as the Exchange server (optional parameter).

The output will be similar to the following if successful:

```
Z:\E2010-Scripts\CAS>legacyeas.vbs -d:W2K3-DC-01 -a:NorthAmerica
Microsoft (R) Windows Script Host Version 5.1 for Windows
Copyright (C) Microsoft Corporation 1996-1999. All rights reserved.
Exchange Server Container - cn=Microsoft-Server-Activesync,cn=1,cn=HTTP,cn=Protoc
Attribute Name & Value - msExchAuthenticationFlags: 6
Attribute Set!!
```

Handoff Test

Before you can complete the diagnostic tasks in this section, you must have already created test mailboxes in your environment by using the New-TestCasConnectivityUser.ps1 script.

Create Test Mailboxes

1. Connect to the Exchange 2010 Mailbox server through Remote Desktop and log on with an account that has local administrative access and was delegated the Server Management role.
2. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010**, and then select **Exchange Management Shell**.
3. Change the directory path to **<***Exchange Server Install Path***>\Scripts**.
4. Type **New-TestCasConnectivityUser.ps1** and press **Enter**.
5. Enter a temporary password and follow the prompts to create the test mailboxes.

Perform Handoff Test

1. If the server has not been restarted as a result of a previous section's instructions, restart the server.
2. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
3. To test Exchange ActiveSync connectivity, run the following command where *<Server>* is the name of the Client Access server:

```
Test-ActiveSyncConnectivity -ClientAccessServer <Server>
```

4. To test Autodiscover connectivity, run the following command where *<EmailAddress>* is the e-mail address of a mailbox:

```
Add-TargetAddress <EmailAddress>
```

5. To test Exchange Web Services functionality, run the following command:

```
Test-WebServicesConnectivity -ClientAccessServer <Server> -AllowUnsecu
```

6. To test Outlook Web App connectivity, run the following command where *<Server>* is the name of the Client Access server:

```
Test-OwaConnectivity -ClientAccessServer:<Server> -AllowUnsecureAccess
```

If this server will be responding to Internet client requests, consider using the Exchange Remote Connectivity Analyzer (https://www.testexchangeconnectivity.com/) to verify your configuration, as well.

1.2.2.11.2 Installation Guide Template - Hub Transport Server

Installation Guide Template - Hub Transport Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-21*

This topic provides you with an installation guide template that you can use as a starting point for formally documenting your organization's server build procedures for Microsoft Exchange Server 2010 servers that will have the Hub Transport server role installed.

The template includes the following key sections:

- Executive Summary
- Server Configuration
- Verification Steps

- Exchange Server Role Installation
- Exchange Server Role Configuration

For purposes of providing an example, the template uses the fictitious company name of Contoso. Also, you can download this template, along with templates for other server roles, as a download package in .zip file format at Microsoft Exchange Server 2010 Install Guide Templates (http://go.microsoft.com/fwlink/?LinkID=187961).

Executive Summary

The purpose of this document is to explain the installation and configurations necessary to install the Exchange 2010 Hub Transport server role on the Windows Server 2008 platform.

Business Justification

By having an installation guide, Contoso will be able to ensure standardization across the enterprise, reducing total cost of ownership (TCO), and easing troubleshooting steps.

Scope

The scope of this document is limited to installation of an Exchange 2010 Hub Transport server for Contoso on the x64 version of the Windows Server 2008 (SP2 or R2) operating system.

Prerequisites

The administrator should have working knowledge of Windows Server 2008 concepts, Exchange 2010 concepts, the Exchange Management Console and Exchange Management Shell, the command line, and various system utilities. This document does not elaborate on the details of any system utility except as necessary to complete the tasks within.

In addition, before implementing the server role, the administrator should review the Understanding Transport topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187524).

Assumptions

This document assumes that Windows Server 2008 x64 Edition is installed on the intended Client Access server per company baseline regulations which include the latest approved service pack and hotfixes. In addition, the following system prerequisites have been installed:

- Microsoft .NET Framework 3.5 SP1 and the update for .NET Framework 3.5 SP1 For more information, see Microsoft Knowledge Base article 959209, An update for the .NET Framework 3.5 Service Pack 1 is available (http://go.microsoft.com/fwlink/?linkid=3052&kbid=959209).
- Windows Management Framework (Windows Remote Management 2.0 and Windows PowerShell 2.0).

This document assumes that forest and domain preparation steps have been performed as described in the Prepare Active Directory and Domains topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187262).

This document assumes that the account you will be using for the Exchange tasks has been delegated the Server Management management role, as described in the Server Management topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187265).

This document also assumes that both Exchange 2010 Windows Server 2008 and Windows Server 2008 will be secured following the best practices found in the Windows Server 2008 Security Guide (http://go.microsoft.com/fwlink/?LinkId=122593).

Important:
The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Server Configuration

The following media are required for this section.

- Windows Server 2008 installation files

The following procedures are in this section:

1. Additional Software Verification
2. Network Interfaces Configuration
3. Drive Configuration
4. Windows Server 2008 Hotfix Installation
5. Domain Membership Configuration
6. Local Administrators Verification
7. Local Administrator Account Password Reset
8. Debugging Tools Installation
9. Page File Modifications
10. Drive Permissions

Additional Software Verification

1. Verify that Remote Desktop is enabled.
2. As an optional process, install Microsoft Network Monitor (http://go.microsoft.com/fwlink/?LinkId=86611).

Network Interfaces Configuration

1. Log on to the server with an account that has been delegated at least local administrative access.
2. Click **Start > Control Panel**, and then double-click **Network and Sharing Center**.
3. Click **Manage Network Connections**.
4. Locate the connection for the internal network and rename it according to your organization's naming standards.
5. Right-click the connection and then select **Properties**.
6. For Internet Protocol Version 4 (TCP/IPv4), add the following:
   6.a. **Static IP Address**, **Subnet Mask**, and **Gateway**
   6.b. DNS Server IP Addresses
   6.c. Select the check box to **Append parent suffixes of the primary DNS suffix**.
   6.d. WINS IP Addresses (if using WINS)
7. If you are using Internet Protocol Version 6 (TCP/IPv6), configure the IPv6 settings according to your organization's network standards.

Drive Configuration

1. Connect to the server through Remote Desktop and then log on with an account that has been delegated local administrative access.
2. Click **Start > Administrative Tools**, and then select **Computer Management**.
3. Expand **Storage** and then click **Disk Management**.
4. Open the Disk Management Microsoft Management Console (MMC) and then format, rename, and assign the appropriate **Drive Letters** so that the volumes and DVD drive match the appropriate server configuration.

Drive configuration

LUN	Drive letter	Usage
1	C	Operating system and Exchange binaries

2	D	Mail.que database
3	E	Exchange transaction logs, tracking logs
4	Z	DVD drive

Windows Server 2008 Hotfix Installation

1. Connect to the server via Remote Desktop and log on with an account that has local administrative access.
2. Obtain the latest hotfixes approved by your company for your version of Windows Server 2008 x64 (SP2 or R2) and copy them to the server.
3. Launch the hotfix setup via one of two ways:
   3.a. Double-click the file and follow the GUI instructions.
   3.b. Perform a silent installation using the following command from an administrative command prompt:

```
<hotfix>.msu /quiet /norestart
```

4. Click **Yes** for any **Digital Signature not Found** dialog boxes that may appear.

> **Note:**
> These dialog boxes will not appear in environments that have not deployed the Windows Security templates.

5. Wait for all file copies to complete, and then restart the server. You can use the **Processes** tab in Windows Task Manager to monitor the hotfix installation progress. When the wusa.exe process has exited, the hotfix installation is complete.

Domain Membership Configuration

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start,** right-click **My Computer**, and then select **Properties**.
3. Under the **Computer Name, domain, and workgroup** settings, click **Change Settings**.
4. Click **Change**.
5. Choose the **Domain** option button, and then enter the appropriate domain name.
6. Enter the appropriate credentials.
7. Click **OK** and **OK**.
8. Click **OK** to close **System Properties**.
9. Restart the server.

Local Administrators Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Verify (or add if not already there) that the Domain Admins account and the user account that will perform the Exchange installation are members of the local Administrators group on this server.
3. Verify that your user account is a member of a group which is a member of the local Administrators group on the Windows Server 2008 server. If it is not, use an account that is a member of the local Administrators group before continuing.

Local Administrator Account Password Reset

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Manage**.
3. Expand the nodes to find **Configuration\Local Users and Groups\Users**.

4. Right-click **Administrator**, and then select **Set Password**. Change the password so that it meets strong complexity requirements.

Debugging Tools Installation

This section describes several useful tools that aid administrators in Exchange administration and in troubleshooting support issues.

Debugging Tools for Windows allow administrators to debug processes that are affecting service and determine root cause.

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Download and install the latest 64-bit Debugging Tools from Install Debugging Tools for Windows 64-bit Version (http://go.microsoft.com/fwlink/?LinkID=123594).

Page File Modifications

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Properties**.
3. Select the **Advanced System Settings**.
4. Under **Startup and Recovery**, click **Settings**.
   4.a. Under **Write Debugging Information**, select **Kernel Memory Dump** from the memory dump drop-down list.
   4.b. Click **OK**.
5. Under **Performance**, click **Settings**.
6. Click the **Advanced** tab.
7. Under **Virtual Memory**, click **Change**.
8. On servers that have a dedicated page file drive, follow these steps:
   8.a. In the **Drive** list, click **C:**, and then click **Custom size**.
   8.b. For the C: drive, set the **Initial Size (MB)** value to a minimum of 200 MB. (Windows requires between 150 MB and 2 GB page file space, depending on server load and the amount of physical RAM that is available for page file space on the boot volume when Windows is configured for a kernel memory dump. Therefore, you may be required to increase the size.)
   8.c. For the C: drive, set the **Maximum Size (MB)** value to that of the **Initial Size**.
   8.d. In the **Drive** list, select the page file drive (for example, the P: drive), and then click **Custom size**.
   8.e. In the **Initial Size (MB)** box, type the result of one of the following calculations:
      If the server has less than 8 GB of RAM, multiply the amount of RAM times 1.5.
      If the server has 8 GB of RAM or more, add the amount of RAM plus 10 MB.
   8.f. In the **Maximum Size (MB)** box, type the same amount that you typed in the **Initial Size** box.
   8.g. Delete all other page files.
   8.h. Click **OK**.
9. On servers that do not have a dedicated page file drive, follow these steps:
   9.a. In the **Drive** list, click **C:**, and then click **Custom size**.
   9.b. For the C: drive, in the **Initial Size (MB)** box, type the result of one of the following calculations:
      If the server has less than 8 GB of RAM, multiply the amount of RAM times 1.5.
      If the server has 8 GB of RAM or more, add the amount of RAM plus 10 MB.
   9.c. Delete all other page files.
   9.d. Click **OK**.
10. Click **OK** two times to close the **System Properties** dialog box.
11. Click **No** if prompted to restart the system.

Note:
For more information about page file recommendations, see the following Microsoft Knowledge Base articles: How to determine the appropriate page file size for 64-bit versions of Windows Server 2003 or Windows XP (http://go.microsoft.com/fwlink/?linkid=3052&kbid=889654); and Overview of memory dump file options for Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 2000 (http://go.microsoft.com/fwlink/?linkid=3052&kbid=254649).

Drive Permissions

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, and then select **Computer**.
3. Right-click **D Drive**, and then select **Properties**.
4. Click the **Security** tab.
5. Click **Edit**.
6. Click **Add**, and then select the local server from **Locations**.
7. Grant the following permissions as outlined in the following table.

Drive permissions

Account	Permissions
Administrators	Full Control
SYSTEM	Full Control
Authenticated Users	Read and Execute, List, Read
CREATOR OWNER	Full Control

8. Click the **Advanced** button.
9. Select the **CREATOR OWNER** permission entry, and then click **View/Edit**.
10. Select **Subfolders and Files Only** from the drop-down list.
11. Click **OK** two times.
12. Click **OK** to close the drive properties.
13. Repeat steps 3-12 for each additional drive (other than the C drive).

Verification Steps

The following procedures are in this section:

1. Organizational Unit Verification
2. Active Directory Site Verification
3. Domain Controller Diagnostics Verification
4. Exchange Best Practices Analyzer Verification

Important:
The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Organizational Unit Verification

Submit a change request to the appropriate operations group and have the computer object moved to the appropriate organizational unit (OU).

Active Directory Site Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open a Command Prompt window.
3. Verify that the server is in the correct domain and Active Directory site. At the command line, type the following:

```
NLTEST /server:%COMPUTERNAME% /dsgetsite
```

4. The name of the Active Directory site to which the server belongs will be displayed. If the server is not in the correct Active Directory site, submit a

change request to the appropriate operations group and have the server moved to the appropriate Active Directory site.

Domain Controller Diagnostics Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open a Command Prompt window, and then change paths to the C drive.
3. Run the following command:

```
dcdiag /s:<Domain Controller> /f:c:\dcdiag.log
```

Note:

Change **<domain Controller>** to a domain controller contained within the same Active Directory site as the Exchange server.

4. Review the output of **C:\dcdiag.log** file, and verify that there are no connectivity issues with the local domain controller.
5. Repeat steps 3 and 4 for each domain controller in the local Active Directory site.

Note:

Domain Controller Diagnostics (DCDiag) is a Windows support tool that tests network connectivity and DNS resolution for domain controllers. If the account being used does not have administrative privileges, several tests under the **Doing primary tests** heading may not pass. These tests can be ignored if the connectivity tests pass. In addition, the log file may report that some service validation tests did not pass. These messages can be ignored if the services do not exist on the domain controller.

Exchange Best Practices Analyzer Verification

The Microsoft Exchange Analyzers help administrators troubleshoot various operational support issues. Connect to a server in the environment that either has the Exchange 2010 SP1 (or later) Management tools installed through Remote Desktop and log on with an account that has local administrative access.

1. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010**, and then select **Exchange Management Console**.
2. Open the **Toolbox** node.
3. Double-click **Best Practices Analyzer**.
4. Check and apply any updates for the Best Practices Analyzer engine.
5. Provide the appropriate information to connect to Active Directory and then click **Connect to the Active Directory server**.
6. In the **Start a New Best Practices Scan**, select **Health Check**, and then click **Start Scanning**.
7. Review the report, and take action on any errors or warnings that are reported by following the resolution articles that are provided within the Best Practices Analyzer.

Exchange Server Role Installation

The following media are required for this section.

- Microsoft Exchange Server 2010 installation files

The following procedures are in this section:

1. Exchange 2010 Prerequisites Installation for:
   - Windows Server 2008 SP2

     -or-
   - Windows Server 2008 R2
2. Exchange 2010 Installation
3. Exchange 2010 Update Rollup Installation
4. Product Key Configuration
5. Exchange Search Configuration

6. System Performance Verification

Important:
The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Exchange 2010 Prerequisites Installation for Windows Server 2008 SP2

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open an administrative command prompt window.
3. Install the Microsoft Filter Pack. For details, see 2007 Office System Converter: Microsoft Filter Pack (http://go.microsoft.com/fwlink/?linkid=137042).
4. Open an elevated command prompt, navigate to the Setup\ServerRoles\Common folder on the Exchange 2010 installation media and then use the following command to install the necessary operating system components:

```
ServerManagerCmd -ip Exchange-Hub.xml -Restart
```

Exchange 2010 Prerequisites Installation for Windows Server 2008 R2

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Install the Microsoft Filter Pack. For details, see 2007 Office System Converter: Microsoft Filter Pack (http://go.microsoft.com/fwlink/?linkid=137042).
3. On the Start Menu, navigate to **All Programs** > **Accessories > Windows PowerShell**. Open an elevated Windows PowerShell console, and run the following command:

```
Import-Module ServerManager
```

4. Use the **Add-WindowsFeature** cmdlet to install the necessary operating system components:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,W
```

Exchange 2010 Installation

This document uses the command-line method for installing the Exchange 2010 server roles; however, you can also use a GUI called the Setup Wizard. For more information about how to use the Setup Wizard to install an Exchange 2010 server role, see the Perform a Custom Exchange 2010 Installation topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187220).

1. Connect to the server via Remote Desktop, and then log on with an account that has local administrative access and has been delegated the Delegated Setup management role (or higher) if the server has been pre-created.
2. Follow the procedure detailed in the Install Exchange 2010 in Unattended Mode topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187229). For example, this command installs the Hub Transport server role and prevents the service from starting:

```
setup.com /r:HT /DoNotStartTransport
```

Do not restart the server, even if required.

Exchange 2010 Update Rollup Installation

1. Connect to the server through Remote Desktop, and then log on with an account that has local administrative access.
2. Obtain the latest company approved rollup, and then copy it to the server.
3. Launch the Windows Installer patch (the MSP file) setup via one of two ways:
   3.a. Double-click the MSP file, and then follow the GUI instructions.
   3.b. Perform a silent installation using the following command from an

administrative command prompt:

```
msiexec /i <Path and filename of MSP file> /q
```

4. Click **Yes** for any **Digital Signature not Found** dialog boxes that may appear.

Note:
These dialog boxes will appear only in environments that have deployed the Windows Security templates.

Product Key Configuration

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Follow the procedure documented in the Enter Product Key topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187234).

Exchange Search Configuration

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Follow the procedure documented in the Register Filter Pack IFilters with Exchange 2010 topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187516).
3. Optional: If you want the ability to search PDF files, install the Adobe PDF iFilter (http://www.adobe.com/support/downloads/detail.jsp?ftpID=4025) and follow the Configuring PDF iFilter for MS Exchange Server 2007 (http://www.adobe.com/special/acrobat/configuring_pdf_ifilter_for_ms_exchange_server_2007.pdf) documentation.

Note:
The third-party Web site information in this topic is provided to help you find the technical information you need. The URLs are subject to change without notice.

System Performance Verification

By default, Exchange 2010 optimizes the server's processor scheduling management for background services.

1. Connect to the server through Remote Desktop, and then log on with an account that has local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Properties**.
3. Select the **Advanced System Settings**.
4. Under **Performance**, click **Settings**.
   4.a. Click the **Advanced** tab.
   4.b. Verify that **Processor Scheduling** is set to **Background Services**.
5. Click **OK**.

Exchange Server Role Configuration

The following procedures are in this section:

1. Default Receive Connector Configuration
2. Transport Server Configuration
3. Transaction Log Location
4. Transport Logs Location
5. Temporary Storage Path
6. Handoff Test

Default Receive Connector Configuration

By default, the default Receive connector will accept various authentication mechanisms and allow users as well as Exchange servers to connect. The following steps modify this behavior by restricting the type of authentication that can occur and ensuring only Exchange servers can connect and transmit messages to this Receive connector. Also, in

addition to the default Receive connector, each Hub Transport server has a client Receive connector that listens on TCP 587.

For more information, see the Understanding Receive Connectors topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=183419).

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Modify the default Receive connector's permissions and authentication mechanisms using the following command:

```
Set-ReceiveConnector "<ServerName>\Default <ServerName>" -PermissionGr
```

Transport Server Configuration

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Modify various settings on the default Receive connector by running the following command:

```
Set-TransportServer <ServerName> -MessageTrackingLogMaxAge <MaxAge> -M
```

You can use the following table for information you need for the command.

Important:
The values in the following table are example values only, not recommended values. Revise these values to reflect the actual values required for your organization.

Parameter values for Hub Transport server configuration

Parameter	Default value	Contoso value
ActiveUserStatisticsLogMaxAge	30.00:00:00	30.00:00:00
ActiveUserStatisticsLogMaxDirectorySize	250 MB	250 MB
ActiveUserStatisticsLogMaxFileSize	10 MB	10 MB
ExternalDsnReportingAuthority	[None]	SMTP namespace
ExternalPostmasterAddress	[None]	postmaster@smtpnamespace
MaxPerDomainOutboundConnections	20	50
MessageTrackingLogEnabled	True	True
MessageTrackingLogMaxAge	30.00:00:00	10.00:00:00
MessageTrackingLogMaxDirectorySize	1000 MB	150 GB
MessageTrackingLogMaxFileSize	10 MB	10 MB
MessageTrackingLogSubject LoggingEnabled	True	True
ReceiveProtocolLogMaxAge	30.00:00:00	10.00:00:00
ReceiveProtocolLogMaxDirectorySize	250 MB	15 GB
ReceiveProtocolLogMaxFil	10 MB	10 MB

eSize		
SendProtocolLogMaxAge	30.00:00:00	10.00:00:00
SendProtocolLogMaxDirectorySize	250 MB	15 GB
SendProtocolLogMaxFileSize	10 MB	10 MB
ServerStatisticsLogMaxAge	30.00:00:00	30.00:00:00
ServerStatisticsLogMaxFileSize	250 MB	250 MB
ServerStatisticsLogPath	10 MB	10 MB

Transaction Log Location

1. Connect to an Exchange 2010 server via Remote Desktop, and then log on with an account that has local administrative access and that has been delegated the Server Management role (or higher).
2. Verify that the MSExchangeTransport service is stopped. If it is not stopped, stop the service.
3. Create the folder E:\Exchange\QueueLogs.
4. Move the TRNxxxx.LOG and *.JRS files from <*Exchange Install Path*>\TransportRoles\Data\Queue to E:\Exchange\QueueLogs.
5. Navigate to <*Exchange Install Path*>\bin.
6. Open the EdgeTransport.exe.config file in Notepad and edit the following entry:

```
<add key="QueueDatabaseLoggingPath" value="E:\Exchange\QueueLogs" />
```

7. Save the file.

Transport Logs Location

1. Connect to an Exchange 2010 server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Verify that the MSExchangeTransport service is stopped. If it is not stopped, stop the service.
3. Create the E:\Exchange\Logs folder.
4. Move the folders that reside in <*Exchange Install Path*>\TransportRoles\Logs to the E:\Exchange\Logs folder.
5. Launch the Exchange Management Shell with an account that has been delegated the Server Management role and then run the following command:

```
Set-TransportServer <ServerName> -ConnectivityLogPath "E:\Exchange\Log
```

6. Open a command prompt and start the Transport service by running the following command:

```
net start MSExchangeTransport
```

Temporary Storage Path

1. Connect to an Exchange 2010 server via Remote Desktop, and then log on by using an account that has been delegated local administrative access and that has been delegated the Server Management role (or higher).
2. Verify that the MSExchangeTransport service is stopped. If it is not stopped, stop the service.
3. Move to the <*Exchange Install Path*>\bin directory.
4. Open the EdgeTransport.exe.config file in Notepad, and then change the TemporaryStoragePath entry to point to the mail.que drive. By default, this path is "C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\data\Temp."

```
<add key="TemporaryStoragePath" value="<path of mail queue>" />
```

5. Save the file.
6. Restart the server.

Handoff Test

Before you can complete the diagnostic tasks in this section, you must have already created test mailboxes in your environment by using the New-TestCasConnectivityUser.ps1 script.

Create Test Mailboxes

1. Connect to the Exchange 2010 Mailbox server through Remote Desktop and log on with an account that has local administrative access and was delegated the Server Management role.
2. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010**, and then select **Exchange Management Shell**.
3. Change the directory path to *<Exchange Server Install Path>*\Scripts.
4. Type **New-TestCasConnectivityUser.ps1** and press **Enter**.
5. Enter a temporary password and follow the prompts to create the test mailboxes.

Perform Handoff Test

1. If the server had not been restarted as a result of a previous section's instructions, then restart the server.
2. Using a test mailbox, send sample messages to various mailboxes and verify that mail is successfully delivered.
3. Send sample messages from Internet mailboxes to various internal test mailboxes, and verify that the mail is successfully delivered.
4. Review the event logs and tracking logs and ensure that the Hub Transport server is operating correctly.

Consider using the Exchange Remote Connectivity Analyzer (https://www.testexchangeconnectivity.com/) to verify your configuration, as well.

1.2.2.11.3 Installation Guide Template - Mailbox Server

Installation Guide Template - Mailbox Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-21*

This topic provides you with an installation guide template that you can use as a starting point for formally documenting your organization's server build procedures for Microsoft Exchange Server 2010 servers that will have the Mailbox server role installed.

The template includes the following key sections:

- Executive Summary
- Server Configuration
- Verification Steps
- Exchange Server Role Installation
- Exchange Server Role Configuration
- Appendix: Server Configuration

For purposes of providing an example, the template uses the fictitious company name of

Contoso. Also, you can download this template, along with templates for other server roles, as a download package in .zip file format at Microsoft Exchange Server 2010 Install Guide Templates (http://go.microsoft.com/fwlink/?LinkID=187961).

Executive Summary

The purpose of this document is to explain the installation and configurations necessary to install the Exchange 2010 Mailbox server role on the Windows Server 2008 platform.

Business Justification

By having an installation guide, Contoso will be able to ensure standardization across the enterprise, reducing total cost of ownership (TCO), and easing troubleshooting steps.

Scope

The scope of this document is limited to installation of an Exchange 2010 Mailbox server for Contoso on the x64 version of the Windows Server 2008 (SP2 or R2) operating system.

Prerequisites

The administrator should have working knowledge of Windows Server 2008 concepts, Exchange 2010 concepts, the Exchange Management Console and Exchange Management Shell, the command line, and various system utilities. This document does not elaborate on the details of any system utility except as necessary to complete the tasks within.

In addition, before implementing the server role, the administrator should review the Overview of the Mailbox Server Role topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187526).

Assumptions

This document assumes that Windows Server 2008 x64 Edition is installed on the intended Client Access server per company baseline regulations which include the latest approved service pack and hotfixes. In addition, the following system prerequisites have been installed:

- Microsoft .NET Framework 3.5 SP1 and the update for .NET Framework 3.5 SP1 For more information, see Microsoft Knowledge Base article 959209, An update for the .NET Framework 3.5 Service Pack 1 is available (http://go.microsoft.com/fwlink/?linkid=3052&kbid=959209).
- Windows Management Framework (Windows Remote Management 2.0 and Windows PowerShell 2.0).

This document assumes that forest and domain preparation steps have been performed as described in the Prepare Active Directory and Domains topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187262).

This document assumes that the account you will be using for the Exchange tasks has been delegated the Server Management management role, as described in the Server Management topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187265).

This document also assumes that both Exchange 2010 Windows Server 2008 and Windows Server 2008 will be secured following the best practices found in the Windows Server 2008 Security Guide (http://go.microsoft.com/fwlink/?LinkId=122593).

Important:

The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Server Configuration

The following media are required for this section.

- Windows Server 2008 installation files

The following procedures are in this section:

1. Additional Software Verification
2. Network Interfaces Configuration
3. Drive Configuration
4. Windows Server 2008 Hotfix Installation
5. Domain Membership Configuration
6. Local Administrators Verification
7. Local Administrator Account Password Reset
8. Debugging Tools Installation
9. Page File Modifications
10. Drive Permissions

Additional Software Verification

1. Verify that Remote Desktop is enabled.
2. As an optional process, install Microsoft Network Monitor (http://go.microsoft.com/fwlink/?LinkId=86611).

Network Interfaces Configuration

1. Log on to the server with an account that has been delegated at least local administrative access.
2. Click **Start > Control Panel**, and then double-click **Network and Sharing Center**.
3. Click **Manage Network Connections**.
4. Locate the connection for the internal network and rename it according to your organization's naming standards.
5. Right-click the connection and then select **Properties**.
6. For Internet Protocol Version 4 (TCP/IPv4), add the following:
   6.a. **Static IP Address**, **Subnet Mask**, and **Gateway**
   6.b. DNS Server IP Addresses
   6.c. Select the check box to **Append parent suffixes of the primary DNS suffix**.
   6.d. WINS IP Addresses (if using WINS)
7. If you are using Internet Protocol Version 6 (TCP/IPv6), configure the IPv6 settings according to your organization's network standards.

Drive Configuration

1. Connect to the server through Remote Desktop and log on with an account that has local administrative access.
2. Click **Start, Administrative Tools**, and select **Computer Management**.
3. Expand Storage and click on **Disk Management**.
4. Using the Disk Management snap-in of the Microsoft Management Console (MMC), format, rename, and assign the appropriate **Drive Letters** so that the volumes and DVD drive match the appropriate server configuration. Refer to the Database Log LUN appendix at the end of this document for the actual drive configuration that should be used.

Drive configuration

LUN	Drive letter	Usage
1	C	Operating system, Exchange binaries, and tracking logs
2	E	Exchange databases

4	L	Exchange transaction logs
5-x	--	Additional drives for databases and logs
6	Z	DVD drive

Windows Server 2008 Hotfix Installation

1. Connect to the server via Remote Desktop and log on with an account that has local administrative access.
2. Obtain the latest hotfixes approved by your company for your version of Windows Server 2008 x64 (SP2 or R2) and copy them to the server.
3. Launch the hotfix setup via one of two ways:
   3.a. Double-click the file and follow the GUI instructions.
   3.b. Perform a silent installation using the following command from an administrative command prompt:

```
<hotfix>.msu /quiet /norestart
```

4. Click **Yes** for any **Digital Signature not Found** dialog boxes that may appear.

> **Note:**
> These dialog boxes will not appear in environments that have not deployed the Windows Security templates.

5. Wait for all file copies to complete, and then restart the server. You can use the **Processes** tab in Windows Task Manager to monitor the hotfix installation progress. When the wusa.exe process has exited, the hotfix installation is complete.

Domain Membership Configuration

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start,** right-click **My Computer**, and then select **Properties**.
3. Under the **Computer Name, domain, and workgroup** settings, click **Change Settings**.
4. Click **Change**.
5. Choose the **Domain** option button, and then enter the appropriate domain name.
6. Enter the appropriate credentials.
7. Click **OK** and **OK**.
8. Click **OK** to close **System Properties**.
9. Restart the server.

Local Administrators Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Verify (or add if not already there) that the Domain Admins account and the user account that will perform the Exchange installation are members of the local Administrators group on this server.
3. Verify that your user account is a member of a group which is a member of the local Administrators group on the Windows Server 2008 server. If it is not, use an account that is a member of the local Administrators group before continuing.

Local Administrator Account Password Reset

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Manage**.

3. Expand the nodes to find **Configuration\Local Users and Groups\Users**.
4. Right-click **Administrator**, and then select **Set Password**. Change the password so that it meets strong complexity requirements.

Debugging Tools Installation

This section describes several useful tools that aid administrators in Exchange administration and in troubleshooting support issues.

Debugging Tools for Windows allow administrators to debug processes that are affecting service and determine root cause.

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Download and install the latest 64-bit Debugging Tools from Install Debugging Tools for Windows 64-bit Version (http://go.microsoft.com/fwlink/?LinkID=123594).

Page File Modifications

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Properties**.
3. Select the **Advanced System Settings**.
4. Under **Startup and Recovery**, click **Settings**.
   4.a. Under **Write Debugging Information**, select **Kernel Memory Dump** from the memory dump drop-down list.
   4.b. Click **OK**.
5. Under **Performance**, click **Settings**.
6. Click the **Advanced** tab.
7. Under **Virtual Memory**, click **Change**.
8. On servers that have a dedicated page file drive, follow these steps:
   8.a. In the **Drive** list, click **C:**, and then click **Custom size**.
   8.b. For the C: drive, set the **Initial Size (MB)** value to a minimum of 200 MB. (Windows requires between 150 MB and 2 GB page file space, depending on server load and the amount of physical RAM that is available for page file space on the boot volume when Windows is configured for a kernel memory dump. Therefore, you may be required to increase the size.)
   8.c. For the C: drive, set the **Maximum Size (MB)** value to that of the **Initial Size**.
   8.d. In the **Drive** list, select the page file drive (for example, the P: drive), and then click **Custom size**.
   8.e. In the **Initial Size (MB)** box, type the result of one of the following calculations:
      If the server has less than 8 GB of RAM, multiply the amount of RAM times 1.5.
      If the server has 8 GB of RAM or more, add the amount of RAM plus 10 MB.
   8.f. In the **Maximum Size (MB)** box, type the same amount that you typed in the **Initial Size** box.
   8.g. Delete all other page files.
   8.h. Click **OK**.
9. On servers that do not have a dedicated page file drive, follow these steps:
   9.a. In the **Drive** list, click **C:**, and then click **Custom size**.
   9.b. For the C: drive, in the **Initial Size (MB)** box, type the result of one of the following calculations:
      If the server has less than 8 GB of RAM, multiply the amount of RAM times 1.5.
      If the server has 8 GB of RAM or more, add the amount of RAM plus 10 MB.
   9.c. Delete all other page files.
   9.d. Click **OK**.
10. Click **OK** two times to close the **System Properties** dialog box.

11. Click **No** if prompted to restart the system.

> **Note:**
> For more information about page file recommendations, see the following Microsoft Knowledge Base articles: How to determine the appropriate page file size for 64-bit versions of Windows Server 2003 or Windows XP (http://go.microsoft.com/fwlink/?linkid=3052&kbid=889654); and Overview of memory dump file options for Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 2000 (http://go.microsoft.com/fwlink/?linkid=3052&kbid=254649).

Drive Permissions

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, and then select **Computer**.
3. Right-click **D Drive**, and then select **Properties**.
4. Click the **Security** tab.
5. Click **Edit**.
6. Click **Add**, and then select the local server from **Locations**.
7. Grant the following rights as outlined in the following table.

Drive permissions

Account	Permissions
Administrators	Full Control
SYSTEM	Full Control
Authenticated Users	Read and Execute, List, Read
CREATOR OWNER	Full Control

8. Click the **Advanced** button.
9. Select the **CREATOR OWNER** permission entry, and then click **View/Edit**.
10. Select **Subfolders and Files Only** from the drop-down list.
11. Click **OK** two times.
12. Click **OK** to close the drive properties.
13. Repeat steps 3-12 for each additional drive (other than the C drive).

Verification Steps

The following procedures are in this section:

1. Organizational Unit Verification
2. Active Directory Site Verification
3. Domain Controller Diagnostics Verification
4. Exchange Best Practices Analyzer Verification

> **Important:**
> The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Organizational Unit Verification

Submit a change request to the appropriate operations group and have the computer object moved to the appropriate organizational unit (OU).

Active Directory Site Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open a Command Prompt window.
3. Verify that the server is in the correct domain and Active Directory site. At the command line, type the following:

```
NLTEST /server:%COMPUTERNAME% /dsgetsite
```

4. The name of the Active Directory site to which the server belongs will be

displayed. If the server is not in the correct Active Directory site, submit a change request to the appropriate operations group and have the server moved to the appropriate Active Directory site.

Domain Controller Diagnostics Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open a Command Prompt window, and then change paths to the C drive.
3. Run the following command:

```
dcdiag /s:<Domain Controller> /f:c:\dcdiag.log
```

Note:

Change **<domain Controller>** to a domain controller contained within the same Active Directory site as the Exchange server.

4. Review the output of **C:\dcdiag.log** file, and verify that there are no connectivity issues with the local domain controller.
5. Repeat steps 3 and 4 for each domain controller in the local Active Directory site.

Note:

Domain Controller Diagnostics (DCDiag) is a Windows support tool that tests network connectivity and DNS resolution for domain controllers. If the account being used does not have administrative privileges, several tests under the **Doing primary tests** heading may not pass. These tests can be ignored if the connectivity tests pass. In addition, the log file may report that some service validation tests did not pass. These messages can be ignored if the services do not exist on the domain controller.

Exchange Best Practices Analyzer Verification

The Microsoft Exchange Analyzers help administrators troubleshoot various operational support issues. Connect to a server in the environment that either has the Exchange 2010 SP1 (or later) Management tools installed through Remote Desktop and log on with an account that has local administrative access.

1. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010**, and then select **Exchange Management Console**.
2. Open the **Toolbox** node.
3. Double-click **Best Practices Analyzer**.
4. Check and apply any updates for the Best Practices Analyzer engine.
5. Provide the appropriate information to connect to Active Directory and then click **Connect to the Active Directory server**.
6. In the **Start a New Best Practices Scan**, select **Health Check**, and then click **Start Scanning**.
7. Review the report, and take action on any errors or warnings that are reported by following the resolution articles that are provided within the Best Practices Analyzer.

Exchange Server Role Installation

The following media are required for this section.

- Microsoft Exchange Server 2010 installation files

The following procedures are in this section:

1. Exchange 2010 Prerequisites Installation for:
   - Windows Server 2008 SP2

     -or-
   - Windows Server 2008 R2
2. Exchange 2010 Installation
3. Exchange 2010 Update Rollup Installation
4. Product Key Configuration

5. System Performance Verification
6. Test Mailbox Creation

Important:
The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Exchange 2010 Prerequisites Installation for Windows Server 2008 SP2

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open an administrative command prompt window.
3. Install the Microsoft Filter Pack. For details, see 2007 Office System Converter: Microsoft Filter Pack (http://go.microsoft.com/fwlink/?linkid=137042).
4. Open an elevated command prompt, navigate to the \Setup\ServerRoles\Common folder on the Exchange 2010 installation media and use the following command to install the necessary operating system components:

```
ServerManagerCmd -ip Exchange-MBX.xml -Restart
```

Exchange 2010 Prerequisites Installation for Windows Server 2008 R2

1. Connect to the server via Remote Desktop and log on with an account that has local administrative access.
2. Install the Microsoft Filter Pack. For details, see 2007 Office System Converter: Microsoft Filter Pack (http://go.microsoft.com/fwlink/?linkid=137042).
3. On the Start Menu, navigate to **All Programs** > **Accessories > Windows PowerShell**. Open an elevated Windows PowerShell console, and run the following command:

```
Import-Module ServerManager
```

4. Use the **Add-WindowsFeature** cmdlet to install the necessary operating system components:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,W
```

Exchange 2010 Installation

This document uses the command-line method for installing the Exchange 2010 server roles; however, you can also use a GUI called the Setup Wizard. For more information about how to use the Setup Wizard to install an Exchange 2010 server role, see the Perform a Custom Exchange 2010 Installation topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187220).

Important:
If this is the first Mailbox server role being installed into an organization that does not contain any version of Microsoft Exchange, and you have client computers running Microsoft Office Outlook 2003, you must also specify the optional */EnableLegacyOutlook* setup parameter. In addition, if this is the first Exchange 2010 server role being installed into an environment that does not contain any version of Microsoft Exchange, you must also specify the */OrganizationName* setup parameter.

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access. If the Exchange server has been provisioned for delegated setup, the account must be delegated the Server Management or the Delegated Setup role (or higher).
2. Follow the procedure detailed in the Install Exchange 2010 in Unattended Mode topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187229). For example, the following command installs the Mailbox server role, provides a custom database name, database path, and transaction log file location.

```
setup.com /r:M /mdbName "<Server Name> MBX DB1" /dbfilepath e:\MBXDB1\
```

3. Do not restart the server, even if required.

Exchange 2010 Update Rollup Installation

1. Connect to the server through Remote Desktop, and then log on with an account that has local administrative access.
2. Obtain the latest company approved rollup, and then copy it to the server.
3. Launch the Windows Installer patch (the MSP file) setup via one of two ways:
   3.a. Double-click the MSP file, and then follow the GUI instructions.
   3.b. Perform a silent installation using the following command from an administrative command prompt:

```
msiexec /i <Path and filename of MSP file> /q
```

4. Click **Yes** for any **Digital Signature not Found** dialog boxes that may appear.

Note:
These dialog boxes will appear only in environments that have deployed the Windows Security templates.

Product Key Configuration

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Follow the procedure documented in the Enter Product Key topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187234).

Exchange Search Configuration

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Follow the procedure documented in the Register Filter Pack IFilters with Exchange 2010 topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187516).
3. Optional: If you want the ability to search PDF files, install the Adobe PDF iFilter (http://www.adobe.com/support/downloads/detail.jsp?ftpID=4025) and follow the Configuring PDF iFilter for MS Exchange Server 2007 (http://www.adobe.com/special/acrobat/configuring_pdf_ifilter_for_ms_exchange_server_2007.pdf) documentation.

Note:
The third-party Web site information in this topic is provided to help you find the technical information you need. The URLs are subject to change without notice.

System Performance Verification

By default, Exchange 2010 optimizes the server's processor scheduling management for background services.

1. Connect to the server through Remote Desktop, and then log on with an account that has local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Properties**.
3. Select the **Advanced System Settings**.
4. Under **Performance**, click **Settings**.
   4.a. Click the **Advanced** tab.
   4.b. Verify that **Processor Scheduling** is set to **Background Services**.
5. Click **OK**.

Test Mailbox Creation

Several of the diagnostics tasks used to monitor Exchange require that you create test mailboxes on the mailbox servers.

1. Connect to the Exchange 2010 Mailbox server through Remote Desktop, and

then log on with an account that has been delegated local administrative access and was also delegated the Server Management role (or higher).
2. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010** and then select **Exchange Management Shell**.
3. Change the directory path to *<Exchange Server Install Path>*\Scripts.
4. Type **New-TestCasConnectivityUser.ps1** and press **Enter**.
5. Enter a temporary password, and then follow the prompts to create the test mailboxes.

Exchange Server Role Configuration

The following procedures are in this section:

1. First Database Configuration
2. Second Database Configuration
3. Records Management Configuration
4. Message Tracking Server Configuration
5. Additional Databases

Important:

The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

First Database Configuration

If you provided the */mdbname*, */dbfilepath*, and */logfolderpath* parameters when you installed the mailbox server, you can skip this section.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.

   Important:

   The values in the following table are example values, not recommended values. Revise these values to reflect the actual values for your organization.

   ### First database configuration at Contoso

Database parameter	Old	New example
Name	Mailbox Database *<GUID>*	*<ServerName>* MBX DB 1
Log Path	%ProgramFiles% \Microsoft\Exchange Server\v14\Mailbox \Mailbox Database <GUID>	L:\LOG01
Database Filename and Path	%ProgramFiles% \Microsoft\Exchange Server\v14\Mailbox \Mailbox Database <GUID>\Mailbox database <GUID>.edb	E:\MBXDB1\Priv01.edb

2. To dismount the database, run the following command:

   ```
   Dismount-Database "Mailbox Database <GUID>"
   ```

3. To change the mailbox database name, run the following command:

   ```
   Set-MailboxDatabase "<Old DB Name>" -Name "<New DB Name>"
   ```

4. To change the location of the database's transaction logs and the location of the database file, run the following command:

   ```
   Move-DatabasePath "<Database Name>" -LogFolderPath "<New Log Location>
   ```

5. To mount the database, run the following command:

   ```
   Mount-Database "<New DB Name>"
   ```

Second Database Configuration

If a public folder database was created during the installation of the Mailbox server role, the public folder database will be placed in the default location. If there is no public folder database, you can skip this section.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.

Important:
The values in the following table are example values, not recommended values. Revise these values to reflect the actual values for your organization.

Public folder database configuration at Contoso

Database parameter	Old	New example
Name	Public Folder Database <*GUID*>	<*ServerName*> PUB Store 2
Log Path	%ProgramFiles% \Microsoft\Exchange Server\Mailbox\Public Folder Database <GUID>	L:\LOG02
Database Filename and Path	%ProgramFiles% \Microsoft\Exchange Server\Mailbox\Public Folder Database <GUID> \Public Folder database <GUID>.edb	E:\MBXDB2\Pub02.edb

2. To dismount the database, run the following command:

```
Dismount-Database "Public Folder Database <GUID>"
```

3. To change the public folder database name, run the following command:

```
Set-PublicFolderDatabase "<Old DB Name>" -Name "<New DB Name>"
```

4. To change the location of the database's transaction logs and the location of the database file, run the following command:

```
Move-DatabasePath "<Database Name>" -LogFolderPath "<New Log Location>
```

5. To mount the database, run the following command:

```
Mount-Database "<New DB Name>"
```

Records Management Configuration

You can skip this section if the default schedule for the Managed Folder Assistant to apply messaging records management (MRM) settings does not need to be changed.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. To enable the Managed Folder Assistant, run the following command:

```
Set-MailboxServer <MailboxServerName> -ManagedFolderAssistantSchedule
```

Note:
Refer to the "Records management configuration for Contoso" table in the Server Configuration Appendix at the end of this document for the information that you need for the commands.

Message Tracking Server Configuration

You can skip this section if the default message tracking parameters are appropriate for the environment.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.

2. To configure message tracking settings, run the following command:

```
Set-MailboxServer <MailboxServerName> -MessageTrackingLogPath <LogPath
```

Note:
Refer to the "Message tracking configuration for Contoso" table in the Server Configuration Appendix at the end of this document for the information that you need for the commands.

Additional Databases

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Use the appropriate tables in Database / Log LUN Appendix and Database Configuration Appendix at the end of this document for information that you need for the commands.
3. To create the database, run the following command:

```
New-MailboxDatabase -Name "<DB Name>" -LogFolderPath <Transaction Log
```

4. To mount the database, run the following command:

```
Mount-Database "<Database Name>"
```

5. Repeat steps 3 and 4 for each database that needs to be created.

Appendix: Server Configuration

The following information is included in this section:

- Records Management Configuration
- Message Tracking Configuration
- Database / Log LUN Appendix
- Database Configuration Appendix

Records Management Configuration

The following table is an example configuration that can be applied to the Mailbox server, depending on requirements.

Important:
The values in the following table are example values, not recommended values. Revise these values to reflect the actual values for your organization.

Records management configuration for Contoso

Parameter	Default value	Contoso value
Server Name	*<ServerName>*	*<ServerName>*
Managed Folder Assistant Schedule	Sun.1:00 AM-Sun.9:00 AM, Mon.1:00 AM-Mon.9:00 AM, Tue.1:00 AM-Tue.9:00 AM, Wed.1:00 AM-Wed.9:00 AM, Thu.1:00 AM-Thu.9:00 AM, Fri.1:00 AM-Fri. 9:00 AM, Sat.1:00 AM-Sat.9:00 AM	"Sun.6:00 PM-Sun.7:45 PM", "Mon.6:00 PM-Mon.7:45 PM", "Tue.6:00 PM-Tue.7:45 PM", "Wed.6:00 PM-Wed.7:45 PM", "Thu.6:00 PM-Thu.7:45 PM", "Fri.6:00 PM-Fri.7:45 PM", "Sat.6:00 PM-Sat.7:45 PM"

Message Tracking Configuration

The following table is an example configuration that can be applied to the Mailbox server, depending on requirements.

Important:
The values in the following table are example values, not recommended values. Revise

these values to reflect the actual values for your organization.

Message tracking configuration for Contoso

Parameter	Default value	Contoso value
Server Name	*<ServerName>*	*<ServerName>*
Message Tracking Log Path	*<Exchange Install Path>* \TransportRoles\Logs \MessageTracking	L:\exchsrvr\MessageTracking
Message Tracking Log Enabled	True	True
Message Tracking Log Max Age	30.00:00:00	45.00:00:00
Message Tracking Log Max Directory Size	1 GB	20 GB
Message Tracking Log Max File Size	10 MB	10 MB
Message Tracking Log Subject Logging Enabled	True	True

Database / Log LUN Appendix

With mailbox resiliency, you do not have to perform daily full backups because the mailbox database copies and other features provide the first line of defense against physical corruption and data loss. Therefore, there are two approaches to how backups can be performed in an environment enabled for mailbox resiliency:

- Use an Exchange -aware, Volume ShadowCopy Service (VSS)-based application to perform backups and restores, as needed.
- Use Exchange Native Data Protection features as your backup methodology. For more information about Exchange Native Data Protection, see the Understanding Backup, Restore and Disaster Recovery topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187541).

As a result of the backup methodology selected, the LUN layout has to be altered.

Exchange 2010 supports the following LUN layout architectures:

- **One LUN per database** A single LUN per database architecture means that both the database and its corresponding log files are placed on the same LUN. To deploy this architecture, you must have two or more copies of your databases, and you must not be using a hardware-based VSS solution.
- **Two LUNs per database** With Exchange 2010, in the maximum case of 100 databases, the number of LUNs you provision will depend upon your backup strategy. If your recovery time objective (RTO) is small, or if you use VSS clones for fast recovery, it may be best to place each database on its own transaction log LUN and database LUN. This approach will exceed the number of available drive letters; therefore, volume mount points must be used.
- **Two LUNs per backup set** A backup set is the number of databases fully backed up in a night. A solution that performs a full backup on 1/7th of the databases nightly (for example, using a weekly or bimonthly full backup with daily incremental or differential backups) can reduce complexity by placing all of the databases to be backed up on the same log and database LUN. This approach can reduce the number of LUNs on the server.

Two LUNs per Database / LUN Layout

Exchange 2010 uses VSS included in Windows Server 2008 to take volume shadow copies of Exchange 2010 databases and transaction log files. For basic information about VSS, including both clone and snapshot techniques, review the white paper, Best Practices for Using Volume Shadow Copy Service with Exchange Server 2003 (http://go.microsoft.com/fwlink/?LinkId=122556).

Exchange 2010 enables you to make software-based VSS snapshots of both the active and passive database copies. Taking a VSS snapshot of the passive copy offloads the disk I/O from the active LUN during both the checksum integrity (ESEUTIL), and subsequent copy to tape or disk.

Creating two LUNs (log and database) for a database was the standard best practice for Exchange 2003. With Exchange 2010, in the maximum case of 100 databases, the number of LUNs you provision will depend on your backup strategy. If your recovery time objective (RTO) is very small, or if you use VSS clones for fast recovery, it may be best to place each database on its own transaction log LUN and database LUN. Depending on the number of LUNs required, volume mount points may need to be used.

Some benefits of this strategy include the following:

- Enables hardware-based VSS at a database level, providing single database backup and restore.
- Flexibility to isolate the performance between databases when not sharing spindles between LUNs.
- Increased reliability: A capacity or corruption problem on a single LUN will only affect one database.
- This is also the recommended strategy for databases that do not participate in mailbox resiliency.

Some concerns with this strategy include the following:

- 100 databases using mailbox resiliency could require 400 LUNs which would exceed some storage array maximums. 100 databases without mailbox resiliency could require 200 LUNs which would exceed some storage array maximums.
- A separate LUN for each database causes more LUNs per server increasing the administrative costs and complexity.

Note:
In the following table, the reference to MP stands for Mount Point. X and Y refer to unique databases.

LUN design approach: Two LUNs per database

Database	Database name	Database location	Database file name	Transaction log location
Anchor LUN	--	E:\	--	L:\
DBx	<DAGName> MBX DB x	MP:\MDB0x	Priv0x.edb	MP:\LOG0x
DBy	<DAGName> MBX DB y	MP:\MDB0y	Priv0y.edb	MP:\LOG0y
…	…	…	…	…

One LUN per Database / LUN Layout

Single LUN per database architecture means that both the database and its corresponding log files are placed on the same LUN. To deploy this architecture, you must have two or more copies, and you must not be using a hardware-based VSS solution.

Some of the benefits of this strategy include:

- Simplifies storage administration with fewer LUNs to manage.
- Reduces (potentially) the number of backup jobs.
- Provides flexibility to isolate the performance between databases when not sharing spindles between LUNs.

A concern with this strategy is that it limits the ability to perform hardware-based VSS backup and restore procedures (for example, clone snapshots). For VSS details, review the white paper, Best Practices for Using Volume Shadow Copy Service with Exchange Server 2003 (http://go.microsoft.com/fwlink/?LinkId=122556).

Note:
In the following table, the reference to MP stands for Mount Point. X and Y refer to unique databases.

LUN design approach: One LUN per database

DB	Database name	Database location	Database file name
Anchor LUN	--	E:\	--
DBx	<DAGName> MBX Store X	MP:\ \MDBx \LOGx	PrivX.edb
DBy	<DAGName> MBX Store Y	MP:\ \MDBy \LOGy	PrivY.edb
…	…	…	…

Database / LUN Layout

Exchange 2010 uses VSS included in Windows Server 2008 to take volume shadow copies of Exchange 2010 databases and transaction log files. For basic information about VSS, including both clone and snapshot techniques, review the white paper, Best Practices for Using Volume Shadow Copy Service with Exchange Server 2003 (http://go.microsoft.com/fwlink/?LinkId=122556).

Exchange 2010 enables you to make software-based VSS snapshots of both the active and passive database copies. Taking a VSS snapshot of the passive copy offloads the disk I/O from the active LUN during both the checksum integrity (ESEUTIL), and subsequent copy to tape or disk.

Creating two LUNs (log and database) for a database is the standard best practice for Exchange 2003. With Exchange 2010, in the maximum case of 100 databases, the number of LUNs you provision will depend on your backup strategy. If your recovery time objective (RTO) is very small, or if you use VSS clones for fast recovery, it may be best to place each database on its own transaction log LUN and database LUN. Depending on the number of LUNs required, volume mount points may need to be used.

Some benefits of this strategy include the following:

- Enables hardware-based VSS at a database level, providing single database backup and restore.
- Flexibility to isolate the performance between databases when not sharing spindles between LUNs.
- Increased reliability: A capacity or corruption problem on a single LUN will only affect one database.
- This is also the recommended strategy for databases that do not participate in

mailbox resiliency.

Some concerns with this strategy include the following:

- 100 databases using mailbox resiliency could require 400 LUNs which would exceed the maximum capacity of some storage arrays. 100 databases without mailbox resiliency could require 200 LUNs which could also exceed the maximum capacity of some storage arrays.
- A separate LUN for each database causes more LUNs per server increasing the administrative costs and complexity.

Note:
In the following table, the reference to MP stands for Mount Point.
DB2 may contain either a mailbox database or a public folder database, depending on the configuration.

VSS approach LUN design for Contoso

Database	Database name	Database location	Database file name	Transaction log location
Anchor LUN	--	E:\	--	L:\
DB1	<ServerName> MBX DB 1	MP:\MBXDB1	Priv01.edb	MP:\LOG1
DB2	<ServerName> MBX DB 2	MP:\MBXDB2	Priv02.edb	MP:\LOG2
PF2	<ServerName> PUB DB 2	MP:\PFMDB2	Pub02.edb	MP:\PFLOG2
DB3	<ServerName> MBX DB 3	MP:\MBXDB3	Priv03.edb	MP:\LOG3
DB4	<ServerName> MBX DB 4	MP:\MBXDB4	Priv04.edb	MP:\LOG4
DB5	<ServerName> MBX DB 5	MP:\MBXDB5	Priv05.edb	MP:\LOG5
DB6	<ServerName> MBX DB 6	MP:\MBXDB6	Priv06.edb	MP:\LOG6
DB7	<ServerName> MBX DB 7	MP:\MBXDB7	Priv07.edb	MP:\LOG7
DB8	<ServerName> MBX DB 8	MP:\MBXDB8	Priv08.edb	MP:\LOG8
DB9	<ServerName> MBX DB 9	MP:\MBXDB9	Priv09.edb	MP:\LOG9
DB10	<ServerName> MBX DB 10	MP:\MBXDB10	Priv10.edb	MP:\LOG10
DB11	<ServerName> MBX DB 11	MP:\MBXDB11	Priv11.edb	MP:\LOG11
DB12	<ServerName> MBX DB 12	MP:\MBXDB12	Priv12.edb	MP:\LOG12
DB13	<ServerName> MBX DB 13	MP:\MBXDB13	Priv13.edb	MP:\LOG13

DB14	<ServerName> MBX DB 14	MP:\MBXDB14	Priv14.edb	MP:\LOG14
DB15	<ServerName> MBX DB 15	MP:\MBXDB15	Priv15.edb	MP:\LOG15
DB16	<ServerName> MBX DB 16	MP:\MBXDB16	Priv16.edb	MP:\LOG16
DB17	<ServerName> MBX DB 17	MP:\MBXDB17	Priv17.edb	MP:\LOG17
DB18	<ServerName> MBX DB 18	MP:\MBXDB18	Priv18.edb	MP:\LOG18
DB19	<ServerName> MBX DB 19	MP:\MBXDB19	Priv19.edb	MP:\LOG19
DB20	<ServerName> MBX DB 20	MP:\MBXDB20	Priv20.edb	MP:\LOG20
DB21	<ServerName> MBX DB 21	MP:\MBXDB21	Priv21.edb	MP:\LOG21
DB22	<ServerName> MBX DB 22	MP:\MBXDB22	Priv22.edb	MP:\LOG22
DB23	<ServerName> MBX DB 23	MP:\MBXDB23	Priv23.edb	MP:\LOG23
DB24	<ServerName> MBX DB 24	MP:\MBXDB24	Priv24.edb	MP:\LOG24
DB25	<ServerName> MBX DB 25	MP:\MBXDB25	Priv25.edb	MP:\LOG25
DB26	<ServerName> MBX DB 26	MP:\MBXDB26	Priv26.edb	MP:\LOG26
DB27	<ServerName> MBX DB 27	MP:\MBXDB27	Priv27.edb	MP:\LOG27
DB28	<ServerName> MBX DB 28	MP:\MBXDB28	Priv28.edb	MP:\LOG28
DB29	<ServerName> MBX DB 29	MP:\MBXDB29	Priv29.edb	MP:\LOG29
DB30	<ServerName> MBX DB 30	MP:\MBXDB30	Priv30.edb	MP:\LOG30
DB31	<ServerName> MBX DB 31	MP:\MBXDB31	Priv31.edb	MP:\LOG31
DB32	<ServerName> MBX DB 32	MP:\MBXDB32	Priv32.edb	MP:\LOG32
DB33	<ServerName> MBX DB 33	MP:\MBXDB33	Priv33.edb	MP:\LOG33
DB34	<ServerName> MBX DB 34	MP:\MBXDB34	Priv34.edb	MP:\LOG34

DB35	<ServerName> MBX DB 35	MP:\MBXDB35	Priv35.edb	MP:\LOG35
DB36	<ServerName> MBX DB 36	MP:\MBXDB36	Priv36.edb	MP:\LOG36
DB37	<ServerName> MBX DB 37	MP:\MBXDB37	Priv37.edb	MP:\LOG37
DB38	<ServerName> MBX DB 38	MP:\MBXDB38	Priv38.edb	MP:\LOG38
DB39	<ServerName> MBX DB 39	MP:\MBXDB39	Priv39.edb	MP:\LOG39
DB40	<ServerName> MBX DB 40	MP:\MBXDB40	Priv40.edb	MP:\LOG40
DB41	<ServerName> MBX DB 41	MP:\MBXDB41	Priv41.edb	MP:\LOG41
DB42	<ServerName> MBX DB 42	MP:\MBXDB42	Priv42.edb	MP:\LOG42
DB43	<ServerName> MBX DB 43	MP:\MBXDB43	Priv43.edb	MP:\LOG43
DB44	<ServerName> MBX DB 44	MP:\MBXDB44	Priv44.edb	MP:\LOG44
DB45	<ServerName> MBX DB 45	MP:\MBXDB45	Priv45.edb	MP:\LOG45
DB46	<ServerName> MBX DB 46	MP:\MBXDB46	Priv46.edb	MP:\LOG46
DB47	<ServerName> MBX DB 47	MP:\MBXDB47	Priv47.edb	MP:\LOG47
DB48	<ServerName> MBX DB 48	MP:\MBXDB48	Priv48.edb	MP:\LOG48
DB49	<ServerName> MBX DB 49	MP:\MBXDB49	Priv49.edb	MP:\LOG49
DB50	<ServerName> MBX DB 50	MP:\MBXDB50	Priv50.edb	MP:\LOG50

Database Configuration Appendix

The following table is an example configuration that can be applied to each database that is created or customized for each database on the server, depending on requirements.

Important:

The values in the following table are example values, not recommended values. Revise these values to reflect the actual values for your organization.

Database configuration for Contoso

Parameter	Default value	Contoso value
Database Name	<ServerName> MBX DB xx	<ServerName> MBX DB xx

Offline Address Book	[None]	Default Offline Address List
Public Folder Database	<ServerName> PUB DB xx	<ServerName> PUB DB xx
Warning Quota	1991680 KB	1700000 KB
Send Quota	2097152 KB	1900000 KB
Send Receive Quota	2411520 KB	2090000 KB
Maintenance Schedule	Sun.1:00 AM-Sun.5:00 AM, Mon.1:00 AM-Mon.5:00 AM, Tue.1:00 AM-Tue.5:00 AM, Wed.1:00 AM-Wed.5:00 AM, Thu.1:00 AM-Thu.5:00 AM, Fri.1:00 AM-Fri.5:00 AM, Sat.1:00 AM-Sat.5:00 AM	"Sun.12:00 AM-Sun.4:00 AM", "Mon.12:00 AM-Mon.4:00 AM", "Tue.12:00 AM-Tue.4:00 AM", "Wed.12:00 AM-Wed.4:00 AM", "Thu.12:00 AM-Thu.4:00 AM", "Fri.12:00 AM-Fri.4:00 AM", "Sat.12:00 AM-Sat.4:00 AM"
Quota Notification Schedule	Sun.1:00 AM-Sun.1:15 AM, Mon.1:00 AM-Mon.1:15 AM, Tue.1:00 AM-Tue.1:15 AM, Wed.1:00 AM-Wed.1:15 AM, Thu.1:00 AM-Thu.1:15 AM, Fri.1:00 AM-Fri.1:15 AM, Sat.1:00 AM-Sat.1:15 AM	"Sun.12:00 AM-Sun.12:15 AM", "Mon.12:00 AM-Mon.12:15 AM", "Tue.12:00 AM-Tue.12:15 AM", "Wed.12:00 AM-Wed.12: 15 AM", "Thu.12:00 AM-Thu.12:15 AM", "Fri.12:00 AM-Fri.12:15 AM", "Sat.12:00 AM-Sat.12:15 AM"
Mailbox Retention	30.00:00:00	30.00:00:00
Deleted Item Retention	14.00:00:00	14.00:00:00
Keep Deleted Items Until Backup	False	True

1.2.2.11.4 Installation Guide Template - DAG Member

Installation Guide Template - DAG Member

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-06*

This topic provides you with an installation guide template that you can use as a starting point for formally documenting your organization's server build procedures for Microsoft Exchange Server 2010 servers that will have the Mailbox server role installed in a database availability group (DAG) configuration.

The template includes the following key sections:

- Executive Summary
- Server Configuration
- Verification Steps
- Exchange Server Role Installation
- Exchange Server Role Configuration
- Appendix: Server Configuration

For purposes of providing an example, the template uses the fictitious company name of Contoso. Also, you can download this template, along with templates for other server roles, as a download package in .zip file format at Microsoft Exchange Server 2010 Install Guide Templates (http://go.microsoft.com/fwlink/?LinkID=187961).

Executive Summary

The purpose of this document is to explain the installation and configurations necessary to install the Exchange 2010 Mailbox server role and create a database availability group (DAG) on the Windows Server 2008 platform.

Business Justification

By having an installation guide, Contoso will be able to ensure standardization across the enterprise, reducing total cost of ownership (TCO), and easing troubleshooting steps.

Scope

The scope of this document is limited to installation of an Exchange 2010 Mailbox server and creation of a database availability group (DAG) for Contoso on the x64 version of the Windows Server 2008 (SP2 or R2) operating system.

Prerequisites

The administrator should have working knowledge of Windows Server 2008 concepts, Exchange 2010 concepts, the Exchange Management Console and Exchange Management Shell, the command line, and various system utilities. This document does not elaborate on the details of any system utility except as necessary to complete the tasks within.

In addition, before implementing the server role, the administrator should review the Overview of the Mailbox Server Role topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187526).

Assumptions

This document assumes that Windows Server 2008 x64 Edition is installed on the intended Client Access server per company baseline regulations which include the latest approved service pack and hotfixes. In addition, the following system prerequisites have been installed:

- Microsoft .NET Framework 3.5 SP1 and the update for .NET Framework 3.5 SP1 For more information, see Microsoft Knowledge Base article 959209, An update for the .NET Framework 3.5 Service Pack 1 is available (http://go.microsoft.com/fwlink/?linkid=3052&kbid=959209).
- Windows Management Framework (Windows Remote Management 2.0 and Windows PowerShell 2.0).

This document assumes that forest and domain preparation steps have been performed as described in the Prepare Active Directory and Domains topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187262).

This document assumes that the account you will be using for the Exchange tasks has been delegated the Server Management management role, as described in the Server Management topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187265).

This document also assumes that both Exchange 2010 Windows Server 2008 and Windows Server 2008 will be secured following the best practices found in the Windows Server 2008 Security Guide (http://go.microsoft.com/fwlink/?LinkId=122593).

Important:

The procedures within this document should be followed sequentially. If changes are

made out of sequence, unexpected results may occur.

Server Configuration

The following media are required for this section.

- Windows Server 2008 installation files

The following procedures are in this section:

1. Additional Software Verification
2. Network Interfaces Configuration - MAPI Network
3. Network Interfaces Configuration - Replication Network
4. Drive Configuration
5. Windows Server 2008 Hotfix Installation
6. Domain Membership Configuration
7. Local Administrators Verification
8. Local Administrator Account Password Reset
9. Debugging Tools Installation
10. Page File Modifications
11. Drive Permissions

Additional Software Verification

1. Verify that Remote Desktop is enabled.
2. As an optional process, install Microsoft Network Monitor (http://go.microsoft.com/fwlink/?LinkId=86611).

Network Interfaces Configuration - MAPI Network

Make sure that the IP address scheme for the MAPI network is not using the same subnet or network as any replication network adapters. The MAPI network must use the subnet or network that is used to route network traffic within your intranet.

Teaming can be used on the MAPI network in redundancy mode, but it cannot be used in load balancing mode. However, even when using teaming, this does not prevent the network itself from being a single point of failure. In addition, if problems or issues occur that are related to teaming, Microsoft Customer Support Services may require you to disable teaming. If this resolves the issue, you must seek assistance from the hardware manufacturer. For more information about teaming, see Microsoft Knowledge Base article 254101, Network adapter teaming and server clustering (http://go.microsoft.com/fwlink/?linkid=3052&kbid=254101).

1. Connect to what will become the first member of the DAG through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start** > **Control Panel**, and then double-click **Network and Sharing Center**.
3. Click **Manage network connections**.
4. Locate the connection for the MAPI network, and then rename the connection with an appropriate name.
5. Right-click the connection and then select **Properties**.
6. In the network connection's properties on the **General** tab, make sure that the **Client for Microsoft Networks**, **Internet Protocol Version 4 (TCP/IPv4)** and **File and Printer Sharing for Microsoft Networks** check boxes are selected in the **This connection uses the following items** area.
7. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
8. In **Internet Protocol Version 4 (TCP/IPv4) Properties**, click **Advanced**.
9. In **Advanced TCP/IP Settings**, verify the following information on the **DNS** tab:
   9.a. Make sure that all the required addresses are listed in the **DNS server addresses, in order of use** area.
   9.b. Make sure that the correct suffixes are listed in the **Append these DNS suffixes (in order)** area.

10. On the **WINS** tab, make sure that **Disable NetBIOS over TCP/IP** is not selected.
11. Click **OK** two times to save the changes, and then click **Close** to exit **Properties**.
12. If you are using Internet Protocol Version 6 (TCP/IPv6), configure the IPv6 settings according to your organization's network standards.

Network Interfaces Configuration - Replication Network

For any optional replication networks, make sure that the IP address scheme is not using the same subnet or network as the MAPI network or any other replication network adapters.

1. Connect to what will become the first member of the DAG through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start** > **Control Panel**, and then double-click **Network and Sharing Center**.
3. Click **Manage network connections**.
4. Locate the connection for the replication network, and then rename the connection with an appropriate name.
5. Right-click the connection, and then click **Properties**.
6. In the network connection properties, on the **General** tab, verify that the **Internet Protocol Version 4 (TCP/IPv4)** check box is selected and that **File and Printer Sharing for Microsoft Networks** and **Client for Microsoft Networks** are not selected in the **This connection uses the following items** area.
7. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
8. In **Internet Protocol Version 4 (TCP/IPv4) Properties**, click **Advanced**.
9. On the **DNS** tab, verify the following information in **Advanced TCP/IP Settings**:
   9.a. Make sure that addresses are not listed in the **DNS server addresses, in order of use** area if this is a private network.
   9.b. Make sure that the **Register this connection's addresses in DNS** check box is cleared.
10. On the **WINS** tab, make sure that **Disable NetBIOS over TCP/IP** is not selected.
11. Click **OK** two times to save the changes, and then click **Close** to exit **Properties**.
12. If you are using Internet Protocol Version 6 (TCP/IPv6), configure the IPv6 settings according to your organization's network standards.

Drive Configuration

1. Connect to the server through Remote Desktop and log on with an account that has local administrative access.
2. Click **Start** > **Administrative Tools**, and select **Computer Management**.
3. Expand Storage and click **Disk Management**.
4. Open the Disk Management Microsoft Management Console (MMC) and format, rename, and assign the appropriate **Drive Letters** so that the volumes and DVD drive match the appropriate server configuration. Refer to the Database Log/LUN Appendix at the end of this document for the actual drive configuration that should be used.

Drive configuration

LUN	Drive letter	Usage
1	C	Operating system, Exchange binaries, and tracking logs
2	E	Exchange databases
4	L	Exchange transaction

		logs
5-x	--	Additional drives for databases and logs
6	Z	DVD drive

Windows Server 2008 Hotfix Installation

1. Connect to the server via Remote Desktop and log on with an account that has local administrative access.
2. Obtain the latest hotfixes approved by your company for your version of Windows Server 2008 x64 (SP2 or R2) and copy them to the server. Microsoft strongly recommends the hotfix documented in Microsoft Knowledge Base article 2550886 - A transient communication failure causes a Windows Server 2008 R2 failover cluster to stop working. This hotfix resolves a potential race condition and cluster database deadlock issue that can occur when a Windows Failover cluster encounters a transient communication failure. If this situation occurs, it causes the cluster database to hang, resulting in quorum loss in the failover cluster and the dismounting of all databases within the DAG.
3. Launch the hotfix setup via one of two ways:
   3.a.Double-click the file and follow the GUI instructions.
   3.b.Perform a silent installation using the following command from an administrative command prompt:

```
<hotfix>.msu /quiet /norestart
```

4. Click **Yes** for any **Digital Signature not Found** dialog boxes that may appear.

> **Note:**
> These dialog boxes will not appear in environments that have not deployed the Windows Security templates.

5. Wait for all file copies to complete, and then restart the server. You can use the **Processes** tab in Windows Task Manager to monitor the hotfix installation progress. When the wusa.exe process has exited, the hotfix installation is complete.

Domain Membership Configuration

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start,** right-click **My Computer**, and then select **Properties**.
3. Under the **Computer Name, domain, and workgroup** settings, click **Change Settings**.
4. Click **Change**.
5. Choose the **Domain** option button, and then enter the appropriate domain name.
6. Enter the appropriate credentials.
7. Click **OK** and **OK**.
8. Click **OK** to close **System Properties**.
9. Restart the server.

Local Administrators Verification

1. Connect to the server through Remote Desktop and then log on with an account that has been delegated local administrative access.
2. Verify (or add if not already there) that the Domain Admins account and the user account that will perform the Exchange installation are members of the local Administrators group on this server.
3. Verify that your user account is a member of a group which is a member of the local Administrators group on the Windows Server 2008 server. If it is not, use an account that is a member of the local Administrators group before

continuing.

Local Administrator Account Password Reset

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Manage**.
3. Expand the nodes to find **Configuration\Local Users and Groups\Users**.
4. Right-click **Administrator**, and then select **Set Password**. Change the password so that it meets strong complexity requirements.

Debugging Tools Installation

This section describes several useful tools that aid administrators in Exchange administration and in troubleshooting support issues.

Debugging Tools for Windows allow administrators to debug processes that are affecting service and determine root cause.

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Download and install the latest 64-bit Debugging Tools from Install Debugging Tools for Windows 64-bit Version (http://go.microsoft.com/fwlink/?LinkID=123594).

Page File Modifications

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Properties**.
3. Select the **Advanced System Settings**.
4. Under **Startup and Recovery**, click **Settings**.
   4.a. Under **Write Debugging Information**, select **Kernel Memory Dump** from the memory dump drop-down list.
   4.b. Click **OK**.
5. Under **Performance**, click **Settings**.
6. Click the **Advanced** tab.
7. Under **Virtual Memory**, click **Change**.
8. On servers that have a dedicated page file drive, follow these steps:
   8.a. In the **Drive** list, click **C:**, and then click **Custom size**.
   8.b. For the C: drive, set the **Initial Size (MB)** value to a minimum of 200 MB. (Windows requires between 150 MB and 2 GB page file space, depending on server load and the amount of physical RAM that is available for page file space on the boot volume when Windows is configured for a kernel memory dump. Therefore, you may be required to increase the size.)
   8.c. For the C: drive, set the **Maximum Size (MB)** value to that of the **Initial Size**.
   8.d. In the **Drive** list, select the page file drive (for example, the P: drive), and then click **Custom size**.
   8.e. In the **Initial Size (MB)** box, type the result of one of the following calculations:
      If the server has less than 8 GB of RAM, multiply the amount of RAM times 1.5.
      If the server has 8 GB of RAM or more, add the amount of RAM plus 10 MB.
   8.f. In the **Maximum Size (MB)** box, type the same amount that you typed in the **Initial Size** box.
   8.g. Delete all other page files.
   8.h. Click **OK**.
9. On servers that do not have a dedicated page file drive, follow these steps:
   9.a. In the **Drive** list, click **C:**, and then click **Custom size**.
   9.b. For the C: drive, in the **Initial Size (MB)** box, type the result of one of the following calculations:
      If the server has less than 8 GB of RAM, multiply the amount of

RAM times 1.5.
If the server has 8 GB of RAM or more, add the amount of RAM plus 10 MB.

9.c.Delete all other page files.
9.d.Click **OK**.
10.Click **OK** two times to close the **System Properties** dialog box.
11.Click **No** if prompted to restart the system.

Note:
For more information about page file recommendations, see the following Microsoft Knowledge Base articles: How to determine the appropriate page file size for 64-bit versions of Windows Server 2003 or Windows XP (http://go.microsoft.com/fwlink/?linkid=3052&kbid=889654); and Overview of memory dump file options for Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 2000 (http://go.microsoft.com/fwlink/?linkid=3052&kbid=254649).

Drive Permissions

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Click **Start** and select **Computer**.
3. Right-click **D Drive** and select **Properties**.
4. Click the **Security** tab.
5. Click **Edit**.
6. Click **Add**, and then select the local server from **Locations**.
7. Grant the following rights as outlined in the following table.

Drive permissions

Account	Permissions
Administrators	Full Control
SYSTEM	Full Control
Authenticated Users	Read and Execute, List, Read
CREATOR OWNER	Full Control

8. Click the **Advanced** button.
9. Select the **CREATOR OWNER** permission entry, and then click **View/Edit**.
10. Select **Subfolders and Files Only** from the drop-down list.
11. Click **OK** two times.
12. Click **OK** to close the drive properties.
13. Repeat steps 3-12 for each additional drive (other than the C drive).

Verification Steps

The following procedures are in this section:

1. Organizational Unit Verification
2. Active Directory Site Verification
3. Domain Controller Diagnostics Verification
4. Exchange Best Practices Analyzer Verification

Important:
The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Organizational Unit Verification

Submit a change request to the appropriate operations group and have the computer object moved to the appropriate organizational unit (OU).

Active Directory Site Verification

1. Connect to the server through Remote Desktop, and then log on with an

account that has been delegated local administrative access.
2. Open a Command Prompt window.
3. Verify that the server is in the correct domain and Active Directory site. At the command line, type the following:

```
NLTEST /server:%COMPUTERNAME% /dsgetsite
```

4. The name of the Active Directory site to which the server belongs will be displayed. If the server is not in the correct Active Directory site, submit a change request to the appropriate operations group and have the server moved to the appropriate Active Directory site.

Domain Controller Diagnostics Verification

1. Connect to the server through Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open a Command Prompt window, and then change paths to the C drive.
3. Run the following command:

```
dcdiag /s:<Domain Controller> /f:c:\dcdiag.log
```

Note:
Change **<domain Controller>** to a domain controller contained within the same Active Directory site as the Exchange server.

4. Review the output of **C:\dcdiag.log** file, and verify that there are no connectivity issues with the local domain controller.
5. Repeat steps 3 and 4 for each domain controller in the local Active Directory site.

Note:
Domain Controller Diagnostics (DCDiag) is a Windows support tool that tests network connectivity and DNS resolution for domain controllers. If the account being used does not have administrative privileges, several tests under the **Doing primary tests** heading may not pass. These tests can be ignored if the connectivity tests pass. In addition, the log file may report that some service validation tests did not pass. These messages can be ignored if the services do not exist on the domain controller.

Exchange Best Practices Analyzer Verification

The Microsoft Exchange Analyzers help administrators troubleshoot various operational support issues. Connect to a server in the environment that either has the Exchange 2010 SP1 (or later) Management tools installed through Remote Desktop and log on with an account that has local administrative access.

1. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010**, and then select **Exchange Management Console**.
2. Open the **Toolbox** node.
3. Double-click **Best Practices Analyzer**.
4. Check and apply any updates for the Best Practices Analyzer engine.
5. Provide the appropriate information to connect to Active Directory, and then click **Connect to the Active Directory server**.
6. In the **Start a New Best Practices Scan**, select **Health Check**, and then click **Start Scanning**.
7. Review the report, and take action on any errors or warnings that are reported by following the resolution articles that are provided within the Best Practices Analyzer.

Exchange Server Role Installation

The following media are required for this section.

- Microsoft Exchange Server 2010 installation files

The following procedures are in this section:

1. Exchange 2010 Prerequisites Installation for:
   - Windows Server 2008 SP2

   -or-

   - Windows Server 2008 R2
2. Exchange 2010 Installation
3. Exchange 2010 Update Rollup Installation
4. Product Key Configuration
5. Exchange Search Configuration
6. System Performance Verification
7. Test Mailbox Creation

Important:

The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Exchange 2010 Prerequisites Installation for Windows Server 2008 SP2

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Open an administrative command prompt window.
3. Install the Microsoft Filter Pack. For details, see 2007 Office System Converter: Microsoft Filter Pack (http://go.microsoft.com/fwlink/?linkid=137042).
4. Open an elevated command prompt, navigate to the \Setup\ServerRoles\Common folder on the Exchange 2010 installation media and use the following command to install the necessary operating system components:

```
ServerManagerCmd -ip Exchange-MBX.xml -Restart
```

Exchange 2010 Prerequisites Installation for Windows Server 2008 R2

1. Connect to the server via Remote Desktop and log on with an account that has local administrative access.
2. Install the Microsoft Filter Pack. For details, see 2007 Office System Converter: Microsoft Filter Pack (http://go.microsoft.com/fwlink/?linkid=137042).
3. On the Start Menu, navigate to **All Programs** > **Accessories > Windows PowerShell**. Open an elevated Windows PowerShell console, and run the following command:

```
Import-Module ServerManager
```

4. Use the **Add-WindowsFeature** cmdlet to install the necessary operating system components:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,W
```

Exchange 2010 Installation

This document uses the command-line method for installing the Exchange 2010 server roles; however, you can also use a GUI called the Setup Wizard. For more information about how to use the Setup Wizard to install an Exchange 2010 server role, see the Perform a Custom Exchange 2010 Installation topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187220).

Important:

If this is the first Mailbox server role being installed into an organization that does not contain any version of Microsoft Exchange, and you have client computers running Microsoft Office Outlook 2003, you must also specify the optional */EnableLegacyOutlook* setup parameter. In addition, if this is the first Exchange 2010 server role being installed into an environment that does not contain any version of Microsoft Exchange, you must also specify the */OrganizationName* setup parameter.

1. Connect to the server through Remote Desktop and log on with an account

that has local administrative access and was delegated the Server Management or Delegated Setup role if the server was pre-created.

2. Follow the procedure detailed in the Install Exchange 2010 in Unattended Mode topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187229). For example, the following command installs the Mailbox server role , provides a custom database name, database path, and transaction log file location.

```
setup.com /r:MB /mdbName "<DAGName> MBX Store 1" /dbfilepath e:\mdb1\p
```

3. Do not restart the server, even if required.

Exchange Server 2010 Update Rollup Installation

1. Connect to the server through Remote Desktop, and then log on with an account that has local administrative access.
2. Obtain the latest company approved rollup, and then copy it to the server.
3. Launch the Windows Installer patch (the MSP file) setup via one of two ways:
   3.a. Double-click the MSP file, and then follow the GUI instructions.
   3.b. Perform a silent installation using the following command from an administrative command prompt:

```
msiexec /i <Path and filename of MSP file> /q
```

4. Click **Yes** for any **Digital Signature not Found** dialog boxes that may appear.

Note:
These dialog boxes will appear only in environments that have deployed the Windows Security templates.

Product Key Configuration

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Follow the procedure documented in the Enter Product Key topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187234).

Exchange Search Configuration

1. Connect to the server via Remote Desktop, and then log on with an account that has been delegated local administrative access.
2. Follow the procedure documented in the Register Filter Pack IFilters with Exchange 2010 topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187516).
3. Optional: If you want the ability to search PDF files, install the Adobe PDF iFilter (http://www.adobe.com/support/downloads/detail.jsp?ftpID=4025) and follow the Configuring PDF iFilter for MS Exchange Server 2007 (http://www.adobe.com/special/acrobat/configuring_pdf_ifilter_for_ms_exchange_server_2007.pdf) documentation.

Note:
The third-party Web site information in this topic is provided to help you find the technical information you need. The URLs are subject to change without notice.

System Performance Verification

By default, Exchange 2010 optimizes the server's processor scheduling management for background services.

1. Connect to the server through Remote Desktop, and then log on with an account that has local administrative access.
2. Click **Start**, right-click **Computer**, and then select **Properties**.
3. Select the **Advanced System Settings**.
4. Under **Performance**, click **Settings**.
   4.a. Click the **Advanced** tab.
   4.b. Verify that **Processor Scheduling** is set to **Background Services**.

5. Click **OK**.

Test Mailbox Creation

Several of the diagnostics tasks used to monitor Exchange require that you create test mailboxes on the mailbox servers.

1. Connect to the Exchange 2010 Mailbox server through Remote Desktop, and then log on with an account that has been delegated local administrative access and was also delegated the Server Management role (or higher).
2. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010** and then select **Exchange Management Shell**.
3. Change the directory path to **<***Exchange Server Install Path***>\Scripts**.
4. Type **New-TestCasConnectivityUser.ps1** and press **Enter**.
5. Enter a temporary password, and then follow the prompts to create the test mailboxes.

Exchange Server Role Configuration

The following procedures are in this section:

1. Database Availability Group Creation
2. Database Availability Group Member Server Addition
3. Database Availability Group Network Configuration
4. First Database Configuration
5. Public Folder Database Configuration
6. Mailbox Database Copy Addition
7. Records Management Configuration
8. Message Tracking Server Configuration
9. Additional Databases

Important:

The procedures within this document should be followed sequentially. If changes are made out of sequence, unexpected results may occur.

Database Availability Group Creation

If the DAG has been created, you can skip this section.

1. Make sure that there are no pending reboots for the server before adding it to a DAG.
2. Launch the Exchange Management Shell with an account that has been delegated the Organization Management role.
3. In environments where computer account creation is restricted or where computer accounts are created in a container other than the default computers container, you must pre-stage the cluster network object (CNO) and then provision the CNO by assigning permissions to it. Follow the procedures documented in the Pre-stage the Cluster Network Object for a Database Availability Group topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187665).
4. Create a database availability group by following the procedures documented in the Create a Database Availability Group topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187666).
5. Configure the database availability group properties such as the witness settings, replication port, compression, and encryption by following the procedures documented in the Configure Database Availability Group Properties topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187667).

Database Availability Group Member Server Addition

1. Launch the Exchange Management Shell with an account that has been delegated the Organization Management role.
2. Add the mailbox server to the database availability group by following the procedures documented in the Manage Database Availability Group Membership topic in the Exchange Server 2010 Library (http://

go.microsoft.com/fwlink/?LinkId=187669).

Database Availability Group Network Configuration

1. Launch the Exchange Management Shell with an account that has been delegated the Organization Management role.
2. When the Windows Failover Cluster is formed it will create a cluster-managed network for each subnet detected within the failover cluster. When the DAG is formed, the initial DAG network configuration is based on the enumeration of the cluster networks. If the DAG will span subnets, the recommendation is to collapse the DAG networks into a single MAPI network and a single replication network. You can do this by adding the additional subnets to the appropriate DAG networks and deleting unused networks. For example, consider the following environment:

   Sites
   - Two Active Directory sites: Exchange-1 and Exchange-2

   DAG Members
   - DAG members MBX-1 and MBX-2 located in Exchange-1
   - DAG members MBX-3 and MBX-4 located in Exchange-2

   MAPI Networks
   - MBX-1 and MBX-2 have MAPI networks on 192.168.0.0/24
   - MBX-3 and MBX-4 have MAPI networks on 192.168.1.0/24

   Replication Networks
   - MBX-1 and MBX-2 have replication networks on 10.0.0.0/24
   - MBX-3 and MBX-4 have replication networks on 10.0.1.0/24

   The database availability group networks are configured as follows:

Network	Subnets
DAGNetwork01	192.168.0.0/24
DAGNetwork02	10.0.0.0/24
DAGNetwork03	192.168.1.0/24
DAGNetwork04	10.0.1.0/24

3. To collapse these networks, run the following commands.

```
Set-DatabaseAvailabilityGroupNetwork <DAGName>\DAGNetwork01 -Subnets 1
Set-DatabaseAvailabilityGroupNetwork <DAGName>\DAGNetwork02 -Subnets 1
Remove-DatabaseAvailabilityGroupNetwork <DAGName>\DAGNetwork03
Remove-DatabaseAvailabilityGroupNetwork <DAGName>\DAGNetwork04
```

4. To rename the networks according to their behavior, run the following commands.

```
Set-DatabaseAvailabilityGroupNetwork <DAGName>\DAGNetwork01 -Name MAPI
Set-DatabaseAvailabilityGroupNetwork <DAGName>\DAGNetwork02 -Name Repl
```

5. If both MAPI and replication networks are deployed, run the following command to enable replication and seeding traffic on the replication network (unless it is unavailable).

```
Set-DatabaseAvailabilityGroupNetwork <DAGName\MAPINetworkName> -Replic
```

First Database Configuration

If you provided the */mdbname*, */dbfilepath*, and */logfolderpath* parameters when you installed the mailbox server, you can skip this section.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.

Important:

The values in the following table are example values, not recommended values. Revise these values to reflect the actual values for your organization.

First database configuration at Contoso

Database parameter	Old	New example
Name	Mailbox Database <GUID>	<DAGName> MBX Store 1
Log Path	%Program Files% \Microsoft\Exchange Server\v14\Mailbox \Mailbox Database <GUID>	E:\LOG01
Path and Filename	%Program Files% \Microsoft\Exchange Server\v14\Mailbox \Mailbox Database <GUID>\Mailbox database <GUID>.edb	E:\MDB01\Priv01.edb

2. To dismount the database, run the following command:

```
Dismount-Database "Mailbox Database <GUID>"
```

3. To change the mailbox database name from "Mailbox Database <GUID>" to "<DAGName> MBX Store 1", run the following command:

```
Set-MailboxDatabase "<Old DB Name>" -Name "<New DB Name>"
```

4. To change the location of the database's transaction logs and the location of the database file, run the following command:

```
Move-DatabasePath "<Database Name>" -LogFolderPath:<New Log Location>
```

5. To mount the database, run the following command:

```
Mount-Database "<New DB Name>"
```

6. To add a database copy for a specific mailbox database, follow the procedures documented in the Add a Mailbox Database Copy topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187673).

Public Folder Database Configuration

If a public folder database was created during the installation of the Mailbox server role, the public folder database will be placed in the default location. If there is no public folder database, you can skip this section.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.

Important:

The values in the following table are example values, not recommended values. Revise these values to reflect the actual values for your organization.

Public folder database configuration at Contoso

Database parameter	Old	New example
Name	Public Folder Database <GUID>	<DAGName> PUB Store 2
Log Path	%Program Files% \Microsoft\Exchange Server\Mailbox\Public Folder Database <GUID>	E:\LOG02
Path and Filename	%Program Files% \Microsoft\Exchange Server\Mailbox\Public Folder Database <GUID> \ Public Folder database <GUID>.edb	E:\MDB02\Pub02.edb

2. To dismount the database, run the following command:

```
Dismount-Database "Public Folder Database <GUID>"
```

3. To change the mailbox database name from "Mailbox Database <GUID>" to "<ServerName> MBX Store 1", run the following command:

```
Set-PublicFolderDatabase "<Old DB Name>" -Name "<New DB Name>"
```

4. To change the location of the database's transaction logs and the location of the database file, run the following command:

```
Move-DatabasePath "<Database Name>" -LogFolderPath:<New Log Location>
```

5. To mount the database, run the following command:

```
Mount-Database "<New DB Name>"
```

Mailbox Database Copy Addition

If mailbox databases already exist within the DAG, follow these steps to add mailbox database copies to the mailbox server.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Make sure that the directory and path structure exists on the target server for the database in question. Then, to add a database copy for a specific mailbox database, follow the Exchange Management Shell procedures outlined in the Add a Mailbox Database Copy topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187673).

Records Management Configuration

You can skip this section if the default schedule for the Managed Folder Assistant to apply messaging records management (MRM) settings does not need to be changed.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. To enable the Managed Folder Assistant, run the following command:

```
Set-MailboxServer <MailboxServerName> -ManagedFolderAssistantSchedule
```

Note:

Refer to the "Records management configuration for Contoso" table in the Server Configuration Appendix at the end of this document for the information that you need for the commands.

Message Tracking Server Configuration

You can skip this section if the default message tracking parameters are appropriate for the environment.

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. To configure message tracking settings, run the following command:

```
Set-MailboxServer <MailboxServerName> -MessageTrackingLogPath <LogPath
```

Note:

Refer to the "Message tracking configuration for Contoso" table in the Server Configuration Appendix at the end of this document for the information that you need for the commands.

Additional Databases

1. Launch the Exchange Management Shell with an account that has been delegated the Server Management role.
2. Use the appropriate table in the Database/Log LUN Appendix and Database Configuration Appendix at the end of this document for information that you need for the commands.
3. To create the database, run the following command:

```
New-MailboxDatabase -Name "<DB Name>" -LogFolderPath <Transaction Log
```

4. To mount the database, run the following command:

```
Mount-Database "<Database Name>"
```

5. To add replicas for this mailbox database, follow the procedures outlined in the Add a Mailbox Database Copy topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187673) after ensuring that the directory and path structure exists on the target server for the database in question.
6. Repeat steps 3, 4, and 5 for each database that needs to be created.

Appendix: Server Configuration

The following information is included in this section:

- Records Management Configuration
- Message Tracking Configuration
- Database Log LUN Appendix
- Two LUNs per Database/LUN Layout
- One LUN per Database/LUN Layout
- Database Configuration Appendix

Records Management Configuration

The following table is an example configuration that can be applied to the Mailbox server, depending on requirements.

Important:
The values in the following table are example values, not recommended values. Revise these values to reflect the actual values for your organization.

Records management configuration for Contoso

Parameter	Default value	Contoso value
Server Name	<ServerName>	<ServerName>
Managed Folder Assistant Schedule	Sun.1:00 AM-Sun.9:00 AM, Mon.1:00 AM-Mon.9:00 AM, Tue.1:00 AM-Tue.9:00 AM, Wed.1:00 AM-Wed.9:00 AM, Thu.1:00 AM-Thu.9:00 AM, Fri.1:00 AM-Fri. 9:00 AM, Sat.1:00 AM-Sat.9:00 AM	"Sun.6:00 PM-Sun.7:45 PM", "Mon.6:00 PM-Mon.7:45 PM", "Tue.6:00 PM-Tue.7:45 PM", "Wed.6:00 PM-Wed.7:45 PM", "Thu.6:00 PM-Thu.7:45 PM", "Fri.6:00 PM-Fri.7:45 PM", "Sat.6:00 PM-Sat.7:45 PM"

Message Tracking Configuration

The following table is an example configuration that can be applied to the Mailbox server, depending on requirements.

Important:
The values in the following table are example values, not recommended values. Revise these values to reflect the actual values for your organization.

Message tracking configuration for Contoso

Parameter	Default value	Example value
Server Name	<ServerName>	<ServerName>
Message Tracking Log Path	<Exchange Install Path>	L:\exchsrvr\MessageTracking

	\TransportRoles\Logs \MessageTracking	
Message Tracking Log Enabled	True	True
Message Tracking Log Max Age	30.00:00:00	45.00:00:00
Message Tracking Log Max Directory Size	1 GB	20 GB
Message Tracking Log Max File Size	10 MB	10 MB
Message Tracking Log Subject Logging Enabled	True	True

Database / Log LUN Appendix

With mailbox resiliency, you do not have to perform daily full backups as the mailbox database copy provides the first line of defense against corruption and data loss. Therefore, there are two approaches to how backups can be performed in an environment enabled for mailbox resiliency.

- Use an Exchange-aware, Volume ShadowCopy Service (VSS) application to perform backups.
- Use Exchange Native Data Protection features as your backup methodology. For more information about Exchange Native Data Protection, see the Understanding Backup, Restore and Disaster Recovery topic in the Exchange Server 2010 Library (http://go.microsoft.com/fwlink/?LinkId=187541).

As a result of the backup methodology selected, the LUN layout has to be altered. Exchange 2010 supports the following LUN layout architectures:

- **One LUN per database** A single LUN per database architecture means that both the database and its corresponding log files are placed on the same LUN. To deploy this architecture, you must have two or more copies of your databases, and you must not be using a hardware-based VSS solution.
- **Two LUNs per database** With Exchange 2010, in the maximum case of 100 databases, the number of LUNs you provision will depend upon your backup strategy. If your recovery time objective (RTO) is small, or if you use VSS clones for fast recovery, it may be best to place each database on its own transaction log LUN and database LUN. This approach will exceed the number of available drive letters; therefore, volume mount points must be used.
- **Two LUNs per backup set** A backup set is the number of databases fully backed up in a night. A solution that performs a full backup on 1/7th of the databases nightly (for example, using a weekly or bimonthly full backup with daily incremental or differential backups) can reduce complexity by placing all of the databases to be backed up on the same log and database LUN. This approach can reduce the number of LUNs on the server.

Two LUNs per Database / LUN Layout

Exchange 2010 uses VSS included in Windows Server 2008 to take volume shadow copies of Exchange 2010 databases and transaction log files. For basic information about VSS, including both clone and snapshot techniques, review the white paper, Best Practices for Using Volume Shadow Copy Service with Exchange Server 2003 (http://go.microsoft.com/fwlink/?LinkId=122556).

Exchange 2010 enables you to make software-based VSS snapshots of both the active and passive database copies. Taking a VSS snapshot of the passive copy offloads the disk I/O from the active LUN during both the checksum integrity (ESEUTIL), and subsequent copy to tape or disk.

Creating two LUNs (log and database) for a database was the standard best practice for Exchange 2003. With Exchange 2010, in the maximum case of 100 databases, the number of LUNs you provision will depend on your backup strategy. If your recovery time objective (RTO) is very small, or if you use VSS clones for fast recovery, it may be best to place each database on its own transaction log LUN and database LUN. Depending on the number of LUNs required, volume mount points may need to be used.

Some benefits of this strategy include the following:

- Enables hardware-based VSS at a database level, providing single database backup and restore.
- Flexibility to isolate the performance between databases when not sharing spindles between LUNs.
- Increased reliability: A capacity or corruption problem on a single LUN will only affect one database.
- This is also the recommended strategy for databases that do not participate in mailbox resiliency.

Some concerns with this strategy include the following:

- 100 databases using mailbox resiliency could require 400 LUNs which would exceed some storage array maximums. 100 databases without mailbox resiliency could require 200 LUNs which would exceed some storage array maximums.
- A separate LUN for each database causes more LUNs per server increasing the administrative costs and complexity.

Note:

In the following table, the reference to MP stands for Mount Point. X and Y may refer to unique databases.

LUN design approach: Two LUNs per database

DB	Database name	Database location	Database file name	Transaction log location
Anchor LUN	--	E:\	--	L:\
DBx	<DAGName> MBX DB x	MP:\MDB0x	Priv0x.edb	MP:\LOG0x
DBy	<DAGName> MBX DB y	MP:\MDB0y	Priv0y.edb	MP:\LOG0y
…	…	…	…	…

One LUN per Database / LUN Layout

Single LUN per database architecture means that both the database and its corresponding log files are placed on the same LUN. To deploy this architecture, you must have two or more copies, and you must not be using a hardware-based VSS solution.

Some of the benefits of this strategy include:

- Simplifies storage administration with fewer LUNs to manage.
- Reduces (potentially) the number of backup jobs.
- Provides flexibility to isolate the performance between databases when not sharing spindles between LUNs.

A concern with this strategy is that it limits the ability to perform hardware-based VSS backup and restore procedures (for example, clone snapshots). For VSS details, review the white paper, Best Practices for Using Volume Shadow Copy Service with Exchange Server 2003 (http://go.microsoft.com/fwlink/?LinkId=122556).

Note:
In the following table, the reference to MP stands for Mount Point. X and Y refer to unique databases.

LUN design approach: One LUN per database

DB	Database name	Database location	Database file name
Anchor LUN	--	E:\	--
DBx	<DAGName> MBX Store X	MP:\ \MDBx \LOGx	PrivX.edb
DBy	<DAGName> MBX Store Y	MP:\ \MDBy \LOGy	PrivY.edb
…	…	…	…

Database Configuration Appendix

The following table is an example configuration that can either be applied to each database that is created or customized for each database on the server depending on requirements.

Important:
The values in the following table are example values, not recommended values. Revise these values to reflect the actual values for your organization.

Database configuration for Contoso

Parameter	Default value	Contoso value
Database Name	Mailbox Database <GUID>	<DAGName> MBX DB xx
Offline Address Book	[None]	Default Offline Address List
Public Folder Database	Public Folder Database <GUID>	<ServerName> PUB DB xx
Warning Quota	1991680 KB	1700000 KB
Send Quota	2097152 KB	1900000 KB
Send Receive Quota	2411520 KB	2090000 KB
Maintenance Schedule	Sun.1:00 AM-Sun.5:00 AM, Mon.1:00 AM-Mon.5:00 AM, Tue.1:00 AM-Tue.5:00 AM, Wed.1:00 AM-Wed.5:00 AM, Thu.1:00 AM-Thu.5:00 AM, Fri.1:00 AM-Fri.5:00 AM, Sat.1:00 AM-Sat.5:00 AM	"Sun.12:00 AM-Sun.4:00 AM", "Mon.12:00 AM-Mon.4:00 AM", "Tue.12:00 AM-Tue.4:00 AM", "Wed.12:00 AM-Wed.4:00 AM", "Thu.12:00 AM-Thu.4:00 AM", "Fri.12:00 AM-Fri.4:00 AM", "Sat.12:00 AM-Sat.4:00 AM"
Quota Notification Schedule	Sun.1:00 AM-Sun.1:15 AM, Mon.1:00 AM-Mon.1:15 AM,	"Sun.12:00 AM-Sun.12:15 AM", "Mon.12:00 AM-

	Tue.1:00 AM-Tue.1:15 AM, Wed.1:00 AM-Wed.1:15 AM, Thu.1:00 AM-Thu.1:15 AM, Fri.1:00 AM-Fri.1:15 AM, Sat.1:00 AM-Sat.1:15 AM	Mon.12:15 AM", "Tue.12:00 AM-Tue.12:15 AM", "Wed.12:00 AM-Wed.12: 15 AM", "Thu.12:00 AM-Thu.12:15 AM", "Fri.12:00 AM-Fri.12:15 AM", "Sat.12:00 AM-Sat.12:15 AM"
Mailbox Retention	30.00:00:00	30.00:00:00
Deleted Item Retention	14.00:00:00	14.00:00:00
Keep Deleted Items Until Backup	False	True

1.2.2.12 Exchange 2010 Servicing

Exchange 2010 Servicing

Exchange Server 2010 > Planning and Deployment > Deploying Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-04-06*

This topic describes the servicing strategy for Microsoft Exchange Server 2010, discusses the release schedule and distribution methods related to updates, provides guidance about how to deploy fixes for Exchange 2010, provides information about interim updates and how they interact with update rollups, and provides guidance related to Microsoft Exchange and daylight saving time and time zone changes.

Several improvements have been made in servicing for Exchange 2010, including:

- An integrated automated test product that is built together with the shipping product. Therefore, we can perform better integrated, end-to-end system testing than was possible with previous versions of Microsoft Exchange.
- Windows Installer is used instead of the Update.exe installation program.
- Update rollup packages are cumulative. For example, if you apply Update Rollup 4 on a computer that is running Exchange 2010, you receive all the fixes in that specific update package together with all the fixes that were released in all earlier update rollup packages. That is, in Update Rollup 4, you receive all the updates that were released in the previous Update Rollup 1 through Update Rollup 3 packages plus the updates in Update Rollup 4.

Note:
This approach to updating doesn't replace service packs for the product. Additional product fixes and features are released in separately available service packs for Exchange 2010.

For more information about Exchange 2010 servicing, see Install the Latest Update Rollup for Exchange 2010. For information about build numbers and release dates for various versions of Microsoft Exchange, see Exchange Server Build Numbers and Release Dates.

Release Schedule and Distribution Methods

Microsoft releases update rollup packages approximately every six to eight weeks. The

rollup packages are available via Microsoft Update and the Microsoft Download Center. In the Search box on the Microsoft Download Center, type "**Exchange 2010 update rollup**" to find links to the rollup packages.

Deployment Order of Update Rollups

Exchange update rollups work across multiple server roles. Because the update rollups aren't segmented for different Exchange server roles or for specific file configurations, apply each update rollup package to all Exchange 2010 servers in your environment.

For Exchange 2010 configurations, the recommended order in which to apply the update rollup is as follows: Client Access server, Hub Transport server, Mailbox server, and Unified Messaging server.

If you have multiple Active Directory sites and have deployed a Client Access server in the proxy sites that aren't Internet-facing, apply the update rollup to the Internet-facing Client Access servers before you apply the update rollup to the non-Internet-facing Client Access servers. For more information about Client Access to Client Access server proxying, see Understanding Proxying and Redirection.

Interim Updates

The critical fix process for Exchange 2010 is similar to the critical fix process for earlier versions of Exchange.

After working with a Customer Support Specialist or with Escalation Services personnel to troubleshoot an issue, Microsoft Support personnel may escalate a request to the Exchange Customer Experience team. The Customer Experience team may fix the specific problem and give you an interim update to resolve the issue. The interim update is intended to support your Exchange installation until the next scheduled update rollup package is released. The interim updates benefit from much of the same testing that the cumulative updates experience. However, interim update testing isn't as comprehensive as update rollup testing.

Interim updates for Exchange 2010 are update rollup-specific. For example, an interim update that is created to fix a problem on a server that is running the release to manufacturing version of Exchange 2010 doesn't function correctly on an Exchange 2010 server that has Update Rollup 2 installed. If you receive an error message when you install an interim update, check for one of the following issues:

- You have another interim update installed.
- You're installing an interim update that was targeted for a different update rollup baseline.

We deliver the interim update to you under your existing service level agreement. However, you must agree to remove the interim update and install the official update rollup package that resolves your problem when it becomes available. This process ensures that your Exchange 2010 configuration returns to a known, quantifiable state.

If you have an interim update installed on an Exchange 2010 server, you must remove the update before you install the next update rollup package. If the interim update isn't removed, you may receive an error message when you try to install the next update rollup package.

Note:

You will also receive an error message if you try to install an earlier update rollup package over a later update rollup package.

Exchange Server and Daylight Saving Time

For information related to daylight saving time and time zones, see Update Your Exchange Organization When Daylight Saving Time or the Time Zone Changes.

1.2.2.12.1 Install the Latest Update Rollup for Exchange 2010

Install the Latest Update Rollup for Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic describes how to deploy the latest update rollup for Microsoft Exchange Server 2010. Service packs and update rollups are part of the servicing strategy for Exchange 2010. They provide an effective and easy-to-use method to distribute Exchange 2010 fixes and modifications. We recommend that you install the latest service pack and update rollup to keep the product up-to-date.

Update rollups for the release to manufacture (RTM) version of Exchange Server 2010, also known as Exchange Server 2010 Service Pack 0, will continue to be released as long as Exchange 2010 is supported as per the support timeline that is described on the Microsoft Support Lifecycle Web site. For more information about which versions and service packs are supported, see the Support Lifecycle Index.

Note:
The latest update rollup in the series includes the fixes that were released in previous update rollups for the same series. For example, if you install Update Rollup 3 for Exchange 2010 RTM, it includes the fixes that were released in Update Rollup 1 for Exchange 2010 RTM and Update Rollup 2 for Exchange 2010 RTM.

Important Considerations Prior to Installing an Exchange 2010 Update Rollup

The following sections discuss important issues to consider before you deploy an Exchange 2010 update rollup package.

Certificate Revocation List

When you install an update rollup package, Exchange tries to connect to the certificate revocation list (CRL) Web site. Exchange examines the CRL list to verify the code signing certificate. (To download and view the CRL list, see CodeSignPCA.crl.) If Exchange can't connect to the CRL Web site, the following symptoms may occur:

- The installation takes a long time to complete.
- You receive the following message during the installation: **Creating native images for .Net assemblies**

When Exchange isn't connected to the Internet, each CRL request must complete before the installation can continue.

To work around this issue and to reduce installation times, turn off the **Check for publisher's certificate revocation** option on the server that is being upgraded. Use the following steps:

1. Start Internet Explorer.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Advanced** tab, and then locate the **Security** section.
4. Clear the **Check for publisher's certificate revocation** check box, and then click **OK**.
5. After the update rollup installation is complete, select the **Check for publisher's certificate revocation** option.

Note:

The **Check for publisher's certificate revocation** option is set on a per-account basis.

For more information, see Microsoft Knowledge Base article 971445, Generating NGEN images takes longer than expected.

Outlook Web App Customizations

When you apply an update rollup package, the update process may update the Logon.aspx file. If you have modified the Logon.aspx file, the file can't be updated successfully. Therefore, Microsoft Office Outlook Web App may not be updated correctly. In this scenario, after the update process is finished, Outlook Web App may display a blank page.

To work around this issue, rename the Logon.aspx file before you apply the update rollup, and then, after you apply the update, re-create the Outlook Web App customizations in the Logon.aspx file.

We recommend that you make a backup copy of any customized Outlook Web App files before you apply an update rollup. For more information about Outlook Web App customization details, see Customize the Outlook Web App Sign-In and Sign-Out Pages.

Proxying between Client Access Servers

If you have deployed Client Access server to Client Access server proxying, you must apply the update rollup to the Internet-facing Client Access servers before you apply the update rollup to non-Internet-facing Client Access servers. For other Exchange 2010 configurations, the recommended order in which to apply the update rollup is as follows: Client Access server, Hub Transport server, and Mailbox server.

For more information about Client Access to Client Access server proxying, see Understanding Proxying and Redirection.

Backup Recommendations

We strongly recommend that you create the following backups before you install an update rollup package:

- A full backup of all Exchange databases on the server.
- A system state backup of the server.

Exchange and Internet Services Considerations

When you install an update rollup, the Setup program automatically stops the appropriate Exchange services and Internet Information Services (IIS)-related services. Therefore, during the installation process, the server may be unable to service user requests. We recommend that you install an update rollup during a period of scheduled maintenance or during a period of low business impact.

Slipstream Update Rollup Installations

Exchange 2010 doesn't support the slipstream installation of an update rollup during the installation of a service pack.

The Exchange installation folder includes an Updates folder. The Updates folder supports a new installation of Exchange. When you perform a new Exchange installation, you can copy an update rollup to the Updates folder. In this scenario, the update rollup package is applied during the installation of Exchange.

To perform a supported new installation, follow these example steps:

1. Copy the Exchange 2010 RTM files to a local directory on the server or to a network share.
2. Place the appropriate update rollup package in the **Updates** subdirectory.
3. Install Exchange. The update rollup is automatically applied during the installation of Exchange.

The Updates folder isn't supported for use during a service pack installation. Therefore, you can't include (that is, slipstream) an update rollup along with the installation of a service pack. The slipstream installation of an update rollup during a service pack installing hasn't been tested. Therefore, you may experience unintended results.

To perform a supported upgrade installation, follow these example steps:

1. Install Exchange 2010 Service Pack 1 (SP1) on a computer that is running Exchange 2010 RTM together with Exchange 2010 Update Rollup 1.
2. Install Exchange 2010 SP1 Update Rollup 2.

Note:

You can't use the Updates folder in combination with running the **Setup /m:upgrade** unattended install.

Antivirus Services Considerations

Before you install an update rollup package or a service pack, make sure that all antivirus services are stopped.

Pre-Installation Checklist for an Exchange 2010 Update Rollup

Before you install an Exchange 2010 update rollup, we recommend that you review Exchange 2010 Servicing. That topic contains more information about the updates that are included in an update rollup and the methodology behind the Exchange update process.

Applying update rollups to Mailbox servers that are part of a database availability group (DAG) requires specific planning and application steps. For more information about how to apply update rollups to Exchange 2010 DAG member servers, see Installing Update Rollups on Database Availability Group Members.

You can use the following pre-installation checklist to help you install an Exchange 2010 update rollup:

1. **Determine which update rollup packages are installed on your Exchange server roles**
   Installed update rollup packages are shown in the **Programs and Features** dialog box in Control Panel. To see the list of installed updates, click **View installed updates**. Update rollup packages appear as "Update Rollup N for Exchange Server 2010 KBNNNNNN." You can use this information to help determine whether any update rollup packages are installed on the computer.
2. **Determine whether any interim updates are installed**
   Out-of-band fixes for certain Exchange issues are known as *interim updates*. The issue or issues that an interim update resolves may be fixed in a later update rollup package. Before you install an update rollup package, you must remove any interim updates from the computer. Interim updates appear in

the **Programs and Features** dialog box in Control Panel. These updates appear as "Interim Update for Exchange Server 2010 KBNNNNNN."

Note:
You can remove the interim updates on a per-computer basis. You don't have to remove all the interim updates from all the computers in the organization before you install an update rollup.

3. **Review interim updates**
   Examine any interim updates to determine whether they are resolved in the update rollup that you plan to install. To do this, read the Microsoft Knowledge Base article that corresponds to the interim update. If the Knowledge Base article mentions that the issue is resolved in the update rollup package that you plan to install or in an earlier update rollup package, you can remove the interim update and then install the update rollup without the risk of experiencing the specific issue that the interim update resolves. In this scenario, you don't have to obtain a replacement interim update. However, if the Knowledge Base article doesn't mention that the issue is resolved in the update rollup package that you plan to install, you must obtain a replacement interim update from Microsoft Customer Support Services (CSS). In this scenario, you must remove the interim update, install the specific update rollup package, and then install an interim update that is appropriate for the update rollup level of the computer.

   Important:
   Interim updates are created for a specific Exchange build. Therefore, an interim update that is suitable for Exchange 2010 Update Rollup 1 is not suitable for Exchange 2010 Update Rollup 2. You must contact CSS to obtain an interim update that is appropriate for the specific Exchange build that you're running. As previously mentioned, if the issue that the interim update resolves is fixed in the specific update rollup that you install, you don't have to obtain and install a replacement interim update.

4. **Obtain the latest update rollup package**
   The update rollup packages are available via Microsoft Update and the Microsoft Download Center. In the Search box on the Microsoft Download Center, type "**Exchange 2010 update rollup**" to find links to the rollup packages. We strongly recommend that you install the most recent update rollup package that is available. Microsoft releases update rollup packages approximately every six to eight weeks. This step makes sure that you benefit from the latest fixes for Exchange 2010.

Install an Exchange 2010 Update Rollup

Microsoft releases update rollup packages approximately every six to eight weeks. The rollup packages are available via Microsoft Update and the Microsoft Download Center. In the Search box on the Microsoft Download Center, type "**Exchange 2010 update rollup**" to find links to the rollup packages.

Note:
If you use Microsoft Update to install an update rollup package or if you install an update rollup package in silent mode, some Exchange services may be disabled. This issue occurs if the update rollup package must update a file that is being used.

1. Ensure that you have downloaded the appropriate rollup to a local drive on your Exchange servers, or on a remote network share.
2. Run the Windows Installer *.msp Setup file that you downloaded in step 1.

Post-Installation of an Exchange 2010 Update Rollup

When the installation is finished, complete the following tasks:

- Start the Services MMC snap-in, and then verify that all the Exchange-related services are started successfully.
- Log on to Outlook Web App to verify that it's running correctly.
- Restore Outlook Web App customizations, and then check Outlook Web App for correct functionality.
- After the update rollup installation is complete, select the **Check for publisher's certificate revocation** option in Internet Explorer. See "Certificate Revocation List" earlier in this topic.

View the Exchange 2010 Version Number

After you install an update rollup for Exchange 2010, the version of Exchange Server isn't updated to show that the update rollup is installed. This issue occurs because the version number that is displayed by the Exchange Management Console or by other administrative mechanisms is obtained from the Exchange Server Object in Active Directory.

For more information about Exchange 2010 version information, see Exchange 2010: Editions and Versions.

View Installed Update Rollups

The account must be a member of the local administrators group in Active Directory to view the installed update rollups.

1. Click **Start**, click **Control Panel**, and then click **Programs and Features**.
2. In the **Tasks** list, click **View installed updates**.
3. In the **Name** column, locate the Exchange Update Rollups that are installed on the computer.

Remove an Update Rollup

If you need to remove a specific update rollup, use the following procedure.

1. Click **Start**, and then click **Control Panel**.
2. Select **Installed Updates**, and in the Name column, select the update that you want to remove, and then click **Uninstall**.

Exchange Server Build Numbers and Release Dates

For information about build numbers and release dates for each version of Microsoft Exchange, see Exchange Server Build Numbers and Release Dates.

1.2.2.12.2 Update Your Exchange Organization When Daylight Saving Time or the Time Zone Changes

Update Your Exchange Organization When Daylight Saving Time or the Time Zone Changes

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2011-11-01*

If the country or region where your organization or some of your users reside has changed their policy of recognizing Daylight Saving Time (DST), or changed the local time offset from Coordinated Universal Time (UTC), you need may need to update Microsoft Windows, Microsoft Exchange, Microsoft Outlook, or other programs to accommodate these changes.

For more information about DST changes around the world, including links, see the Microsoft Daylight Saving Time Help and Support Center. To find out if there are current DST or time zone issues, see the Office 365 release notes. Also visit the support Web

sites of your other software suppliers to see if they require any additional updates.

Even if your time zone hasn't changed, if you interact with other computers or users globally, your computer needs to be able to perform accurate date and time calculations for events elsewhere in the world.

Installing time zone updates as soon as possible minimizes the number of meetings or appointments that are scheduled during the transition from the old time and date to the new one.

Step 1: Install the Windows DST update on all client and desktop computers

Because the Office 365 authentication system is updated when DST or a time zone changes, all Office 365 client computers need to be updated or they may experience connectivity issues.

- Make sure all client and desktop computers have installed the Windows DST update. For more information, see How to configure daylight saving time for Microsoft Windows operating systems.

Step 2: Install the Windows DST update on all servers

1. Update all your on-premises servers with the Windows DST update.
2. If you're running Office 365, update any servers that interact with the Office 365 authentication system, such as DirSync or AD FS servers. These servers must be updated to ensure uptime.

Note If you're updating server clusters, make sure you follow the usual process for updating clusters. You update the passive server first, fail over to the passive server (which becomes active), and then update the formerly active (now passive) server. For more information about how to update server clusters and high-availability server clusters, see Update Exchange Server Clusters and High Availability Servers.

Step 3: Update Exchange 2003 SP2 and Exchange 2007 SP3 servers with the latest updates

1. Install the latest DST update on your Exchange servers. For more information, see CDO time zone tables.

Note If you're updating server clusters, make sure you follow the usual process for updating clusters. You update the passive server first, fail over to the passive server (which becomes active), and then update the formerly active (now passive) server. For more information about how to update server clusters and high-availability server clusters, see Update Exchange Server Clusters and High Availability Servers.

Step 4: Update Exchange and Outlook on all client and desktop computers

1. Determine which of your users need to run the Exchange or Outlook time

zone tools, and which tool to run, using the table following this procedure.
2. Send a message to your users who need to update their computers, giving them a link to the appropriate tool.

The following table shows when users should run the Exchange Calendar Update Tool or the Time Zone Data Update Tool for Microsoft Office Outlook. Find which version your organization's servers are running, and then determine which client programs your users are running.

	Client Version		
Organization version	**Outlook 2003**	**Outlook 2007**	**Outlook 2010**
Exchange 2003 on premises	Exchange Calendar Tool or Time Zone Data Update Tool for Microsoft Office Outlook	Exchange Calendar Tool or Time Zone Data Update Tool for Microsoft Office Outlook	No action required
Exchange 2007 on premises	Exchange Calendar Tool or Time Zone Data Update Tool for Microsoft Office Outlook	Exchange Calendar Tool or Time Zone Data Update Tool for Microsoft Office Outlook	No action required
Exchange 2010 on premises	Time Zone Data Update Tool for Microsoft Office Outlook	Time Zone Data Update Tool for Microsoft Office Outlook	No action required
BPOS-S (Exchange 2007)	Time Zone Data Update Tool for Microsoft Office Outlook	Time Zone Data Update Tool for Microsoft Office Outlook	No action required
BPOS-D (Exchange 2010)	Time Zone Data Update Tool for Microsoft Office Outlook	Time Zone Data Update Tool for Microsoft Office Outlook	No action required
Office 365 (Exchange 2010)	Not supported	Time Zone Data Update Tool for Microsoft Office Outlook	No action required

1.2.2.12.2.1 Update Exchange Server Clusters and High Availability Servers

Update Exchange Server Clusters and High Availability Servers

Deploying Exchange 2010 > Exchange 2010 Servicing > Update Your Exchange Organization When Daylight Saving Time or the Time Zone Changes >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2011-11-09*

If you need to update clustered or high availability servers, the instructions are different depending on which version of Microsoft Exchange is running on your on-premises servers.

Choose from the following instructions:

- **Exchange 2003** See How to apply Exchange service packs and hotfixes.
- **Exchange 2007** See How to Install Update Rollups in a CCR Environment.
- **Exchange 2010** See Installing Update Rollups on Database Availability Group Members.
- **Windows updates (Windows 2003, Windows 2008 and Windows 2008 R2)** See How to install service packs in a cluster.

1.3 Permissions

Permissions

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-10*

Understanding Permissions

Learn about the permissions models that are used by Microsoft Exchange Server 2010.

Feature Permissions

This topic provides access to information about the permissions required to perform operations in each area of Exchange 2010, such as Transport and Unified Messaging.

Managing Permissions

This topic is a collection of links that provide information about managing permissions in your organization.

1.3.1 Understanding Permissions

Understanding Permissions

Exchange Server 2010 > Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 includes a large set of predefined permissions, based on the Role Based Access Control (RBAC) permissions model, which you can use right away to easily grant permissions to your administrators and users. You can use the permissions features in Exchange 2010 so that you can get your new organization up and running quickly.

RBAC grants permissions to manage the Mailbox, Hub Transport, Client Access, and Unified Messaging server roles. For information about permissions on the Edge Transport server role, see Edge Transport Permissions later in this topic.

Note:

Several RBAC features and concepts aren't discussed in this topic because they're

advanced features. If the functionality discussed in this topic doesn't meet your needs, and you want to further customize your permissions model, see Understanding Role Based Access Control.

Looking for management tasks related to permissions? See Managing Permissions.

Role-Based Permissions

In Exchange 2010, the permissions that you grant to administrators and users are based on management roles. A role defines the set of tasks that an administrator or user can perform. For example, a management role called `Mail Recipients` defines the tasks that someone can perform on a set of mailboxes, contacts, and distribution groups. When a role is assigned to an administrator or user, that person is granted the permissions provided by the role.

There are two types of roles, administrative roles and end-user roles:

- **Administrative roles** These roles contain permissions that can be assigned to administrators or specialist users using role groups that manage a part of the Exchange organization, such as recipients, servers, or databases.
- **End-user roles** These roles, assigned using role assignment policies, enable users to manage aspects of their own mailbox and distribution groups that they own. End-user roles begin with the prefix `My`.

Roles give permissions to perform tasks to administrators and users by making cmdlets available to those who are assigned the roles. Because the Exchange Management Console (EMC), Exchange Control Panel (ECP), and Exchange Management Shell use cmdlets to manage Exchange, granting access to a cmdlet gives the administrator or user permission to perform the task in each of the Exchange management interfaces.

Exchange 2010 includes approximately 60 roles that can be used to grant permissions. For a list of roles included with Exchange 2010, see Built-in Management Roles.

Role Groups and Role Assignment Policies

Roles grant permissions to perform tasks in Exchange 2010, but you need an easy way to assign them to administrators and users. Exchange 2010 provides you with the following to help you do that:

- **Role groups** Role groups enable you to grant permissions to administrators and specialist users.
- **Role assignment policies** Role assignment policies enable you to grant permissions to end users to change settings on their own mailbox or distribution groups that they own.

For more information about role groups and role assignment policies, see the following sections.

Role Groups

Every administrator that manages Exchange 2010 must be assigned at least one or more roles. Administrators might have more than one role because they may perform job functions that span multiple areas in Exchange. For example, one administrator might manage both recipients and Exchange servers. In this case, that administrator might be assigned both the `Mail Recipients` and `Exchange Servers` roles.

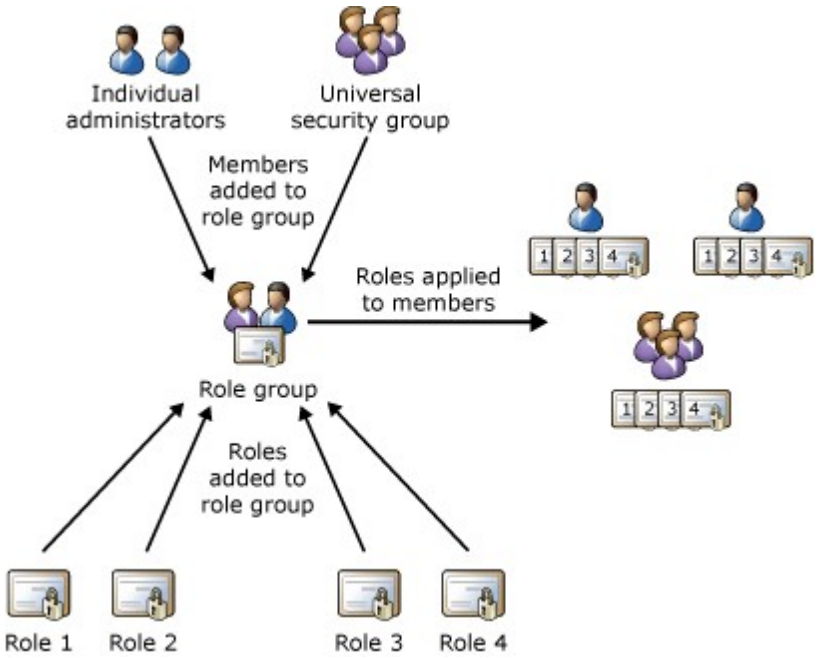
To make it easier to assign multiple roles to an administrator, Exchange 2010 includes role groups. Role groups are special universal security groups (USGs) used by Exchange 2010 that can contain Active Directory users, USGs, and other role groups. When a role is assigned to a role group, the permissions granted by the role are granted to all the members of the role group. This enables you to assign many roles to many role group

members at once. Role groups typically encompass broader management areas, such as recipient management. They're used only with administrative roles, and not end-user roles.

Note:

It's possible to assign a role directly to a user or USG without using a role group. However, that method of role assignment is an advanced procedure and isn't covered in this topic. We recommend that you use role groups to manage permissions.

The following figure shows the relationship between users, role groups, and roles.



Exchange 2010 includes several built-in role groups, each one providing permissions to manage specific areas in Exchange 2010. Some role groups may overlap with others. The following table lists each role group with a description of its use. If you want to see the roles assigned to each role group, click the name of the role group in the table, and then open the "Management Roles Assigned to This Role Group" section.

Built-in role groups

Role group	Description
Organization Management	Administrators who are members of the Organization Management role group have administrative access to the entire Exchange 2010 organization and can perform almost any task against any Exchange 2010 object, with some exceptions, such as the `Discovery Management` role. **Important:** Because the Organization Management role group is a powerful role, only users or USGs that perform organizational-level administrative tasks that can potentially impact the entire Exchange organization should be members of this role group.

View-Only Organization Management	Administrators who are members of the View Only Organization Management role group can view the properties of any object in the Exchange organization.
Recipient Management	Administrators who are members of the Recipient Management role group have administrative access to create or modify Exchange 2010 recipients within the Exchange 2010 organization.
UM Management	Administrators who are members of the UM Management role group can manage features in the Exchange organization such as Unified Messaging (UM) server configuration, UM properties on mailboxes, UM prompts, and UM auto attendant configuration.
Help Desk	The Help Desk role group, by default, enables members to view and modify the Microsoft Office Outlook Web App options of any user in the organization. These options might include modifying the user's display name, address, and phone number. They don't include options that aren't available in Outlook Web App options, such as modifying the size of a mailbox or configuring the mailbox database on which a mailbox is located.
Hygiene Management	Administrators who are members of the Hygiene Management role group can configure the antivirus and anti-spam features of Exchange 2010. Third-party programs that integrate with Exchange 2010 can add service accounts to this role group to grant those programs access to the cmdlets required to retrieve and configure the Exchange configuration.
Records Management	Users who are members of the Records Management role group can configure compliance features, such as retention policy tags, message classifications, and transport rules.
Discovery Management	Administrators or users who are members of the Discovery Management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria and can also configure legal holds on mailboxes. For more information, see Discovery and Understanding Litigation Hold.
Public Folder Management	Administrators who are members of the Public Folder Management role group can manage public folders and databases on servers running Exchange 2010.

Server Management	Administrators who are members of the Server Management role group can configure server-specific configuration of transport, Unified Messaging, client access, and mailbox features such as database copies, certificates, transport queues and Send connectors, virtual directories, and client access protocols.
Delegated Setup	Administrators who are members of the Delegated Setup role group can deploy servers running Exchange 2010 that have been previously provisioned by a member of the Organization Management role group. For more information about delegated setup, see Provision Exchange 2010 Server and Delegate Setup.

If you work in a small organization that has only a few administrators, you might need to add those administrators to the Organization Management role group only, and you may never need to use the other role groups. If you work in a larger organization, you might have administrators who perform specific tasks administering Exchange, such as recipient or server management. In those cases, you might add one administrator to the Recipient Management role group, and another administrator to the Server Management role group. Those administrators can then manage their specific areas of Exchange 2010 but won't have permissions to manage areas they're not responsible for.

If the built-in role groups in Exchange 2010 don't match the job function of your administrators, you can create role groups and add roles to them. For more information, see Work with Role Groups later in this topic.

Role Assignment Policies

Exchange 2010 provides role assignment policies so that you can control what settings your users can configure on their own mailboxes and on distribution groups they own. These settings include their display name, contact information, voice mail settings, and distribution group membership.

Your Exchange 2010 organization can have multiple role assignment policies that provide different levels of permissions for the different types of users in your organizations. Some users can be allowed to change their address or create distribution groups, while others can't, depending on the role assignment policy associated with their mailbox. Role assignment policies are added directly to mailboxes, and each mailbox can only be associated with one role assignment policy at a time.

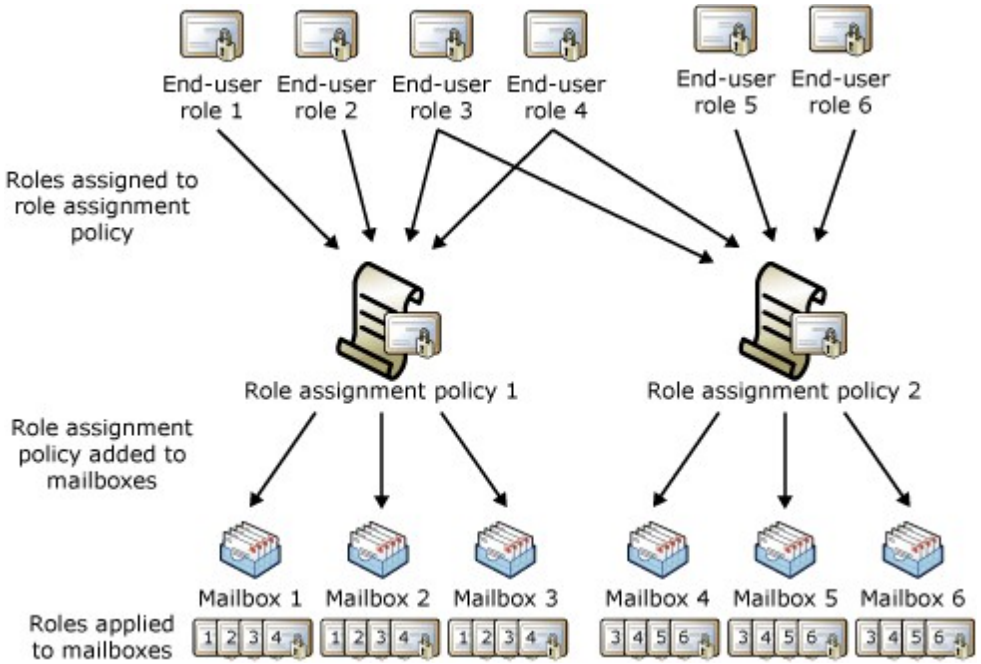
Of the role assignment policies in your organization, one is marked as default. The default role assignment policy is associated with new mailboxes that aren't explicitly assigned a specific role assignment policy when they're created. The default role assignment policy should contain the permissions that should be applied to the majority of your mailboxes.

Permissions are added to role assignment policies using end-user roles. End-user roles begin with My and grant permissions for users to manage only their mailbox or distribution groups they own. They can't be used to manage any other mailbox. Only end-user roles can be assigned to role assignment policies.

When an end-user role is assigned to a role assignment policy, all of the mailboxes associated with that role assignment policy receive the permissions granted by the role. This enables you to add or remove permissions to sets of users without having to configure individual mailboxes. The following figure shows:

- End-user roles are assigned to role assignment policies. Role assignment

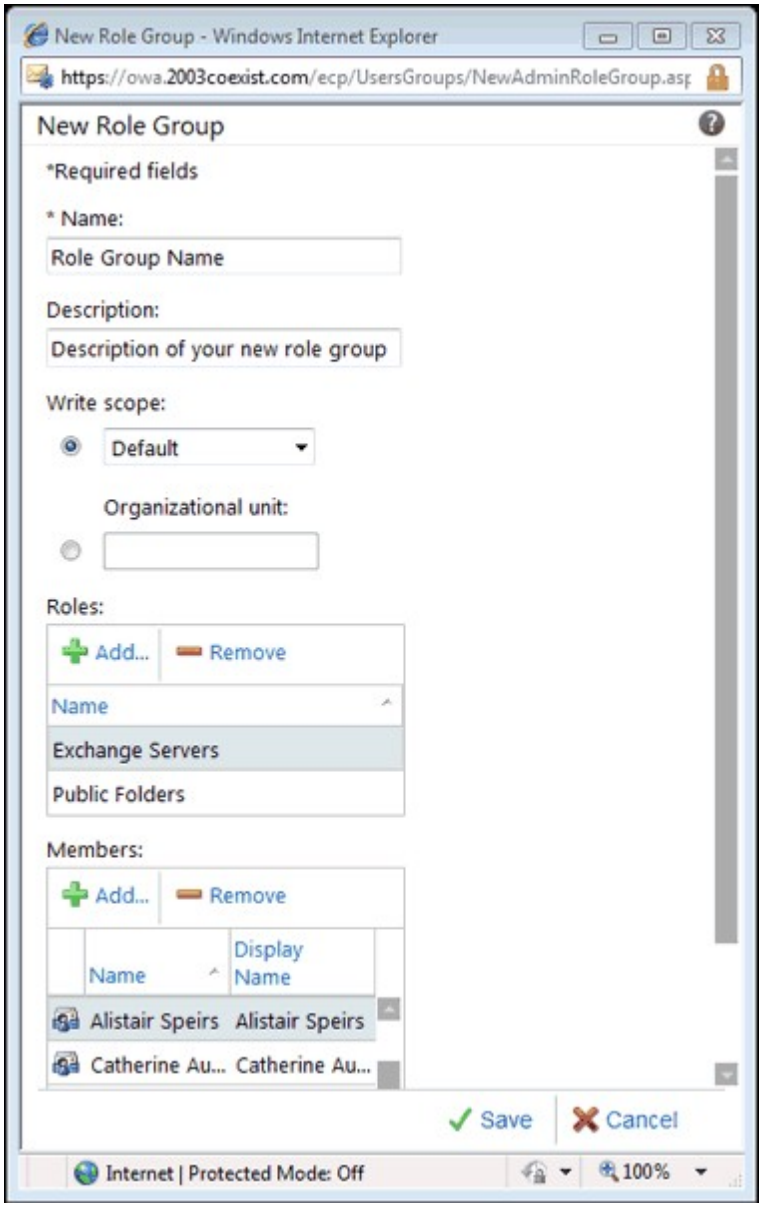
policies can share the same end-user roles.
- Role assignment policies are associated with mailboxes. Each mailbox can only be associated with one role assignment policy.
- After a mailbox is associated with a role assignment policy, the end-user roles are applied to that mailbox. The permissions granted by the roles are granted to the user of the mailbox.



The Default Role Assignment Policy role assignment policy is included with Exchange 2010. As the name implies, it's the default role assignment policy. If you want to change the permissions provided by this role assignment policy, or if you want to create role assignment policies, see Work with Role Assignment Policies later in this topic.

Work with Role Groups

To manage your permissions using role groups in Exchange 2010 Service Pack 1 (SP1), we recommend that you use the ECP. When you use the ECP to manage role groups, you can add and remove roles and members, create role groups, and copy role groups with a few clicks of your mouse. The ECP provides simple dialog boxes, such as the **New Role Group** dialog box, shown in the following figure, to perform these tasks.



As mentioned earlier in this topic, Exchange 2010 includes several role groups that separate permissions into specific administrative areas. If these existing role groups provide the permissions your administrators need to manage your Exchange 2010 organization, you need only add your administrators as members of the appropriate role groups. After you add administrators to a role group, they can administer the features that relate to that role group. To add or remove members to or from a role group, open the role group in the ECP, and then add or remove members from the membership list. For a list of built-in role groups, see Built-in Role Groups.

Important:

If an administrator is a member of more than one role group, Exchange 2010 grants the administrator all of the permissions provided by the role groups he or she is a member of.

If none of the role groups included with Exchange 2010 have the permissions you need, you can use the ECP to create a role group and add the roles that have the permissions you need. For your new role group, you will:

1. Choose a name for your role group.

2. Select the roles you want to add to the role group.
3. Add members to the role group.
4. Save the role group.

After you create the role group, you manage it like any other role group.

If there's an existing role group that has some, but not all of the permissions you need, you can copy it and then make changes to create a role group. You can copy an existing role group and make changes to it, without affecting the original role group. As part of copying the role group, you can add a new name and description, add and remove roles to and from the new role group, and add new members. When you create or copy a role group, you use the same dialog box that's shown in the preceding figure.

Existing role groups can also be modified. You can add and remove roles from existing role groups, and add and remove members from it at the same time, using an ECP dialog box similar to the one in the preceding figure. By adding and removing roles to and from role groups, you turn on and off administrative features for members of that role group. For a list of roles you can add to a role group, see Built-in Management Roles.

Note:

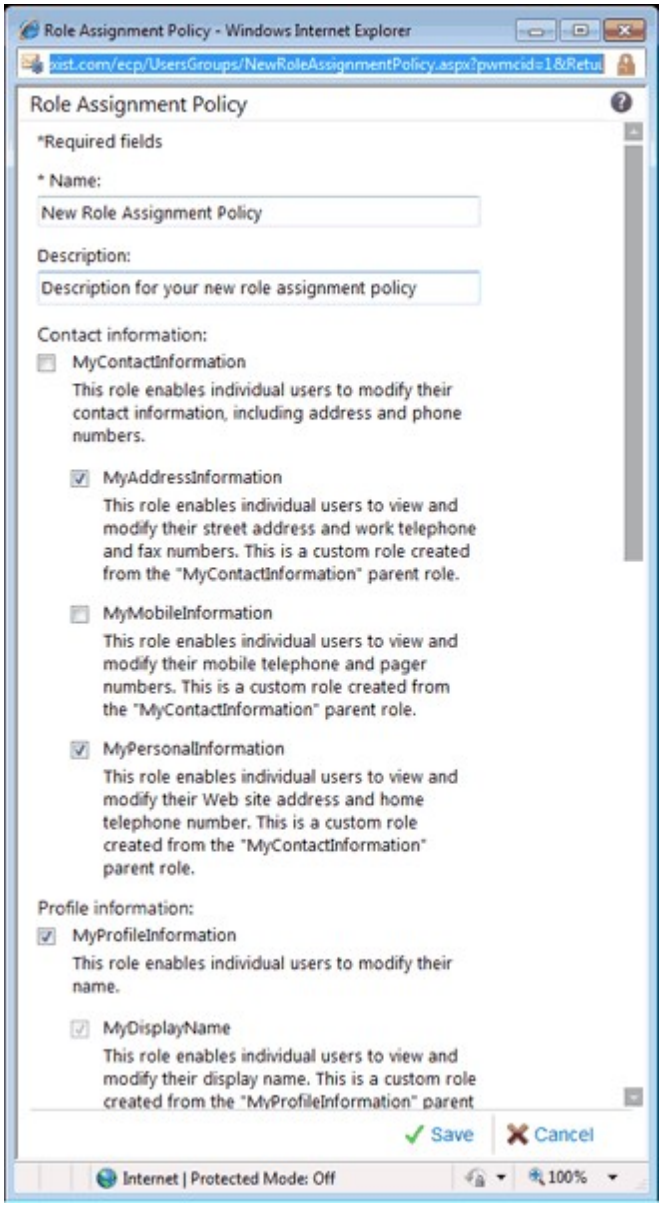
Although you can change which roles are assigned to built-in role groups, we recommend that you copy built-in role groups, modify the role group copy, and then add members to the role group copy.

For detailed steps about how to create or copy role groups, or make changes to existing role group roles and membership, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group
- Create a Role Group
- Copy a Role Group
- Remove a Role Group
- Add a Role to a Role Group
- Remove a Role from a Role Group

Work with Role Assignment Policies

To manage the permissions that you grant end users to manage their own mailbox in Exchange 2010 SP1, we recommend that you use the ECP. When you use the ECP to manage end-user permissions, you can add roles, remove roles, and create role assignment policies with a few clicks of your mouse. The ECP provides simple dialog boxes, such as the **Role Assignment Policy** dialog box, shown in the following figure, to perform these tasks. To apply a role assignment policy to a mailbox, you can use either the EMC or the ECP.



Exchange 2010 includes a role assignment policy named Default Role Assignment Policy. This role assignment policy enables users whose mailboxes are associated with it to do the following:

- Join or leave distribution groups that allow members to manage their own membership.
- View and modify basic mailbox settings on their own mailbox, such as Inbox rules, spelling behavior, junk mail settings, and Microsoft ActiveSync devices.
- Modify their contact information, such as address and phone number.
- Create, modify, or view text message settings.
- View or modify voice mail settings.

If you want to add or remove permissions from the Default Role Assignment Policy or any other role assignment policy, you can use the ECP. The dialog box you use is similar to the one in the preceding figure. When you open the role assignment policy in the ECP, select the check box next to the roles you want to assign to it or clear the check box next to the roles you want to remove. The change you make to the role assignment policy is applied

to every mailbox associated with it.

If you want to assign different end-user permissions to the various types of users in your organization, you can create role assignment policies. When you create a role assignment policy, you see a dialog box similar to the one in the preceding figure. You can specify a new name for the role assignment policy, and then select the roles you want to assign to the role assignment policy. After you create a role assignment policy, you can associate it with mailboxes using the EMC or the ECP.

If you want to change which role assignment policy is the default, you must use the Shell. When you change the default role assignment policy, any mailboxes that are created will be associated with the new default role assignment policy if one wasn't explicitly specified. The role assignment policy associated with existing mailboxes doesn't change when you select a new default role assignment policy.

Note:

If you select a check box for a role that has child roles, the check boxes for the child roles are also selected. If you clear the check box for a role with child roles, the check boxes for the child roles are also cleared.

For detailed steps about how to create role assignment policies or make changes to existing role assignment policies, see the following topics:

- Add an Assignment Policy
- Remove an Assignment Policy
- Add a Role to an Assignment Policy
- Remove a Role from an Assignment Policy
- Change the Assignment Policy on a Mailbox
- Change the Default Assignment Policy

Edge Transport Permissions

The Edge Transport server role is deployed in an organization's perimeter network, which is also known as the boundary network or screened subnet. An Edge Transport server can be deployed as a stand-alone server or as a member of a perimeter Active Directory domain.

On Edge Transport servers, RBAC isn't used to control permissions. The local Administrators group is used to control who can configure Exchange features on the local server. If you have multiple Edge Transport servers, you need to add the user you want to manage those servers to the local Administrators group on each server.

For more information about permissions on Edge Transport servers, see Setting Administrator Permissions for the Edge Transport Server Role.

For More Information

Understanding Role Based Access Control

Understanding Split Permissions

Understanding Permissions Coexistence with Exchange 2007

Understanding Permissions Coexistence with Exchange 2003

Understanding Multiple-Forest Permissions

Feature Permissions

1.3.1.1 Understanding Role Based Access Control

Understanding Role Based Access Control

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Role Based Access Control (RBAC) is the new permissions model in Microsoft Exchange Server 2010. With RBAC, you don't need to modify and manage access control lists (ACLs), which was done in Exchange Server 2007. ACLs created several challenges in Exchange 2007, such as modifying ACLs without causing unintended consequences, maintaining ACL modifications through upgrades, and troubleshooting problems that occurred due to using ACLs in a nonstandard way.

RBAC enables you to control, at both broad and granular levels, what administrators and end-users can do. RBAC also enables you to more closely align the roles you assign users and administrators to the actual roles they hold within your organization. In Exchange 2007, the server permissions model applied only to the administrators who managed the Exchange 2007 infrastructure. In Exchange 2010, RBAC now controls both the administrative tasks that can be performed and the extent to which users can now administer their own mailbox and distribution groups.

RBAC has two primary ways of assigning permissions to users in your organization, depending on whether the user is an administrator or specialist user, or an end-user: management role groups and management role assignment policies. Each method associates users with the permissions they need to perform their jobs. A third, more advanced method, direct user role assignment, can also be used. The following sections in this topic explain RBAC and provide examples of its use.

Note:

This topic focuses on advanced RBAC functionality. If you want to manage basic Exchange 2010 permissions, such as using the Exchange Control Panel (ECP) to add and remove members to and from role groups, create and modify role groups, or create and modify role assignment policies, see Understanding Permissions.

Contents

Management Role Groups

Management role groups associate management roles to a group of administrators or specialist users. Administrators manage a broad Exchange organization or recipient configuration. Specialist users manage the specific features of Exchange, such as compliance. Or they may have limited management abilities, such as Help desk members, but aren't given broad administrative rights. Role groups typically associate administrative

management roles that enable administrators and specialist users to manage the configuration of their organization and recipients. For example, whether administrators can manage recipients or use mailbox discovery features is controlled using role groups.

Adding or removing users to or from role groups is how you most often assign permissions to administrators or specialist users. For more information, see Understanding Management Role Groups.

Role groups consist of the following components that define what administrators and specialist users can do:

- **Management role group** The *management role group* is a special universal security group (USG) that contains mailboxes, users, USGs, and other role groups that are members of the role group. This is where you add and remove members, and it's also what management roles are assigned to. The combination of all the roles on a role group defines everything that users added to a role group can manage in the Exchange organization.
- **Management role** A *management role* is a container for a grouping of management role entries. Roles are used to define the specific tasks that can be performed by the members of a role group that's assigned the role. A *management role entry* is a cmdlet, script, or special permission that enables each specific task in a role to be performed. For more information, see Understanding Management Roles.
- **Management role assignment** A *management role assignment* links a role and a role group. Assigning a role to a role group grants members of the role group the ability to use the cmdlets and parameters defined in the role. Role assignments can use management scopes to control where the assignment can be used. For more information, see Understanding Management Role Assignments.
- **Management role scope** A *management role scope* is the scope of influence or impact on a role assignment. When a role is assigned with a scope to a role group, the management scope targets specifically what objects that assignment is allowed to manage. The assignment, and its scope, are then given to the members of the role group, and restrict what those members can manage. A scope can consist of a list of servers or databases, organizational units (OUs), or filters on server, database or recipient objects. For more information, see Understanding Management Role Scopes.

When you add a user to a role group, the user is given all of the roles assigned to the role group. If scopes are applied to any of the role assignments between the role group and the roles, those scopes control what server configuration or recipients the user can manage.

If you want to change what roles are assigned to role groups, you need to change the role assignments that link the role groups to roles. Unless the assignments built into Exchange 2010 don't suit your needs, you won't have to change these assignments. For more information, see Understanding Management Role Assignments.

For more information about role groups, see Understanding Management Role Groups.

Return to top

Management Role Assignment Policies

Management role assignment policies associate end-user management roles to users. Role assignment policies consist of roles that control what a user can do with his or her mailbox or distribution groups. These roles don't allow management of features that aren't directly associated with the user. When you create a role assignment policy, you define everything a user can do with his or her mailbox. For example, a role assignment policy may allow a user to set the display name, set up voice mail, and configure Inbox

rules. Another role assignment policy might allow a user to change the address, use text messaging, and set up distribution groups. Every user with an Exchange 2010 mailbox, including administrators, is given a role assignment policy by default. You can decide which role assignment policy should be assigned by default, choose what the default role assignment policy should include, override the default for certain mailboxes, or not assign role assignment policies by default at all.

Assigning a user to an assignment policy is how you most often manage permissions for users to manage their own mailbox and distribution group options. For more information, see Understanding Management Role Assignment Policies.

Role assignment policies consist of the following components that define what users can do with their own mailboxes. Notice that some of the same components also apply to role groups. When used with role assignment policies, these components are limited to enable users to manage only their own mailbox:

- **Management role assignment policy** The *management role assignment policy* is a special object in Exchange 2010. Users are associated with the role assignment policy when their mailboxes are created or if you change the role assignment policy on a mailbox. This is also what you assign end-user management roles to. The combination of all the roles on a role assignment policy defines everything that the user can manage on his or her mailbox or distribution groups.
- **Management role** A *management role* is a container for a grouping of management role entries. Roles are used to define the specific tasks that a user can do with his or her mailbox or distribution groups. A *management role entry* is a cmdlet, script or special permission that enables each specific task in a management role to be performed. You can only use end-user roles with role assignment policies. For more information, see Understanding Management Roles.
- **Management role assignment** A *management role assignment* is the link between a role and a role assignment policy. Assigning a role to a role assignment policy grants the ability to use the cmdlets and parameters defined in the role. When you create a role assignment between a role assignment policy and a role, you can't specify any scope. The scope applied by the assignment is either `Self` or `MyGAL`. All role assignments are scoped to the user's mailbox or distribution groups. For more information, see Understanding Management Role Assignments.

If you want to change what roles are assigned to role assignment policies, you need to change the role assignments that link the role assignment policies to roles. Unless the assignments built into Exchange 2010 don't suit your needs, you won't have to change these assignments. For more information, see Understanding Management Role Assignments.

For more information, see Understanding Management Role Assignment Policies.

Return to top

Direct User Role Assignment

Direct role assignment is an advanced method for assigning management roles directly to a user or USG without using a role group or role assignment policy. Direct role assignments can be useful when you need to provide a granular set of permissions to a specific user and no others. However, using direct role assignments can significantly increase the complexity of your permissions model. If a user changes jobs or leaves the company, you need to manually remove the assignments and add them to the new employee. We recommend that you use role groups to assign permissions to administrators and specialist users, and role assignment policies to assign permissions to users.

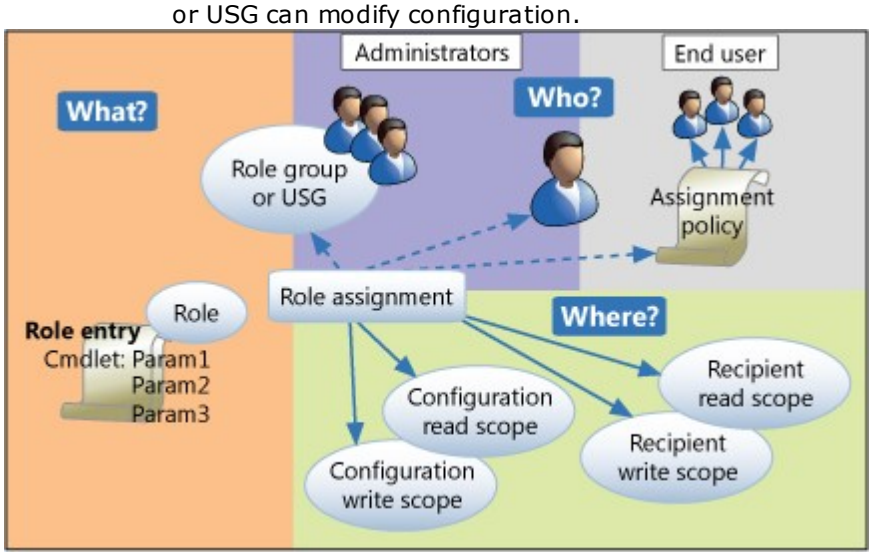
For more information about direct user assignment, see Understanding Management Role Assignments.

Return to top

Summary and Examples

The following figure shows the components in RBAC and how they fit together:

- Role groups:
  - One or more administrators can be members of a role group. They can also be members of more than one role group.
  - The role group is assigned one or more role assignments. These link the role group with one or more administrative roles that define what tasks can be performed.
  - The role assignments can contain management scopes that define where the users of the role group can perform actions. The scopes determine where the users of the role group can modify configuration.
- Role assignment policies:
  - One or more users can be associated with a role assignment policy.
  - The role assignment policy is assigned one or more role assignments. These link the role assignment policy with one or more end-user roles. The end-user roles define what the user can configure on his or her mailbox.
  - The role assignments between role assignment policies and roles have built-in scopes that restrict the scope of assignments to the user's own mailbox or distribution groups.
- Direct role assignment (advanced):
  - A role assignment can be created directly between a user or USG and one or more roles. The role defines what tasks the user or USG can perform.
  - The role assignments can contain management scopes that define where the user or USG can perform actions. The scopes determine where the user or USG can modify configuration.



As shown in the preceding figure, many components in RBAC are related to each other. It's how each component is put together that defines the permissions applied to each administrator or user. The following examples provide some additional context about how role groups and role assignment policies are used in an organization.

Jane the Administrator

Jane is an administrator for the medium-size company, Contoso. She's responsible for

managing the company's recipients in their Vancouver office. When the permissions model for Contoso was created, Jane was made a member of the Recipient Management - Vancouver custom role group. The Recipient Management - Vancouver custom role group most closely matches her job's duties, which include creating and removing recipients, such as mailboxes and contacts, managing distribution group membership and mailbox properties, and similar tasks.

In addition to the Recipient Management - Vancouver custom role group, Jane also needs a role assignment policy to manage her own mailbox's configuration settings. The organization administrators have decided that all users, except for senior management, receive the same permissions when they manage their own mailboxes. They can configure their voice mail, set up retention policies and change their address information. The default role assignment policy provided with Exchange 2010 now reflects these requirements.

Note:

You may have noticed that because Jane is a member of the Recipient Management - Vancouver custom role group, that should give her permissions to manage her own mailbox. This is true; however, the role group doesn't provide her all of the permissions necessary to manage all of the features of her mailbox. The permissions needed to manage voice mail and retention policy settings aren't included in her role group. Those are provided only by the default role assignment policy assigned to her.

To allow for this, consider the role group, which provides Jane's administrative permissions over the recipients in Vancouver:

1. A custom role group called Recipient Management - Vancouver was created. When it was created, the following occurred:
   a. The role group was assigned all of the same management roles that are also assigned to the Recipient Management built-in role group. This gives users added to the Recipient Management - Vancouver custom role group the same permissions as those users added to the Recipient Management role group. However, the following steps limit where they can use those permissions.
   b. The Vancouver Recipients custom management scope was created, which matches only recipients who are located in Vancouver. This was done by creating a scope that filters on a user's city or other unique information.
   c. The role group was created with the Vancouver Recipients custom management scope. This means while administrators added to the Recipient Management - Vancouver custom role group have full recipient management permissions, they can only use those permissions against recipients based in Vancouver.
2. Jane is then added as a member of the Recipient Management - Vancouver custom role group.
   For more information about creating a custom role group, see the following topics:
   a. Create a Role Group
   b. Add a Role to a Role Group
   c. Change the Scope of Role Assignments to a Role Group
   d. Add Members to a Role Group
   To give Jane the ability to manage her own mailbox settings, a role assignment policy needs to be configured with the required permissions.
3. The default role assignment policy is used to provide users with the permissions they need to configure their own mailbox. The following is done to provide these permissions:
   a. All end-user roles are removed from the default role assignment policy, except for: `MyBaseOptions`, `MyContactInformation`, `MyVoicemail` and `MyRetentionPolicies`. `MyBaseOptions` is included because this management role provides the basic user functionality in Microsoft Office Outlook Web App, such as Inbox rules, calendar configuration, and other tasks.

Nothing else needs to be done because Jane is already assigned the default role assignment policy. This means that the changes made to that role assignment policy are immediately applied to her mailbox, and any other mailboxes also assigned to the default role assignment policy.

For more information about customizing the default role assignment policy, see Change the Default Assignment Policy.

Joe the Specialist

Joe works for Contoso, the same company that Jane works for. He's responsible for performing legal discovery, setting the retention policies, and configuring transport rules and journaling for the whole organization. As with Jane, when the permissions model for Contoso was created, Joe was added to the role groups that match his job duties. The Records Management role group provides Joe with the permissions to configure retention policies, journaling, and transport rules. The Discovery Management role group provides him with the ability to perform mailbox searches.

As with Jane, Joe also needs permissions to manage his own mailbox. He is also given the same permissions as Jane: He can set up his voice mail and retention policies, and change his address information.

To give Joe the permissions to perform his job duties, Joe is added to the Records Management and Discovery Management role groups. The role groups don't need to be changed in any way because they already provide him with the permissions he needs, and the management scopes applied to them encompass the entire organization.

For more information about adding a user to a role group, see Add Members to a Role Group.

Joe's mailbox is also assigned the same default role assignment policy that's applied to Jane's mailbox. This gives him all the permissions he needs to manage the features of his mailbox that he's allowed to manage.

Isabel the Vice President

Isabel is the Vice President of Marketing at Contoso. Isabel, as part of the senior leadership team of Contoso, is given more permissions than the average user. This includes the permissions she's provided to manage her mailbox, with one exception: Isabel isn't allowed to manage her own retention policies for legal compliance reasons. Isabel can configure her voice mail, change her contact information, change her profile information, create and manage her own distribution groups, and add or remove herself from existing distribution groups owned by others.

So Isabel is given different permissions on her own mailbox. Most users at Contoso are assigned to the default role assignment policy. Senior leadership, however, is assigned to the Senior Leadership role assignment policy. The following is done to create the custom role assignment policy:

1. A custom role assignment policy called Senior Leadership is created. The role assignment policy is assigned the `MyBaseOptions`, `MyContactInformation`, `MyVoicemail`, `MyProfileInformation`, `MyDistributionGroupMembership`, and `MyDistributionGroups` roles. `MyBaseOptions` is included because this role provides the basic user functionality in Outlook Web App, such as Inbox rules, calendar configuration, and other tasks.
2. Isabel is then manually assigned the Senior Leadership role assignment policy.

Isabel's mailbox now has the permissions provided by the Senior Leadership role assignment policy. Any changes made to this role assignment policy are automatically applied to her mailbox, and any other mailboxes also assigned to the same role

assignment policy.

Return to top

For More Information

Add an Assignment Policy

Change the Assignment Policy on a Mailbox

Add a Role to an Assignment Policy

1.3.1.1.1 Understanding Management Role Groups

Understanding Management Role Groups

Permissions > Understanding Permissions > Understanding Role Based Access Control >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-16*

A *management role group* is a universal security group (USG) used in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. A management role group simplifies the assignment of management roles to a group of users. All members of a role group are assigned the same set of roles. Role groups are assigned administrator and specialist roles that define major administrative tasks in Exchange 2010 such as organization management, recipient management, and other tasks. Role groups enable you to more easily assign a broader set of permissions to a group of administrators or specialist users.

Note:

This topic focuses on advanced RBAC functionality. If you want to manage basic Exchange 2010 permissions, such as using the Exchange Control Panel (ECP) to add and remove members to and from role groups, create and modify role groups, or create and modify role assignment policies, see Understanding Permissions.

Contents

Note:

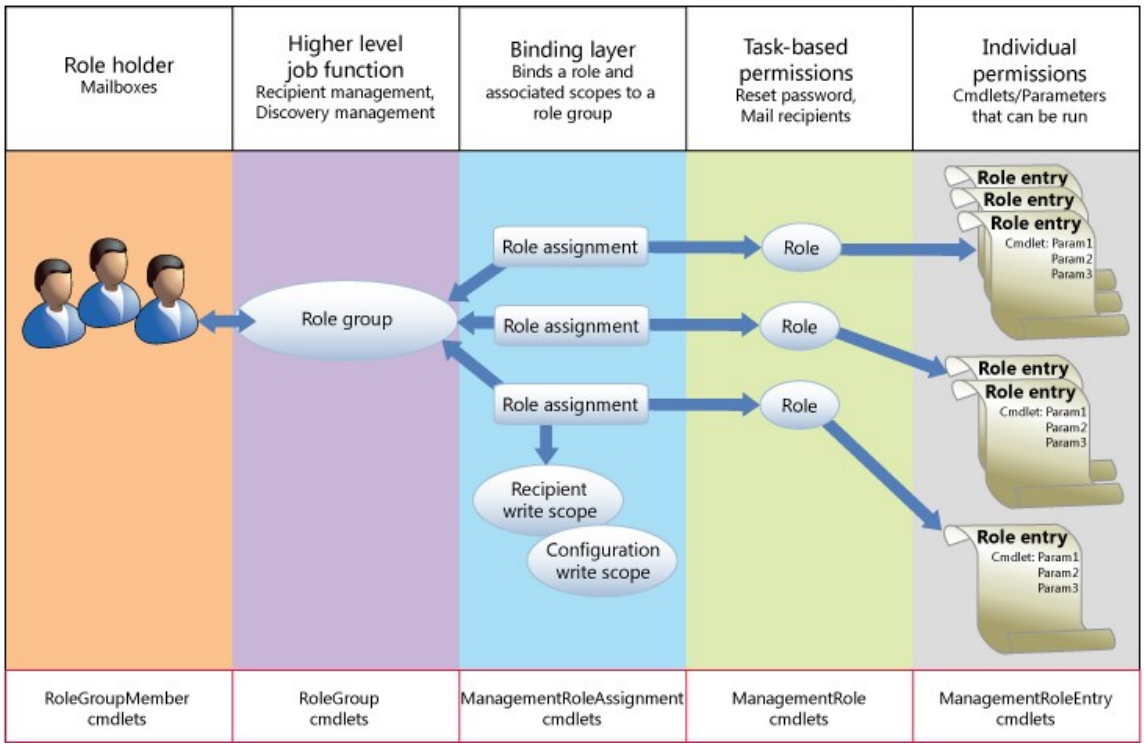
If you want to assign permissions to users to manage their own mailbox or distribution groups, see Understanding Management Role Assignment Policies.

Role Group Layers

The following are the layers that make up the role group model:

- **Role holder** A *role holder* is a mailbox that can be added as a member of a role group. When a mailbox is added as a member of a role group, the assignments that have been made between management roles and a role group are applied to the mailbox. This grants the mailbox all of the permissions provided by the management roles.
- **Management role group** The *management role group* is a special USG that contains mailboxes that are members of the role group. This is where you add and remove members, and it's also what management roles are assigned to. The combination of all the roles on a role group defines everything that users added to a role group can manage in the Exchange organization.
- **Management role assignment** A *management role assignment* links a management role and a role group. Assigning a management role to a role group grants members of the role group the ability to use the cmdlets and parameters defined in the management role. Role assignments can use management scopes to control where the assignment can be used. For more information, see Understanding Management Role Assignments.
- **Management role scope** A *management role scope* is the scope of influence or impact on a role assignment. When a role is assigned with a scope to a role group, the management scope targets specifically what objects that assignment is allowed to manage. The assignment, and its scope, are then given to the members of the role group, which restricts what those members can manage. A scope can be made up of lists of servers or databases, organizational units, or filters on server, database or recipient objects. For more information, see Understanding Management Role Scopes.
- **Management role** A *management role* is a container for a grouping of management role entries. Roles are used to define the specific tasks that can be performed by the members of a role group assigned the role. For more information, see Understanding Management Roles.
- **Management role entries** *Management role entries* are the individual entries on a management role that provide access to cmdlets, scripts, and other special permissions that enable access to perform a specific task. Most often, role entries consist of a single cmdlet and the parameters that can be accessed by the management role, and therefore the role group to which the role is assigned.

The following figure shows each of the role group layers in the preceding list and how each of the layers relates to the other.



For more information about RBAC, see Understanding Role Based Access Control.

Return to top

Role Group Management

When you create a role group, you create the USG that holds the members of the role group, and you create the assignments between the role group and the management roles you specify. Optionally, you can also specify a management scope to apply to the role assignments, and you can add any mailboxes that you want to be members of the new role group.

After you create a role group, each layer becomes an independent object. The role group continues to be the central point at which all of the layers are joined together, however, each layer is managed individually. For example, to modify the management scope that you applied to the role group when it was created, you need to change the scope on each individual role assignment after the role group is created. The management of the role group model is performed using the cmdlets that manage the individual layers of the role group model.

The following table lists the role group layer and the procedural topics that you can use to manage each layer.

Role group management topics

Role group model layer	Management topic
Role holder	Add Members to a Role Group Remove Members from a Role Group
Role group	Create a Role Group

	Change a Linked Foreign USG on a Linked Role Group Add or Remove a Role Group Delegate Remove a Role Group
Management roles and assignments	Add a Role to a Role Group Remove a Role from a Role Group Change the Scope of Role Assignments to a Role Group
Management role entries	Add a Role Entry to a Role Change a Role Entry Remove a Role Entry from a Role **Note:** Changing the management role entries in management roles in a role group is an advanced task and is generally not required in most cases. You may, instead, be able to use a preexisting management role that suits your requirements. For more information, see Built-in Role Groups.

Return to top

Built-in Role Groups

Built-in roles groups are roles shipped with Exchange 2010. They provide you with a set of role groups that you can use to provide varying levels of administrative permissions to groups of users. You can add or remove users to or from any built-in role group. You can also add or remove role assignments to or from most role groups. The only exceptions are the following:

- You can't remove any delegating role assignments from the Organization Management role group.
- You can't remove the Role Management role from the Organization Management role group.

The following table lists all of the built-in role groups included with Exchange 2010. For more information about built-in role groups, see Built-in Role Groups.

Built-in role groups

Role group	Description
Organization Management	Administrators who are members of the Organization Management role group have administrative access to the entire Exchange 2010 organization and can perform almost any task against any Exchange 2010 object.
View-Only Organization Management	Administrators who are members of the View Only Organization Management role

	group can view the properties of any object in the Exchange organization.
Recipient Management	Administrators who are members of the Recipient Management role group have administrative access to create or modify Exchange 2010 recipients within the Exchange 2010 organization.
UM Management	Administrators who are members of the UM Management role group can manage the Unified Messaging (UM) features in the Exchange organization such as Unified Messaging server configuration, UM properties on mailboxes, UM prompts, and UM auto attendant configuration.
Discovery Management	Administrators or users who are members of the Discovery Management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.
Records Management	Users who are members of the Records Management role group can configure compliance features, such as retention policy tags, message classifications, transport rules, and more.
Server Management	Administrators who are members of the Server Management role group have administrative access to Exchange 2010 server configuration. They don't have access to administer Exchange 2010 recipient configuration.
Help Desk	Users who are members of the Help Desk role group can perform limited recipient management of Exchange 2010 recipients.
Hygiene Management	Administrators who are members of the Hygiene Management role group can configure the antivirus and anti-spam features of Exchange 2010. Third-party programs that integrate with Exchange 2010 can add service accounts to this role group to grant those programs access to the cmdlets required to retrieve and configure the Exchange configuration.
Public Folder Management	Administrators who are members of the Public Folder Management role group can manage public folders and databases on Exchange 2010 servers.
Delegated Setup	Administrators who are members of the Delegated Setup role group can deploy previously provisioned Exchange 2010 servers.

Return to top

Linked Role Groups

Linked role groups are used in organizations that install Exchange 2010 in a dedicated resource forest and place users in other, trusted foreign forests. Linked role groups, as the name implies, create a link between a role group in the Exchange forest and a USG in a foreign forest. This is useful when the Active Directory Domain Services (AD DS) user accounts of the administrators you want to administer Exchange don't reside in the same resource forest as Exchange. Linked role groups can only be associated with one foreign USG. Additionally, you don't need to create a two-way trust between the Exchange forest and the foreign forest. The Exchange forest needs to trust the foreign forest but the foreign forest doesn't need to trust the Exchange forest.

For more information about permissions in multiple-forest topologies, see Understanding Multiple-Forest Permissions.

A linked role group consists of two parts:

- **Linked role group** The linked role group is a container object that associates the foreign USG with the management role assignments assigned to the role group.
- **Foreign USG** The foreign USG contains the members that should be granted the permissions provided by the linked role group.

When you create a linked role group, you provide a domain controller in the foreign forest that contains the users you want to manage the Exchange forest and the USG that contains those users as members, the foreign USG name, and the credentials required to access the foreign forest. Exchange adds the security identifier (SID) of the foreign USG to the linked role group. Because the USG SID is the only identification of the foreign USG, we strongly recommend that you specify the foreign forest in the name of the role group if you have multiple foreign forests.

A linked role group doesn't contain any members. All of the members of that role group are managed using the foreign USG. This means you can't use the **Update-RoleGroupMember**, **Add-RoleGroupMember**, or **Remove-RoleGroupMember** cmdlets to add or remove role group members. When you add members to the foreign USG, they are given the permissions provided by the linked role group.

You can't change a standard role group, which contains its own members, to a linked role group and vice versa. If you want to change a role group from a standard role group to a linked role group, you must create a new linked role group and replicate the management role assignments that are present on the standard role group on the linked role group. This is also the case for built-in role groups because they're standard role groups. If you want to perform all of the management of your Exchange forest from a foreign forest, you need to create new linked role groups and add the management roles that exist on the built-in role groups to the new linked role groups. For more information about how to accomplish this, see Create Linked Role Groups that Mirror Built-in Role Groups.

For more information about deploying Exchange in a resource forest, see Deploy Exchange 2010 in an Exchange Resource Forest Topology.

Return to top

Role Group Delegation

By default, members of the Organization Management role group can add and remove members to and from role groups. However, you might want to enable users who aren't

members of the Organization Management role group to add and remove role group members. If so, you can use role group delegation.

Role group delegation is controlled by the **ManagedBy** property on each role group. The **ManagedBy** property contains a list of users who can add and remove members to and from that role group or change the configuration of a role group. The users aren't assigned any permissions given by the role group unless they're also members of the role group.

If the **ManagedBy** property is set on a role group, only those users who are listed as role group managers on that property can modify a role group or the membership of a role group by default. However, an optional parameter on cmdlets that modify role groups or role group membership can override that restriction. The *BypassSecurityGroupManagerCheck* switch can be used by users who are members of the Organization Management role or are assigned, either directly or indirectly, the Role Management management role. When this switch is used, the **ManagedBy** property is ignored and the user can modify the role group or role group membership.

If the **ManagedBy** property isn't set on a role group, only users who are members of the Organization Management role or are assigned, either directly or indirectly, the Role Management management role can modify a role group or role group membership.

Note:

Roles assigned to a role group may be assigned using delegating role assignments. With delegating role assignments, members of a role group that's assigned a delegated role can assign that role to another role group, assignment policy, user, or USG. Members of the role group can assign only that role and can't delegate the role group, unless they're also added to the **ManagedBy** property. For more information about delegated role assignments, see Understanding Management Role Assignments.

For more information about how to manage role group delegation, see Add or Remove a Role Group Delegate.

Return to top

Role Group Membership

When a user is made a member of a role group, the management roles assigned to the role group are assigned to the user. If a user is a member of multiple role groups, the management roles from each role group are aggregated and assigned to the user. Users, USGs, and other role groups can be members of role groups.

Only users who are members of the Organization Management or Role Management role groups and users who have been delegated the ability to add and remove users to or from role groups can manage role group membership.

For more information about how to manage role group membership, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group
- View the Members of a Role Group

Role Group Creation Workflow

As mentioned previously, a role group is made up of several layers. To help you understand what happens when a role group is created, consider the following example, which creates a new role group.

```
New-RoleGroup -Name "Seattle Recipient Management" -Roles "Mail Recipients", "Dis
```

When the preceding command is run, the following happens:

1. A new role group object, which is a special USG, called Seattle Recipient Management is created.
2. The mailboxes for Ray, Jens, Maria, Chris, Maira, Carter, Jesse, Lukas, Isabel, Rick, and Katie are added as members of the role group. These users receive the permissions provided by this role group.
3. The users Brian and David are added to the **ManagedBy** property of the role group. These users can add and remove members to and from the role group but won't be given any permissions provided by the role group because they're not members. Katie is also added to the **ManagedBy** property of the role group. Because she's added to the **ManagedBy** property, and she's a member of the role group, she can add or remove members to and from the role group, and she also receives the permissions provided by the role group.
4. The following management role assignments are created. The role assignments assign each management role specified in the command to the role group. The management scope Seattle Users is added to each role assignment. The name of each role assignment is a combination of the management role being assigned and the role group name.
   4.a. `Mail Recipients_Seattle Recipient Management`
   4.b. `Distribution Groups_Seattle Recipient Management`
   4.c. `Move Mailboxes_Seattle Recipient Management`
   4.d. `UM Mailboxes_Seattle Recipient Management`

If you compare the results of this command to the Management role group layers figure earlier in this topic, you can see where each step correlates to the role group layers. You can then refer to the Management role group management topics shown in "Role Group Management" earlier in this topic to manage each role group layer.

Return to top

1.3.1.1.2 Understanding Management Role Assignment Policies

Understanding Management Role Assignment Policies

Permissions > Understanding Permissions > Understanding Role Based Access Control >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-16*

A *management role assignment policy* is a collection of one or more end-user management roles that enables end users to manage their own Microsoft Exchange Server 2010 mailbox and distribution group configuration. Role assignment policies, which are part of the Role Based Access Control (RBAC) permissions model in Exchange 2010, enable you to control what specific mailbox and distribution group configuration settings your end users can modify. Different groups of users can have role assignment policies specialized to them.

Note:

This topic focuses on advanced RBAC functionality. If you want to manage basic Exchange 2010 permissions, such as using the Exchange Control Panel (ECP) to add and remove members to and from role groups, create and modify role groups, or create and modify role assignment policies, see Understanding Permissions.

For more information about RBAC, see Understanding Role Based Access Control.

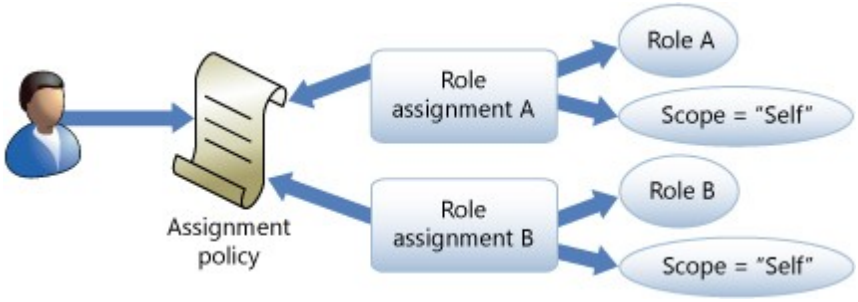
Contents

Role Assignment Policy Layers

The following are the various layers that make up the role assignment policy model:

- **Mailbox** Mailboxes are assigned a single role assignment policy. When a mailbox is assigned a role assignment policy, the assignments between management roles and a role assignment policy are applied to the mailbox. This grants the mailbox all of the permissions provided by the management roles.
- **Management role assignment policy** The *management role assignment policy* is a special object in Exchange 2010. Users are associated with a role assignment policy when their mailboxes are created, or if you change the role assignment policy on a mailbox. This is also what you assign end-user management roles to. The combination of all the roles on a role assignment policy defines everything that the user can manage on his or her mailbox or distribution groups.
- **Management role assignment** A *management role assignment* is the link between a management role and a role assignment policy. Assigning a management role to a role assignment policy grants the ability to use the cmdlets and parameters defined in the management role. When you create a role assignment between a role assignment policy and a management role, you can't specify any scope. The scope applied by the assignment is based on the management role and is either `Self` or `MyGAL`. For more information, see Understanding Management Role Assignments.
- **Management role** A *management role* is a container for a grouping of management role entries. Roles are used to define the specific tasks that a user can do with his or her mailbox or distribution groups. A *management role entry* is a cmdlet, script, or special permission that enables each specific task in a management role to be performed. You can only use end-user management roles with role assignment policies. For more information, see Understanding Management Roles.
- **Management role entry** Management role entries are the individual entries on a management role that determine what cmdlets and parameters are available to the management role and the role group. Each role entry consists of a single cmdlet and the parameters that can be accessed by the management role.

The following figure shows each of the role assignment policy layers in the preceding list and how each of the layers relates to the other.



For more information about management roles, role assignments, and scopes, see Understanding Role Based Access Control.

Return to top

Default and Explicit Role Assignment Policies

The following sections describe the two types of role assignment policies in Exchange 2010.

Default Role Assignment Policy

A default role assignment policy is one assigned to a mailbox when the mailbox is created or moved to a server running Exchange 2010, and a role assignment policy wasn't provided using the *RoleAssignmentPolicy* parameter on the **New-Mailbox** or **Enable-Mailbox** cmdlets.

Exchange 2010 includes a default role assignment policy that provides end users with the permissions most commonly used. You can change the default permissions on the default role assignment policy by adding or removing management roles to or from it.

If you want to replace the built-in default role assignment policy with your own default role assignment policy, you can use the **Set-RoleAssignmentPolicy** cmdlet to select a new default. When you do this, any new mailboxes are assigned the role assignment policy you specified by default if you don't explicitly specify a role assignment policy.

When you change the default role assignment policy, mailboxes assigned the default role assignment policy aren't automatically assigned the new default role assignment policy. If you want to update previously created mailboxes to use the role assignment policy you've set as default, you must use the **Set-Mailbox** cmdlet to do so.

Explicit Role Assignment Policy

An explicit role assignment policy is a policy that you assign to a mailbox manually using the *RoleAssignmentPolicy* parameter on the **New-Mailbox**, **Set-Mailbox**, or **Enable-Mailbox** cmdlets. When you assign an explicit role assignment policy, the new policy takes effect immediately and replaces the previously assigned explicit role assignment policy.

Return to top

Using Role Assignment Policies

Role assignment policies enable you to tailor permissions based on what your business needs your users to be able to configure. If the default role assignment policy meets your needs, you don't need to do any customization. However, if you have many different user groups with specialized needs, you can create role assignment policies for each of them.

The default role assignment policy you use should contain the permissions that apply to your broadest set of users. Then, create role assignment policies for each of your specialized user groups and tailor those role assignment policies to grant more or less restrictive permissions to them. When you organize your role assignment policies this way, you reduce complexity by only explicitly assigning role assignment policies to your specialized users while the majority of your users receive the more common permissions provided by the default role assignment policy.

A mailbox can have only one role assignment policy. All users, including administrators and specialist users, are assigned one role assignment policy. If you want a user to have a different set of permissions, you must assign that user's mailbox another role assignment policy with the required permissions.

Return to top

Role Assignment Policy Management

To add a new role assignment policy, you first create one and decide whether it should be the default role assignment policy. After you create a role assignment policy, you assign management roles to the role assignment policy, and then assign the role assignment policy to mailboxes. You can later choose to add or remove management roles or choose a different role assignment policy to be the default.

The following table lists the role assignment policy layer and the procedural topics that you can use to manage each layer.

Role assignment policy management topics

Role assignment policy model layer	Management topics
Mailbox	Create a Mailbox Change the Assignment Policy on a Mailbox
Role assignment policy	Add an Assignment Policy Remove an Assignment Policy Change the Default Assignment Policy
Management roles and assignments	Add a Role to an Assignment Policy Remove a Role from an Assignment Policy
Management role entries	Add a Role Entry to a Role Change a Role Entry Remove a Role Entry from a Role **Note:** Changing the management role entries in management roles in a role assignment policy is an advanced task and is generally not required in most cases. You may, instead, be able to use a preexisting management role that suits your requirements. For more information, see Built-in Role Groups.

Return to top

1.3.1.1.3 Understanding Management Roles

Understanding Management Roles

Permissions > Understanding Permissions > Understanding Role Based Access Control >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-25*

Management roles are part of the Role Based Access Control (RBAC) permissions model used in Microsoft Exchange Server 2010. Roles act as a logical grouping of cmdlets that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. Management roles can be further combined into larger groupings called management role groups and management role assignment policies, which enable management of feature areas and recipient configuration. Role groups and role assignment policies assign permissions to administrators and end users, respectively. For more information about management role groups and management role assignment policies, see Understanding Role Based Access Control.

Note:

This topic focuses on advanced RBAC functionality. If you want to manage basic Exchange 2010 permissions, such as using the Exchange Control Panel (ECP) to add and remove members to and from role groups, create and modify role groups, or create and modify role assignment policies, see Understanding Permissions.

Contents

Management role scopes and management role assignments are important components for the operation of management roles. For more information about these components, see the following topics:

- Understanding Management Role Scopes
- Understanding Management Role Assignments

Looking for management tasks related to management roles? See Managing Permissions.

Built-in Management Roles

Exchange 2010 provides many built-in management roles that you can use to administer your organization. Each role includes the cmdlets and parameters necessary for users to manage specific Exchange components. The following are examples of some built-in management roles:

- **Mail Recipients** Enables administrators to manage mailboxes, contacts, and mail users.
- **Transport Rules** Enables administrators or specialist users assigned the role to manage the transport rules feature.
- **Distribution Groups** Enables administrators or specialist users assigned the role to manage distribution groups and distribution group members.
- **MyPersonalInformation** Enables end users to modify their own home phone number and Web site address.

For a complete list of the management roles included with Exchange 2010, see Built-in Management Roles.

You can take the built-in roles provided with Exchange 2010 and combine them in any way to create a permissions model that works with your business. For example, if you want members of a role group to manage recipients and public folders, you assign both the Mail Recipients and Public Folders roles to the role group. Most often, you assign roles to role groups or role assignment policies. You can also assign management roles directly to users if you want to control permissions at a granular level. We recommend that you use role groups and role assignment policies rather than direct user role assignment to simplify your permissions model.

Note:
You can only assign end-user management roles to role assignment policies.

Built-in management roles can't be changed. You can, however, create management roles based on the built-in management roles, and then assign those new roles to role groups or role assignment policies. You can then change the new management roles to suit your needs. Doing so is an advanced task that you should rarely, if ever, need to do.

For more information about creating custom roles based on the built-in Exchange roles, see Custom Management Roles later in this topic.

You need to assign management roles for them to take effect. Most often, you assign management roles to role groups and role assignment policies. In certain circumstances, you might also assign roles directly to users, although this is an advanced task that you should rarely, if ever, need to do.

For more information about assigning management roles, see the following topics:

- Add a Role to a Role Group
- Add a Role to an Assignment Policy
- Add a Role to a User or USG

For more information about management role assignments, see Understanding Management Role Assignments.

Return to top

Unscoped Top-Level Management Roles

Unscoped top-level management roles are a special type of management role that enables you to grant access to custom scripts and non-Exchange cmdlets to users using RBAC. Regular management roles provide access only to Exchange cmdlets. If you need to provide access to non-Exchange cmdlets that run on an Exchange server, or if you need to publish a script that can be run by your users, you need to add them to an unscoped role. They're called a top-level role because if an unscoped role is created without deriving

it from a parent role, it has no parent and is a peer of the built-in management roles provided with Exchange 2010. To indicate that you want to create an unscoped top-level role entry, you need to use the *UnscopedTopLevel* switch with the **New-ManagementRole** cmdlet.

Unscoped roles are named as such because, unlike regular management roles, they can't be scoped to a specific target. Unscoped roles are always organization wide. This means that someone assigned an unscoped role can modify any object in the Exchange 2010 organization. For this reason, care must be taken to make sure that scripts and cmdlets made available through an unscoped role are thoroughly tested so that you know what they will modify, and that you carefully assign unscoped roles.

Unscoped roles can be assigned to role assignees such as role groups, management roles, users, and universal security groups (USGs). They can't be assigned to management role assignment policies.

Although Exchange cmdlets can't be added as a management role entry on an unscoped role, they can be included in scripts added as role entries. This enables you to create custom scripts that perform Exchange tasks that you can then assign to users. A useful scenario is where a user must perform a highly privileged task that's normally outside his or her administrative level and where crafting a new management role or role group would be problematic. You can create a script that performs this specific function, add it to an unscoped role, and then assign the unscoped role to the user. The user can then perform only the specific function provided by the script.

The role entries that you add to an unscoped role must also be designated as an unscoped top-level role entry. For more information about unscoped top-level role entries, see Unscoped Top-Level Role Entries later in this topic.

The Organization Management role group doesn't, by default, have permissions to create or manage unscoped role groups. This is to prevent unscoped role groups from mistakenly being created or modified. The Organization Management role group can delegate the Unscoped Role Management management role to itself and other role assignees. For more information about how to create an unscoped top-level management role, see Create an Unscoped Role.

Return to top

Custom Management Roles

You can create custom management roles based on built-in Exchange roles when the built-in management roles don't match the needs of your users. When you create a custom management role, the new child role inherits all of the management role entries of the parent role. You can then choose which management role entries you want to keep in the custom management role and remove all of the entries you don't want.

Custom roles become children of the role used to create the new role. You can only use management role entries in the new child role that exist in the parent role. For more information, see the following sections later in this topic:

- Management Role Hierarchy
- Management Role Entries

Creating custom management roles requires multiple steps and is an advanced task that you should rarely, if ever, need to perform. Before you create a custom management role, make sure one of the existing built-in management roles doesn't provide the permissions you need. For more information about the built-in management roles, or if you want to create custom management roles, see the following topics:

- Built-in Management Roles
- Managing Advanced Permissions

For more information about how to create a management role, see Create a Role.

Return to top

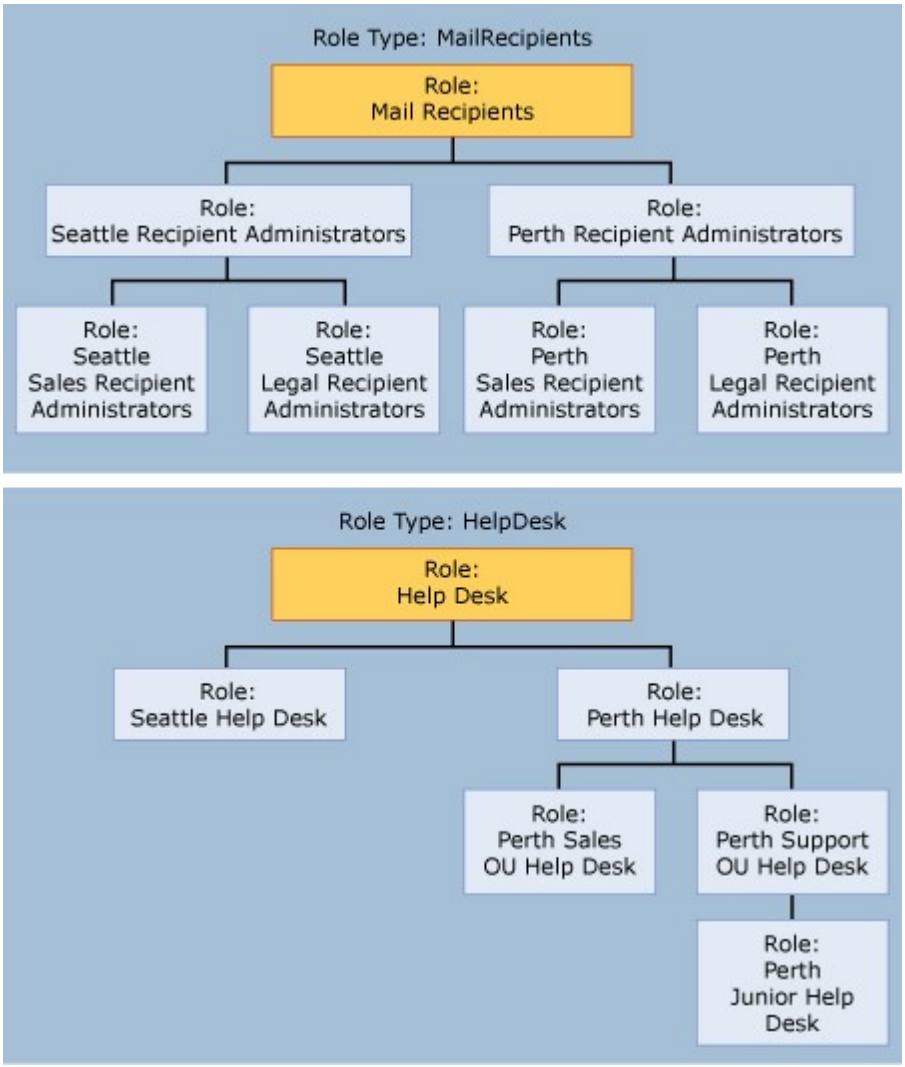
Management Role Hierarchy

Management roles exist in a parent and child hierarchy. At the top of the hierarchy are the built-in management roles provided in Exchange 2010 by default. When you create a role, a copy of a parent role is made. The new role is a child of the role you copied from. You can then customize the new role to suit the needs of the administrators or users you want to assign it to.

Customized roles can be used to create roles. When you create a role from an existing customized role, the existing customized role remains a child of its parent role, but also becomes the parent for the new role. Each time a role is copied, the new child role can contain only the role entries that exist in the immediate parent role.

Each management role is given a role type that can't be changed. The role type defines the base context of use for the role. The role type is copied from the parent role when the child role is created.

Management role hierarchy



The preceding figure illustrates the hierarchical relationship of several management roles. The Mail Recipients and Help Desk roles are built-in roles. All of the child roles derived from these roles inherit the role type of each built-in role. For example, all child roles derived either directly or indirectly from the Mail Recipients role inherit the `MailRecipients` role type.

The Seattle Recipient Administrators custom role is a child of the Mail Recipients built-in role but it's also the parent of the Seattle Sales Recipient Administrators custom role and the Seattle Legal Recipient Administrators custom role. The Seattle Recipient Administrators custom role contains only a subset of cmdlets that are available in the Mail Recipients role. The child roles of the Seattle Recipient Administrators custom role can only contain cmdlets that also exist in that role. For example, if a cmdlet exists in the Mail Recipients role, but the cmdlet doesn't exist in the Seattle Recipient Administrators custom role, the cmdlet can't be added to the Seattle Sales Recipient Administrators custom role.

All of the custom roles follow the same pattern as the roles discussed previously. For more information about how access to cmdlets is controlled on management roles, see Management Role Entries next in this topic.

Return to top

Management Role Entries

Every management role, whether it's a custom Exchange role or an unscoped role, must have at least one management role entry. An entry consists of a single cmdlet and its parameters, a script, or a special permission that you want to make available. If a cmdlet or script doesn't appear as an entry on a management role, that cmdlet or script isn't accessible via that role. Likewise, if a parameter doesn't exist in an entry, the parameter on that cmdlet or script isn't accessible via that role.

Exchange 2010 enables you to manage role entries based on built-in Exchange management top-level roles and role entries based on unscoped top-level management roles. Roles based on built-in Exchange top-level roles can only contain role entries that are Exchange 2010 cmdlets. To add custom scripts or non-Exchange cmdlets so that your users can use them, you need to add them as unscoped role entries to an unscoped top-level role. For more information about unscoped role entries, see Unscoped Top-Level Role Entries later in this topic.

All role entries, regardless of whether the role entry is an Exchange cmdlet-based role entry or an unscoped role entry, adhere to the same principles explained in the following sections.

For more information about managing role entries, see Management Roles and Role Entries.

Parent and Child Management Role Relationship

As mentioned previously, a management role entry, including the cmdlet and its parameters, must exist in the immediate parent role to add the entry to the child role. For example, if the parent role doesn't have an entry for **New-Mailbox**, the child role can't be assigned that cmdlet. Additionally, if **Set-Mailbox** is on the parent role but the *Database* parameter has been removed from the entry, the *Database* parameter on the **Set-Mailbox** cmdlet can't be added to the entry on the child role.

Because you can't add management role entries to child roles if the entries don't appear in parent roles, and because the role is based on a specific role type, you must carefully choose the parent role to copy when you want to create a customized role.

Return to top

Management Role Entry Names

Management role entry names are a combination of the management role that they're associated with, and the name of the cmdlet or script. The role name and the cmdlet or script are separated by a backslash character (\). For example, the role entry name for the **Set-Mailbox** cmdlet on the Mail Recipients role is `Mail Recipients\Set-Mailbox`. If the name of a role entry contains spaces, enclose the entire name in quotation marks (").

The wildcard character (*) can be used in the role entry name to return all of the role entries that match the input you provide. The wildcard character can be used on either side of the backslash character. The following table contains a few variations on how you can use the wildcard character in a role entry name.

Management role entry name with wildcard characters

Example	Description
`*\*`	Returns a list of all role entries for all roles.
`*\Set-Mailbox`	Returns a list of all role entries that contain the **Set-Mailbox** cmdlet.

`Mail Recipients\*`	Returns a list of all role entries on the Mail Recipients role.
`Mail Recipients\*Mailbox`	Returns a list of all role entries on the Mail Recipients role that contain cmdlets that end in Mailbox.
`My*\*Group*`	Returns a list of all role entries that contain the string Group in the cmdlet name for all roles that begin with My.

Unscoped Top-Level Role Entries

Unscoped top-level role entries are used with unscoped top-level management roles to create roles based on custom scripts or non-Exchange cmdlets. Each unscoped role entry is associated with a single custom script or a non-Exchange cmdlet. To indicate that you want to create an unscoped role entry on an unscoped role, you need to specify the *UnscopedTopLevel* parameter on the **Add-ManagementRoleEntry** cmdlet.

When you add the unscoped role entry, you need to specify all of the parameters that can be used with the script or non-Exchange cmdlet. Exchange attempts to verify the parameters that you provide when you add the role entry. Only the parameters that you add to the role entry when it's created will be available to the users assigned to the unscoped role. If you add parameters to the script or non-Exchange cmdlet, or if a parameter is renamed, you must update the role entry manually. Exchange doesn't check whether existing parameters on an unscoped role entry have changed. If a parameter on a role entry changes in a script and you try to use that parameter, the command fails.

Scripts that you add to an unscoped role entry must reside in the Exchange 2010 scripts directory on every server where administrators and users connect using the Exchange Management Shell. If you try to add an unscoped role entry based on a script that doesn't exist in the Exchange 2010 scripts directory on the server you're using to add the role entry, an error occurs. The default installation location of the Exchange 2010 scripts directory is C:\Program Files\Microsoft\Exchange Server\V14\Scripts.

Non-Exchange cmdlets that you add to an unscoped role entry must be installed on every Exchange 2010 server where administrators and users connect using the Shell and want to use the cmdlets. If you try to add an unscoped role entry based on a non-Exchange cmdlet that isn't installed on the Exchange 2010 server you're using to add the role entry, an error occurs. When you add a non-Exchange cmdlet, you must specify the Windows PowerShell snap-in name that contains the non-Exchange cmdlet.

For more information about how to add an unscoped management role entry, see Add a Role Entry to a Role.

Return to top

Management Role Types

Management role types are the foundation of all management roles. Types define the implicit scopes defined on all management roles of a specified role type and also act as a logical grouping of related roles. All management roles derived from the parent built-in management role have the same role type. Refer to the Management role hierarchy figure earlier in this topic for an illustration of this relationship. Management role types also represent the maximum set of cmdlets and their parameters that can be added to a role associated with a role type.

Management role types are split into the following categories:

- **Administrative or specialist** Roles associated with an administrative or specialist role type have a broader scope of impact in the Exchange organization. Roles of this role type enable tasks such as server or recipient management, organization configuration, compliance administration, auditing, and more.
- **User-focused** Roles associated with a user-focused role type have a scope of impact closely tied with an individual user. Roles of this role type enable tasks such as user profile configuration and self management, management of user-owned distribution groups, and more.
  The names of roles associated with user-focused role types and user-focused role type names begin with My.
- **Specialty** Roles associated with specialty role types enable tasks that aren't administrative or user-focused role types. Roles of this role type enable tasks such as application impersonation and the use of non-Exchange cmdlets or scripts.

The following table lists all of the administrative management role types in Exchange 2010 and whether the configuration that's permitted by the role type is applied across the whole Exchange organization or only to an individual server. For more information about each of the management roles associated with these role types, including a description of each role, who may benefit from being assigned the role, and other information, see Built-in Management Roles.

Administrative role types

Management role type	Built-in management role	Description	Organization or server
ActiveDirectoryPermissions	Active Directory Permissions Role	This role type is associated with roles that enable administrators to configure Active Directory permissions in an organization. Some features that use Active Directory permissions or an access control list (ACL) include transport Receive and Send connectors, and Send As and send on behalf permissions for mailboxes. **Note:** Permissions set directly on Active Directory objects may not be enforced through RBAC.	Organization
AddressLists	Address Lists Role	This role type is associated with roles that enable administrators to manage address lists, the global address list (GAL), and offline address lists in an organization.	Organization
ApplicationImpersonation	ApplicationImpersonation Role	This role type is associated with roles that enable applications to impersonate users in an organization to perform tasks on behalf of the user.	Organization
AuditLogs	Audit Logs Role	This role type is associated with roles that enable administrators to manage the administrator audit logging configuration in an	Organization

		organization.	
CmdletExtensionAgents	Cmdlet Extension Agents Role	This role type is associated with roles that enable administrators to manage cmdlet extension agents in an organization.	Organization
DatabaseAvailabilityGroups	Database Availability Groups Role	This role type is associated with roles that enable administrators to manage database availability groups (DAGs) in an organization. Administrators assigned this role either directly or indirectly are the highest level administrators responsible for the high availability configuration in an organization.	Organization
DatabaseCopies	Database Copies Role	This role type is associated with roles that enable administrators to manage database copies on individual servers.	Server
Databases	Databases Role	This role type is associated with roles that enable administrators to create, manage, mount, and dismount mailbox and public folder databases on individual servers.	Server
DisasterRecovery	Disaster Recovery Role	This role type is associated with roles that enable administrators to restore mailboxes and DAGs in an organization.	Organization
DistributionGroups	Distribution Groups Role	This role type is associated with roles that enable administrators to create and manage distribution groups and distribution group members in an organization.	Organization
EdgeSubscriptions	Edge Subscriptions Role	This role type is associated with roles that enable administrators to manage edge synchronization and subscription configuration between Edge Transport servers and Hub Transport servers in an organization.	Organization
EmailAddressPolicies	E-Mail Address Policies Role	This role type is associated with roles that enable administrators to manage e-mail address policies in an organization.	Organization
ExchangeConnectors	Exchange Connectors Role	This role type is associated with roles that enable administrators to manage connectors that aren't Send and Receive connectors in an organization.	Organization

		These connectors include routing group connectors and delivery agent connectors.	
ExchangeServerCertificates	Exchange Server Certificates Role	This role type is associated with roles that enable administrators to create, import, export, and manage Exchange server certificates on individual servers.	Server
ExchangeServers	Exchange Servers Role	This role type is associated with roles that enable administrators to manage Exchange server configuration on individual servers.	Server
ExchangeVirtualDirectories	Exchange Virtual Directories Role	This role type is associated with roles that enable administrators to manage Microsoft Office Outlook Web App, Microsoft ActiveSync, offline address book (OAB), Autodiscover, Windows PowerShell, and Web administration interface virtual directories on individual servers.	Server
FederatedSharing	Federated Sharing Role	This role type is associated with roles that enable administrators to manage cross-forest and cross-organization sharing in an organization.	Organization
InformationRightsManagement	Information Rights Management Role	This role type is associated with roles that enable administrators to manage the Information Rights Management (IRM) features of Exchange in an organization.	Organization
Journaling	Journaling Role	This role type is associated with roles that enable administrators to manage journaling configuration in an organization.	Organization
LegalHold	Legal Hold Role	This role type is associated with roles that enable administrators to configure whether data within a mailbox should be retained for litigation purposes in an organization.	Organization
MailboxImportExport	Mailbox Import Export Role	This role type is associated with roles that enable administrators to import and export mailbox content and to purge unwanted content from a mailbox.	Organization
MailboxSearch	Mailbox Search Role	This role type is associated with roles that enable administrators to search the content of one or	Organization

		more mailboxes in an organization.	
MailEnabledPublicFolders	Mail Enabled Public Folders Role	This role type is associated with roles that enable administrators to configure whether individual public folders are mail-enabled or mail-disabled in an organization. This role type enables you to manage the e-mail properties of public folders only. It doesn't enable you to manage properties of public folders that aren't e-mail properties. To manage properties of public folders that aren't e-mail properties, you need to be assigned a role associated with the PublicFolders role type.	Organization
MailRecipientCreation	Mail Recipient Creation Role	This role type is associated with roles that enable administrators to create mailboxes, mail users, mail contacts, distribution groups, and dynamic distribution groups in an organization. Roles associated with this role type can be combined with roles associated with the MailRecipients role type to enable the creation and management of recipients. This role type doesn't enable you to mail-enable public folders. To mail-enable public folders, you must be assigned a role associated with the MailEnabledPublicFolders role type. If your organization maintains a split permissions model where recipient creation is performed by a different group from the group that performs recipient management, assign the MailRecipientCreation role to the group that performs recipient creation, and the MailRecipients role to the group that performs recipient management.	Organization
MailRecipients	Mail Recipients Role	This role type is associated with roles that enable administrators to manage existing mailboxes, mail users, mail contacts,	Organization

		distribution groups, and dynamic distribution groups in an organization. Roles associated with this role type can't create these recipients but can be combined with roles associated with the MailRecipientCreation role type to enable the creation and management of recipients. This role type doesn't enable you to manage mail-enabled public folders or distribution groups. To manage mail-enabled public folders, you must be assigned a role associated with the MailEnabledPublicFolders role type. To manage distribution groups, you must be assigned a role associated with the DistributionGroups role type. If your organization maintains a split permissions model where recipient creation is performed by a different group from the group that performs recipient management, assign the MailRecipientCreation role to the group that performs recipient creation, and the MailRecipients role to the group that performs recipient management.	
MailTips	Mail Tips Role	This role type is associated with roles that enable administrators to manage MailTips in an organization.	Organization
MessageTracking	Message Tracking Role	This role type is associated with roles that enable administrators to track messages in an organization.	Organization
Migration	Migration Role	This role type is associated with roles that enable administrators to migrate mailboxes and mailbox content into or out of a server.	Server
Monitoring	Monitoring Role	This role type is associated with roles that enable administrators to monitor the Microsoft Exchange services and component availability in an organization. In addition to	Organization

		administrators, roles associated with this role type can be used with the service account used by monitoring applications to collect information about the state of Exchange servers.	
MoveMailboxes	Move Mailboxes Role	This role type is associated with roles that enable administrators to move mailboxes between servers in an organization and between servers in the local organization and another organization.	Organization
OrganizationClientAccess	Organization Client Access Role	This role type is associated with roles that enable administrators to manage Client Access server settings in an organization.	Organization
OrganizationConfiguration	Organization Configuration Role	This role type is associated with roles that enable administrators to manage organization-wide settings in an organization. Organization configuration that can be controlled with this role type include the following and more: • Whether MailTips are enabled or disabled for the organization. • The URL for the managed folder home page. • The Microsoft Exchange recipient SMTP address and alternate e-mail addresses. • The resource mailbox property schema configuration. • The Help URLs for the Exchange Management Console and Outlook Web App. This role type doesn't include the permissions included in the OrganizationClientAccess or OrganizationTransportSettings role types.	Organization
OrganizationTransportSettings	Organization Transport Settings Role	This role type is associated with roles that enable administrators to manage organization-wide	Organization

		transport settings, such as system messages, site configuration, and other organization-wide transport settings in an organization. This role doesn't enable you to create or manage transport Receive or Send connectors, queues, hygiene, agents, remote and accepted domains, or rules. To create or manage each of the transport features, you must be assigned roles associated with the following role types: • **Receive connectors** ReceiveConnectors • **Send connectors** SendConnectors • **Transport queues** TransportQueues • **Transport hygiene** TransportHygiene • **Transport agents** TransportAgents • **Remote and accepted domains** RemoteAndAcceptedDomains • **Transport rules** TransportRules	
POP3AndIMAP4Protocols	POP3 and IMAP4 Protocols Role	This role type is associated with roles that enable administrators to manage POP3 and IMAP4 configuration, such as authentication and connection settings, on individual servers.	Server
PublicFolderReplication	Public Folder Replication Role	This role type is associated with roles that enable administrators to start and stop public folder replication in an organization.	Organization
PublicFolders	Public Folders Role	This role type is associated with roles that enable administrators to manage public folders in an organization. This role type doesn't enable you to manage whether public folders are mail-enabled or manage public folder replication. To mail-enable or disable a public folder, you must be assigned a role associated with the	Organization

		MailEnabledPublicFolders role type. To configure public folder replication, you must be assigned a role associated with the PublicFolderReplication role type.	
ReceiveConnectors	Receive Connectors Role	This role type is associated with roles that enable administrators to manage transport Receive connector configuration, such as size limits on an individual server.	Server
RecipientPolicies	Recipient Policies Role	This role type is associated with roles that enable administrators to manage recipient policies, such as provisioning policies, in an organization.	Organization
RemoteAndAcceptedDomains	Remote and Accepted Domains Role	This role type is associated with roles that enable administrators to manage remote and accepted domains in an organization.	Organization
RetentionManagement	Retention Management Role	This role type is associated with roles that enable administrators to manage retention policies in an organization.	Organization
RoleManagement	Role Management Role	This role type is associated with roles that enable administrators to manage management role groups, role assignment policies, management roles, role entries, assignments, and scopes in an organization. Users assigned roles associated with this role type can override the **role group managed by** property, configure any role group, and add or remove members to or from any role group.	Organization
SecurityGroupCreationAndMembership	Security Group Creation and Membership Role	This role type is associated with roles that enable administrators to create and manage USGs and their memberships in an organization. If your organization maintains a split permissions model where USG creation and management is performed by a different group from the group that manages Exchange servers,	Organization

		assign roles associated with this role type to that group.	
SendConnectors	Send Connectors Role	This role type is associated with roles that enable administrators to manage transport Send connectors in an organization.	Organization
SupportDiagnostics	Support Diagnostics Role	This role type is associated with roles that enable administrators to perform advanced diagnostics under the direction of Microsoft support services in an organization. **Caution:** Roles associated with this role type grant permissions to cmdlets and scripts that should only be used under the direction of Microsoft Customer Service and Support.	Organization
TransportAgents	Transport Agents Role	This role type is associated with roles that enable administrators to manage transport agents in an organization.	Organization
TransportHygiene	Transport Hygiene Role	This role type is associated with roles that enable administrators to manage antivirus and anti-spam features in an organization.	Organization
TransportQueues	Transport Queues Role	This role type is associated with roles that enable administrators to manage transport queues on an individual server.	Server
TransportRules	Transport Rules Role	This role type is associated with roles that enable administrators to manage transport rules in an organization.	Organization
UMMailboxes	UM Mailboxes Role	This role type is associated with roles that enable administrators to manage the Unified Messaging (UM) configuration of mailboxes and other recipients in an organization.	Organization
UMPrompts	UM Prompts Role	This role type is associated with roles that enable administrators to create and manage custom UM voice prompts in an organization.	Organization
UnifiedMessaging	Unified Messaging Role	This role type is associated with roles that enable administrators to manage Unified Messaging servers in an organization.	Organization

		This role doesn't enable you to manage UM-specific mailbox configuration or UM prompts. To manage UM-specific mailbox configuration, use roles associated with the UMMailboxes role type. To manage UM prompts, use the roles associated with the UMPrompts role type.	
UnScopedRoleManagement	Unscoped Role Management Role	This role type is associated with roles that enable administrators to create and manage unscoped top-level management roles in an organization.	Organization
UserOptions	User Options Role	This role type is associated with roles that enable administrators to view the Outlook Web App options of a user in an organization. Roles associated with this role type can be used to help a user with diagnosing problems with his or her configuration.	Organization
ViewOnlyAuditLogs	View-Only Audit Logs Role	This role type is associated with roles that enable administrators to search the administrator audit log in an organization.	Organization
ViewOnlyConfiguration	View-Only Configuration Role	This role type is associated with roles that enable administrators to view all of the non-recipient Exchange configuration settings in an organization. Examples of configuration that are viewable are server configuration, transport configuration, database configuration, and organization-wide configuration. Roles associated with this role type can be combined with roles associated with the ViewOnlyRecipients role type to create a role that can view every object in an organization.	Organization
ViewOnlyRecipients	View-Only Recipients Role	This role type is associated with roles that enable administrators to view the configuration of recipients, such as mailboxes, mail users, mail contacts, distribution groups, and dynamic distribution groups.	Organization

		Roles associated with this role type can be combined with roles associated with the `ViewOnlyConfiguration` role type to create a role that can view every object in the organization.	

The following table lists all of the user-focused management role types and their associated built-in management roles in Exchange 2010.

User-focused role types

Management role type	Built-in user-focused roles	Description
`MyBaseOptions`	MyBaseOptions Role	This role type is associated with roles that enable individual users to view and modify the basic configuration of their own mailbox and associated settings.
`MyContactInformation`	MyAddressInformation Role MyContactInformation Role MyMobileInformation Role MyPersonalInformation Role	This role type is associated with roles that enable individual users to modify their contact information. This information includes their address and phone numbers.
`MyDistributionGroupMembership`	MyDistributionGroupMembership Role	This role type is associated with roles that enable individual users to view and modify their membership in distribution groups in an organization, provided that those distribution groups allow manipulation of group membership.
`MyDistributionGroups`	MyDistributionGroups Role	This role type is associated with roles that enable individual users to create, modify, and view distribution groups and modify, view, remove, and add members to distribution groups they own.
`MyProfileInformation`	MyDisplayName Role MyName Role MyProfileInformation Role	This role type is associated with roles that enable individual users to modify their name.
`MyRetentionPolicies`	MyRetentionPolicies Role	This role type is associated with roles that enable individual users to view their retention tags and view and modify their retention tag

		settings and defaults.
MyTextMessaging	MyTextMessaging Role	This role type is associated with roles that enable individual users to create, view, and modify their text messaging settings.
MyVoiceMail	MyVoiceMail Role	This role type is associated with roles that enable individual users to view and modify their voice mail settings.

Return to top

For More Information

New-ManagementRole

New-ManagementRoleAssignment

Set-ManagementRoleAssignment

New-ManagementScope

Set-ManagementScope

New-ManagementRoleAssignment

Set-ManagementRoleAssignment

1.3.1.1.4 Understanding Management Role Scopes

Understanding Management Role Scopes

Permissions > Understanding Permissions > Understanding Role Based Access Control >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-05*

Management role scopes enable you to define the specific scope of impact or influence of a management role when a management role assignment is created. When you apply a scope, the role assignee assigned to the role can only modify the objects contained within that scope. A role assignee can be a management role group, management role, management role assignment policy, user, or universal security group (USG). For more information about management roles, see Understanding Role Based Access Control.

Every management role, whether built-in or custom, has management scopes. Management scopes can be either of the following:

- **Regular** A *regular scope* isn't exclusive. It determines where, in Active Directory, objects can be viewed or modified by users assigned the management role. In general, a management role indicates what you can create or modify, and a management role scope indicates where you can create or modify. Regular scopes can be either implicit or explicit scopes, both

of which are discussed later in this topic.

- **Exclusive** An *exclusive scope* behaves almost the same as a regular scope. The key difference is that it enables you to deny users access to objects contained within the exclusive scope if those users aren't assigned a role associated with the exclusive scope. All exclusive scopes are explicit scopes, which are discussed later in this topic.
  For more information about exclusive scopes, see Understanding Exclusive Scopes.

Scopes can be inherited from the management role, specified as a predefined relative scope on a management role assignment, or created using custom filters and added to a management role assignment. Scopes inherited from management roles are called *implicit scopes* while predefined and custom scopes are called *explicit scopes*. The following sections describe each type of scope:

- Implicit Scopes
- Explicit Scopes
- Predefined Relative Scopes
- Custom Scopes
  - Recipient Filter Scopes
  - Configuration Scopes

Each role can have the following types of scopes:

- **Recipient read scope** The implicit recipient read scope determines what recipient objects the user assigned the management role is allowed to read from Active Directory.
- **Recipient write scope** The implicit recipient write scope determines what recipient objects the user assigned the management role is allowed to modify in Active Directory.
- **Configuration read scope** The implicit configuration read scope determines what configuration objects the user assigned the management role is allowed to read from Active Directory.
- **Configuration write scope** The implicit configuration write scope determines what organizational, database, and server objects the user assigned the management role is allowed to modify in Active Directory.

Recipient objects include mailboxes, distribution groups, mail enabled users, and other objects. Configuration objects include servers running Microsoft Exchange Server 2010, and databases located on servers running Exchange. Each type of scope can be either an implicit scope or explicit scope.

Implicit Scopes

Implicit scopes are the default scopes that apply to a management role type. Because implicit scopes are associated with a management role type, all of the parent and child management roles with the same role type also have the same implicit scopes. Implicit scopes apply to both built-in management roles and also to custom management roles. For more information about management roles and management role types, see Understanding Management Roles.

The following tables list all of the implicit scopes that can be defined on management roles.

Implicit scopes defined on management roles

Implicit scopes	Description
`Organization`	If `Organization` is present in the role's recipient write scope, the role can create or modify recipient objects across the Exchange organization.

	If Organization is present in the role's recipient read scope, roles can view any recipient object across the Exchange organization. This scope is used only with recipient read and write scopes.
MyGAL	If MyGAL is present in the role's recipient write scope, the role can view the properties of any recipient within the current user's global address list (GAL). If MyGAL is present in the role's recipient read scope, the role can view the properties of any recipient within the current GAL. This scope is used only with recipient read scopes.
Self	If Self is present in the role's recipient write scope, the role can modify only the properties of the current user's mailbox. If Self is present in the role's recipient read scope, the role can view only the properties of the current user's mailbox. This scope is used only with recipient read and write scopes.
MyDistributionGroups	If MyDistributionGroups is present in the role's recipient write scope, the role can create or modify distribution list objects owned by the current user. If MyDistributionGroups is present in the role's recipient read scope, the role can view distribution list objects owned by the current user. This scope is used only with recipient read and write scopes.
OrganizationConfig	If OrganizationConfig is present in the role's configuration write scope, the role can create or modify any server or database configuration object across the Exchange organization. If OrganizationConfig is present in the role's configuration read scope, the role can view any server or database configuration object across the Exchange organization. This scope is used only with configuration read and write scopes.

None	If None is in a scope, that scope isn't available to the role. For example, a role that has None in the recipient write scope can't modify recipient objects in the Exchange organization.

If a role is assigned to a role assignee and no predefined or custom scopes are specified, the implicit scopes defined on the role are used to control the recipient or organization objects the user can view or modify.

The implicit write scope of a role is always equal to, or less than, the implicit read scope. This means that a role can never modify objects that can't be seen by the scope.

You can't change the implicit scopes defined on management roles. You can, however, override the implicit write scope and configuration scope on a management role. When a predefined relative scope or custom scope is used on a role assignment, the implicit write scope of the role is overridden, and the new scope takes precedence. The implicit read scope of a role can't be overridden and always applies. For more information, see Predefined Relative Scopes and Custom Scopes.

Expand the following table to see a list of all the built-in management roles and their implicit scopes. For more information about each built-in role, see Built-in Management Roles.

Built-in management role implicit scopes

Management role	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Active Directory Permissions	Organization	Organization	OrganizationConfig	OrganizationConfig
Address Lists	Organization	Organization	OrganizationConfig	OrganizationConfig
ApplicationImpersonation	Organization	Organization	None	None
Audit Logs	Organization	Organization	OrganizationConfig	OrganizationConfig
Cmdlet Extension Agents	Organization	Organization	OrganizationConfig	OrganizationConfig
Database Availability Groups	Organization	Organization	OrganizationConfig	OrganizationConfig
Database Copies	Organization	Organization	OrganizationConfig	OrganizationConfig
Databases	Organization	Organization	OrganizationConfig	OrganizationConfig
Disaster Recovery	Organization	Organization	OrganizationConfig	OrganizationConfig
Distribution Groups	Organization	Organization	OrganizationConfig	OrganizationConfig
Edge Subscriptions	Organization	Organization	OrganizationConfig	OrganizationConfig

E-Mail Address Policies	Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Connectors	Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Server Certificates	Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Servers	Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Virtual Directories	Organization	Organization	OrganizationConfig	OrganizationConfig
Federated Sharing	Organization	Organization	OrganizationConfig	OrganizationConfig
Information Rights Management	Organization	Organization	OrganizationConfig	OrganizationConfig
Journaling	Organization	Organization	OrganizationConfig	OrganizationConfig
Legal Hold	Organization	Organization	OrganizationConfig	None
Mail Enabled Public Folders	Organization	Organization	OrganizationConfig	OrganizationConfig
Mail Recipient Creation	Organization	Organization	OrganizationConfig	OrganizationConfig
Mail Recipients	Organization	Organization	OrganizationConfig	OrganizationConfig
Mail Tips	Organization	Organization	OrganizationConfig	OrganizationConfig
Mailbox Import Export	Organization	Organization	OrganizationConfig	OrganizationConfig
Mailbox Search	Organization	Organization	None	None
Message Tracking	Organization	Organization	OrganizationConfig	OrganizationConfig
Migration	Organization	Organization	OrganizationConfig	OrganizationConfig
Monitoring	Organization	Organization	OrganizationConfig	OrganizationConfig
Move Mailboxes	Organization	Organization	OrganizationConfig	OrganizationConfig
MyAddressInformation	Self	Self	OrganizationConfig	OrganizationConfig

MyBaseOptions	Self	Self	OrganizationConfig	OrganizationConfig
MyContactInformation	Self	Self	OrganizationConfig	OrganizationConfig
MyDiagnostics	Self	Self	OrganizationConfig	OrganizationConfig
MyDisplayName	Self	Self	OrganizationConfig	OrganizationConfig
MyDistributionGroupMembership	MyGAL	MyGAL	None	None
MyDistributionGroups	MyGAL	MyDistributionGroups	OrganizationConfig	None
MyMobileInformation	Self	Self	OrganizationConfig	OrganizationConfig
MyName	Self	Self	OrganizationConfig	OrganizationConfig
MyPersonalInformation	Self	Self	OrganizationConfig	OrganizationConfig
MyProfileInformation	Self	Self	OrganizationConfig	OrganizationConfig
MyRetentionPolicies	Self	Self	OrganizationConfig	OrganizationConfig
MyTextMessaging	Self	Self	OrganizationConfig	OrganizationConfig
MyVoiceMail	Self	Self	OrganizationConfig	OrganizationConfig
Organization Client Access	Organization	Organization	OrganizationConfig	OrganizationConfig
Organization Configuration	Organization	Organization	OrganizationConfig	OrganizationConfig
Organization Transport Settings	Organization	Organization	OrganizationConfig	OrganizationConfig
POP3 And IMAP4 Protocols	Organization	Organization	OrganizationConfig	OrganizationConfig
Public Folder Replication	Organization	Organization	OrganizationConfig	OrganizationConfig
Public Folders	Organization	Organization	OrganizationConfig	OrganizationConfig
Receive Connectors	Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Policies	Organization	Organization	OrganizationConfig	OrganizationConfig

Remote and Accepted Domains	Organization	Organization	OrganizationConfig	OrganizationConfig
Retention Management	Organization	Organization	OrganizationConfig	OrganizationConfig
Role Management	Organization	Organization	OrganizationConfig	OrganizationConfig
Security Group Creation and Membership	Organization	Organization	OrganizationConfig	OrganizationConfig
Send Connectors	Organization	Organization	OrganizationConfig	OrganizationConfig
Support Diagnostics	Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Agents	Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Hygiene	Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Queues	Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Rules	Organization	Organization	OrganizationConfig	OrganizationConfig
UM Mailboxes	Organization	Organization	OrganizationConfig	OrganizationConfig
UM Prompts	Organization	Organization	OrganizationConfig	OrganizationConfig
Unified Messaging	Organization	Organization	OrganizationConfig	OrganizationConfig
UnScoped Role Management	Organization	Organization	OrganizationConfig	OrganizationConfig
User Options	Organization	Organization	OrganizationConfig	OrganizationConfig
View-Only Audit Logs	Organization	None	OrganizationConfig	None
View-Only Configuration	Organization	None	OrganizationConfig	None
View-Only Recipients	Organization	None	OrganizationConfig	None

Explicit Scopes

Explicit scopes are scopes that you set yourself to control which objects a management role can modify. Although implicit scopes are defined on a management role, explicit scopes are defined on a management role assignment. This enables the implicit scopes to be applied consistently across all management roles unless you choose to use an overriding explicit scope. For more information about management role assignments, see Understanding Management Role Assignments.

Explicit scopes override the implicit write and configuration scopes of a management role. They don't override the implicit read scope of a management role. The implicit read scope continues to define what objects the management role can read.

Explicit scopes are useful when the implicit write scope of a management role doesn't meet the needs of your business. You can add an explicit scope to include nearly anything you want as long as the new scope doesn't exceed the bounds of the implicit read scope. The cmdlets that are part of a management role must be able to read information about the objects or containers that contain objects for the cmdlets to create or modify objects. For example, if the implicit read scope on a management role is set to `Self`, you can't add an explicit write scope of `Organization` because the explicit write scope exceeds the bounds of the implicit read scope.

For more information, see the following sections:

- Predefined Relative Scopes
- Custom Scopes

Predefined Relative Scopes

Exchange 2010 provides several predefined relative write scopes that you can use to modify scope of a management role. Predefined relative scopes provide an easy way for you to more closely match the needs of your business without having to create custom scopes manually. They're called relative scopes because they're relative to the role assignee to which the associated role assignment is assigned. For example, the `Self` predefined relative scope restricts that write scope to the current user only. The `MyDistributionGroups` predefined relative scope restricts the write scope to the distribution group the current user owns only. Predefined relative scopes can only be used to scope recipient objects. Predefined relative scopes can't be used to scope configuration objects. The following table lists the predefined relative scopes that you can use.

Predefined relative scopes

Implicit scopes	Description
`Organization`	If `Organization` is present in the role's recipient write scope, the role can create or modify recipient objects across the Exchange organization. If `Organization` is present in the role's recipient read scope, roles can view any recipient object across the Exchange organization. This scope is used only with recipient read and write scopes.
`Self`	If `Self` is present in the role's recipient write scope, the role can modify only the properties of the current user's mailbox. If `Self` is present in the role's recipient read scope, the role can view only the properties of the current user's mailbox. This scope is used only with recipient read and write scopes.

MyDistributionGroups	If MyDistributionGroups is present in the role's recipient write scope, the role can create or modify distribution list objects owned by the current user. If MyDistributionGroups is present in the role's recipient read scope, the role can view distribution list objects owned by the current user. This scope is used only with recipient read and write scopes.

Predefined relative scopes are applied when you create a new management role assignment. During the creation of the role assignment, using the **New-ManagementRoleAssignment** cmdlet, you can specify a predefined relative scope using the *RecipientRelativeWriteScope* parameter. When the new role assignment is created, the new predefined role overrides the implicit write scope of the management role. You can't specify a custom recipient scope when you create a role assignment with a predefined relative scope. You can, however, specify a custom configuration scope if needed.

For more information about how to add a management role assignment with a predefined relative scope, see Add a Role to a User or USG.

Custom Scopes

Custom scopes are needed when neither the implicit write scope nor the predefined relative scopes meets the needs of your business. Custom scopes enable you to define at a granular level, the scope to which your management role will be applied. For example, you might want to target a specific organizational unit (OU), a specific type of recipient, or both. Or, you might only want to allow a group of administrators to be able to manage a specific set of mailbox databases.

As with predefined relative scopes, custom scopes override the implicit write and organization configuration scopes defined on management roles. The implicit read scope on management roles continue to apply and the resulting custom scope must not exceed the boundaries of the implicit read scope. You can create the following three types of custom scopes:

- **OU scope** An OU scope, which is the simplest custom scope, is created using the *RecipientOrganizationalUnitScope* parameter on the **New-ManagementRoleAssignment** cmdlet. By specifying an OU scope when a role is assigned, the role assignee assigned the role can modify only recipient objects within that OU. For more information about how to add a management role assignment with an OU scope, see Add a Role to a User or USG.
- **Recipient filter scope** Recipient filter scopes use filters to target specific recipients based on recipient type or other recipient properties such as department, manager, location, and more. For more information, see the Recipient Filter Scopes section.
- **Configuration scope** Configuration scopes use filters or lists to target specific servers based on server lists or filterable properties that can be defined on servers, such as an Active Directory site or a server role. In Exchange 2010 Service Pack 1 (SP1), configuration scopes can also use database scopes to target specific databases based on database lists or filterable database properties. For more information, see the Configuration Scopes section.

Simple and broad or complex and granular recipient and configuration custom scopes can be created by using the **New-ManagementScope** cmdlet. When you create either a recipient or configuration scope, only the recipient, server, or database objects that match

their respective scopes are returned. When these scopes are applied to a role assignment using the **New-ManagementRoleAssignment** or **Set-ManagementRoleAssignment** cmdlets, only the objects that match the scopes can be modified by the role assignees who are assigned the role. After a custom scope has been created, you can't change the scope type. A recipient scope is always a recipient scope and a configuration scope is always a configuration scope.

By default, a custom scope enables a role assignee to access a set of objects that match the scopes you define. However, they don't actively exclude access to other role assignees who aren't also assigned the same or equivalent scope. Any custom scope can access the same objects if the lists or filters on those scopes match the same objects. There might be objects where this behavior isn't wanted, such as in the case of important personnel, such as executives. For these objects, you can define exclusive scopes. Exclusive scopes use filters or lists in the same way as regular scopes but unlike regular scopes, deny access to objects included in the scope to anyone who isn't part of the same or equivalent exclusive scope. For more information about exclusive scopes, see Understanding Exclusive Scopes.

Recipient Filter Scopes

Recipient filter scopes enable you to control which recipient objects role assignees can manage by evaluating one or more properties on a recipient object against a value that you specify in a filter statement. Recipients included in recipient scopes are mailboxes, mail-enabled users, distribution groups and mail contacts. Only the recipients that match the filter you specify can be managed by the role assignees assigned that role assignment. An example of a filter statement is `{ Name -Eq "David" }` where **Name** is the property on the recipient object that's being evaluated and **David** is the value you want to evaluate against the property. The **-Eq** comparison operator indicates that the value stored in the property must be equal to the value that was specified for the filter to be true. If the filter is true, that recipient is included in scope.

Recipient filter scopes are created by specifying the recipient filter to use with the *RecipientRestrictionFilter* parameter on the **New-ManagementScope** cmdlet. By default, the **New-ManagementScope** cmdlet creates regular scopes. If you want to create an exclusive scope, include the *Exclusive* switch along with the *RecipientRestrictionFilter* parameter.

When you create a recipient restriction filter, Exchange evaluates the filter you provided against every recipient object in the organization by default. If you want to limit which recipients the scope evaluates, you can use the *RecipientRoot* parameter along with the *RecipientRestrictionFilter* parameter. The *RecipientRoot* parameter accepts an OU. When you use the *RecipientRoot* parameter, Exchange evaluates only the recipients included in the specified OU against the filter you provided.

When you add a recipient filter scope to a role assignment, specify the name of the recipient scope in the *CustomRecipientWriteScope* parameter on the **New-ManagementRoleAssignment** if you're creating a new role assignment, or the **Set-ManagementRoleAssignment** cmdlet if you're updating an existing role assignment. Each role assignment can have one recipient scope, including predefined relative scopes. You can add one configuration scope to the same role assignment you added a recipient scope to.

For more information about filter syntax and for a full list of filterable recipient properties on recipients, see Understanding Management Role Scope Filters.

Configuration Scopes

The following are the two types of configuration scopes offered in Exchange 2010:

- **Server scopes** There are two types of server scopes, server filter scopes and server list scopes. Server configuration that can be managed if a server object is included in a server scope include Receive connectors, transport queues,

server certificates, virtual directories, and so on.

- **Server filter scopes** Server filter scopes enable you to control which server objects role assignees can manage by evaluating one or more properties on a server object against a value that you specify in a filter statement. To create a server filter scope, use the *ServerRestrictionFilter* parameter on the **New-ManagementScope** cmdlet.
- **Server list scopes** Server list scopes enable you to control which server objects role assignees can manage by defining a list of servers that a role assignee can access. To create a server list scope, use the *ServerList* parameter on the **New-ManagementScope** cmdlet.

- **Database scopes** There are two types of database scopes, database filter scopes and database list scopes. Database configuration that can be managed if a database object is included in a database scope include database quota limits, database maintenance, public folder replication, whether a database is mounted, and so on. In addition to database configuration, database scopes can also be used to control which databases recipients can be created in. Database scopes are available only in Exchange 2010 SP1.
  - **Database filter scopes** Database filter scopes enable you to control which database objects role assignees can manage by evaluating one or more properties on a database object against a value that you specify in a filter statement. To create a database filter scope, use the *DatabaseRestrictionFilter* parameter on the **New-ManagementScope** cmdlet.
  - **Database list scopes** Database list scopes enable you to control which database objects role assignees can manage by defining a list of databases that a role assignee can access. To create a database list scope, use the *DatabaseList* parameter on the **New-ManagementScope** cmdlet.

For more information about filter syntax and for a full list of filterable server and database properties, see Understanding Management Role Scope Filters.

Server and database lists can be defined by specifying each server and database you want to include in their respective scopes. Multiple servers or databases can be specified in their respective scopes by separating the server and database names with commas.

When you add a server or database configuration scope to a role assignment, specify the name of the server or database configuration scope in the *CustomConfigWriteScope* parameter on the **New-ManagementRoleAssignment** cmdlet if you're creating a new role assignment, or the **Set-ManagementRoleAssignment** cmdlet if you're updating an existing role assignment. Each role assignment can only have one configuration scope.

In addition to controlling which databases role assignees can manage, database scopes also enable you to control which databases role assignees can create mailboxes on. This is separate from controlling which recipients a role assignee can manage. If a role assignee has permissions to create a new mailbox, mail-enable an existing user, or move mailboxes, you can further refine their permissions by using database scopes to control the database on which the mailbox is created, or which database a mailbox is moved to. Controlling which recipients a role assignee can manage is done using a recipient scope specified in the *CustomRecipientWriteScope* parameter on the **New-ManagementRoleAssignment** or **Set-ManagementRoleAssignment** cmdlet. Controlling which databases a mailbox can be created on or moved to is controlled using a database scope specified in the *CustomConfigurationWriteScope* parameter on the same cmdlets.

Note:

Automatic mailbox distribution can be controlled using database scopes. For more information, see Understanding Automatic Mailbox Distribution.

Exchange 2010 SP1 features may require either server scopes, database scopes, or both, to be managed. If a feature requires both server and database scopes to be managed, two role assignments must be created and assigned to the role assignee that should

have access to manage the feature. One role assignment should be associated with the server scope, and one role assignment should be associated with the database scope.

Some cmdlets may use configuration scopes that aren't immediately obvious. The following table includes a list of cmdlets and the configuration scopes that you can use to control their usage. For cmdlets included in the recipients feature area, configuration scopes enable you to control on which databases recipients can be created. They don't control which recipients can be managed. The **Required scopes** column can contain the following:

- **Database** To run the cmdlet, the role assignee must be assigned a role assignment with a database scope that includes the database to be managed or the role's implicit configuration write scope must include the database to be managed.
- **Server** To run the cmdlet, the role assignee must be assigned a role assignment with a server scope that includes the server to be managed or the role's implicit configuration write scope must include the server to be managed.
- **Server or database** To run the cmdlet, the role assignee must be assigned a role assignment where either a database scope includes the database being managed, or where a server scope includes the server where the database is located. Or, the role's implicit configuration write scope must contain the database to be managed, or contain the server where the database is located, and the role assignment can't have a custom write scope.
- **Server and database** To run this cmdlet, the role assignee must be assigned two role assignments. The first role assignment must include a database scope that includes the database to be managed. The second role assignment must include a server scope that includes the server where the database is located. The role assignments can have custom configuration scopes defined, or the role assignments can inherit the implicit configuration write scope from the role. To inherit the implicit write scope from the role, the role assignment can't have a custom write scope.

Feature areas and applicable database and server scopes

Feature area	Cmdlet	Required scopes
Databases	**Clean-MailboxDatabase**	Database
Databases	**Dismount-Database**	Database
Databases	**Mount-Database**	Database
Databases	**Move-DatabasePath**	Server and database
Databases	**Remove-MailboxDatabase**	Server or database
Databases	**Remove-PublicFolderDatabase**	Server or database
Databases	**Set-MailboxDatabase**	Database
Databases	**Set-PublicFolderDatabase**	Database
High availability	**Add-DatabaseAvailabilityGroupServer**	Server
High availability	**Add-MailboxDatabaseCopy**	Server
High availability	**Move-ActiveMailboxDatabase**	Server

High availability	**New-DatabaseAvailabilityGroup**	Server
High availability	**Remove-DatabaseAvailabilityGroup**	Server
High availability	**Remove-DatabaseAvailabilityGroupServer**	Server
High availability	**Remove-MailboxDatabaseCopy**	Server or database
High availability	**Resume-MailboxDatabaseCopy**	Server or database
High availability	**Set-DatabaseAvailabilityGroup**	Server
High availability	**Set-MailboxDatabaseCopy**	Server or database
High availability	**Start-DatabaseAvailabilityGroup**	Server
High availability	**Stop-DatabaseAvailabilityGroup**	Server
High availability	**Suspend-MailboxDatabaseCopy**	Server or database
High availability	**Update-MailboxDatabaseCopy**	Server or database
Recipients	**Connect-Mailbox**	Database
Recipients	**Enable-Mailbox**	Database
Recipients	**New-Mailbox**	Database
Recipients	**New-MoveRequest**	Database
Troubleshooting	**Test-MapiConnectivity**	Database

Database scopes and pre-Exchange 2010 SP1 installations

Database scopes are new in Exchange 2010 SP1. The release to manufacturing (RTM) version of Exchange 2010 supports only recipient scopes and server configuration scopes. When you create a new database scope on an Exchange 2010 SP1 server, you'll receive the following warning:

```
WARNING: Database management scopes will only apply when connected to a server ru
Exchange 2010 RTM servers will not apply any roles from a role assignment linked
management scopes will also not be visible to reporting cmdlets (Get-ManagementSc
2010 RTM server.
```

When you create a database scope, it's only applied to users who connect to servers running Exchange 2010 SP1. Users who connect to servers running Exchange 2010 RTM won't have any role assignments associated with database scopes applied to them. This means that any permissions provided by these role assignments won't be granted to users when they connect to Exchange 2010 RTM servers. Database scopes can't be created, removed, modified, or viewed from Exchange 2010 RTM servers.

A database scope can include any database in your Exchange organization. This includes Exchange Server 2007 and Exchange 2010 RTM. This enables you to control which databases, regardless of Exchange version, that users can manage. As with other

database scopes, role assignments associated with database scopes that contain Exchange 2007 and Exchange 2010 RTM databases are only applied to users when they connect to an Exchange 2010 SP1 server.

Users who connect to an Exchange 2010 RTM server can view and modify role assignments associated with database scopes. This includes changing the configuration scope on an existing role assignment to a server scope if it's currently associated with a database scope. However, if the configuration scope on a role assignment is changed to a server scope and a user later wants to change it back to a database scope, or if the user wants to change the configuration scope to another database scope, the user must make the change while connected to an Exchange 2010 SP1 server. Users can only specify server scopes when they change the configuration scope on a role assignment if they're connected to an Exchange 2010 RTM server.

1.3.1.1.4.1 Understanding Management Role Scope Filters

Understanding Management Role Scope Filters

Understanding Permissions > Understanding Role Based Access Control > Understanding Management Role Scopes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role scope filters can be used to define management scopes that are highly customizable. Using scope filters, you can create a scope that matches how you segment your recipients, databases, and servers so that administrators can manage only those objects they should have access to. Scope filters can use nearly any recipient, database, or server object property.

To use management role scope filters, you must be familiar with management role scopes. For more information about management role scopes, see Understanding Management Role Scopes.

Filtered custom scopes in Microsoft Exchange Server 2010 are created by using the **New-ManagementScope** cmdlet. The two types of filtered scopes, recipient and configuration (which consists of server and database scopes), are divided into regular scopes and exclusive scopes. The following list shows which parameter on the **New-ManagementScope** cmdlet to use to create each type of filtered scope:

- **Recipient regular filtered scope** To create this type of filtered scope, use the *RecipientRestrictionFilter* parameter.
- **Recipient exclusive filtered scope** To create this type of filtered scope, use the *RecipientRestrictionFilter* parameter along with the *Exclusive* switch.
- **Server-based configuration regular filtered scope** To create this type of filtered scope, use the *ServerRestrictionFilter* parameter.
- **Server-based configuration exclusive filtered scope** To create this type of filtered scope, use the *ServerRestrictionFilter* parameter along with the *Exclusive* switch.
- **Database-based configuration regular filtered scope** To create this type of filtered scope, use the *DatabaseRestrictionFilter* parameter.
- **Database-based configuration exclusive filtered scope** To create this type of filtered scope, use the *DatabaseRestrictionFilter* parameter along with the *Exclusive* switch.

When you create a filtered custom scope, the scope attempts to match the filter with any objects accessible within the implicit read scope of the management role. If an object is

found, it's included in the results returned by the filter, and the object is made available to the management role by the custom scope. A filter can't return results that are outside of the implicit read scope of the management role.

If you specify a recipient filter using the *RecipientRestrictionFilter* parameter, you can use the *RecipientRoot* parameter to specify an organizational unit (OU) to restrict the filter to. When you specify an OU in the *RecipientRoot* parameter, the recipient filter attempts to match recipients that reside in that OU only, rather than within the entire implicit read scope.

To create a management scope using the filterable properties included in this topic, see Create a Regular or Exclusive Scope.

Filter Syntax

Both recipient and configuration filters use the same syntax to create a filter query. All filter queries must have, at minimum, the following components:

- **Opening bracket** The opening brace ({) indicates the start of the filter query.
- **Property to examine** The property is the value on an object that you want to test. For example, this can be the city or department on a recipient object, an Active Directory site name or server name on a server configuration object, or a database name on a database configuration object.
- **Comparison operator** The comparison operator directs how the query should evaluate the value that you specify against the value that's stored in the property. For example, comparison operators can be **Eq**, which means equal to; **Ne**, which means not equal to; **Like**, which means similar to, and so on. For a full list of operators that you can use in the Exchange Management Shell, see Comparison Operators.
- **Value to compare** The value you specify in the filter query will be compared to the value that's stored in the property you specified. The value you specify must be enclosed in quotation marks ("). If you want to specify a partial string, you can enclose the string you provide in wildcard characters (*) and use a comparison operator that supports wildcard characters, such as **Like**. Any string that contains the partial string will match the filter query.
- **Closing bracket** The closing brace (}) indicates the end of the filter query.

The following components are optional and enable you to create more complex filter queries:

- **Parentheses** As in mathematics, parentheses, ( ), in a filter query enable you to force the order in which an operation occurs. Innermost parentheses are evaluated first and the filter query works outward to the outermost parentheses.
- **Logical operators** Logical operators tie together one or more comparison operations and require the filter query to evaluate the entire statement. For example, logical operators include **And**, **Or**, and **Not**.

When put together, a simple query looks like `{ City -Eq "Vancouver" }`. This filter matches any recipient where the value in the property **City** equals the string "Vancouver".

Another, more complex, query is `{ ((City -Eq "Vancouver") -And (Department -Eq "Sales")) -Or (Title -Like "*Manager*") }`. The filter query is evaluated in the following order:

1. The properties **City** and **Department** are evaluated. Each is set to either `True` or `False`, depending on the values stored in each property.
2. The results of the **City** and **Department** statements are then evaluated. If both are `True`, the entire **And** statement becomes `True`. If one or both are `False`, the entire **And** statement becomes `False`. The following applies:
   - If the **And** statement evaluates as `True`, the entire filter query becomes

`True` because the **Or** operator indicates that one side of the query, or the other, must be `True`. The object is exposed to the role assignment.
- If the **And** statement is `False`, the filter query continues on to evaluate the **Title** property.

3. The **Title** property is then evaluated. It's set to `True` or `False`, depending on the value that's stored in the **Title** property. The following applies:
   - If the **Title** property evaluates as `True`, the entire filter query becomes `True` because the **Or** operator indicates that one side of the query, or the other, must be `True`. The object is exposed to the role assignment.
   - If the **Title** property evaluates as `False`, the entire filter query evaluates as `False`, and the object isn't exposed to the role assignment.

The following table shows an example with values, which indicates when the complex query would evaluate as `True`, and when it would evaluate as `False`.

Complex query

City	Department	Title	Result
Vancouver (True)	Sales (True)	CEO (False)	True because both **City** and **Department** evaluated as True. **Title** isn't evaluated because the filter query conditions are already satisfied.
Seattle (False)	Sales (True)	IT Manager (True)	True because **Title** evaluated as True. The results of the **City** and **Department** comparison are discarded because **Title** evaluated as True, which satisfied the filter query conditions. **Note:** IT Manager matches the filter query because the **Like** comparison operator was used, which matches partial strings when wildcard characters (*) are used in the filter query.
Vancouver (True)	Marketing (False)	Writer (False)	False because **City** and **Department** didn't both evaluate as True, and **Title** also didn't evaluate as True.

Filterable Recipient Properties

You can use almost any property on a recipient object when you create a recipient filter. For a list of filterable recipient properties, see Filterable Properties for the -Filter

Parameter. Although this topic discusses the properties that can be used with the *Filter* parameter on other cmdlets, most of these properties also work with the *RecipientRestrictionFilter* parameter on the **New-ManagementScope** cmdlet.

Filterable Server Properties

You can use the following server properties when you create a management scope with the *ServerRestrictionFilter* parameter:

- **CurrentServerRole**
- **CustomerFeedbackEnabled**
- **DataPath**
- **DistinguishedName**
- **ExchangeLegacyDN**
- **ExchangeLegacyServerRole**
- **ExchangeVersion**
- **Fqdn**
- **Guid**
- **InternetWebProxy**
- **Name**
- **NetworkAddress**
- **ObjectCategory**
- **ObjectClass**
- **ProductID**
- **ServerRole**
- **ServerSite**
- **WhenChanged**
- **WhenChangedUTC**
- **WhenCreated**
- **WhenCreatedUTC**

Filterable Database Properties

You can use the following database properties when you create a management scope with the *DatabaseRestrictionFilter* parameter:

- **AdminDisplayName**
- **AllowFileRestore**
- **BackgroundDatabaseMaintenance**
- **CircularLoggingEnabled**
- **DatabaseCreated**
- **DeletedItemRetention**
- **Description**
- **DistinguishedName**
- **EdbFilePath**
- **EventHistoryRetentionPeriod**
- **ExchangeLegacyDN**
- **ExchangeVersion**
- **Guid**
- **IssueWarningQuota**
- **LogFilePrefix**
- **LogFileSize**
- **LogFolderPath**
- **MasterServerOrAvailabilityGroup**
- **MountAtStartup**
- **Name**
- **ObjectCategory**
- **ObjectClass**

- **PublicFolderDatabase**
- **RetainDeletedItemsUntilBackup**
- **Server**
- **WhenChanged**
- **WhenChangedUTC**
- **WhenCreated**
- **WhenCreatedUTC**

1.3.1.1.4.2 Understanding Exclusive Scopes

Understanding Exclusive Scopes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-06-25*

Exclusive scopes are a special type of explicit management scope that can be associated with management role assignments. Exclusive scopes are designed to enable situations where you have a group of highly valuable objects, such as a CEO mailbox, and you want to tightly control who has access to manage those objects.

A role assignment that has an exclusive scope is called an *exclusive role assignment*.

When you create an exclusive scope, only those who are assigned that exclusive scope, or an equivalent exclusive scope, can modify the objects that match the scope. Role assignees who aren't assigned that exclusive scope, or an equivalent, can't modify the objects that match the scope, even if their own roles have scopes that would otherwise include the objects. Exclusive scopes override any other regular scope that isn't exclusive. This behavior is similar to how a deny access control entry (ACE) on an Active Directory access control list (ACL) functions.

An *equivalent exclusive scope* refers to another exclusive scope that matches some of the same objects as another exclusive scope. The scopes don't have to match the same complete set of objects. Both scopes may be able to modify some, or all, of the objects that match them.

Creating Exclusive Scopes

Exclusive scopes can be created like any other explicit scope. You can specify a prebuilt relative scope; a recipient, database, or server filter; or a database or server list. Unlike regular scopes, which don't take effect until you associate a scope to a management role assignment, the deny aspect of an exclusive scope takes effect immediately. This means that as soon as an exclusive scope is created, the objects contained within that scope are immediately no longer accessible by any user until the role assignment has been created.

After the assignment has been created, the exclusive scope provides access to those assigned the management role and scope. If another equivalent exclusive scope matches the same objects, the role assignment associated with that exclusive scope is still able to access the objects.

For more information about management scope filters, see Understanding Management Role Scope Filters.

Important:
Active Directory replication times should be taken into account when making changes to any management role components, including exclusive scopes.

If you have objects contained within more than one exclusive scope, being assigned to any one of the exclusive scopes provides access to the objects. For more information, see Exclusive and Regular Scope Interaction later in this topic.

Exclusive scopes control only the explicit recipient or configuration write scope of a role assignment. The implicit recipient or configuration read scope of the role assigned to a user or group still applies. This means that the following applies:

- Those assigned a role continue to see objects that match the role's implicit read scope.
- Those assigned other roles may be able to see objects contained within an exclusive scope, if the read scopes of the other roles include the objects. However, the objects can only be modified by those who are assigned a role associated with the exclusive scope.

Exclusive scopes can only be used with administrative or specialist roles and can't be used with end-user roles. For more information about roles, see Understanding Management Roles.

Exclusive and Regular Scope Interaction

The figure at the end of this section illustrates how exclusive scopes interact with each other, and with regular scopes. The users in the figure all have the following attributes associated with them.

User	City	Title	Department
Terry	Vancouver	Accountant	Accounting
David	Vancouver	Writer	Marketing
Walter	Vancouver	Manager	Marketing
Bob	Vancouver	CEO	Board
Christine	Vancouver	President	Board
Fred	Vancouver	CFO	Executives
Martin	Vancouver	CIO	Executives
Kim	Vancouver	Vice President, Operations	Executives
Jennifer	Vancouver	Vice President, Technology	Executives

The following three management role assignments in the figure manage the users in the preceding table. Each has an associated scope, some of which are exclusive scopes.

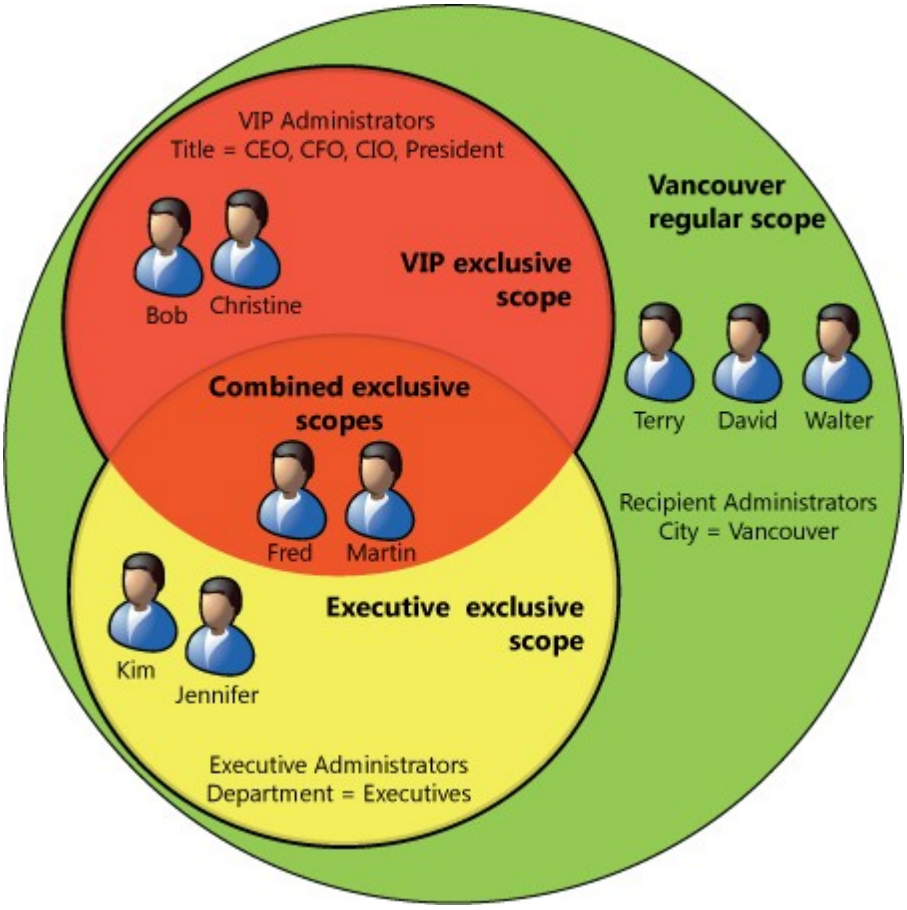
Role assignment	Scope filter	Exclusive or regular
Recipient Administrators	City = Vancouver	Regular
VIP Administrators	Title = CEO or CFO or CIO or President	Exclusive
Executive Administrators	Department = Executives	Exclusive

The Recipient Administrators role assignment has a scope that matches all of the users because every user is located in Vancouver. Without any exclusive scopes, this would mean that the Recipient Administrators role assignment could manage any of the users. However, this organization has created two exclusive scopes: VIP Administrators and Executive Administrators. These exclusive scopes restrict who can manage the users that match their respective scope filters. The VIP Administrators role assignment has a scope filter that matches any user who has a title of CEO, CFO, CIO, or President. The Executive Administrators role assignment has a scope filter that matches any user who is in the Executives department.

When the regular and exclusive scopes are evaluated, the following is the result:

- The Recipient Administrators role assignment can manage the users Terry, David, and Walter. This role assignment can't manage any of the other users because they match the exclusive scope filters of the VIP Administrators and Executive Administrators role assignments.
- The VIP Administrators role assignment can manage the users Bob, Christine, Fred, and Martin. This is because the exclusive scope filter associated with this role assignment matches the attributes on these objects. This role assignment can't manage the users Kim and Jennifer because their attributes don't match this exclusive scope.
- The Executive Administrators role assignment can manage the users Kim, Jennifer, Fred, and Martin. This is because the exclusive scope filter associated with this role assignment matches the attributes on these objects. This role assignment can't manage the users Bob and Christine because their attributes don't match this exclusive scope.

Notice that Fred and Martin are accessible by both exclusive scopes. This is because the attributes on these users match the filters of both exclusive scopes.



For more information about management scopes, see Understanding Management Role Scopes.

1.3.1.1.5 Understanding Management Role Assignments

Understanding Management Role Assignments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-16*

A *management role assignment*, which is part of the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010, is the link between a management role and a role assignee. A *role assignee* is a role group, role assignment policy, user, or universal security group (USG). A role must be assigned to a role assignee for it to take effect. For more information about RBAC, see Understanding Role Based Access Control.

Note:

This topic focuses on advanced RBAC functionality. If you want to manage basic Exchange 2010 permissions, such as using the Exchange Control Panel (ECP) to add and remove members to and from role groups, create and modify role groups, or create and modify role assignment policies, see Understanding Permissions.

This topic discusses the assignment of roles to role groups and role assignment policies and direct role assignment to users and USGs. It doesn't talk about assignment of role groups or role assignment policies to users. For more information about role groups and role assignment policies, which are the recommended way to assign permissions to users, see the following topics:

- Understanding Management Role Groups
- Understanding Management Role Assignment Policies

You can create the following types of role assignments, which are explained in detail later in this topic:

- Regular and delegating role assignments
- Exclusive role assignments

Managing Role Assignments

When you change role assignments, the changes you make will probably be between role groups and role assignment policies. By adding, removing, or modifying role assignments to or from these role assignees, you can control what permissions are given to your administrators and users, in effect turning on and off management of related features.

You might also want to assign roles directly to users or USGs. This is a more advanced task that enables you to define at a granular level what permissions your users are given. Although this provides you with flexibility, it also increases the complexity of your permissions model. For example, if the user changes jobs, you might need to manually reassign the roles assigned to that user to another user. This is why we recommend that you use role groups and role assignment policies to give permissions to your users. You can assign the roles to a role group or role assignment policy, and then just add or remove members of the role group, or change role assignment policies as needed.

You can add, remove, and enable role assignments, modify the management scope on an existing role assignment, and move role assignments to other role assignees. The process of assigning roles to role groups, role assignment policies, users, and USGs is largely the same for each role assignee. The following are the only exceptions:

- Role assignment policies can only be assigned end-user management roles.
- Role assignment policies can't be assigned delegating role assignments.
- You can't specify a management scope when creating a role assignment to role assignment policies.

For more information about managing role assignments, see the following topics:

- Role groups:
  - Add a Role to a Role Group
  - Remove a Role from a Role Group
  - Change a Role Assignment
  - Change the Scope of Role Assignments to a Role Group
  - Delegate Role Assignments
- Role assignment policies:
  - Add a Role to an Assignment Policy
  - Remove a Role from an Assignment Policy
  - Change a Role Assignment
- Users and USGs:
  - Add a Role to a User or USG
  - Remove a Role from a User or USG
  - Change a Role Assignment
  - Change a Role Scope
  - Delegate Role Assignments

Regular and Delegating Role Assignments

Regular role assignments enable the role assignee to access the management role entries made available by the associated management role. If multiple management roles are assigned to a role assignee, the management role entries from each management role are aggregated and applied. This means that if a role assignee is assigned the Transport Rules and Journaling roles, the roles are combined, and all the associated management role entries are given to the role assignee. If the role assignee is a role group or role assignment policy, the permissions provided by the roles are then given to the users assigned to the role group or role assignment policy. For more information about management roles and role entries, see Understanding Management Roles.

Delegating role assignments doesn't give access to manage features. Delegating role assignments gives a role assignee the ability to assign the specified role to other role assignees. If the role assignee is a role group, any member of the role group can assign the role to another role assignee. By default, only the Organization Management role group has the ability to assign roles to other role assignees. Only the user that installed Exchange 2010 is a member of the Organization Management role group by default. You can, however, add other users to this role group as needed, or create other role groups and assign delegating role assignments to those groups.

Note:

Delegating role assignments enables role assignees to delegate management roles to other role assignees. This doesn't enable users to delegate role groups. For more information about role group delegation, see Understanding Management Role Groups.

If you want a user to be able to manage a feature and assign the role that gives permissions to use the feature to other users, assign the following:

1. A regular role assignment for each management role that grants access to the features that need to be managed.
2. A delegating role assignment for each management role that you allow to be assigned to other role assignees.

The regular and delegating role assignments for a role assignee don't need to be identical. For example, a user is a member of a role group assigned the Transport Rules role using a regular role assignment. This enables the user to manage the Transport Rules feature. However the user isn't assigned a delegating role assignment for the Transport Rules role so the user can't assign this role to other users. However, the user is a member of a role group assigned the Journaling management role using a delegating role assignment. The role group the user is a member of doesn't have a regular role assignment for the Journaling role but because it has a delegating role assignment, the user can assign the role to other role assignees.

Management Scopes

When you create either a regular or delegating management role assignment, you have the option of creating the assignment with a management scope to limit the objects that the user can manipulate. You can create recipient scopes or configuration scopes. Recipient scopes enable you to control who can manipulate mailboxes, mail users, distribution groups, and so on. Configuration scopes enable you to control who can manipulate servers and databases.

Recipient and configuration scopes enable you to segment the management of server, database or recipient objects in your organization. For example, a recipient scope can be added to a role assignment so that administrators in Vancouver can only manage recipients in the same office. A server configuration scope could be added to a different role assignment so that administrators in Sydney can only manage servers in their Active Directory site.

Scopes enable permissions to be assigned to groups of users and enable you to direct

where those administrators can perform their administration. This enables you to create a permissions model that maps to your geographic or organizational boundaries.

You can create an assignment with a predefined scope, or you can add a custom scope to the assignment. Predefined scopes, such as limiting a user to only his or her mailbox or distribution groups, can be applied using options available on the assignment itself. Alternatively, you can create a custom recipient or configuration scope, and then add that scope to the role assignment. Custom scopes give you more granularity over which objects are included in the scope.

You can't specify predefined and custom scopes on the same assignment. You also can't mix exclusive and regular scopes on the same assignment.

Each role assignment can only have one recipient scope and one configuration scope. If you want to apply more than one recipient scope, or one configuration scope, to a role assignee for the same management role, you must create multiple role assignments.

With neither a custom or predefined scope, role assignments are limited to the recipient and configuration scopes that are defined on the role itself. These scopes are called implicit scopes. Any role assignment that doesn't have a predefined or custom scope inherits the implicit scopes from the role it's associated with.

For more information about scopes, see Understanding Management Role Scopes.

Exclusive Role Assignments

Exclusive role assignments are created when you associate an exclusive scope with a role assignment. Exclusive scopes work like regular scopes and enable role assignees to manage recipients that match the exclusive scope. However, unlike regular scopes, all other role assignees are denied the ability to manage the recipient, even if the recipient matches scopes applied to their role assignments. This can be useful when you want to limit who can manage a recipient to a few administrators. Only those specific administrators can manage the recipient, and all other administrators are denied access.

For example, consider the following:

- John is an executive at Contoso. His mailbox matches an exclusive scope called VIP Users, which is associated with the VIP Restricted exclusive assignment.
- John's mailbox is also included in a regular scope called Redmond Users, which is associated with the Redmond Administration regular assignment.
- Bill is an administrator who is associated with the VIP Restricted exclusive assignment.
- Chris is an administrator who is associated with the Redmond Administration regular assignment.

Because John's mailbox matches the VIP Users exclusive scope, only Bill can manage his mailbox. Even though John's mailbox also matches the Redmond Users regular scope, Chris isn't associated with the VIP Restricted exclusive assignment. Therefore, Exchange denies Chris the ability to manage John's mailbox. For Chris to manage John's mailbox, Chris needs to be assigned an exclusive assignment that has an exclusive scope that matches John's mailbox.

For more information, see Understanding Management Role Scopes.

1.3.1.1.6 Built-in Role Groups

Built-in Role Groups

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-09*

Microsoft Exchange Server 2010 includes several management role groups by default. The following built-in role groups provide you with a preconfigured set of roles that you can assign to various administrator and specialist users in your organization.

Note:

Role groups don't control access to end-user mailbox features. To control access to end-user mailbox features, see Understanding Management Role Assignment Policies.

- Organization Management
- View-Only Organization Management
- Recipient Management
- UM Management
- Help Desk
- Hygiene Management
- Records Management
- Discovery Management
- Public Folder Management
- Server Management
- Delegated Setup

For more information about role groups, see Understanding Management Role Groups.

1.3.1.1.6.1 Organization Management

Organization Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Organization Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Administrators that are members of the Organization Management role group have administrative access to the entire Microsoft Exchange Server 2010 organization and can perform almost any task against any Exchange 2010 object, with some exceptions. By default, members of this role group can't perform mailbox searches and management of unscoped top-level management roles. For more information, see the "Delegating Only Role Assignments" section later in this topic.

Important:

The Organization Management role group is a very powerful role and as such, only users or universal security groups (USGs) that perform organizational-level administrative tasks

that can potentially impact the entire Exchange organization should be members of this role group.

This role group is equivalent to the Exchange Organization Administrators role in Exchange Server 2007.

For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

By default, the account that's used to install Exchange 2010 in the organization is added as a member of the Organization Management role group. This account can then add other members to the role group as needed.

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or USGs that are members of this role group.

```
Get-RoleGroupMember "Organization Management"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group

- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

The following are some ways you might want to customize this role:

- **Permissions owner** If the permissions in your organization are controlled by a specific group other than the Exchange administrators, you can create a role group and move the regular and delegating role assignments for the Role Management role to the new role group. Doing so prevents members of the Organization Management role group from managing any RBAC permissions.
- **Active Directory split permissions** If the creation of security principals in your organization, such as user accounts, is controlled by a specific group other than the Exchange administrators, you can create a role group and move the regular and delegating role assignments for the Mail Recipient Creation role and the Security Group Creation and Membership role to the new role group. Doing so prevents members of the Organization Management role group from creating Active Directory objects. They can, however, continue to mail-enable the new Active Directory objects. For more information about split permissions, see Understanding Split Permissions.

Customization Limitations

Any role can be added to or removed from this role group, with the following limitations:

- Every role must have at least one delegating role assignment to a role group or USG before the delegating role assignment can be removed from this role group.
- The Role Management role must have at least one regular role assignment to a role group or USG before the regular role assignment can be removed from this role group.

These limitations are intended to help prevent you from inadvertently locking yourself out of the system. By requiring that at least one delegating role assignment exists between every role and one or more role groups or USGs, you will always be able to assign roles to role assignees. By requiring that at least one regular role assignment exists between the Role Management role and one or more role groups or USGs, you will always be able to configure role groups and role assignments.

Important:

These limitations require that role groups or USGs be the targets of the delegating and regular role assignments. You can't remove a delegating role assignment or the regular assignment for the Role Management role if the last assignment is to a user.

Delegating Only Role Assignments

Some role assignments between the Organization Management role group and management roles, such as Mailbox Search and Unscoped Role Management, are delegating only role assignments. These roles allow access to sensitive or personal information, such as the contents of mailboxes, or enable the creation of powerful unscoped management roles.

Delegating only role assignments enable members of the Organization Management role group only to assign the associated roles to other role groups, management role assignment policies, users, or USGs. Members of the Organization Management role group aren't given, by default, any permissions that the roles provide. This helps avoid accidental exposure to personal information or accidental elevation of privileges.

Members of the Organization Management role group can, however, assign themselves any role, in effect enabling them to perform any task. For example, a member of the Organization Management role group can assign the Mailbox Search role to the

Organization Management role group. After this role assignment is made, members of the Organization Management role group can perform tasks enabled by the Mailbox Search role.

For more information about delegating role assignments, see Understanding Management Role Assignments.

Additional Permissions

The permissions granted to members of the Organization Management role group are primarily determined by the management roles assigned to the role group. However, not all tasks that you need to perform are covered by management roles. Some tasks occur outside of the Exchange management tools, and therefore the RBAC permissions model doesn't apply. For these tasks, permissions are provided by adding the Organization Management role group to the access control lists (ACLs) of certain Active Directory objects.

The following tasks are granted permissions by way of ACLs on Active Directory objects and not by management roles assigned to the Organization Management role group:

- Running DomainPrep and ForestPrep using Setup.exe
- Deploying additional servers in the organization
- Provisioning servers using delegated setup
- Creating, managing, and deleting top level public folders
- Managing permissions of top level public folders

To see all permissions granted to the Organization Management role group by way of ACLs, see Exchange 2010 Deployment Permissions Reference.

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Managemen	Regular	Delegating	Recipient	Recipient	Configurati	Configurati

t role	assignment	assignment	read scope	write scope	on read scope	on write scope
Active Directory Permissions Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Address Lists Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
ApplicationImpersonation Role		X	Organization	Organization	None	None
Audit Logs Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Cmdlet Extension Agents Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Database Availability Groups Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Database Copies Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Databases Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Disaster Recovery Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Distribution Groups Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Edge Subscriptions Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
E-Mail Address Policies Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Connectors Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Server Certificates Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Servers Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Virtual Directories Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Federated Sharing Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Information Rights Management Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Journaling Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Legal Hold Role	X	X	Organization	Organization	OrganizationConfig	None
Mail Enabled Public Folders Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Mail Recipient Creation Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Mail Recipients Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Mail Tips Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Mailbox Import Export Role		X	Organization	Organization	OrganizationConfig	OrganizationConfig
Mailbox Search Role		X	Organization	Organization	None	None
Message Tracking Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Migration Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Monitoring Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Move Mailboxes Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Organization Client Access Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Organization Configuration Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Organization Transport	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Settings Role						
POP3 and IMAP4 Protocols Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Public Folder Replication Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Public Folders Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Receive Connectors Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Policies Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Remote and Accepted Domains Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Retention Management Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Role Management Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Security Group Creation and Membership Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Send Connectors Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Support Diagnostics Role		X	Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Agents Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Hygiene Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Queues Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Transport	X	X	Organizat	Organizat	Organizat	Organizat

Rules Role			ion	ion	ionConfig	ionConfig
UM Mailboxes Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
UM Prompts Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Unscoped Role Management Role		X	Organization	Organization	OrganizationConfig	OrganizationConfig
Unified Messaging Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
User Options Role	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
View-Only Audit Logs Role	X	X	Organization	None	OrganizationConfig	None
View-Only Configuration Role	X	X	Organization	None	OrganizationConfig	None
View-Only Recipients Role	X	X	Organization	None	OrganizationConfig	None
MyBaseOptions Role		X	Self	Self	OrganizationConfig	OrganizationConfig
MyContactInformation Role		X	Self	Self	OrganizationConfig	OrganizationConfig
MyDiagnostics Role		X	Self	Self	OrganizationConfig	OrganizationConfig
MyDistributionGroupMembership Role		X	MyGAL	MyGAL	None	None
MyDistributionGroups Role		X	MyGAL	MyDistributionGroups	OrganizationConfig	None
MyProfileInformation Role		X	Self	Self	OrganizationConfig	OrganizationConfig
MyRetentionPolicies Role		X	Self	Self	OrganizationConfig	OrganizationConfig
MyTextMessaging Role		X	Self	Self	OrganizationConfig	OrganizationConfig

MyVoiceMail Role		X	Self	Self	OrganizationConfig	OrganizationConfig

1.3.1.1.6.2 View-Only Organization Management

View-Only Organization Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The View-Only Organization Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Administrators who are members of the View-Only Organization Management role group can view the properties of any object in the Exchange organization.

This role is equivalent to the Exchange View-Only Administrators role in Microsoft Exchange Server 2007.

For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or universal security groups (USGs) that are members of this role group.

```
Get-RoleGroupMember "View-Only Organization Management"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to

perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Monitoring Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig

View-Only Configuration Role	X		Organization	None	OrganizationConfig	None
View-Only Recipients Role	X		Organization	None	OrganizationConfig	None

1.3.1.1.6.3 Recipient Management

Recipient Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Recipient Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Administrators who are members of the Recipient Management role group have administrative access to create or modify Microsoft Exchange Server 2010 recipients within the Exchange 2010 organization.

This role group is equivalent to the Exchange Recipient Administrators role in Exchange Server 2007.

For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or universal security groups (USGs) that are members of this role group.

```
Get-RoleGroupMember "Recipient Management"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are

listed in the "Management Roles Assigned to this Role Group" section. You can add or remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

If the creation of security principals in your organization, such as user accounts, is controlled by a specific group other than the Exchange administrators, you can create a role group and move the Mail Recipient Creation role and the Security Group Creation and Membership role to the new role group. Doing so prevents members of the Recipient Management role group from creating Active Directory objects. They can, however, continue to mail-enable the new Active Directory objects. For more information about split permissions, see Understanding Split Permissions.

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following

topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Distribution Groups Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Mail Enabled Public Folders Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Mail Recipient Creation Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Mail Recipients Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Message Tracking Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Migration Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Move Mailboxes Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Policies Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig

1.3.1.1.6.4 UM Management

UM Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The UM Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Administrators who are members of the UM Management role group can manage features in the Exchange organization such as Unified Messaging (UM) server configuration, UM

properties on mailboxes, UM prompts, and UM auto attendant configuration.

For more information about Unified Messaging, see Unified Messaging.

For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or universal security groups (USGs) that are members of this role group.

```
Get-RoleGroupMember "UM Management"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
UM Mailboxes Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
UM Prompts Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Unified Messaging Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig

1.3.1.1.6.5 Help Desk

Help Desk

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Help Desk management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more

information about role groups, see Understanding Management Role Groups.

Users who are members of the Help Desk role group can perform limited recipient management of Microsoft Exchange Server 2010 recipients.

The Help Desk role group, by default, enables members to view and modify the Outlook Web App options of any user in the organization. These options might include modifying the user's display name, address, phone number, and so on. They don't include options that aren't available in Outlook Web App options, such as modifying the size of a mailbox or configuring the mailbox database on which a mailbox is located.

The members of this role group can only modify the Outlook Web App options that the user can modify. This means that if a user can modify his or her display name, a member of the Help Desk role group can also modify that user's display name. However, if another user isn't allowed to modify his or her display name, a member of the Help Desk role group can't modify that user's display name.

Caution:

The limitations on which Outlook Web App options a member of the Help Desk role group can modify are enforced by the Exchange Web interface. If a member of the Help Desk role group has access to the Exchange Management Shell, he or she can modify any Outlook Web App option for any user. You should carefully consider who you make a member of the Help Desk role group and whether they should also be given access to the Shell.

The Help Desk role group doesn't enable any other tasks because there are so many different types of organizations. Instead, you can add management roles to this role group to create a Help Desk role group that matches the needs of your organization. For example, if you want members of the Help Desk role group to be able to manage mailboxes, mail contacts, and mail-enabled users, assign the Mail Recipients management role to this role group. For more information about how to add management roles to this role group, see the "Role Group Customization" section later in this topic.

For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or universal security groups (USGs) that are members of this role group.

```
Get-RoleGroupMember "Help Desk"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or

remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope

User Options Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
View-Only Recipients Role	X		Organization	None	OrganizationConfig	None

1.3.1.1.6.6 Hygiene Management

Hygiene Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Hygiene Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Users who are members of the Hygiene Management role group can configure the antivirus and anti-spam features of Exchange Server 2010. Third-party programs that integrate with Exchange 2010 can add service accounts to this role group to grant those programs access to the cmdlets required to retrieve and configure the Exchange configuration.

For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or universal security groups (USGs) that are members of this role group.

```
Get-RoleGroupMember "Hygiene Management"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or

remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope

ApplicationImpersonation Role	X		Organization	Organization	None	None
Receive Connectors Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Agents Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Hygiene Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
View-Only Configuration Role	X		Organization	None	OrganizationConfig	None
View-Only Recipients Role	X		Organization	None	OrganizationConfig	None

1.3.1.1.6.7 Records Management

Records Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Records Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Users who are members of the Records Management role group can configure compliance features, such as retention policy tags, message classifications, and transport rules.

For more information about compliance features, see Messaging Policy and Compliance. For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or universal security groups

(USGs) that are members of this role group.

```
Get-RoleGroupMember "Records Management"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server

objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Audit Logs Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Journaling Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Message Tracking Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Retention Management Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Rules Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig

1.3.1.1.6.8 Discovery Management

Discovery Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Discovery Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Administrators or users who are members of the Discovery Management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria and can also configure legal holds on mailboxes. For more information, see Discovery and Understanding Litigation Hold.

Important:

The Organization Management role group doesn't, by default, enable the discovery search feature for users or universal security groups (USGs) that are members of that role group. Members of the Organization Management role group must either be made members of this role group, or the Mailbox Search role listed later in this topic must be manually assigned to the Organization Management role group. For information about how to assign a role to a role group, see Add a Role to a Role Group.

For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or USGs that are members of this role group.

```
Get-RoleGroupMember "Discovery Management"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

Management Roles Assigned to This Role

Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Legal Hold Role	X		Organization	Organization	OrganizationConfig	None
Mailbox Search Role	X		Organization	Organization	None	None

1.3.1.1.6.9 Public Folder Management

Public Folder Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Public Folder Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Administrators who are members of the Public Folder Management role group can manage public folders and databases on servers running Exchange 2010.

For more information about public folders, see Understanding Public Folders. For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or universal security groups (USGs) that are members of this role group.

```
Get-RoleGroupMember "Public Folder Management"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

Additional Permissions

The permissions granted to members of the Public Folder Management role group are primarily determined by the management roles assigned to the role group. However, not all tasks that you need to perform are covered by management roles. This is because some tasks occur outside of the Exchange management tools and therefore the RBAC

permissions model doesn't apply. For these tasks, permissions are provided by adding the Public Folder Management role group to the access control lists (ACLs) of certain Active Directory objects.

The following tasks are granted permissions by way of ACLs on Active Directory objects and not by management roles assigned to the Public Folder Management role group:

- Creation, management, and deletion of top level public folders
- Permissions management of top level public folders

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Mail Enabled Public Folders Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Public Folders Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig

1.3.1.1.6.10 Server Management

Server Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Server Management management role group is one of several built-in role groups

that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Administrators who are members of this role group can configure server-specific configuration of transport, Unified Messaging, client access, and mailbox features such as database copies, certificates, transport queues and Send connectors, virtual directories, and client access protocols.

This role group is similar to the Exchange Server Administrators role in Microsoft Exchange Server 2007. It grants access to manage the configuration of physical servers. However, unlike the Exchange Server Administrators role in Exchange 2007, which provided access only to a local server running Exchange 2007, the Server Management role group enables access to view and configure all Exchange Server 2010 servers in the organization.

If you want to allow administrators to manage only specific servers in your organization, you can change the management scopes that are applied to this role group. Alternatively, you can create a role group, based on the Server Management role group, and customize the management scopes on the new role group. For more information, see the "Role Group Customization" section later in this topic.

For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or universal security groups (USGs) that are members of this role group.

```
Get-RoleGroupMember "Server Management"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Database Copies Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Databases Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Connectors Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Exchange Server Certificates Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Servers Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Exchange Virtual Directories Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Monitoring Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
POP3 and IMAP4 Protocols Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Receive Connectors Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Transport Queues Role	X		Organization	Organization	OrganizationConfig	OrganizationConfig

1.3.1.1.6.11 Delegated Setup

Delegated Setup

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Delegated Setup management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Administrators who are members of the Delegated Setup role group can deploy servers running Exchange 2010 that have been previously provisioned by a member of the Organization Management role group. For more information about delegated setup, see Provision Exchange 2010 Server and Delegate Setup.

Members of the Delegated Setup role group can only deploy Exchange 2010 servers. They can't manage the server after it's been deployed. To manage a server after it's been deployed, a user must be a member of the Server Management role group.

For more information about RBAC, see Understanding Role Based Access Control.

Role Group Membership

If you want to add or remove members to or from this role group, see the following topics:

- Add Members to a Role Group
- Remove Members from a Role Group

By default, only members of the Organization Management role group can add or remove members from this role group. For more information about how to add additional role group delegates, see Add or Remove a Role Group Delegate.

You can use the following command to view a list of users or universal security groups (USGs) that are members of this role group.

```
Get-RoleGroupMember "Delegated Setup"
```

For more information about the members of a role group, see View the Members of a Role Group.

Role Group Customization

This role group is assigned management roles by default. The roles that are included are listed in the "Management Roles Assigned to this Role Group" section. You can add or remove role assignments to or from this role group to match the needs of your organization.

The role groups provided with Exchange 2010 are designed to match more granular tasks. By assigning roles to a role group, you enable the members of that role group to perform the tasks associated with the role. For example, the Journaling role enables the management of the Journaling agent and journaling rules. For more information about how roles are assigned to role groups, see Understanding Management Role Assignments.

The roles assigned to this role group are given default management scopes. Management scopes determine what Exchange objects can be viewed or modified by the members of a role group. You can change the scopes associated with assignments between roles and role groups. For example, you might want to do this if you only want members of a role group to be able to change recipients that are under a specific organizational unit or in a specific location. For more information about management scopes, see Understanding Management Role Scopes.

For more information about how to customize this role group, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Change the Scope of Role Assignments to a Role Group

If you want to create a role group and assign some of the roles that are assigned to this role group to the new role group, see Create a Role Group.

Additional Permissions

The permissions granted to members of the Delegated Setup role group are primarily determined by the management roles assigned to the role group. However, not all tasks that you need to perform are covered by management roles. This is because some tasks occur outside of the Exchange management tools and therefore the RBAC permissions

model doesn't apply. For these tasks, permissions are provided by adding the Delegated Setup role group to the access control lists (ACLs) of certain Active Directory objects.

The following task is granted permissions by way of ACLs on Active Directory objects and not by management roles assigned to the Delegated Setup role group:

- Deployment of servers that have been previously provisioned by a member of the Organization Management role group.

To see all permission granted to the Delegated Setup role group by way of ACLs on Active Directory objects, see Exchange 2010 Deployment Permissions Reference.

Management Roles Assigned to This Role Group

The following table lists all the management roles that are assigned to this role group and the following attributes of each role assignment:

- **Regular assignment** Enables members of the role group to access the management role entries made available by the associated management role.
- **Delegating assignment** Gives members of the role group the ability to assign the specified role to other role groups, role assignment policies, users, or USGs.
- **Recipient read scope** Determines what recipient objects members of the role group are allowed to read from Active Directory.
- **Recipient write scope** Determines what recipient objects members of the role group are allowed to modify in Active Directory.
- **Configuration read scope** Determines what configuration and server objects members of the role group are allowed to read from Active Directory.
- **Configuration write scope** Determines what organizational and server objects members of the role group are allowed to modify in Active Directory.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Management roles assigned to this role group

Management role	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
View-Only Configuration Role	X		Organization	None	OrganizationConfig	None

1.3.1.1.7 Built-in Management Roles

Built-in Management Roles

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-15*

Microsoft Exchange Server 2010 includes many management roles by default. The

following roles are assigned to management role groups or management role assignment policies in various combinations that grant permissions to manage and use the features provided by Exchange 2010. For more information about roles, see Understanding Management Roles.

Active Directory Permissions Role

Address Lists Role

ApplicationImpersonation Role

Audit Logs Role

Cmdlet Extension Agents Role

Database Availability Groups Role

Database Copies Role

Databases Role

Disaster Recovery Role

Distribution Groups Role

Edge Subscriptions Role

E-Mail Address Policies Role

Exchange Connectors Role

Exchange Server Certificates Role

Exchange Servers Role

Exchange Virtual Directories Role

Federated Sharing Role

Information Rights Management Role

Journaling Role

Legal Hold Role

Mail Enabled Public Folders Role

Mail Recipient Creation Role

Mail Recipients Role

Mail Tips Role

Mailbox Import Export Role

Mailbox Search Role

Message Tracking Role

Support Diagnostics Role

Transport Agents Role

Transport Hygiene Role

Transport Queues Role

Transport Rules Role

UM Mailboxes Role

UM Prompts Role

Unified Messaging Role

Unscoped Role Management Role

User Options Role

View-Only Audit Logs Role

View-Only Configuration Role

View-Only Recipients Role

1.3.1.1.7.1 Active Directory Permissions Role

Active Directory Permissions Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Active Directory Permissions` management role enables administrators to configure Active Directory permissions in an organization. Some features that use Active Directory permissions or an access control list (ACL) include transport Receive and Send connectors, and Send As and Send on behalf of permissions for mailboxes.

Note:

Permissions set directly on Active Directory objects may not be enforced through Role Based Access Control (RBAC).

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.2 Address Lists Role

Address Lists Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Address Lists` management role enables administrators to create, modify, view, and remove address lists, global address lists (GALs), and offline address lists (OABs) in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment

should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.3 ApplicationImpersonation Role

ApplicationImpersonation Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `ApplicationImpersonation` management role enables applications to impersonate users in an organization to perform tasks on behalf of the user.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a

cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:
There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in

Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Hygiene Management	X		Organization	Organization	None	None
Organization Management		X	Organization	Organization	None	None

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group

- Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.4 Audit Logs Role

Audit Logs Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Audit Logs` management role enables administrators to configure the administrator audit log in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a

Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Records Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group

- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.5 Cmdlet Extension Agents Role

Cmdlet Extension Agents Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Cmdlet Extension Agents` management role enables administrators to enable, disable, and set the priority of cmdlet extension agents in an organization.

This management role is one of several built-in roles in the Role Based Access Control

(RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.

- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.6 Database Availability Groups Role

Database Availability Groups Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Database Availability Groups` management role enables administrators to manage database availability groups in an organization. Administrators assigned this role either directly or indirectly are the highest level administrators responsible for the high availability configuration in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.

- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.7 Database Copies Role

Database Copies Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Database Copies` management role enables administrators to add, remove, suspend, resume, view, and update database copies on individual servers.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which

are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and

USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Additional Scope Considerations

The **Set-MailboxDatabaseCopy** and **Remove-MailboxDatabaseCopy** cmdlets, which are included with this role, require that the database you want to configure or remove must be within the database scope and the database must reside on a server that's within the server scope. For more information about scopes, see Understanding Management Role Scopes.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the

following topics:
- Change a Role Entry
- Remove a Role Entry from a Role

3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.8 Databases Role

Databases Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Databases management role enables administrators to create, manage, mount, and dismount mailbox and public folder databases on individual servers.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the

combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what

objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Additional Scope Considerations

The **Move-DatabasePath** cmdlet, which is included with this role, requires that the database you want to configure must be within the database scope and the database must reside on a server that's within the server scope.

Also, the **Remove-MailboxDatabase** and **Remove-PublicFolderDatabase** cmdlets, which are also included with this role, require that the database you want to remove must either be within the database scope or the database must reside on a server that's within the server scope. This means you control who can remove mailbox or public folder databases using either database or server scopes.

For more information, see the following topics:

- Understanding Management Role Scopes
- Understanding Automatic Mailbox Distribution

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in

Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group

- Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.9 Disaster Recovery Role

Disaster Recovery Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Disaster Recovery` management role enables administrators to restore mailboxes and database availability groups, create mailbox databases, and start and stop database availability groups in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a

Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:
The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.10 Distribution Groups Role

Distribution Groups Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Distribution Groups` management role enables administrators to create, modify, view, and remove distribution groups, and add or remove distribution group members in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or

scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

This limitation helps prevent you from locking yourself out of the system.

Important:
There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.

- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Management	X	Not applicable	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following

topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.11 Edge Subscriptions Role

Edge Subscriptions Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Edge Subscriptions` management role enables administrators to manage edge synchronization and subscription configuration between Edge Transport servers and Hub Transport servers in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.

- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.12 E-Mail Address Policies Role

E-Mail Address Policies Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `E-Mail Address Policies` management role enables administrators to manage e-mail address policies in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which

are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and

USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what

configuration and server objects the role assignee is allowed to read from Active Directory.

- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group

- Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.13 Exchange Connectors Role

Exchange Connectors Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Exchange Connectors management role enables administrators to create, modify, view, and remove routing group connectors and delivery agent connectors.

This role can't be used to manage Send and Receive connectors. To manage Send and Receive connectors, use the Send Connectors and Receive Connectors roles. For more information, see:

- Send Connectors Role
- Receive Connectors Role

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions

granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope

- Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of

this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.14 Exchange Server Certificates Role

Exchange Server Certificates Role

Understanding Permissions > Understanding Role Based Access Control > Built-in Management Roles >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Exchange Server Certificates` management role enables administrators to create, import, export, and manage Exchange server certificates on individual servers.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee

the ability to assign this role to role groups, users, or USGs.

- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role

3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.15 Exchange Servers Role

Exchange Servers Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Exchange Servers management role enables administrators to do the following on individual servers:

- Add and remove database availability groups
- Enable and disable Unified Messaging servers
- Enable and disable Microsoft Outlook Anywhere on Client Access servers
- Modify Mailbox, Hub Transport, Client Access, and Unified Messaging server configuration
- Modify Outlook Anywhere configuration on Client Access servers
- Modify content filtering configuration on Hub Transport servers
- Modify general Exchange server configuration
- View the configuration for each server role

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group

- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organizatio	X	X	Organizat	Organizat	Organizat	Organizat

n Management			ion	ion	ionConfig	ionConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.16 Exchange Virtual Directories Role

Exchange Virtual Directories Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Exchange Virtual Directories` management role enables administrators to manage Microsoft Office Outlook Web App, Microsoft ActiveSync, offline address books (OABs), Autodiscover, Windows PowerShell, and Web administration interface virtual directories on individual servers.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.17 Federated Sharing Role

Federated Sharing Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Federated Sharing` management role enables administrators to manage cross-forest and cross-organization sharing in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are

included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to

add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.18 Information Rights Management Role

Information Rights Management Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Information Rights Management` management role enables administrators to manage the Information Rights Management (IRM) features of Exchange in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the

following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your

permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.19 Journaling Role

Journaling Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Journaling` management role enables administrators to create, modify, enable, disable, view, and remove journal rules in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries,

see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this

role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Records Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the

role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.20 Legal Hold Role

Legal Hold Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Legal Hold` management role enables administrators to configure whether data within a mailbox should be retained for litigation purposes in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the

following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Additional Scope Considerations

In addition to recipient scopes, the **Enable-Mailbox** cmdlet, which is included with this role, is also scoped using database configuration scopes. Database configuration scopes control which databases the cmdlet can create new mailboxes on. The database where you want to create a mailbox must be within the database scope. This applies both when you specify a database using the *Database* parameter on the **Enable-Mailbox** cmdlet, or if you allow automatic mailbox distribution to select the database for you. For more information, see the following topics:

- Understanding Management Role Scopes
- Understanding Automatic Mailbox Distribution

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Discovery Management	X		Organization	Organization	OrganizationConfig	None
Organization Management	X	X	Organization	Organization	OrganizationConfig	None

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.21 Mail Enabled Public Folders Role

Mail Enabled Public Folders Role

Understanding Permissions > Understanding Role Based Access Control > Built-in Management Roles >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Mail Enabled Public Folders` management role enables administrators to configure whether individual public folders are mail-enabled or mail-disabled in an organization.

This role enables you to manage only the e-mail properties of public folders. It doesn't enable you to manage public folder properties that aren't related to e-mail. To manage public folder properties that aren't related to e-mail, use the `Public Folders` role. For more information, see Public Folders Role.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role

assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Public Folder Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your

permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.22 Mail Recipient Creation Role

Mail Recipient Creation Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Mail Recipient Creation` management role enables administrators to create mailboxes, mail users, mail contacts, distribution groups, and dynamic distribution groups in an organization. This role can be combined with the `Mail Recipients` role to enable the creation and management of recipients. For more information, see Mail Recipients Role.

This role doesn't enable you to mail-enable public folders. To mail-enable public folders, the `Mail Enabled Public Folders` role must be used. For more information, see Mail Enabled Public Folders Role.

If your organization maintains a Role Based Access Control (RBAC) split permissions model where recipient creation is performed by a different group than those who perform

recipient management, assign the `Mail Recipient Creation` role to the management role group that performs recipient creation, and the `Mail Recipients` role to the role group that performs recipient management.

If your organization has enabled Active Directory split permissions, all non-delegating management role assignments to this management role were removed. When Active Directory split permissions is enabled, only Active Directory administrators using Active Directory management tools can create new security principals such as users and security groups.

For more information about RBAC and Active Directory split permissions, see Understanding Split Permissions.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role

assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Additional Scope Considerations

In addition to recipient scopes, the **New-Mailbox** cmdlet, which is included with this role, is also scoped using database configuration scopes. Database configuration scopes control which databases the cmdlet can create new mailboxes on. The database where you want to create a mailbox must be within the database scope. This condition applies when you specify a database using the *Database* parameter on the **New-Mailbox** cmdlet or if you allow automatic mailbox distribution to select the database for you. For more information, see the following topics:

- Understanding Management Role Scopes
- Understanding Automatic Mailbox Distribution

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group

- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.23 Mail Recipients Role

Mail Recipients Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Mail Recipients` management role enables administrators to manage existing mailboxes, mail users, and mail contacts in an organization. This role can't create these recipients. Use the `Mail Recipient Creation` role to create them.

This role type doesn't enable you to manage mail-enabled public folders or distribution groups. Use the following roles to manage these objects:

- Mail Enabled Public Folders Role
- Distribution Groups Role

If your organization has a split permissions model where recipient creation and management are performed by different groups, assign the `Mail Recipient Creation` role to the group that performs recipient creation and the `Mail Recipients` role to the group that performs recipient management. For more information, see the following topics:

- Mail Recipient Creation Role
- Mail Recipients Role
- Understanding Split Permissions

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign

the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Additional Scope Considerations

In addition to recipient scopes, the **Connect-Mailbox** and **Enable-Mailbox** cmdlets, which are included with this role, are also scoped using database configuration scopes. Database configuration scopes control which databases the cmdlets can create new mailboxes on. The database where you want to create a mailbox must be within the database scope. This condition applies when you specify a database using the *Database* parameter on either cmdlet or if you allow automatic mailbox distribution to select the database for you. For more information, see the following topics:

- Understanding Management Role Scopes
- Understanding Automatic Mailbox Distribution

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group

- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.24 Mail Tips Role

Mail Tips Role

Understanding Permissions > Understanding Role Based Access Control > Built-in Management Roles >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Mail Tips management role enables administrators to manage mail tips in an organization.

This management role is one of several built-in roles in the Role Based Access Control

(RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.

- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.25 Mailbox Import Export Role

Mailbox Import Export Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Mailbox Import Export` management role enables administrators to import and export mailbox content and to purge unwanted content from a mailbox.

For information about how to assign this role to a role group, see Managing Mailbox Import and Export Requests.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more

information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-**

ManagementRoleAssignment cmdlet. For more information, see Change a Role Assignment.

- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management		X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group

- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:
The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.26 Mailbox Search Role

Mailbox Search Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Mailbox Search` management role enables administrators to search the content of one or more mailboxes in an organization.

This management role is one of several built-in roles in the Role Based Access Control

(RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.

- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Discovery Management	X		Organization	Organization	None	None
Organization Management		X	Organization	Organization	None	None

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group

- Remove a Role from a User or USG

4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.27 Message Tracking Role

Message Tracking Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Message Tracking` management role enables administrators to track messages in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't

be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment

- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Records Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

Migration Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Migration` management role enables administrators to migrate mailboxes and mailbox content into or out of a server.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role

assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a

role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.29 Monitoring Role

Monitoring Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Monitoring management role enables administrators to monitor Exchange services and component availability in an organization. This role can also be used with service accounts used by monitoring applications to collect information about the state of servers running Exchange.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
View-Only Organization Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following

topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.30 Move Mailboxes Role

Move Mailboxes Role

Understanding Permissions > Understanding Role Based Access Control > Built-in Management Roles >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Move Mailboxes` management role enables administrators to move mailboxes between servers in an organization and between servers in the local organization and another organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.

- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Additional Scope Considerations

In addition to recipient scopes, the **New-MoveRequest** cmdlet, which is included with this role, is also scoped using database configuration scopes. Database configuration scopes control which databases the cmdlet can move mailboxes to. The database where you want to move a mailbox must be within the database scope. This condition applies when you specify a database using the *TargetDatabase* parameter on the **New-MoveRequest** cmdlet or if you allow automatic mailbox distribution to select the database for you. For more information, see the following topics:

- Understanding Management Role Scopes
- Understanding Automatic Mailbox Distribution

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Recipient Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

MyAddressInformation Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyAddressInformation` management role enables individual users to view and modify their street address and work telephone and fax numbers. This is a custom role created from the MyContactInformation Role parent role.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role.

This role is a specific type of role called a custom role. A custom role is one that's created, or derived, from a parent role. It contains a subset of management role entries that exist on the parent role. This role is provided to enable you to control, with a greater level of granularity, the information you allow end users to modify on their own mailboxes. Unlike other built-in roles, custom roles, including this one, can be deleted. If you won't use this role, it can be deleted.

For more information about built-in and custom management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, its parent role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role doesn't have any default role assignments. It's provided in case you want control, at a more granular level, of what end-user information you allow your users to modify. For more information about assigning this role to a role assignment policy, see the "Adding or Removing Role Assignments" section.

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets,

and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.32 MyBaseOptions Role

MyBaseOptions Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyBaseOptions` management role enables individual users to view and modify the basic configuration of their own mailbox and associated settings.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group or assignment policy	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Default role assignment policy. For more	X		Self	Self	OrganizationConfig	OrganizationConfig

information, see Understanding Management Role Assignment Policies.						
Organization Management		X	Self	Self	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.33 MyContactInformation Role

MyContactInformation Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyContactInformation` management role enables individual users to modify their contact information, including address and phone numbers.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:
You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee

the ability to assign this role to role groups, users, or USGs.

- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group or assignment policy	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Default role assignment policy. For more information, see Understanding Management Role Assignment Policies.	X		Self	Self	OrganizationConfig	OrganizationConfig
Organization Management		X	Self	Self	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.34 MyDiagnostics Role

MyDiagnostics Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyDiagnostics` management role enables individual users to perform basic diagnostics on their mailbox such as retrieving calendar diagnostic information.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC

components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group or assignment policy	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management		X	Self	Self	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.35 MyDisplayName Role

MyDisplayName Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyDisplayName` management role enables individual users to view and modify their display name. This is a custom role created from the MyProfileInformation Role parent role.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are

included on a role, that cmdlet or script and its parameters can be run by those assigned the role.

This role is a specific type of role called a custom role. A custom role is one that's created, or derived, from a parent role. It contains a subset of management role entries that exist on the parent role. This role is provided to enable you to control, with a greater level of granularity, the information you allow end users to modify on their own mailboxes. Unlike other built-in roles, custom roles, including this one, can be deleted. If you won't use this role, it can be deleted.

For more information about built-in and custom management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, its parent role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the

"Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role doesn't have any default role assignments. It's provided in case you want control, at a more granular level, of what end-user information you allow your users to modify. For more information about assigning this role to a role assignment policy, see the "Adding or Removing Role Assignments" section.

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:

- Change a Role Entry
- Remove a Role Entry from a Role

3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.36 MyDistributionGroupMembership Role

MyDistributionGroupMembership Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyDistributionGroupMembership` management role enables individual users to view and modify their membership in distribution groups in an organization, provided that those distribution groups allow manipulation of group membership.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group or assignment policy	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Default role assignment policy. For more information, see Understanding Management Role Assignment Policies.	X		MyGAL	MyGAL	None	None
Organization Management		X	MyGAL	MyGAL	None	None

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features.

By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.37 MyDistributionGroups Role

MyDistributionGroups Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyDistributionGroups` management role enables individual users to create, modify, and view distribution groups, and to modify, view, remove, and add members to distribution groups they own.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group or assignment policy	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope

Organization Management		X	MyGAL	MyDistributionGroups	OrganizationConfig	None

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.38 MyMobileInformation Role

MyMobileInformation Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyMobileInformation` management role enables individual users to view and modify their mobile telephone and pager numbers. This is a custom role created from the MyContactInformation Role parent role.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role.

This role is a specific type of role called a custom role. A custom role is one that's created, or derived, from a parent role. It contains a subset of management role entries that exist on the parent role. This role is provided to enable you to control, with a greater level of granularity, the information you allow end users to modify on their own mailboxes. Unlike other built-in roles, custom roles, including this one, can be deleted. If you won't use this role, it can be deleted.

For more information about built-in and custom management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't

add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, its parent role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role doesn't have any default role assignments. It's provided in case you want control, at a more granular level, of what end-user information you allow your users to modify. For more information about assigning this role to a role assignment policy, see the "Adding or Removing Role Assignments" section.

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.39 MyName Role

MyName Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The MyName management role enables individual users to view and modify their full name and their notes field. This is a custom role created from the MyProfileInformation Role parent role.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role.

This role is a specific type of role called a custom role. A custom role is one that's created, or derived, from a parent role. It contains a subset of management role entries that exist on the parent role. This role is provided to enable you to control, with a greater level of granularity, the information you allow end users to modify on their own mailboxes. Unlike other built-in roles, custom roles, including this one, can be deleted. If you won't use this role, it can be deleted.

For more information about built-in and custom management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, its parent role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role doesn't have any default role assignments. It's provided in case you want control, at a more granular level, of what end-user information you allow your users to modify. For more information about assigning this role to a role assignment policy, see the "Adding or Removing Role Assignments" section.

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group

- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.40 MyPersonalInformation Role

MyPersonalInformation Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyPersonalInformation` management role enables individual users to view and modify their Web site address and home telephone number. This is a custom role created from the MyContactInformation Role parent role.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role.

This role is a specific type of role called a custom role. A custom role is one that's created, or derived, from a parent role. It contains a subset of management role entries that exist on the parent role. This role is provided to enable you to control, with a greater level of granularity, the information you allow end users to modify on their own mailboxes. Unlike other built-in roles, custom roles, including this one, can be deleted. If you won't use this role, it can be deleted.

For more information about built-in and custom management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role

assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, its parent role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role doesn't have any default role assignments. It's provided in case you want control, at a more granular level, of what end-user information you allow your users to modify. For more information about assigning this role to a role assignment policy, see the "Adding or Removing Role Assignments" section.

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions.

Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.41 MyProfileInformation Role

MyProfileInformation Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyProfileInformation` management role enables individual users to modify their name.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which

are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs. However, there must always be at

least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group or assignment policy	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management		X	Self	Self	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a

complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.42 MyRetentionPolicies Role

MyRetentionPolicies Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyRetentionPolicies` management role enables individual users to view their retention tags, and to view and modify their retention tag settings and defaults.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment

policies and assign this role to them.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group or assignment policy	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management		X	Self	Self	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

MyTextMessaging Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyTextMessaging` management role enables individual users to create, view, and modify their text messaging settings.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:

You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in

Active Directory.

Default management role assignments for this role

Role group or assignment policy	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Default Role Assignment Policy For more information, see Understanding Management Role Assignment Policies.	X		Self	Self	OrganizationConfig	OrganizationConfig
Organization Management		X	Self	Self	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry

- Remove a Role Entry from a Role

3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.44 MyVoiceMail Role

MyVoiceMail Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `MyVoiceMail` management role enables individual users to view and modify their voice mail settings.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, such as a role assignment policy. This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

Note:
You can also assign this management role to a role group, USG, or directly to a user. However user-focused roles are most effective when used with role assignment policies.

This user-focused role has implicit scopes that can't be modified. Therefore, you shouldn't add custom scopes to role assignments that assign this role to role assignment policies, role groups, USGs, or users.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role may be assigned to one or more role assignment policies by default. For more information, see the "Default Management Role Assignments" section.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role assignment policies, or you can create role assignment policies and assign this role to them.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from the default role assignment policy, role assignment policies and role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group or assignment policy	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Default role assignment policy. For more information, see Understanding Management Role Assignment Policies.	X		Self	Self	OrganizationConfig	OrganizationConfig
Organization Management		X	Self	Self	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:
The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.45 Organization Client Access Role

Organization Client Access Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Organization Client Access` management role enables administrators to manage Client Access server settings in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of

Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:
There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in

Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the

role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.46 Organization Configuration Role

Organization Configuration Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Organization Configuration` management role enables administrators to manage organization-wide settings. Organization configuration that can be controlled with this role includes the following and more:

- Whether MailTips are enabled or disabled for the organization
- URL for the managed folder home page
- Microsoft Exchange recipient SMTP address and alternate e-mail addresses
- Resource mailbox property schema configuration
- Help URLs for the Exchange Management Console and Outlook Web App

This role type doesn't include the permissions included in the `Organization Client Access` or `Organization Transport Settings` roles.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions

granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope

- Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about

customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.47 Organization Transport Settings Role

Organization Transport Settings Role

Understanding Permissions > Understanding Role Based Access Control > Built-in Management Roles >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Organization Transport Settings` management role enables administrators to manage organization-wide transport settings, such as system messages, site

configuration, and other organization-wide transport settings.

This role doesn't enable you to create or manage transport Receive or Send connectors, queues, hygiene, agents, remote and accepted domains, or rules. To create or manage each of the transport features, you must be assigned one or more of the following roles:

- Receive Connectors Role
- Send Connectors Role
- Transport Queues Role
- Transport Hygiene Role
- Transport Agents Role
- Remote and Accepted Domains Role
- Transport Rules Role

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role

assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.

2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.48 POP3 and IMAP4 Protocols Role

POP3 and IMAP4 Protocols Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `POP3 and IMAP4 Protocols` management role enables administrators to manage POP3 and IMAP4 configuration, such as authentication and connection settings, on individual servers.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group

- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organizatio	X	X	Organizat	Organizat	Organizat	Organizat

n Management			ion	ion	ionConfig	ionConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.49 Public Folder Replication Role

Public Folder Replication Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Public Folder Replication` management role enables administrators to start and stop public folder replication in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment

should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.50 Public Folders Role

Public Folders Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Public Folders` management role enables administrators to manage public folders in an organization.

This role doesn't enable you to manage whether public folders are mail-enabled or to manage public folder replication. To mail-enable or disable a public folder, you must be assigned a role associated with the `Mail Enabled Public Folders` role. To configure public folder replication, you must be assigned a role associated with the `Public Folder Replication` role. For more information, see:

- Mail Enabled Public Folders Role
- Public Folder Replication Role

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment

policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between

this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from

Active Directory.

- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Public Folder Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-**

ManagementRoleAssignment cmdlet. For more information, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.51 Receive Connectors Role

Receive Connectors Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Receive Connectors` management role enables administrators to manage transport Receive connector configuration, such as size limits on an individual server.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.

- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Hygiene Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of

this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.52 Recipient Policies Role

Recipient Policies Role

Understanding Permissions > Understanding Role Based Access Control > Built-in Management Roles >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Recipient Policies` management role enables administrators to manage recipient policies, such as provisioning policies, in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee

the ability to assign this role to role groups, users, or USGs.

- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Recipient Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role

3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

> **Important:**
> If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.53 Remote and Accepted Domains Role

Remote and Accepted Domains Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Remote and Accepted Domains` management role enables administrators to manage remote and accepted domains in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or

built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features.

By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.54 Retention Management Role

Retention Management Role

Understanding Permissions > Understanding Role Based Access Control > Built-in Management Roles >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Retention Management` management role enables administrators to manage retention policies in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a

member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.

- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Records Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove

any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:

- Remove a Role from a Role Group
- Remove a Role from a User or USG

4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.55 Role Management Role

Role Management Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Role Management` management role enables administrators to manage management role groups; role assignment policies and management roles; and role entries, assignments, and scopes in an organization.

Users assigned this role can override the role group managed by property, configure any role group, and add or remove members to or from any role group.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the

combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what

objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets,

and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.56 Security Group Creation and Membership Role

Security Group Creation and Membership Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Security Group Creation and Membership` management role enables administrators to create and manage universal security groups (USGs) and their memberships in an organization.

If your organization maintains a Role Based Access Control (RBAC) split permissions model where USG creation and management is performed by a different group other than those who manage servers running Exchange, assign this role to that group.

If your organization has enabled Active Directory split permissions, all non-delegating management role assignments to this management role were removed. When Active Directory split permissions is enabled, only Active Directory administrators using Active Directory management tools can create new security principals such as users and security groups.

For more information, see Understanding Split Permissions.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the

associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a

role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.57 Send Connectors Role

Send Connectors Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Send Connectors management role enables administrators to manage transport Send connectors in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group

- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organizatio	X	X	Organizat	Organizat	Organizat	Organizat

n Managemen t			ion	ion	ionConfig	ionConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.58 Support Diagnostics Role

Support Diagnostics Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Support Diagnostics` management role enables administrators to perform advanced diagnostics under the direction of Microsoft Customer Service and Support in an organization.

Caution:
This role grants permissions to cmdlets and scripts that should only be used under the direction of Customer Service and Support.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the

associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management		X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a

role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.59 Transport Agents Role

Transport Agents Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Transport Agents` management role enables administrators to manage transport agents in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group

- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Hygiene	X		Organizat	Organizat	Organizat	Organizat

Management			ion	ion	ionConfig	ionConfig
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.60 Transport Hygiene Role

Transport Hygiene Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Transport Hygiene` management role enables administrators to manage antivirus and anti-spam features in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment

should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Hygiene Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions.

Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.61 Transport Queues Role

Transport Queues Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Transport Queues` management role enables administrators to manage transport queues on an individual server.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned

the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role

group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Server Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.62 Transport Rules Role

Transport Rules Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Transport Rules` management role enables administrators to manage transport rules in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet.

For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
Records Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a

role as a child of this role, and customize the new role.

Caution:
The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.63 UM Mailboxes Role

UM Mailboxes Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `UM Mailboxes` role enables administrators to manage the Unified Messaging configuration of mailboxes and other recipients in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment

policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between

this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from

Active Directory.

- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
UM Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-**

ManagementRoleAssignment cmdlet. For more information, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.64 UM Prompts Role

UM Prompts Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `UM Prompts` management role enables administrators to create and manage custom Unified Messaging voice prompts in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.

- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
UM Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about

customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.65 Unified Messaging Role

Unified Messaging Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Unified Messaging` role enables administrators to manage Unified Messaging (UM) servers in an organization.

This role doesn't enable you to manage UM-specific mailbox configuration or UM prompts. To manage UM-specific mailbox configuration, use roles associated with the `UM Mailboxes` role. To manage UM prompts, use the roles associated with the `UM Prompts` role. For more information, see:

- UM Mailboxes Role
- UM Prompts Role

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to

them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig
UM Management	X		Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the

following topics:
- Change a Role Entry
- Remove a Role Entry from a Role

3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.66 Unscoped Role Management Role

Unscoped Role Management Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Unscoped Role Management` management role enables administrators to create and manage unscoped top-level management roles in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the

combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what

objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management		X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets,

and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.67 User Options Role

User Options Role

Understanding Permissions > Understanding Role Based Access Control > Built-in Management Roles >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `User Options` management role enables administrators to view the Outlook Web App options of a user in an organization. This role can be used to help diagnose configuration problems.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly

increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.

- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Help Desk	X		Organization	Organization	OrganizationConfig	OrganizationConfig
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role

3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.68 View-Only Audit Logs Role

View-Only Audit Logs Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `Audit Logs` management role enables administrators and specialist users to search the administrator audit logs in an organization.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or

built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Organization Management	X	X	Organization	Organization	OrganizationConfig	OrganizationConfig

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features.

By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:

If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.69 View-Only Configuration Role

View-Only Configuration Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The View-Only Configuration management role enables administrators to view all the non-recipient Exchange configuration settings in an organization. Examples of configuration that are viewable are server configuration, transport configuration, database configuration, and organization-wide configuration.

This role can be combined with roles associated with the View-Only Recipients role to create a role group that can view every object in an organization. For more information, see View-Only Recipients Role.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign

this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:

There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each

column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Delegated Setup	X		Organization	None	OrganizationConfig	None
Hygiene Management	X		Organization	None	OrganizationConfig	None
Organization Management	X	X	Organization	None	OrganizationConfig	None
View-Only Organization Management	X		Organization	None	OrganizationConfig	None

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a

built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Remove a Role from a Role Group
   - Remove a Role from a User or USG
4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

Important:
If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.1.7.70 View-Only Recipients Role

View-Only Recipients Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The `View-Only Recipients` management role enables administrators to view the configuration of recipients, such as mailboxes, mail users, mail contacts, distribution groups, and dynamic distribution groups.

This role can be combined with roles associated with the `View-Only Configuration` role to create a role group that can view every object in the organization. For more information, see View-Only Configuration Role.

This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of

Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

For more information about management roles, management role groups, and other RBAC components, see Understanding Role Based Access Control.

Management Role Assignments

For this role to grant permissions, it must be assigned to a role assignee, which can be a role group, user, or universal security group (USG). This assignment is done using management role assignments. Role assignments link role assignees and roles together. If more than one role is assigned to a role assignee, the role assignee is granted the combination of all the permissions granted by all the assigned roles.

In addition to linking role assignees to roles, role assignments can also apply custom or built-in management scopes. Management scopes control which recipient, server and database objects can be modified by role assignees. If this role is assigned to a role assignee, but a management scope allows the role assignee only to manage certain objects based on a defined scope, the role assignee can only use the permissions granted by this role on those specific objects. The permissions provided by this role can't be applied to objects outside the scope defined on the role assignment. For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

This role is assigned to one or more role groups by default. For more information, see the "Default Management Role Assignments" section later in this topic.

If you want to view a list of role groups, users, or USGs assigned to this role, use the following command.

```
Get-ManagementRoleAssignment -Role "<role name>"
```

Regular and Delegating Role Assignments

This role can be assigned to role assignees using either regular or delegating role assignments. Regular role assignments grant the permissions provided by the role to the role assignee. Delegating role assignments grant the role assignee the ability to assign the role to other role assignees. For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

Adding or Removing Role Assignments

You can change which role assignees are assigned this role. By changing which role assignee is assigned this role, you change who is granted its permissions. You can assign this role to other built-in role groups, or you can create role groups and assign this role to them. You can also assign this role to users or USGs. However, we recommend that you limit assignment of roles to users and USGs because such assignments can greatly increase the complexity of your permissions model.

To assign this role to role assignees, the role must be assigned to a role group you're a member of, directly to you, or to a USG you're a member of, using a delegating role assignment. For more information about delegating role assignments, see the "Regular and Delegating Role Assignments" section.

You can also remove this role from built-in role groups, role groups you create, users, and USGs. However, there must always be at least one delegating role assignment between this role and a role group or USG. You can't delete the last delegating role assignment. This limitation helps prevent you from locking yourself out of the system.

Important:
There must be at least one delegating role assignment between this role and a role group or USG. You can't remove the last delegating role assignment associated with this role if the last assignment is to a user.

For more information about how to add or remove assignments between this role and role groups, users, and USGs, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

Changing the Management Scopes on Role Assignments

You can also change the management scopes on existing role assignments between this role and role assignees. By changing the scopes on role assignments, you control what objects can be managed using the permissions provided by this role. You have several choices when changing the scope on a role assignment. You can do one of the following:

- Add a new custom scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
  - Create a Regular or Exclusive Scope
  - Change a Role Assignment
- Add or change an organizational unit scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Add or change a predefined scope using the **Set-ManagementRoleAssignment** cmdlet. For more information, see Change a Role Assignment.
- Change the recipient, server, or database scope on a custom scope associated with a role assignment using the **Set-ManagementScope** cmdlet. For more information, see Change a Role Scope.

Enabling or Disabling Role Assignments

By enabling or disabling a role assignment, you control whether that role assignment should be in effect. If a role assignment is disabled, the permissions granted by the associated role aren't applied to the role assignee. This is convenient if you want to temporarily remove permissions without deleting a role assignment. For more information, see Change a Role Assignment.

Default Management Role Assignments

This role has role assignments to one or more role assignees. The following table indicates whether the role assignment is regular or delegating, and also indicates the management scopes applied to each assignment. The following list describes each column:

- **Regular assignment** Regular role assignments enable the role assignee to access the permissions provided by the management role entries on this role.
- **Delegating assignment** Delegating role assignments give the role assignee the ability to assign this role to role groups, users, or USGs.
- **Recipient read scope** The recipient read scope determines what recipient objects the role assignee is allowed to read from Active Directory.
- **Recipient write scope** The recipient write scope determines what recipient objects the role assignee is allowed to modify in Active Directory.
- **Configuration read scope** The configuration read scope determines what configuration and server objects the role assignee is allowed to read from Active Directory.
- **Configuration write scope** The configuration write scope determines what organizational and server objects the role assignee is allowed to modify in

Active Directory.

Default management role assignments for this role

Role group	Regular assignment	Delegating assignment	Recipient read scope	Recipient write scope	Configuration read scope	Configuration write scope
Help Desk	X		Organization	None	OrganizationConfig	None
Hygiene Management	X		Organization	None	OrganizationConfig	None
Organization Management	X	X	Organization	None	OrganizationConfig	None
View-Only Organization Management	X		Organization	None	OrganizationConfig	None

Management Role Customization

This role has been configured to provide a role assignee with all of the necessary cmdlets, and their parameters, to manage the features and components listed in the beginning of this topic. Other roles have also been provided to enable management of other features. By adding and removing roles to and from role groups, you can create a customized permissions model without the need to customize individual management roles. For a complete list of roles, see Built-in Management Roles. For more information about customizing role groups, see the following topics:

- Add a Role to a Role Group
- Remove a Role from a Role Group

If you decide that you need to create a customized version of this role, you must create a role as a child of this role, and customize the new role.

Caution:

The following information enables you to perform advanced management of permissions. Customizing management roles can significantly increase the complexity of your permissions model. You could cause certain features to stop functioning if you replace a built-in management role with an incorrectly configured custom role.

The following are the most common steps to create a customized role and assign it to a role assignee:

1. Create a copy of this role using the **New-ManagementRole** cmdlet. For more information, see Create a Role.
2. Change or remove the role entries on the new role using the **Set-ManagementRoleEntry** and **Remove-ManagementRoleEntry** cmdlets. You can't add additional role entries to the new role because it can only contain the role entries on the parent built-in role. For more information, see the following topics:
   - Change a Role Entry
   - Remove a Role Entry from a Role
3. If you want to replace the built-in role with this new customized role, remove any role assignments associated with the built-in role using the **Remove-**

ManagementRoleAssignment cmdlet. For more information, see the following topics:

- Remove a Role from a Role Group
- Remove a Role from a User or USG

4. Add the new customized role to the required role assignees using the **New-ManagementRoleAssignment** cmdlet. For more information, see the following topics:
   - Add a Role to a Role Group
   - Add a Role to a User or USG

> **Important:**
> If you want other users, in addition to the user that created the role, to be able to assign the new customized role, be sure to add a delegating role assignment to at least one role assignee. For more information, see Delegate Role Assignments.

1.3.1.2 Understanding Split Permissions

Understanding Split Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-24*

Organizations that separate the management of Microsoft Exchange Server 2010 objects and Active Directory objects use what's called a *split permissions* model. Split permissions enable organizations to assign specific permissions and related tasks to specific groups within the organization. This separation of work helps to maintain standards and workflows, and helps to control change in the organization.

The highest level of split permissions is the separation of Exchange management and Active Directory management. Many organizations have two groups: administrators that manage the organization's Exchange infrastructure, including servers and recipients, and administrators that manage the Active Directory infrastructure. This is an important separation for many organizations because the Active Directory infrastructure often spans many locations, domains, services, applications, and even Active Directory forests. Active Directory administrators must ensure that changes made to Active Directory don't negatively impact any other services. As a result, typically only a small group of administrators is allowed to manage that infrastructure.

At the same time, the infrastructure for Exchange, including servers and recipients, can also be complex and require specialized knowledge. Additionally, Exchange stores extremely confidential information about the business of the organization. Exchange administrators can potentially access this information. By limiting the number of Exchange administrators, the organization limits who can make changes to Exchange configuration and who can access sensitive information.

Split permissions typically make a distinction between the creation of security principals in Active Directory, such as users and security groups, and the subsequent configuration of those objects. This helps to reduce the chance of unauthorized access to the network by controlling who can create objects that grant access to it. Most often only Active Directory administrators can create security principals while other administrators, such as Exchange administrators, can manage specific attributes on existing Active Directory objects.

To support the varying needs to separate the management of Exchange and Active Directory, Exchange 2010 lets you choose whether you want a shared permissions model or a split permissions model. Microsoft Exchange Server 2010 Service Pack 1 (SP1) offers two types of split permissions models: RBAC and Active Directory. Exchange 2010 SP1 defaults to a shared permissions model.

Contents

Explanation of Role Based Access Control and Active Directory

To understand split permissions, you need to understand how the Role Based Access Control (RBAC) permissions model in Exchange 2010 works with Active Directory. The RBAC model controls who can perform what actions, and on which objects those actions can be performed. For more information about the various components of RBAC that are discussed in this topic, see Understanding Role Based Access Control.

In Exchange 2010, all tasks that are performed on Exchange objects must be done through the Exchange Management Console, the Exchange Management Shell, or the Exchange Web administrative interface. Each of these management tools uses RBAC to authorize all tasks that are performed.

RBAC is a component that exists on every server running Exchange 2010, with the exception of Edge Transport servers. RBAC checks whether the user performing an action is authorized to do so:

- If the user isn't authorized to perform the action, RBAC doesn't allow the action to proceed.
- If the user is authorized to perform the action, RBAC checks whether the user is authorized to perform the action against the specific object being requested:
  - If the user is authorized, RBAC allows the action to proceed.
  - If the user isn't authorized, RBAC doesn't allow the action to proceed.

If RBAC allows an action to proceed, the action is performed in the context of the Exchange Trusted Subsystem and not the user's context. The Exchange Trusted Subsystem is a highly privileged universal security group (USG) that has read/write access to every Exchange-related object in the Exchange organization. It's also a member of the Administrators local security group and the Exchange Windows Permissions USG, which enables Exchange to create and manage Active Directory objects.

Caution:

Don't make any manual changes to the membership of the Exchange Trusted Subsystem security group. Also, don't add it to or remove it from object access control lists (ACLs). By making changes to the Exchange Trusted Subsystem USG yourself, you could cause irreparable damage to your Exchange organization.

It's important to understand that it doesn't matter what Active Directory permissions a user has when using the Exchange management tools. If the user is authorized, via RBAC, to perform an action in the Exchange management tools, the user can perform the action regardless of his or her Active Directory permissions. Conversely, if a user is an Enterprise Admin in Active Directory but isn't authorized to perform an action, such as creating a mailbox, in the Exchange management tools, the action won't succeed because the user doesn't have the required permissions according to RBAC.

Important:
Although the RBAC permissions model doesn't apply to the Active Directory Users and Computers management tool, Active Directory Users and Computers can't manage the Exchange configuration. So although a user may have access to modify some attributes on Active Directory objects, such as the display name of a user, the user must use the Exchange management tools, and therefore must be authorized by RBAC, to manage Exchange attributes.

Return to top

Shared Permissions

The shared permissions model is the default model for Exchange 2010. You don't need to change anything if this is the permissions model you want to use. This model doesn't separate the management of Exchange and Active Directory objects from within the Exchange management tools. It allows administrators using the Exchange management tools to create security principals in Active Directory.

The following table shows the roles that enable the creation of security principals in Exchange and the management role groups they're assigned to by default.

Security principal management roles

Management role	Role group
Mail Recipient Creation Role	Organization Management Recipient Management
Security Group Creation and Membership Role	Organization Management

Only role groups, users, or USGs that are assigned the Mail Recipient Creation role can create security principals such as Active Directory users. By default, the Organization Management and Recipient Management role groups are assigned this role. Therefore members of these role groups can create security principals.

Only role groups, users, or USGs that are assigned the Security Group Creation and Membership role can create security groups or manage their memberships. By default, only the Organization Management role group is assigned this role. Therefore only members of the Organization Management role group can create or manage the membership of security groups.

You can assign the Mail Recipient Creation role and the Security Group Creation and Membership role to other role groups, users, or USGs if you want other users to be able to create security principals.

To enable the management of existing security principals in Exchange 2010, the Mail Recipients role is assigned to the Organization Management and Recipient Management role groups by default. Only role groups, users, or USGs that are assigned the Mail Recipients role can manage existing security principals. If you want other role groups,

users, or USGs to be able to manage existing security principals, you must assign the Mail Recipients role to them.

For more information about how to add roles to role groups, users, or USGs, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

If you switched to a split permissions model and want to change back to a shared permissions model, see Configure Exchange 2010 for Shared Permissions.

Return to top

Split Permissions

If your organization separates Exchange management and Active Directory management, you need to configure Exchange to support the split permissions model. When configured correctly, only the administrators who you want to create security principals, such as Active Directory administrators, will be able to do so and only Exchange administrators will be able to modify the Exchange attributes on existing security principals. This splitting of permissions also falls roughly along the lines of the domain and configuration partitions in Active Directory. Partitions are also called naming contexts. The domain partition stores the users, groups, and other objects for a specific domain. The configuration partition stores the forest-wide configuration information for the services that used Active Directory, such as Exchange. Data that's stored in the domain partition is typically managed by Active Directory administrators, although objects may contain Exchange-specific attributes that can be managed by Exchange administrators. Data that's stored in the configuration partition is managed by the administrators for each respective service that stores data in this partition. For Exchange, this is typically Exchange administrators.

Exchange 2010 SP1 supports the two following types of split permissions:

- **RBAC split permissions** Permissions to create security principals in the Active Directory domain partition are controlled by RBAC. Only Exchange servers, services, and those who are members of the appropriate role groups can create security principals.
- **Active Directory split permissions** Permissions to create security principals in the Active Directory domain partition are completely removed from any Exchange user, service, or server. No option is provided in RBAC to create security principals. Creation of security principals in Active Directory must be performed using Active Directory management tools.

Important:

Although Active Directory split permissions can only be enabled or disabled by running Setup on a computer that has Exchange 2010 SP1 installed, Active Directory split permissions configuration applies to both Exchange 2010 release to manufacturing (RTM) and Exchange 2010 SP1 servers. It doesn't, however, have any impact on Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007 servers.

If your organization chooses to use a split permissions model instead of shared permissions, we recommend that you use the RBAC split permissions model. The RBAC split permissions model provides significantly more flexibility while providing the nearly same administration separation as Active Directory split permissions, with the exception that Exchange servers and services can create security principals in the RBAC split permissions model.

You're asked whether you want to enable Active Directory split permissions during Setup. If you choose to enable Active Directory split permissions, you can only change to shared

permissions or RBAC split permissions by rerunning Setup and disabling Active Directory split permissions. This choice applies to the entire Exchange 2010 organization.

The following sections describe RBAC and Active Directory split permissions in more detail.

Return to top

RBAC Split Permissions

The RBAC security model modifies the default management role assignments to separate who can create security principals in the Active Directory domain partition from those who administer the Exchange organization data in the Active Directory configuration partition. Security principals, such as users with mailboxes and distribution groups, can be created by administrators who are members of the Mail Recipient Creation and Security Group Creation and Membership roles. These permissions remain separate from the permissions required to create security principals outside of the Exchange management tools. Exchange administrators who aren't assigned the Mail Recipient Creation or Security Group Creation and Membership roles can still modify Exchange-related attributes on security principals. Active Directory administrators also have the option of using the Exchange management tools to create Active Directory security principals.

Exchange servers and the Exchange Trusted Subsystem also have permissions to create security principals in Active Directory on behalf of users and third-party programs that integrate with RBAC.

RBAC split permissions is a good choice for your organization if the following are true:

- Your organization doesn't require that security principal creation be performed using only Active Directory management tools and only by users who are assigned specific Active Directory permissions.
- Your organization allows services, such as Exchange servers, to create security principals.
- You want to simplify the process required to create mailboxes, mail-enabled users, distribution groups, and role groups by allowing their creation from within the Exchange management tools.
- You want to manage the membership of distribution groups and role groups within the Exchange management tools.
- You have third-party programs that require that Exchange servers be able to create security principals on their behalf.

If your organization requires a complete separation of Exchange and Active Directory administration where no Active Directory administration can be performed using Exchange management tools or by Exchange services, see the Active Directory Split Permissions section later in this topic.

Switching from shared permissions to RBAC split permissions is a manual process where you remove the permissions required to create security principals from the role groups that are granted them by default. The following table shows the roles that enable the creation of security principals in Exchange and the management role groups they're assigned to by default.

Security principal management roles

Management role	Role group
Mail Recipient Creation Role	Organization Management Recipient Management
Security Group Creation and Membership Role	Organization Management

By default, members of the Organization Management and Recipient Management role groups can create security principals. You must transfer the ability to create security principals from the built-in role groups to a new role group that you create.

To configure RBAC split permissions, you must do the following:

1. Disable Active Directory split permissions if it's enabled.
2. Create a role group, which will contain the Active Directory administrators that will be able to create security principals.
3. Create regular and delegating role assignments between the Mail Recipient Creation role and the new role group.
4. Create regular and delegating role assignments between the Security Group Creation and Membership role and the new role group.
5. Remove the regular and delegating management role assignments between the Mail Recipient Creation role and the Organization Management and Recipient Management role groups.
6. Remove the regular and delegating role assignments between the Security Group Creation and Membership role and the Organization Management role group.

After doing this, only members of the new role group that you create will be able to create security principals, such as mailboxes. The new group will only be able to create the objects. It won't be able to configure the Exchange attributes on the new object. An Active Directory administrator, who is a member of the new group, will need to create the object, and then an Exchange administrator will need to configure the Exchange attributes on the object. Exchange administrators won't be able to use the following cmdlets:

- **New-Mailbox**
- **New-MailContact**
- **New-MailUser**
- **New-RemoteMailbox**
- **Remove-Mailbox**
- **Remove-MailContact**
- **Remove-MailUser**
- **Remove-RemoteMailbox**

Exchange administrators will, however, be able to create and manage Exchange-specific objects, such as transport rules, distribution groups, and so on and manage Exchange-related attributes on any object.

Additionally, the associated features in the Exchange Management Console and Exchange Control Panel, such as the New Mailbox Wizard, will also no longer be available or will generate an error if you try to use them.

If you want the new role group to also be able to manage the Exchange attributes on the new object, the Mail Recipients role also needs to be assigned to the new role group.

For more information about configuring a split permissions model, see Configure Exchange 2010 for Split Permissions.

Return to top

Active Directory Split Permissions

With Active Directory split permissions, the creation of security principals in the Active Directory domain partition, such as mailboxes and distribution groups, must be performed using Active Directory management tools. Several changes are made to the permissions granted to the Exchange Trusted Subsystem and Exchange servers to limit what Exchange administrators and servers can do. The following changes in functionality occur when you enable Active Directory split permissions:

- Creation of mailboxes, mail-enabled users, distribution groups, and other

security principals is removed from the Exchange management tools.
- Adding and removing distribution group members can't be done from the Exchange management tools.
- All permissions granted to the Exchange Trusted Subsystem and Exchange servers to create security principals are removed.
- Exchange servers and the Exchange management tools can only modify the Exchange attributes of existing security principals in Active Directory.

For example, to create a mailbox with Active Directory split permissions enabled, a user must first be created using Active Directory tools by a user with the required Active Directory permissions. Then, the user can be mailbox-enabled using the Exchange management tools. Only the Exchange-related attributes of the mailbox can be modified by Exchange administrators using the Exchange management tools.

Active Directory split permissions is a good choice for your organization if the following are true:

- Your organization requires that security principals be created using only the Active Directory management tools or only by users who are granted specific permissions in Active Directory.
- You want to completely separate the ability to create security principals from those who manage the Exchange organization.
- You want to perform all distribution group management, including creation of distribution groups and adding and removing members of those groups, using Active Directory management tools.
- You don't want Exchange servers, or third-party programs that use Exchange on their behalf, to create security principals.

Important:

Switching to Active Directory split permissions is a choice that you can make when you install Exchange 2010 SP1 either by using the Setup wizard or by using the *ActiveDirectorySplitPermissions* parameter while running `setup.com` from the command line. You can also enable or disable Active Directory split permissions after you've installed Exchange 2010 by rerunning `setup.com` from the command line. To enable Active Directory split permissions, set the *ActiveDirectorySplitPermissions* parameter to `true`. To disable it, set it to `false`. You must always specify the *PrepareAD* switch along with the *ActiveDirectorySplitPermissions* parameter.
If you have multiple domains within the same forest, you must also either specify the *PrepareAllDomains* switch when you apply Active Directory split permissions or run setup with the *PrepareDomain* switch in each domain. If you choose to run setup with the *PrepareDomain* switch in each domain rather than use the *PrepareAllDomains* switch, you must prepare every domain that contains Exchange servers, mail-enabled objects, or global catalog servers that could be accessed by an Exchange server.

Important:

You can't enable Active Directory split permissions if you've installed Exchange 2010 on a domain controller.
After you enable or disable Active Directory split permissions, we recommend that you restart the Exchange 2010 servers in your organization to force them to pick up the new Active Directory access token with the updated permissions.

Exchange 2010 SP1 achieves Active Directory split permissions by removing permissions and membership from the Exchange Windows Permissions security group. This security group, in shared permissions and RBAC split permissions, is given permissions to many non-Exchange objects and attributes throughout Active Directory. By removing the permissions and membership to this security group, Exchange administrators and services are prevented from creating or modifying those non-Exchange Active Directory objects.

For a list of changes that occur to the Exchange Windows Permissions security group and other Exchange components when you enable or disable Active Directory split permissions, see the following table.

Note:
Role assignments to role groups that enable Exchange administrators to create security principals are removed when Active Directory split permissions is enabled. This is done to remove access to cmdlets that would otherwise generate an error when they're run because they don't have permissions to create the associated Active Directory object.

Active Directory split permissions changes

Action	Changes made by Exchange

Enable Active Directory split permissions during first Exchange 2010 SP1 server installation	The following happens when you enable Active Directory split permissions either through the Setup wizard or by running `setup.com` with the `/PrepareAD` and `/ActiveDirectorySplitPermissions:true` parameters:
	• An organizational unit (OU) called **Microsoft Exchange Protected Groups** is created.
	• The **Exchange Windows Permissions** security group is created in the **Microsoft Exchange Protected Groups** OU.
	• The **Exchange Trusted Subsystem** security group isn't added to the **Exchange Windows Permissions** security group.
	• Creation of non-delegating management role assignments to management roles with the following management role types is skipped:
	  • `MailRecipientCreation`
	  • `SecurityGroupCreationandMembership`
	• Access control entries (ACEs) that would have been assigned to the **Exchange Windows Permissions** security group aren't added to the Active Directory domain object.
	
	If you run setup with the *PrepareAllDomains* or *PrepareDomain* switch, the following happens in each child domain that's prepared:
	• All ACEs assigned to the **Exchange Windows Permissions** security group are removed from the domain object.
	• ACEs are set in each domain as defined in Exchange 2010 Deployment Permissions Reference with the exception of any ACEs assigned to the **Exchange Windows Permissions** security group.

Switch from shared permissions or RBAC split permissions to Active Directory split permissions	The following happens when you run the `setup.com` command with the `/PrepareAD` and `/ActiveDirectorySplitPermissions:true` parameters: • An OU called **Microsoft Exchange Protected Groups** is created. • The **Exchange Windows Permissions** security group is moved to the **Microsoft Exchange Protected** Groups OU.

	• The **Exchange Trusted Subsystem** security group is removed from the **Exchange Windows Permissions** security group.
	• Any non-delegating role assignments to management roles with the following role types are removed:
	  • `MailRecipientCreation`
	  • `SecurityGroupCreationandMembership`
	• All ACEs assigned to the **Exchange Windows Permissions** security group are removed from the domain object.
	
	If you run setup with either the *PrepareAllDomains* or *PrepareDomain* switch, the following happens in each child domain that's prepared:
	• All ACEs assigned to the **Exchange Windows Permissions** security group are removed from the domain object.
	• ACEs are set in each domain as defined in Exchange 2010 Deployment Permissions Reference with the exception of any ACEs assigned to the **Exchange Windows Permissions** security group.

Switch from Active Directory split permissions to shared permissions or RBAC split permissions	The following happens when you run the `setup.com` command with the `/PrepareAD` and `/ActiveDirectorySplitPermissions:false` parameters: • The **Exchange Windows Permissions** security group is moved to the **Microsoft Exchange Security Groups** OU. • The **Microsoft Exchange Protected Groups** OU is removed. • The **Exchange Trusted Subsystems** security group is added to the **Exchange Windows Permissions** security group. • ACEs are added to the domain object for the **Exchange Windows Permissions** security group. If you run setup with either the *PrepareAllDomains* or *PrepareDomain* switch, the following happens in each child domain that's prepared: • ACEs are added to the domain object for the **Exchange Windows Permissions** security group. • ACEs are set in each domain as defined in Exchange 2010 Deployment Permissions Reference including ACEs assigned to the **Exchange Windows Permissions** security group. Role assignments to the Mail Recipient Creation and Security Group Creation and Membership roles aren't automatically created when switching from Active Directory split to shared permissions. If

	delegating role assignments were customized prior to Active Directory split permissions being enabled, those customizations are left intact. To create role assignments between these roles and the Organization Management role group, see Configure Exchange 2010 for Shared Permissions.

After you enable Active Directory split permissions, the following cmdlets are no longer available:

- **New-Mailbox**
- **New-MailContact**
- **New-MailUser**
- **New-RemoteMailbox**
- **Remove-Mailbox**
- **Remove-MailContact**
- **Remove-MailUser**
- **Remove-RemoteMailbox**

After you enable Active Directory split permissions, the following cmdlets are accessible but you can't use them to create distribution groups or modify distribution group membership:

- **Add-DistributionGroupMember**
- **New-DistributionGroup**
- **Remove-DistributionGroup**
- **Remove-DistributionGroupMember**
- **Update-DistributionGroupMember**

Some cmdlets, although still available, may offer only limited functionality when used with Active Directory split permissions. This is because they may allow you to configure recipient objects that are in the domain Active Directory partition and Exchange configuration objects that are in the configuration Active Directory partition. They may also allow you to configure Exchange-related attributes on objects stored in the domain partition. Attempts to use the cmdlets to create objects, or modify non-Exchange-related attributes on objects, in the domain partition will result in an error. For example, the **Add-ADPermission** cmdlet will return an error if you attempt to add permissions to a mailbox. However, the **Add-ADPermission** cmdlet will succeed if you configure permissions on a Receive connector. This is because a mailbox is stored in the domain partition while Receive connectors are stored in the configuration partition.

Additionally, the associated features in the Exchange Management Console and Exchange Control Panel, such as the New Mailbox wizard, will also no longer be available or will generate an error if you try to use them.

Exchange administrators will, however, be able to create and manage Exchange-specific objects, such as transport rules, and so on.

For more information about configuring an Active Directory split permissions model, see Configure Exchange 2010 for Split Permissions.

Return to top

1.3.1.3 Understanding Permissions Coexistence with Exchange 2003

Understanding Permissions Coexistence with Exchange 2003

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Permissions in Microsoft Exchange Server 2010 and Exchange Server 2003 are completely separate. This is because the permissions models used by Exchange 2010 and Exchange 2003 are different. You must take steps to grant existing Exchange 2003 administrators permissions to your Exchange 2010 servers, and vice versa. Additionally, management of Exchange 2010 and Exchange 2003 is performed separately using the management tools provided by each version. You can grant permissions to your administrators so that they can manage your combined Exchange 2010 and Exchange 2003 organization.

For more information about planning coexistence between Exchange 2010 and Exchange 2003, see Exchange 2003 - Planning Roadmap for Upgrade and Coexistence.

Exchange 2010 Permissions

Exchange 2010 uses the Role Based Access Control (RBAC) permissions model. This model consists of management role groups that are assigned one of a number of management roles. Management roles contain permissions that enable administrators to perform tasks in the Exchange organization. Administrators are added as members of the role groups and are granted all the permissions the roles provide. The following table provides an example of the role groups, some of the roles that they're assigned, and a description of the type of user who might be a member of the role group.

Examples of role groups and roles in Exchange 2010

Management role group	Management roles	Members of this role group
Organization Management	The following are some of the roles assigned to this role group: • Address Lists • Exchange Servers • Journaling • Mail Recipients • Public Folders	Users who need to manage the entire Exchange 2010 organization should be members of this role group. With some exceptions, members of this role group can manage nearly any aspect of the Exchange 2010 organization. By default, the user account used to prepare Active Directory for Exchange 2010 is a member of this role group. For more information about this role group, and for a complete list of roles assigned to this role group, see Organization

		Management.
View Only Organization Management	The following are the roles assigned to this role group: • Monitoring • View-Only Configuration • View-Only Recipients	Users who need to view the configuration of the entire Exchange 2010 organization should be members of this role group. These users need to be able to view server configuration, recipient information, and be able to perform monitoring functions without the ability to change organization or recipient configuration. For more information about this role group, see View-Only Organization Management.
Recipient Management	The following are the roles assigned to this role group: • Distribution Groups • Mail Enabled Public Folders • Mail Recipient Creation • Mail Recipients • Message Tracking • Migration • Move Mailboxes • Recipient Policies	Users who need to manage recipients, such as mailboxes, contacts, and distribution groups in the Exchange 2010 organization, should be members of this role group. These users can create recipients, modify or delete existing recipients, or move mailboxes. For more information about this role group, and for a complete list of roles assigned to this role group, see Recipient Management.
Server Management	The following are some of the roles assigned to this role group: • Databases • Exchange Connectors • Exchange Servers • Receive Connectors • Transport Queues	Users who need to manage Exchange server configuration, such as Receive connectors, certificates, databases, and virtual directories, should be members of this role group. These users can modify Exchange server configuration, create databases, and restart and manipulate transport queues. For more information

		about this role group, and for a complete list of roles assigned to this role group, see Server Management.
Discovery Management	The following are the roles assigned to this role group: • Legal Hold • Mailbox Search	Users who need to perform searches of mailboxes to support legal proceedings or configure legal holds should be members of this role group. This is an example of a role group that might contain non-Exchange administrators, such as personnel in your legal department. This allows legal personnel to perform their tasks without intervention from Exchange administrators. For more information about this role group, and for a complete list of roles assigned to this role group, see Discovery Management.

As shown in the previous table, Exchange 2010 provides a granular level of control over the permissions you grant to your administrators. You can choose from 11 role groups in Exchange 2010. For a complete list of role groups and the permissions they provide, see Built-in Role Groups.

Because of the number of role groups Exchange 2010 provides, and because further customization is possible by creating role groups with different role combinations, manipulating access control lists (ACLs) on Active Directory objects is no longer necessary and won't have any effect. ACLs are no longer used to apply permissions to individual administrators or groups in Exchange 2010. All tasks, such as an administrator creating a mailbox or a user accessing a mailbox, are managed by RBAC. RBAC authorizes the task and if it's allowed, Exchange performs the task on behalf of the user in the Exchange Trusted Subsystem universal security group (USG). With some exceptions, all of the ACLs on objects in Active Directory that Exchange 2010 needs to access are granted to the Exchange Trusted Subsystem USG. This is a fundamental change from how permissions are handled in Exchange 2003.

The permissions granted to a user in Active Directory are separate from the permissions granted to the user by RBAC when that user is using the Exchange 2010 management tools.

For more information about RBAC, see Understanding Role Based Access Control.

Exchange 2003 Permissions

Exchange 2003 has the following administrative roles:

- **Exchange View Only** This role grants permissions to view Exchange 2003 server and recipient information to an Exchange 2003 administrator.
- **Exchange Administrator** This role grants all permissions to Exchange 2003 servers and recipients except for the ability to take ownership, change permissions, or open user mailboxes, to Exchange 2003 administrators. If the administrator will need to add objects or modify object properties, but won't be required to delegate permissions on the objects, this role is assigned.
- **Exchange Full Administrator** This role grants all permissions to Exchange 2003 servers and recipients, including the ability to change permissions, to an Exchange 2003 administrator. This role is assigned to administrators who are required to delegate permissions to objects.

Exchange 2003 enables you to segment your administrators into one of these roles. The permissions are assigned directly to either the user or to the USG the user is a member of. Any actions performed by the user are performed in the context of that user's Active Directory account.

If you need to assign permissions at a more granular level, you must modify the ACLs on individual Exchange 2003 objects, such as address lists and databases. As with the administrative roles, the user, or the security group the user is a member of, is added to the ACL directly, and the actions are performed in the context of the user.

For more information about Exchange 2003 administrative groups, see Microsoft Knowledge Base article 823018, Overview of Exchange administrative role permissions in Exchange 2003.

Permissions in Exchange 2010 and Exchange 2003 Coexistence

As describe earlier in this topic, the permissions models for Exchange 2010 and Exchange 2003 are different. Exchange 2010 uses role groups to grant permissions, while Exchange 2003 uses a combination of administrative groups and ACLs to grant permissions. Exchange 2010 and Exchange 2003 permissions are completely separate, even though both versions exist in the same forest. This means that by default and without any additional configuration, Exchange 2003 administrators don't have permissions to manage Exchange 2010 servers and Exchange 2010 administrators don't have permissions to manage Exchange 2003 servers. This situation creates questions that you need to consider:

- Do you want to grant Exchange 2010 administrators access to administer Exchange 2003 servers and vice versa?
- Do you want to customize Exchange 2010 permissions so that they match the customizations you made to Exchange 2003?

Grant Exchange 2010 Permissions to Exchange 2003 Administrators

If you want Exchange 2003 administrators to administer Exchange 2010 servers, your Exchange 2003 administrators must be added as members to one or more Exchange 2010 role groups. You can add either users or USGs to role groups. The permissions granted to the role groups will then be applied to the users or USGs you add as members.

Important:

If you use domain local or global Active Directory security groups, you must change them to USGs if you want to add them as members of an Exchange 2010 role group. Exchange

2010 supports only USGs.

The following table provides a mapping between Exchange 2003 administrative roles and Exchange 2010 role groups.

Exchange 2003 administrative roles and Exchange 2010 role groups

Exchange 2003 administrative role	Exchange 2010 role group
Exchange Full Administrator	Organization Management
Exchange Administrator	There is no equivalent role group included with Exchange 2010. A custom role group that's based on the Organization Management role group, but without any delegating role assignments, must be created in Exchange 2010 to have a role group equivalent to the Exchange Administrator role group. For more information about creating custom role groups, see Create a Role Group.
Exchange View Only	View Only Organization Management

If all your Exchange 2003 administrators are members of one of the three Exchange 2003 administrative roles, you need to add the members of each of the administrative groups to their equivalent Exchange 2010 role group. For more information about adding users and USGs to role groups, see Add Members to a Role Group.

If you've modified ACLs on Exchange 2003 objects to grant more granular permissions to Exchange 2003 administrators, and want to assign similar permissions to Exchange 2010 servers to those administrators, you must do the following:

1. Inventory the ACL customization you've done on your Exchange 2003 objects, and identify the administrators granted permissions to each.
2. Classify each Exchange 2003 object, for example, whether it's a database, server, or recipient object.
3. Map the objects to the corresponding Exchange 2010 role group. For a list of built-in role groups, see Built-in Role Groups.
4. Add the USGs or users for each type of object to the corresponding Exchange 2010 role groups. For more information about adding users and USGs to role groups, see Add Members to a Role Group.

When you're done, your Exchange 2003 administrators should be members of the role group that maps to the Exchange 2010 objects they need to administer. They can now use the Exchange 2010 management tools to manage the Exchange 2010 servers and recipients.

Important:

In general, Exchange 2003 servers and recipients must be managed by Exchange 2003 management tools, and Exchange 2010 servers and recipients must be managed by Exchange 2010 management tools. For more information, see Exchange 2003 - Planning Roadmap for Upgrade and Coexistence.

If the built-in role groups don't give you the specific set of permissions you want to grant to some administrators, you can create custom role groups. When you create a custom role group, you can choose which roles you want to add to it. This enables you to define the specific features you want members of the role group to manage. For example, if you only want administrators to manage distribution groups, you can create a custom role group and choose just the Distribution Groups role. Members of that custom role group

will only be able to manage distribution groups. For more information about how to create custom role groups, see Create a Role Group.

If you've given selective permissions to certain Exchange 2003 objects, such as allowing administrators to administer only specific databases, and you want to apply the same configuration to your Exchange 2010 servers, see "Re-Create Exchange 2003 ACL Customization Using Management Scopes in Exchange 2010" later in this topic.

Grant Exchange 2003 Permissions to Exchange 2010 Administrators

If you want Exchange 2010 administrators to administer Exchange 2003 servers, you need to add your Exchange 2010 administrators to one of the three Exchange 2003 administrative groups or add them to the appropriate ACLs if you've customized your Exchange 2003 permissions. You can add either users or USGs to Exchange 2003 administrative groups. Role groups are USGs so they can be added directly to Exchange 2003 administrative groups. This topic discusses adding Exchange 2010 administrators to the built-in Exchange 2003 administrative groups.

The same mapping between Exchange 2010 role groups and Exchange 2003 administrative roles that's shown in the "Exchange 2003 administrative roles and Exchange 2010 role groups" table earlier in this topic applies. If you want your Exchange 2010 organization administrators to have full access to your Exchange 2003 administrative roles, add the Organization Management role group to the Exchange Full Administrators administrative group. Do the same with the View Only Organization Management role group and the Exchange View Only administrative group.

When you're done, your Exchange 2010 administrators should be members of the administrative group that maps to the role group they're in. They can now use the Exchange 2003 management tools to manage the Exchange 2003 servers and recipients.

Important:

In general, Exchange 2003 servers and recipients must be managed by Exchange 2003 management tools and Exchange 2010 servers and recipients must be managed by Exchange 2010 management tools. For more information, see Exchange 2003 - Planning Roadmap for Upgrade and Coexistence.

For more information about adding users or USGs to Exchange 2003 administrative groups, see Knowledge Base article 823018, Overview of Exchange administrative role permissions in Exchange 2003.

Re-Create Exchange 2003 ACL Customization Using Management Scopes in Exchange 2010

In Exchange 2003, if you want to restrict who can administer a specific mailbox store, administer specific users, or control which mailbox store mailboxes are created on, you need to modify the ACLs on the objects you want to restrict. Exchange 2010 provides the same capabilities, but without having to modify any ACLs. It does this by making use of management scopes, which are a component of RBAC.

Management scopes provide the ability to use built-in scopes and custom scopes to define what objects administrators can manage. By applying management scopes, you can define which recipients can be administered, which mailbox databases mailboxes can be created on, and which recipients or servers should be administered by a small group of administrators and no one else.

The following types of management scopes can be created:

- **Predefined relative** Predefined relative scopes are included with Exchange 2010. You can control what a user sees and is able to modify. For example, predefined relative scopes can control whether users see only information about themselves or information about the whole organization.

- **Recipient** Recipient scopes control which recipients an administrator can create, modify, or delete. These can be based on an organizational unit (OU), a recipient filter, or both. Recipient filters specify the criteria that a recipient must match to be included in the scope. For example, you might create a recipient filter scope that includes all users in a certain location or in a specific department. You can even combine OUs and recipient filters to match only users who are within a specific OU and only report to a specific manager.
- **Server** Server scopes control which servers an administrator can manage. You can specify either server lists or server filters. With server lists, you define a static list of servers that can be managed. Server filters work the same way as recipient filters, where you can specify criteria that needs to be matched. For example, you might create a server scope that matches all servers within a particular Active Directory site.
- **Database** Database scopes control which databases an administrator can manage. They can also control which databases mailboxes can be created on or moved to. Like server scopes, they can be defined as lists or as filters. For example, you might want to create a list or filter that allows administrators to create or move mailboxes on specific mailbox databases managed by a particular subsidiary.
- **Exclusive** With the exception of predefined relative scopes, any of the preceding scopes can also be created as exclusive scopes. Exclusive scopes work like deny access control entries (ACEs) in ACLs. If anything matches an exclusive scope, only the administrators assigned an exclusive scope can manage that object, even if another scope that's not exclusive, matches the same object. This is especially useful for executives, where you might want only a few highly trusted individuals to be able to manage their mailboxes. Even if another, broader, regular recipient scope includes the executive's mailbox in their scope, the administrators assigned the broader, regular recipient scope won't be able to manage that executive's mailbox unless they are also assigned the exclusive scope.

Management scopes are used with management roles, management role assignments, and management role groups to control who can manage what objects, and where. For more information, see the following topics:

- Understanding Management Role Scopes
- Understanding Exclusive Scopes
- Understanding Management Role Assignments
- Understanding Management Role Groups
- Understanding Management Roles

To create the same permissions model in Exchange 2010 using management scopes that you might have defined in Exchange 2003 using customized ACLs, you need to inventory the ACLs you've customized and create management scopes that match them. You can use the filterable properties available on recipient, server, and database objects, to create management scopes that include the objects you want each management scope to control access to. For more information about the properties you can use with management scope filters, see Understanding Management Role Scope Filters.

For more information about creating management scopes, see Create a Regular or Exclusive Scope.

1.3.1.4 Understanding Permissions Coexistence with Exchange 2007

Understanding Permissions Coexistence with Exchange 2007

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The permissions model in Microsoft Exchange Server 2010 is improved from the models used in earlier versions of Exchange. Exchange 2010 includes Role Based Access Control (RBAC) permissions that replace the Active Directory access control entry (ACE)-based authorization model used in Microsoft Exchange Server 2007. RBAC is the authorization mechanism used for most of the management of Exchange 2010. This mechanism includes the following management areas:

- Exchange Management Shell
- Exchange Control Panel
- Exchange Management Console (EMC)
- Exchange Web Services
- MAPI on the middle-tier component

For more information about how to plan coexistence between Exchange 2010 and earlier versions of Exchange, see Understanding Upgrade to Exchange 2010.

Looking for management tasks related to permissions? Check out Managing Permissions.

Exchange 2010 Permissions

The Exchange 2010 RBAC permissions model consists of management role groups assigned one of several management roles. Management roles contain permissions that enable administrators to perform tasks in the Exchange organization. Administrators are added as members of the role groups and are granted all the permissions that the roles provide. The following table provides an example of the role groups, some of the roles assigned to role groups, and a description of the kind of user who might be a member of the role group.

Examples of role groups and roles in Exchange 2010

Management role group	Management roles	Members of this role group
Organization Management	The following roles are some of the roles assigned to this role group: • Address Lists • Exchange Servers • Journaling • Mail Recipients • Public Folders	Users who manage the entire Exchange 2010 organization should be members of this role group. With some exceptions, members of this role group can manage nearly any aspect of the Exchange 2010 organization. By default, the user account used to prepare Active Directory for Exchange 2010 is a member of this role group. For more information about this role group and for a complete list of roles assigned to this role group, see Organization Management.

View Only Organization Management	The following roles are assigned to this role group: • Monitoring • View-Only Configuration • View-Only Recipients	Users who view the configuration of the entire Exchange 2010 organization should be members of this role group. These users must be able to view server configuration and recipient information, and perform monitoring functions without the ability to change organization or recipient configuration. For more information about this role group, see View-Only Organization Management.
Recipient Management	The following roles are assigned to this role group: • Distribution Groups • Mail Enabled Public Folders • Mail Recipient Creation • Mail Recipients • Message Tracking • Migration • Move Mailboxes • Recipient Policies	Users who manage recipients such as mailboxes, contacts, and distribution groups in the Exchange 2010 organization should be members of this role group. These users can create recipients, modify or delete existing recipients, or move mailboxes. For more information about this role group and for a complete list of roles assigned to this role group, see Recipient Management.
Server Management	The following roles are some of the roles assigned to this role group: • Databases • Exchange Connectors • Exchange Servers • Receive Connectors • Transport Queues	Users who manage Exchange server configuration such as Receive connectors, certificates, databases, and virtual directories should be members of this role group. These users can modify Exchange server configuration, create databases, and restart and manipulate transport queues. For more information about this role group and for a complete list of roles assigned to this

		role group, see Server Management.
Discovery Management	The following roles are assigned to this role group: • Legal Hold • Mailbox Search	Users who perform searches of mailboxes to support legal proceedings or to configure legal holds should be members of this role group. This is an example of a role group that might contain non-Exchange administrators, such as personnel in the legal department. Legal personnel can perform their tasks without intervention from Exchange administrators. For more information about this role group and for a complete list of roles assigned to this role group, see Discovery Management.

This table shows that Exchange 2010 provides a granular level of control over the permissions that you grant to your administrators. You can choose among 11 role groups in Exchange 2010. For a complete list of role groups and the permissions that they provide, see Built-in Role Groups.

Because Exchange 2010 provides many role groups and because further customization is possible by creating role groups that have different role combinations, the manipulation of access control lists (ACLs) on Active Directory objects is no longer necessary and has no effect. ACLs are no longer used to apply permissions to individual administrators or groups in Exchange 2010. All tasks, such as an administrator creating a mailbox or a user accessing a mailbox, are managed by RBAC. RBAC authorizes the task, and then Exchange performs the task on behalf of the user if allowed. Exchange performs the task in the Exchange Trusted Subsystem universal security group (USG). With some exceptions, all the ACLs on objects in Active Directory that Exchange 2010 has to access are granted to the Exchange Trusted Subsystem USG. This is a fundamental change from how permissions are handled in Exchange 2007.

The permissions granted to a user in Active Directory are separate from the permissions granted to the user by RBAC when that user is using the Exchange 2010 management tools.

For more information about RBAC, see Understanding Role Based Access Control.

Exchange 2007 Permissions

The Exchange 2007 administrative model leverages Active Directory forests to define security boundaries. There is no isolation of security permissions within a particular forest.

Forest owners and enterprise administrators can always gain access to all resources in any domain. In Exchange 2007, you may have to grant enterprise administrator rights and top-level domain administrator rights on a temporary basis only.

Exchange 2007 provides the following predefined administrator roles:

- **Exchange Organization Administrator role** This role grants permissions to control all aspects of the Exchange 2007 organization. Additionally, an administrator who has this role can grant permissions to other Exchange administrators. This role is granted to the account that you use to install Exchange 2007.
- **Exchange View-Only Administrator role** This role grants permissions to view Exchange configuration. However, an administrator who has this role can't modify objects in the Exchange 2007 organization.
- **Exchange Recipient Administrator role** This role grants permissions to manage e-mail recipients. An administrator who has this role can modify Exchange-related items for users, groups, contacts, and distribution groups.
- **Exchange Server Administrator role** This role grants permissions to manage a specific server. However, this role doesn't grant permissions to perform actions that have a global impact on the Exchange 2007 organization.
- **Exchange Public Folder Administrator role** This role was added in Exchange 2007 Service Pack 1**.** This role grants permissions to manage public folders in the Exchange 2007 organization.

This permissions model uses USGs for all roles except for the Exchange Server Administrator role. When you run the Exchange 2007 **Setup /PrepareAD** command, the Setup program creates the USGs in the root domain and gives a forest-wide scope to the USGs. The USGs are assigned ACLs to manage Exchange objects throughout Active Directory.

In Exchange 2007, you can separate administrators by assigning them various roles. The permissions are assigned directly either to the user or to the USG of which the user is a member. Any actions performed by the user are performed in the context of that user's Active Directory account. The following table lists the Exchange 2007 administrator roles together with their Exchange-related permissions.

Exchange 2007 administrator roles

Administrator role	Members	Member of	Exchange permissions
Exchange Organization Administrator	The Administrator account or the account used to install the first Exchange 2007 server	Exchange Recipient Administrator Administrators local group of *<server name>*	Full control of the Microsoft Exchange container in Active Directory
Exchange View-Only Administrator	Exchange Recipient Administrators Exchange Server Administrators (*<server name>*)	Exchange Recipient Administrators Exchange Server Administrators	Read access to the Microsoft Exchange container in Active Directory Read access to all the Windows domains that have Exchange recipients
Exchange Recipient Administrator	Exchange Organization Administrators	Exchange View-Only Administrators	Full control of Exchange properties on Active Directory user objects

Exchange Server Administrator	Exchange Organization Administrators	Exchange View-Only Administrators Administrators local group of *<server name>*	Full control of Exchange *<server name>*
Exchange Server	Each Exchange 2007 computer account	Exchange View-Only Administrators	Special
Exchange Public Folder Administrator	Exchange Organization Administrators	Exchange View-Only Administrators	Full control to manage all public folders (granted the Create top level public folder extended right)

If you need to make more granular permission assignments, you can modify the ACLs on individual Exchange 2007 objects, such as address lists or databases. You must add the user or security group of which the user is a member directly to the ACL. Then, the actions are performed in the context of the particular user.

For more information about how to manage permissions in Exchange 2007, see Configuring Permissions in Exchange Server 2007.

Exchange 2010 and Exchange 2007 Coexistence Permissions

Because the permissions models for Exchange 2010 and for Exchange 2007 differ, Exchange 2010 permission assignments are separate from Exchange 2007 permission assignments. This is true even if both versions of Exchange are installed in the same forest. Without additional configuration, Exchange 2010 administrators don't have the required permissions to manage Exchange 2007-based servers, and Exchange 2007 administrators don't have the required permissions to manage Exchange 2010-based servers. You should consider the following questions:

- Do you want to grant Exchange 2010 administrators access to manage Exchange 2007 servers?
- Do you want to grant Exchange 2007 administrators access to manage Exchange 2010 servers?
- Do you want to customize Exchange 2010 permissions so that they match any customizations that have been made to Exchange 2007 ACLs?

Granting Exchange 2010 Permissions to Exchange 2007 Administrators

If you want Exchange 2007 administrators to administer Exchange 2010 servers, the Exchange 2007 administrators must be added as members of one or more Exchange 2010 role groups. You can add either users or USGs to role groups. The permissions granted to the role groups are then applied to the users or the USGs that you add as members.

Important:

If you use domain local or global Active Directory security groups, you must change them to USGs if you want to add them as members of an Exchange 2010 role group. Exchange 2010 supports only USGs.

The following table describes the mapping between Exchange 2007 administrator roles and Exchange 2010 role groups.

Exchange 2007 administrator roles and Exchange 2010 role groups

Exchange 2007 administrator role	Exchange 2010 role group
Exchange Organization Administrator	Organization Management
Exchange Recipient Administrator	Recipient Management
Exchange Server Administrator	Server Management
Exchange View-Only Administrator	View Only Organization Management
Exchange Server	No equivalent role group in Exchange 2010 (For more information about how to create custom role groups, see Create a Role Group.)
Exchange Public Folder Administrator	Public Folder Management

If all your Exchange 2007 administrators are members of one of the Exchange 2007 administrative roles, you can add the members of each of the administrative groups to their equivalent Exchange 2010 role group. For example, if you want to give all Exchange 2007 organization administrators full access to Exchange 2010 objects, add the Exchange Organization Administrators USG to the Organization Management role group.

For more information about how to add users and USGs to role groups, see Add Members to a Role Group.

If you modify ACLs on Exchange 2007 objects to grant more granular permissions to Exchange 2007 administrators, and if you want to assign similar permissions to Exchange 2010 servers to those administrators, follow these steps:

1. Review the ACL customizations that have been made to the Exchange 2007 objects, and locate the administrators who have been granted permissions to each object.
2. Categorize each Exchange 2007 object. For example, determine whether the object is a database, server, or recipient object.
3. Map the objects to the corresponding Exchange 2010 role group. For a list of built-in role groups, see Built-in Role Groups.
4. Add the USGs or users for each kind of object to the corresponding Exchange 2010 role groups. For more information about how to add users and USGs to role groups, see Add Members to a Role Group.

After you complete these steps, the Exchange 2007 administrators will be members of the specific role group that's mapped to the appropriate Exchange 2010 objects. The Exchange 2007 administrators can use the Exchange 2010 management tools to manage the Exchange 2010 servers and recipients.

Important:

In general, Exchange 2007 servers and recipients must be managed by using Exchange 2007 management tools, and Exchange 2010 servers and recipients must be managed by using Exchange 2010 management tools.

If the built-in role groups don't provide the specific set of permissions that you want to grant to some administrators, you can create custom role groups. When you create a custom role group, you can select which roles to add to it. You can define the specific features you want members of the role group to manage. For example, if you want administrators to manage only distribution groups, you can create a custom role group, and then select only the Distribution Groups role. After you do this, members of that custom role group can manage only distribution groups. For more information about how to create custom role groups, see Create a Role Group.

If you assign selective permissions to certain Exchange 2007 objects (for example, you allow administrators to administer only specific databases), and if you want to apply the same configuration to your Exchange 2010 servers, see "Re-Creating Exchange 2007 ACL Customization Using Management Scopes in Exchange 2010" later in this topic.

Granting Exchange 2007 Permissions to Exchange 2010 Administrators

If you want Exchange 2010 administrators to administer Exchange 2007 servers, add the Exchange 2010 administrators to the USGs or the security group that corresponds to the particular Exchange 2007 administrator role. Alternatively, if you have customized ACL settings, add the administrators to the appropriate ACLs. Role groups are USGs, so role groups can be added directly to Exchange 2007 administrator role USGs.

After you finish, the Exchange 2010 administrators will be members of the appropriate Exchange 2007 administrator role or roles. The Exchange 2010 administrators can use the Exchange 2007 management tools to manage Exchange 2007 servers and recipients.

Re-Creating Exchange 2007 ACL Customization Using Management Scopes in Exchange 2010

In Exchange 2007, when you want to restrict who can administer a specific mailbox store, administer specific users, or control which mailbox store mailboxes are created on, you must modify the ACLs on the objects you want to restrict. Exchange 2010 provides the same capabilities, but without having to modify any ACLs. It does this by using management scopes, which are a component of RBAC.

Management scopes provide built-in scopes and custom scopes to define the objects that administrators can manage. By applying management scopes, you can define which recipients can be administered, which mailbox databases mailboxes can be created on, and which recipients or servers should be administered by a small group of administrators and by no one else.

You can create the following types of management scopes:

- **Predefined relative** Predefined relative scopes are included in Exchange 2010. You can control what a user sees and what a user modifies. For example, predefined relative scopes can control whether users see only information about themselves or information about the entire organization.
- **Recipient** Recipient scopes control which recipients an administrator can create, modify, or delete. These selections can be based on an organizational unit (OU), a recipient filter, or both. Recipient filters specify the criteria that a recipient must match to be included in the scope. For example, you might create a recipient filter scope that includes all users in a certain location or in a specific department. You can even combine OUs and recipient filters to match only users who are within a specific OU and who report to a specific manager.
- **Server** Server scopes control which servers an administrator can manage. You can specify either server lists or server filters. For server lists, you define a static list of servers that can be managed. Server filters work in the same manner as recipient filters in that you can specify the criteria that has to be matched. For example, you might create a server scope that matches all servers within a particular Active Directory site.
- **Database** Database scopes control which databases an administrator can manage. They can also control which databases mailboxes can be created on or which databases mailboxes can be moved to. Like server scopes, they can be defined as lists or as filters. For example, you might create a list or filter that allows administrators to create mailboxes on or move mailboxes to specific mailbox databases managed by a specific subsidiary.
- **Exclusive** Recipient, server, and database scopes can also be created as exclusive scopes. Exclusive scopes work in the same manner as deny access ACEs in ACLs. If anything matches an exclusive scope, only the administrators

assigned an exclusive scope can manage that object. This is true even if another scope that isn't exclusive matches the same object. This is especially useful when you might want only a few, highly trusted individuals to be able to manage an executive's mailbox. Even if another regular recipient scope is broader and includes the executive's mailbox in the scope, the administrators assigned the broader, regular recipient scope won't be able to manage that executive's mailbox unless they are also assigned the exclusive scope.

Management scopes are used with management roles, management role assignments, and management role groups to control who can manage what objects and in what manner they can manage those objects. For more information, see the following topics:

- Understanding Management Role Scopes
- Understanding Exclusive Scopes
- Understanding Management Role Assignments
- Understanding Management Role Groups
- Understanding Management Roles

To create the same permissions model in Exchange 2010 using management scopes that you might have defined using customized ACLs, you must inventory the ACLs that you've customized, and then create management scopes that match them. You can use the filterable properties available on recipient, server, and database objects to create management scopes that include the objects to which you want each management scope to control access. For more information about the properties that you can use with management scope filters, see Understanding Management Role Scope Filters.

For more information about how to create management scopes, see Create a Regular or Exclusive Scope.

1.3.1.5 Understanding Multiple-Forest Permissions

Understanding Multiple-Forest Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-06*

Many organizations deploy multiple forests to create security boundaries within their organizations. Using multiple forests helps administrators to define these security boundaries to better match their requirements, whether that's ensuring the fewest number of people have access to resources, or segmenting divisions within an organization.

Microsoft Exchange Server 2010 supports two types of multiple forest topologies:

- **Cross-forest** Cross-forest topologies can have multiple forests, each with their own installation of Exchange.
- **Resource forest** Resource forest topologies have an Exchange forest and one or more accounts forests.

For the purposes of this topic, the forest that contains the universal security groups (USGs) and users outside of the forest where Exchange 2010 is installed, whether it's an accounts forest or other resource forest, is called a foreign forest.

Configuration of permissions in a multiple forest topology relies on the correct configuration of forest trusts and global address list (GAL) synchronization for the creation of linked mailboxes. The Exchange 2010 forest must trust the foreign forest that contains the USGs associated with linked role groups and users associated with linked mailboxes.

For more information about multiple forest topologies, see Deploy Multiple Forest Topologies.

Exchange 2010 uses a Role Based Access Control (RBAC) permissions model. The management role groups that administrators are members of, and the management role assignment policies that end users are assigned, determine what each administrator and end user can do. To understand multiple-forest permissions, you need to be familiar with RBAC. For more information about RBAC, role groups, and role assignment policies, see the following topics:

- Understanding Role Based Access Control
- Understanding Management Role Groups
- Understanding Management Role Assignment Policies

Looking for management tasks related to managing permissions? See Managing Permissions.

Contents

Permissions in a Multiple Forest Topology

RBAC applies permissions to all Exchange objects within a single forest and the RBAC configuration in each forest is configured independently of all other forests. When you create a role group in one forest, that role group doesn't exist in any other forest and the permissions granted by that role group apply only to the forest in which it was created. For example, a member of a role group that grants permissions to create a mailbox can create a mailbox only in the forest that contains that role group.

If you have multiple Exchange forests and want to configure permissions identically within each forest, you must apply the same configuration explicitly in each forest. For example, if you have two Exchange 2010 forests and want to create a Compliance Management role group to manage permissions for your legal department, you must do the following:

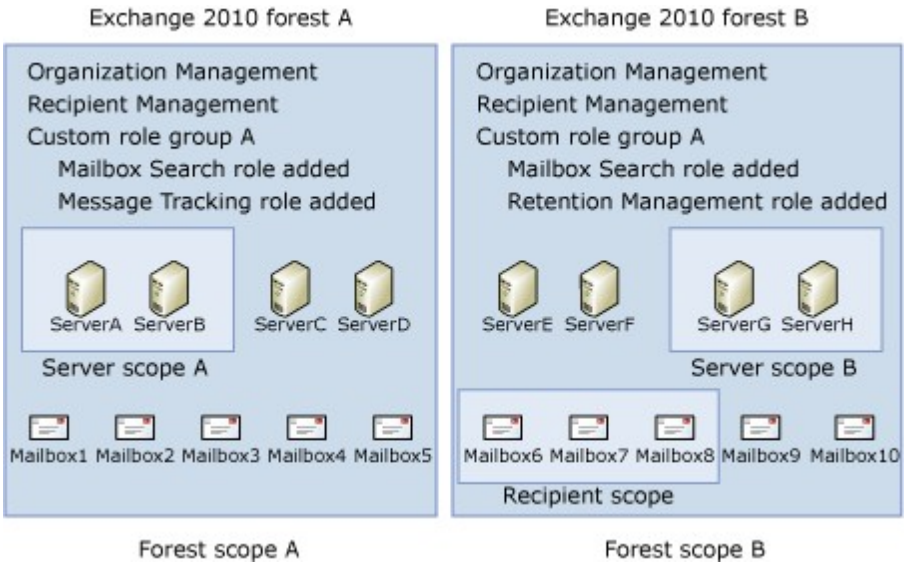
- In each forest, create a role group named Compliance Management. If your administrators are in a separate foreign forest from either Exchange forest, create both role groups as linked role groups. For more information about role groups, see the Cross-Boundary Permissions section.
- In each forest, create role assignments between the new role groups and the roles that you want to use.
- As part of the new role assignments, optionally add management scopes that encompass the server and recipient objects within each forest.
- If you created the role groups as linked role groups, add members to the associated USG in the foreign forest.

The following figure shows how the role groups configured within Exchange 2010 forests are bound to their respective forests. The Organization Management role group in Exchange 2010 forest A grants permissions only to manage the mailboxes and servers that are within that forest. Likewise, the role groups in Exchange 2010 forest B grant permissions only to the mailboxes and servers within that forest.

The figure also shows that the Custom role group A is created in each forest. Even though they were created with the same name, each is its own separate entity. In fact, as the

figure shows, each can be assigned different management roles in their respective forests. Custom role group A in Exchange 2010 forest A is assigned the Mailbox Search and Message Tracking roles while Custom role group A in Exchange 2010 forest B is assigned the Mailbox Search and Retention Management roles.

Finally, management scopes created in each forest are also bound by the forest. Server scopes created in each forest can only contain the servers that are members of that forest. Server scope A can contain only servers within Exchange 2010 forest A while Server scope B can contain only servers that are within Exchange 2010 forest B. Similarly, the recipient scope in Exchange 2010 forest B can only contain mailboxes that are within Exchange 2010 forest B.



Return to top

Cross-Boundary Permissions

The permissions granted by RBAC only allow users to view or modify Exchange objects within a specific forest. However, you can grant permissions to view and modify Exchange objects in a forest to users outside of that forest. By using cross-boundary permissions, you can centralize Exchange management accounts in a single forest rather than having to authenticate against each individual forest to perform tasks.

Note:

The permissions that are granted to a user outside of an Exchange forest still apply only to that specific Exchange forest. For example, if a user in a foreign forest is a member of the Organization Management linked role group that's located in ForestA, the user can manage only the Exchange objects contained within ForestA. A user must be made a member of linked role groups in each Exchange forest to be granted permissions to manage each forest.

Cross-boundary permissions also enable you to apply role assignment policies to the mailboxes of users who have mailboxes in an Exchange forest, but have user accounts that reside in an accounts forest. Exchange 2010 supports cross-boundary permission using linked role groups and linked mailboxes, which are discussed in the following sections.

Administrative Permissions

Administrative permissions are granted cross forest boundaries by the use of linked role

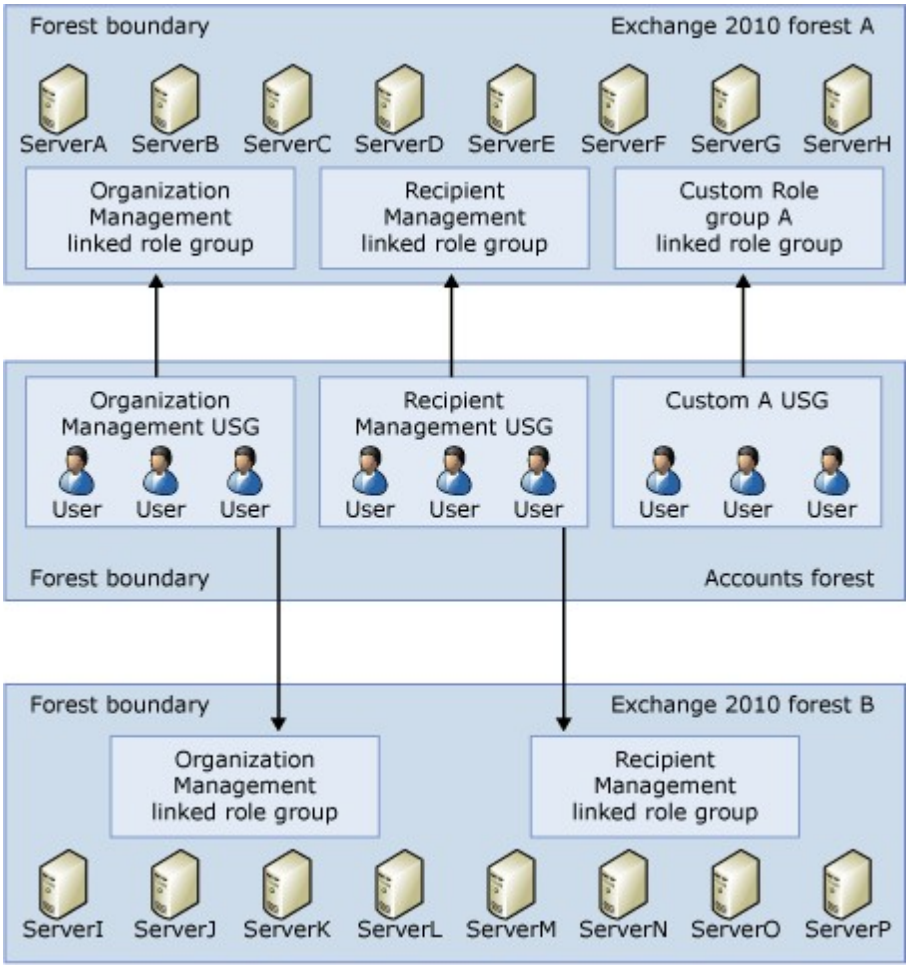
groups and linked mailboxes.

A linked role group is created in the Exchange 2010 organization and is linked to a USG across the forest boundary in the foreign forest. The USG the linked role group is linked to can be any of the following:

- A dedicated USG for the specific use of the linked role group
- A USG that's linked to by linked role groups in multiple Exchange 2010 forests
- A role group USG in another Exchange 2010 forest
- A USG associated with an Exchange Server 2007 administrative role
- A USG that's used to grant permissions to manage an Exchange Server 2003 organization

The USG that a linked role group is linked to must be in another forest. You can't link a linked role group to a USG in the same forest.

The following figure shows that USGs in an accounts forest can be associated with role groups in one or more Exchange 2010 resource forests. The members of the USGs in the accounts forest effectively become members of the role groups through the USGs.



When you create a linked role group, you assign roles to the linked role group in the Exchange 2010 forest. The assignments that associate the roles to the linked role group can include management scopes, if necessary. These scopes are confined to the forest in which the linked role group is created.

Membership of the linked role group is managed by adding and removing members to and

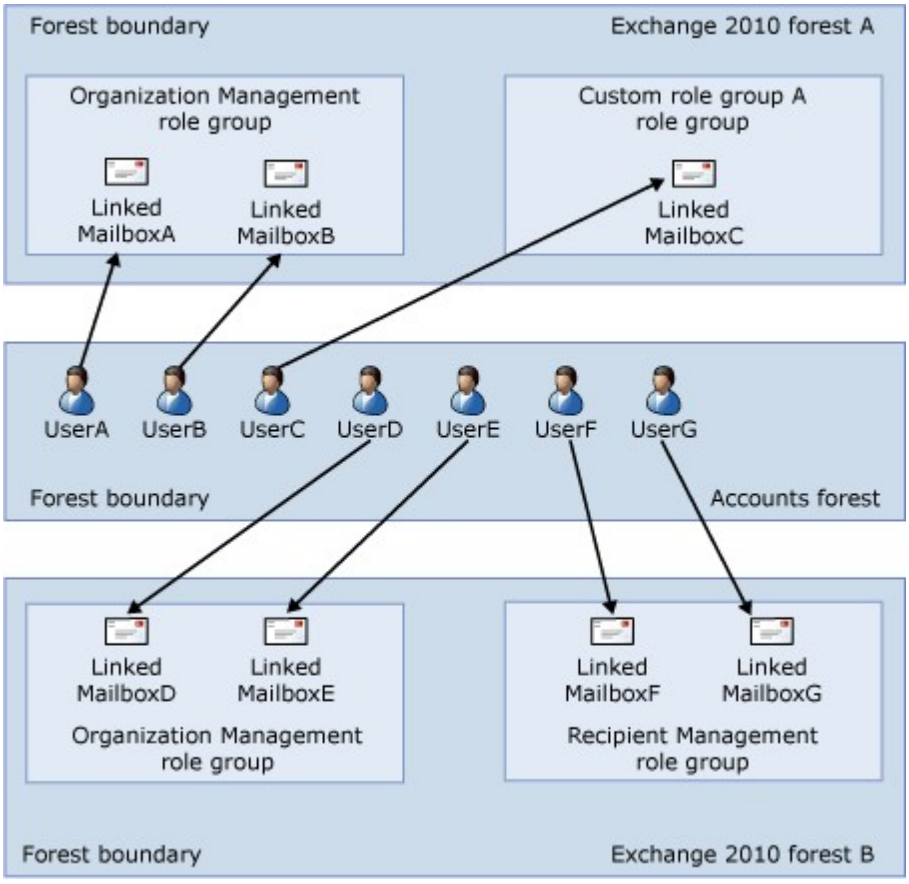
from the USG in the foreign forest. When you add members to this USG, they are granted the permissions assigned to the linked role group in the Exchange 2010 forest. If you've linked multiple linked role groups with the same USG, the members of that USG are granted the permissions assigned to each linked role group in each Exchange 2010 forest.

You can't manage the membership of a linked role group from the Exchange 2010 forest.

A second method to assign administrative permissions across forest boundaries is through the use of linked mailboxes. For users in an accounts forest to use an Exchange 2010 deployment in a separate Exchange 2010 resource forest, you must configure linked mailboxes for each user. Linked mailboxes can be added as members to role groups within the Exchange 2010 forest. When a linked mailbox becomes a member of a role group, that linked mailbox, and in turn the user in the accounts forest associated with the linked mailbox, is granted the permissions provided by the role group.

For more information about linked mailboxes, see Understanding Recipients.

The following figure shows the relationship between users in an accounts forest, the linked mailboxes associated with them, and the role groups in which they're members.



Linked role groups and linked mailboxes both have advantages and disadvantages when used to assign administrative permission across forest boundaries. The following table describes some of them.

Linked role group and linked mailbox advantages and disadvantages

Linked role groups or linked	Advantage	Disadvantage

mailboxes		
Linked role groups	You can associate multiple linked role groups from multiple Exchange 2010 forests to a single USG in an accounts forest or other Exchange resource forest. This enables you to administer complex Exchange forest topologies through a small set of USGs in a single forest.	A regular role group can't be converted to a linked role group. You must manually create linked role groups to replace each regular role group that has the permissions you want to grant across a forest boundary. For more information, see Configure cross-boundary permissions.
Linked mailboxes	Linked mailboxes allow you to use the existing role groups within the Exchange forest. Linked mailboxes are added as members to the existing role groups just like regular mailboxes, USGs, and users in the same Exchange forest.	If you grant permissions in multiple Exchange 2010 forests using linked mailboxes linked to a single user in an accounts forest, you must modify the role group membership in each Exchange 2010 forest if you want to modify the permissions granted to the user.

We recommend that you use linked role groups to grant permission across forest boundaries if you plan on having multiple Exchange resource forests.

End-User Permissions

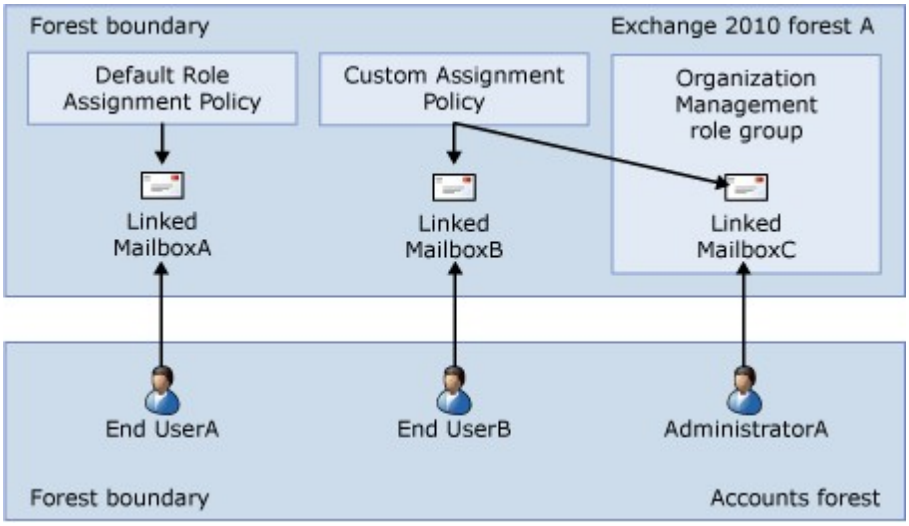
End-user permissions are assigned to individual mailboxes using role assignment policies. When Exchange 2010 is installed in a resource forest, linked mailboxes are created in the resource forest and are associated with user accounts in the accounts forest.

For more information about linked mailboxes, see Understanding Recipients.

When a linked mailbox is created, it's assigned to a default role assignment policy just like a regular mailbox. The role assignment policy determines which end-user permissions are granted to the mailbox. These permissions enable users to view and modify settings related to the following, and other, features:

- End-user profile information
- End-user voicemail
- End-user distribution membership and ownership

When a role assignment policy is assigned to a linked mailbox, the user in the accounts forest associated with the linked mailbox is granted permissions to manage the features available to that user. The permissions apply to only the resources in the Exchange forest where the linked mailbox is located. The following figure shows the relationship between the end user in the accounts forest, its associated linked mailbox, and the role assignment policy assigned to the linked mailbox. Additionally, a linked mailbox associated with an administrative user in the accounts forest can be associated with multiple role groups in addition to a role assignment policy.



For more information about linked mailboxes, see Understanding Recipients.

Return to top

Configure Cross-Boundary Permissions

To configure cross-boundary permissions in a multiple-forest topology, you must create linked role groups for each of the role groups you want to link to USGs in a foreign forest. This means that you must create a linked role group for each built-in role group. You need to:

1. Create a USG in the foreign forest for each linked role group to be created. Add members to this USG that you want to grant permissions to.
2. Create a linked role group for each built-in role group. The following happens when the linked role group is created:
   - The same roles that are assigned to the built-in role group are assigned to the new linked role group.
   - The linked role group is associated with the USG in the foreign forest.
3. Create linked role groups for any custom role groups you created.
4. Optionally assign custom scopes to the new linked role groups.

For detailed information about how to perform these steps, see the following topics:

- Create Linked Role Groups that Mirror Built-in Role Groups
- Create a Linked Role Group
- Change the Scope of Role Assignments to a Role Group

If you need to change the USG that a linked role group is associated with, see Change a Linked Foreign USG on a Linked Role Group.

When a linked mailbox is created, it's automatically assigned to a role assignment policy. You can change the role assignment policy that's assigned to the linked mailbox or change the role assignment policy that's assigned to mailboxes by default when they're created. For more information, see the following topics:

- Change the Assignment Policy on a Mailbox
- Change the Default Assignment Policy

Return to top

1.3.2 Feature Permissions

Feature Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-12*

Permissions in Microsoft Exchange Server 2010 are managed using the Role Based Access Control (RBAC) permissions model. The following topics identify the management role groups required to administer the features associated with each functional area in Exchange 2010. For more information about RBAC, see Understanding Role Based Access Control.

- Mailbox Permissions
- Client Access Permissions
- Transport Permissions
- Unified Messaging Permissions
- Exchange and Shell Infrastructure Permissions
- Role Management Permissions
- High Availability Permissions
- Messaging Policy and Compliance Permissions

1.3.2.1 Mailbox Permissions

Mailbox Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-12-11*

The permissions required to perform tasks on the Mailbox server role vary depending on the procedure being performed or the cmdlet you want to run. For more information about mailbox features, see Mailbox. For a list of permissions related to high availability, see High Availability Permissions.

To find out what permissions you need to perform the procedure or run the cmdlet, do the following:

1. In the table below, find the feature that is most related to the procedure you want to perform or the cmdlet you want to run.
2. Next, look at the permissions required for the feature. You must be assigned one of those role groups, an equivalent custom role group, or an equivalent management role. You can also click on a role group to see its management roles. If a feature lists more than one role group, you only need to be assigned one of the role groups to use the feature. For more information about role groups and management roles, see Understanding Role Based Access Control.
3. Now, run the Get-ManagementRoleAssignment cmdlet to look at the role groups or management roles assigned to you to see if you have the permissions that are necessary to manage the feature.

Note:

You must be assigned the Role Management management role to run the **Get-ManagementRoleAssignment** cmdlet. If you don't have permissions to run the **Get-ManagementRoleAssignment** cmdlet, ask your Exchange administrator to retrieve the role groups or management roles assigned to you.

If you want to delegate the ability to manage a feature to another user, see Delegate Role Assignments.

Mailbox Server Permissions

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Calendar repair, server configuration	Organization Management Server Management
Delegating Mailbox servers	Organization Management
E-mail address policies	Organization Management Server Management
Exchange Search	Organization Management View-Only Organization Management Server Management
Get unsearchable items	Organization Management View-Only Organization Management Support Diagnostics role **Note:** The Support Diagnostics role isn't assigned to a role group. For more information, see Add a Role to a User or USG.
Group metrics	Organization Management Server Management
Import Export	Mailbox Import Export role **Note:** The Mailbox Import Export role isn't assigned to a role group. For more information, see Add the Mailbox Import Export Role to a Role Group.
Mailbox Assistants	Organization Management Server Management
Mailbox moves	Organization Management Recipient Management

Mailbox recovery	Organization Management
Mailbox repair request	Organization Management Server Management Recipient Management
Mailbox restore request	Organization Management
Mailbox server configuration	Organization Management Server Management
Manage Exchange Search Indexer service on a Mailbox server	Local Administrator on the Mailbox server
MAPI connectivity	Organization Management Server Management
OAB virtual directories	Organization Management Server Management
Remove store mailbox	Organization Management Server Management

Calendar and Sharing Permissions

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Calendar configuration	Organization Management Recipient Management
Calendar diagnostics	Organization Management Retention Management Role Help Desk
Calendar processing	Organization Management Recipient Management Help Desk
Notifications	Organization Management Recipient Management
Organization relationships	Organization Management
Sharing policies	Organization Management

Resource Mailbox Configuration Permissions

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Booking policies	Organization Management Recipient Management Help Desk
Delegation	Organization Management Recipient Management
Resource mailbox schema configuration	Organization Management

Address List Permissions

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Address book policies	Organization Management
Address list paging	Organization Management
Address lists	Organization Management
Details templates	Organization Management
File distribution service	Organization Management
Global address lists	Organization Management
Offline address books	Organization Management

Mailbox Database Permissions

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Mailbox databases	Organization Management Server Management

Public Folder Permissions

Users who are assigned the View-Only Management role group can view the configuration

of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Mail-enabled public folders	Organization Management Recipient Management Public Folder Management
Public folder administrative permissions	Organization Management Public Folder Management
Public folder client permissions	Organization Management Public Folder Management
Public folder database repair request	Organization Management Recipient Management Server Management
Public folder databases	Organization Management Server Management
Public folder replication	Organization Management Public Folder Management
Public folders	Organization Management Public Folder Management

Recipient Provisioning Permissions

This table contains the various permissions that are required to manage recipients.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Address list, GAL	Organization Management
Anti-spam	Organization Management Recipient Management
Applying sharing policies	Organization Management Recipient Management
Arbitration	Organization Management
Archive connectivity	Organization Management View-Only Organization Management

	Server Management
Assigning offline address books	Organization Management Recipient Management
Automatic replies	Organization Management Recipient Management Help Desk
Calendar configuration	Organization Management Recipient Management
Calendar repair	Organization Management Recipient Management
Disconnected mailboxes	Organization Management Recipient Management Help Desk
Distribution groups	Organization Management Recipient Management
Dynamic distribution groups	Organization Management Recipient Management
E-mail addresses	Organization Management Recipient Management UM Management
Folder Management	Organization Management Recipient Management
Inbox rules	Organization Management Recipient Management Help Desk
Mail contacts	Organization Management Recipient Management
Mail tips	Organization Management Recipient Management
Mail user	Organization Management Recipient Management

Mailbox folder permissions	Organization Management Recipient Management Help Desk
Mailbox folders	Organization Management Recipient Management
Message configuration	Organization Management Recipient Management Help Desk
Message quotas	Organization Management Recipient Management
Moderation	Organization Management Recipient Management
Permissions and delegation	Organization Management
Personal archives	Organization Management Recipient Management
Recipient data properties	Organization Management Recipient Management
Remote mailboxes	Organization Management Recipient Management
Retention and legal holds	Organization Management Recipient Management Records Management
Send As	Organization Management Recipient Management
Spelling configuration	Organization Management Recipient Management Help Desk
Unified Messaging	Organization Management UM Management
User mailboxes	Organization Management Recipient Management

1.3.2.2 Client Access Permissions

Client Access Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The permissions required to perform tasks on the Client Access server vary depending on the procedure being performed or the cmdlet you want to run. For more information about Client Access features, see Client Access.

To find out what permissions you need to perform the procedure or run the cmdlet, do the following:

1. In the table below, find the feature that is most related to the procedure you want to perform or the cmdlet you want to run.
2. Next, look at the permissions required for the feature. You must be assigned one of those role groups, an equivalent custom role group, or an equivalent management role. You can also click on a role group to see its management roles. If a feature lists more than one role group, you only need to be assigned one of the role groups to use the feature. For more information about role groups and management roles, see Understanding Role Based Access Control.
3. Now, run the Get-ManagementRoleAssignment cmdlet to look at the role groups or management roles assigned to you to see if you have the permissions that are necessary to manage the feature.

Note:
You must be assigned the Role Management management role to run the **Get-ManagementRoleAssignment** cmdlet. If you don't have permissions to run the **Get-ManagementRoleAssignment** cmdlet, ask your Exchange administrator to retrieve the role groups or management roles assigned to you.

If you want to delegate the ability to manage a feature to another user, see Delegate Role Assignments.

Note:
Some features may require that you have local administrator permissions on the server you want to manage. To manage these features, you must be a member of the Local Administrators group on that server.

Client Access Server Permissions

You can configure any of the following for the Client Access server role.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Client Access server settings	Server Management
Client Access server security settings	Server Management

Client Access server management settings	Server Management
Client Access server user settings	Server Management
Client Access server array settings	Organization Management Server Management
Client Access user settings	Server Management
RPC Client Access settings	Organization Management Server Management View-Only Organization Management
Client Access service e-mail channel settings	Organization Management Server Management
Reset Client Access virtual directories	Organization Management Server Management

Exchange ActiveSync Permissions

You can configure any of the following for Exchange ActiveSync.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Exchange ActiveSync settings	Organization Management Server Management
Exchange ActiveSync virtual directory settings	Organization Management Server Management
Exchange ActiveSync mailbox policy settings	Organization Management Server Management
Exchange ActiveSync user settings	Recipient Management
Exchange ActiveSync server settings	Organization Management Server Management
Exchange ActiveSync security settings	Organization Management Server Management
Exchange ActiveSync device settings	Recipient Management

Autodiscover Permissions

You can configure the following for the Autodiscover service.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Autodiscover virtual directory settings	Organization Management Server Management View-Only Organization Management Delegated Setup Hygiene Management
Test Autodiscover service connectivity	Organization Management Server Management View-Only Organization Management
Autodiscover service configuration settings	Organization Management Server Management View-Only Organization Management Delegated Setup Hygiene Management
Autodiscover service site affinity	Organization Management Server Management

Availability Service Permissions

You can configure the following for the Availability service.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Availability service address space settings	Organization Management View-Only Organization Management
Availability service configuration settings	Organization Management Server Management View-Only Organization Management

Client Throttling Permissions

You can configure the following for client throttling.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Client throttling settings	Organization Management View-Only Organization Management

Exchange Control Panel Permissions

You can configure the following for Exchange Control Panel (ECP).

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Exchange Control Panel virtual directory settings	Organization Management View-Only Organization Management
Test ECP	Organization Management
User reporting	Organization Management
User options	Organization Management

Exchange Web Services Permissions

You can configure the following for Web Services virtual directories.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Exchange Web Services virtual directory settings	Organization Management
Test Exchange Web Services	Organization Management Server Management
Test Outlook Web Services	Organization Management

Outlook Anywhere Permissions

You can configure and manage the following settings for Outlook Anywhere.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required

SSL for Outlook Anywhere	ISA Server Enterprise Administrator
SSL offloading for Outlook Anywhere	Organization Management Server Management
Authentication for Outlook Anywhere	Organization Management Server Management
Outlook Anywhere configuration (enable, disable, change, view)	Organization Management Server Management View-Only Organization Management Delegated Setup Hygiene Management
RPC over HTTP Proxy component	Local Server Administrator
Test Outlook Anywhere connectivity	Organization Management View-Only Organization Management Server Management

Outlook Web App Permissions

You can use the following features to view Outlook Web App settings, control security and user access to Outlook Web App, and test Outlook Web App connectivity.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Outlook Web App virtual directories	Organization Management Server Management
Outlook Web App mailbox policies	Organization Management Recipient Management
View Outlook Web App virtual directories	Organization Management Server Management View-Only Organization Management Delegated Setup Hygiene Management
View Outlook Web App mailbox policies	Organization Management Recipient Management

	View-Only Organization Management Delegated Setup Hygiene Management
Test Outlook Web App connectivity	Organization Management Server Management View-Only Organization Management
IIS Manager	Local Server Administrator
Registry Editor	Local Server Administrator
Text editor	Local Server Administrator
Graphics editor	Local Server Administrator
ISA Server 2006	ISA Server Enterprise Administrator

POP3 and IMAP4 Permissions

You can configure the following for POP3 and IMAP4.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
POP3 settings	Organization Management View-Only Organization Management
IMAP4 settings	Organization Management View-Only Organization Management
Test POP3 settings	Organization Management
Test IMAP4 settings	Organization Management

Windows PowerShell Virtual Directory Permissions

You can configure the following for Windows PowerShell.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
PowerShell settings	Organization Management
Test PowerShell	Organization Management

Text Messaging Permissions

You can configure the following for Text Messaging.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Text messaging settings	Recipient Management
Text messaging user settings	Recipient Management
Text messaging notification settings	Recipient Management

1.3.2.3 Transport Permissions

Transport Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-30*

The permissions required to perform tasks on the Edge Transport and Hub Transport server roles vary depending on the procedure being performed or the cmdlet you want to run. For more information about transport features, see Transport.

This topic lists the permissions required to manage the Transport features in Microsoft Exchange Server 2010.

To find out what permissions you need to perform the procedure or run the cmdlet, do the following:

1. In the table below, find the feature that is most related to the procedure you want to perform or the cmdlet you want to run.
2. Next, look at the permissions required for the feature. You must be assigned one of those role groups, an equivalent custom role group, or an equivalent management role. You can also click on a role group to see its management roles. If a feature lists more than one role group, you only need to be assigned one of the role groups to use the feature. For more information about role groups and management roles, see Understanding Role Based Access Control.
3. Now, run the Get-ManagementRoleAssignment cmdlet to look at the role groups or management roles assigned to you to see if you have the permissions that are necessary to manage the feature.

Note:

You must be assigned the Role Management management role to run the **Get-ManagementRoleAssignment** cmdlet. If you don't have permissions to run the **Get-ManagementRoleAssignment** cmdlet, ask your Exchange administrator to retrieve the role groups or management roles assigned to you.

If you want to delegate the ability to manage a feature to another user, see Delegate Role Assignments.

Note:
Some features that you want to manage might exist on Edge Transport servers. To manage features on Edge Transport servers, you need to become a member of the Local Administrators group on the Edge Transport server you want to manage. Edge Transport servers don't use Role Based Access Control (RBAC). Features that can be managed on Edge Transport servers have Edge Transport Local Administrator in the "Permissions required" column in the table below. For more information about Edge Transport permissions, see Setting Administrator Permissions for the Edge Transport Server Role.

Note:
Some features may require that you have local administrator permissions on the server you want to manage. To manage these features, you must be a member of the Local Administrators group on that server.

Transport Permissions

You can use the features in the following table to configure settings on Hub Transport and Edge Transport servers. The permissions that are required to configure each feature are listed.

Users who are assigned the View Only Management role group can view the configuration of the features shown in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Accepted domains	Organization Management
Accepted domains - Edge Transport	Edge Transport Local Administrator
Active Directory site and site link management	Organization Management
Address Rewriting agent	Edge Transport Local Administrator
Anti-spam features	Organization Management Hygiene Management
Anti-spam features - Edge Transport	Edge Transport Local Administrator
Anti-spam updates	Organization Management Hygiene Management
Anti-spam updates - Edge Transport	Edge Transport Local Administrator
Certificate management	Organization Management
Delivery Agent connectors	Organization Management Server Management
DSNs	Organization Management
Edge Transport server	Edge Transport Local Administrator
EdgeSync	Organization Management
EdgeSync - Edge Transport	Edge Transport Local Administrator
Foreign connectors	Organization Management

Hub Transport server	Organization Management Server Management
Journaling	Organization Management Records Management
Mailbox junk e-mail configuration	Organization Management Records Management Recipient Management Help Desk
MailTips	Organization Management
Message classifications	Organization Management Records Management
Message tracking	Organization Management Records Management Recipient Management
Moderated transport	Organization Management Recipient Management
Queues	Organization Management Server Management
Queues - Edge Transport	Edge Transport Local Administrator
Receive connectors	Organization Management Server Management Hygiene Management
Receive connectors - Edge Transport	Edge Transport Local Administrator
Remote domains	Organization Management
Routing Group connectors	Organization Management Server Management
SafeList aggregation	Organization Management Records Management
Send connectors	Organization Management
Send connectors - Edge Transport	Edge Transport Local Administrator
Shadow redundancy	Organization Management

Testing mail flow	Organization Management Server Management
Testing Transport rule processing	Organization Management
Transport agents	Organization Management Records Management
Transport configuration	Organization Management
Transport configuration - Edge Transport	Edge Transport Local Administrator
Transport logs	Organization Management Server Management
Transport logs - Edge Transport	Edge Transport Local Administrator
Transport rules	Organization Management Records Management
Transport rules - Edge Transport	Edge Transport Local Administrator
X.400 domains	Organization Management

1.3.2.4 Unified Messaging Permissions

Unified Messaging Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The permissions required to perform tasks on the Unified Messaging (UM) server role vary depending on the procedure being performed or the cmdlet you want to run. For more information about Unified Messaging features, see Unified Messaging.

To find out what permissions you need to perform the procedure or run the cmdlet, do the following:

1. In the table below, find the feature that is most related to the procedure you want to perform or the cmdlet you want to run.
2. Next, look at the permissions required for the feature. You must be assigned one of those role groups, an equivalent custom role group, or an equivalent management role. You can also click on a role group to see its management roles. If a feature lists more than one role group, you only need to be assigned one of the role groups to use the feature. For more information about role groups and management roles, see Understanding Role Based Access Control.
3. Now, run the Get-ManagementRoleAssignment cmdlet to look at the role groups or management roles assigned to you to see if you have the permissions that are necessary to manage the feature.

Note:

You must be assigned the Role Management management role to run the

Get-ManagementRoleAssignment cmdlet. If you don't have permissions to run the **Get-ManagementRoleAssignment** cmdlet, ask your Exchange administrator to retrieve the role groups or management roles assigned to you.

If you want to delegate the ability to manage a feature to another user, see Delegate Role Assignments.

UM Component Permissions

You can configure settings for the Unified Messaging components and features in the following table.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
UM auto attendants	Organization Management UM Management
UM call data and summary reports	Organization Management UM Management
UM dial plans	Organization Management UM Management
UM hunt groups	Organization Management UM Management
UM IP gateways	Organization Management UM Management
UM mailbox policies	Organization Management UM Management
UM mailboxes	Organization Management UM Management
UM prompts	Organization Management UM Management
UM server	Organization Management Server Management

1.3.2.5 Exchange and Shell Infrastructure Permissions

Exchange and Shell Infrastructure Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The permissions required to perform tasks to configure various components of Microsoft Exchange Server 2010 depend on the procedure being performed or the cmdlet you want to run. See each of the sections in this topic for more information about their respective features.

To find out what permissions you need to perform the procedure or run the cmdlet, do the following:

1. In the table below, find the feature that is most related to the procedure you want to perform or the cmdlet you want to run.
2. Next, look at the permissions required for the feature. You must be assigned one of those role groups, an equivalent custom role group, or an equivalent management role. You can also click on a role group to see its management roles. If a feature lists more than one role group, you only need to be assigned one of the role groups to use the feature. For more information about role groups and management roles, see Understanding Role Based Access Control.
3. Now, run the Get-ManagementRoleAssignment cmdlet to look at the role groups or management roles assigned to you to see if you have the permissions that are necessary to manage the feature.

Note:
You must be assigned the Role Management management role to run the **Get-ManagementRoleAssignment** cmdlet. If you don't have permissions to run the **Get-ManagementRoleAssignment** cmdlet, ask your Exchange administrator to retrieve the role groups or management roles assigned to you.

If you want to delegate the ability to manage a feature to another user, see Delegate Role Assignments.

Note:
Some features may require that you have local administrator permissions on the server you want to manage. To manage these features, you must be a member of the Local Administrators group on that server.

Exchange Infrastructure Permissions

The following table lists the permissions required to perform tasks that configure general Exchange 2010 settings. For more information, see the following topics:

- Overview of Administrator Audit Logging
- Exchange Management Console
- Enter Product Key
- Opt-in or Opt-out of the Customer Experience Improvement Program
- Set-ExchangeAssistanceConfig
- Get-MessageCategory
- Test-SystemHealth

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Administrator audit logging	Organization Management Records Management
Exchange Help settings	Organization Management
Exchange Management Console configuration settings	View-Only Organization Management
Exchange server configuration settings	Organization Management Server Management
Message categories	Organization Management Hygiene Management Recipient Management Help Desk
Test system health	Organization Management Server Management
Product key	Organization Management
View-only administrator audit logging	Organization Management Records Management **Note:** You can also manually assign the View-Only Audit Logs management role to a management role group. For more information, see View-Only Audit Logs Role.
Write to audit log	Users that are members of any role group or assigned any management role can write to the administrator audit log.

Shell Infrastructure Permissions

The following table lists the permissions required to perform tasks that configure features that control how the Exchange Management Shell runs. For more information about each of the features listed in this topic, see the following topics:

- Overview of Exchange Management Shell
- Understanding Cmdlet Extension Agents
- Overview of Administrator Audit Logging

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Active Directory Domain Services server settings	Organization Management Server Management

	Recipient Management UM Management
Cmdlet extension agents	Organization Management
PowerShell virtual directories	Organization Management Server Management
Remote Shell	Organization Management
PowerShell and WinRM installation	Local Server Administrator

Federation and Certificates Permissions

The following table lists permissions required for performing tasks related to federation trusts, certificate management, and hybrid configuration.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Federation trusts	Organization Management
Test federation trusts	Organization Management View-Only Organization Management Server Management
Certificate management	Organization Management Server Management
Hybrid configuration	Organization Management

1.3.2.6 Role Management Permissions

Role Management Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The permissions required to perform tasks to configure management roles vary depending on the procedure being performed or the cmdlet you want to run. For more information about management roles, see Understanding Management Roles.

To find out what permissions you need to perform the procedure or run the cmdlet, do the following:

1. In the table below, find the feature that is most related to the procedure you want to perform or the cmdlet you want to run.

2. Next, look at the permissions required for the feature. You must be assigned one of those role groups, an equivalent custom role group, or an equivalent management role. You can also click on a role group to see its management roles. If a feature lists more than one role group, you only need to be assigned one of the role groups to use the feature. For more information about role groups and management roles, see Understanding Role Based Access Control.
3. Now, run the Get-ManagementRoleAssignment cmdlet to look at the role groups or management roles assigned to you to see if you have the permissions that are necessary to manage the feature.

Note:

You must be assigned the Role Management management role to run the **Get-ManagementRoleAssignment** cmdlet. If you don't have permissions to run the **Get-ManagementRoleAssignment** cmdlet, ask your Exchange administrator to retrieve the role groups or management roles assigned to you.

If you want to delegate the ability to manage a feature to another user, see Delegate Role Assignments.

Role Management Permissions

You can use the features in the following table to manage the management role groups, roles, assignment policies, assignments, scopes that define the permissions you can apply to administrators, and end users. Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Management roles	Organization Management
Unscoped management roles	Unscoped Role Management Role management role
Role groups	Organization Management
Assignment policies	Organization Management
Role assignments	Organization Management
Management scopes	Organization Management
Management role entries	Organization Management
Legacy permissions	Organization Management
Active Directory split permissions	Organization Management **Important:** To run the `setup.com` command with the *PrepareAD* and *ActiveDirectorySplitPermissions* parameters, the account you use must be a member of the Schema Admins and Enterprise Administrators groups.

1.3.2.7 High Availability Permissions

High Availability Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The permissions required to configure high availability vary depending on the procedure being performed or the cmdlet you want to run. For more information about high availability, see High Availability and Site Resilience.

To find out what permissions you need to perform the procedure or run the cmdlet, do the following:

1. In the table below, find the feature that is most related to the procedure you want to perform or the cmdlet you want to run.
2. Next, look at the permissions required for the feature. You must be assigned one of those role groups, an equivalent custom role group, or an equivalent management role. You can also click on a role group to see its management roles. If a feature lists more than one role group, you only need to be assigned one of the role groups to use the feature. For more information about role groups and management roles, see Understanding Role Based Access Control.
3. Now, run the Get-ManagementRoleAssignment cmdlet to look at the role groups or management roles assigned to you to see if you have the permissions that are necessary to manage the feature.

Note:

You must be assigned the Role Management management role to run the **Get-ManagementRoleAssignment** cmdlet. If you don't have permissions to run the **Get-ManagementRoleAssignment** cmdlet, ask your Exchange administrator to retrieve the role groups or management roles assigned to you.

If you want to delegate the ability to manage a feature to another user, see Delegate Role Assignments.

Database Availability Group Permissions

You can use the features in the following table to add, remove, and configure settings for database availability groups (DAGs).

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Database availability group membership	Organization Management Database Availability Groups Role
Database availability group properties	Organization Management Database Availability Groups Role
Database availability groups	Organization Management Database Availability Groups Role

Database availability networks	Organization Management Database Availability Groups Role

Mailbox Database Copy Permissions

You can use the features in the following table to add, remove, and update, and activate mailbox database copies.

Feature	Permissions required
Database switchover	Organization Management Database Copies Role
Mailbox database copies	Organization Management Database Copies Role
Server switchover	Organization Management Database Copies Role
Update a mailbox database copy	Organization Management Database Copies Role

1.3.2.8 Messaging Policy and Compliance Permissions

Messaging Policy and Compliance Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-27*

The permissions required to configure messaging policy and compliance vary depending on the procedure being performed or the cmdlet you want to run. For more information about messaging policy and compliance, see Messaging Policy and Compliance.

To find out what permissions you need to perform the procedure or run the cmdlet, do the following:

1. In the table below, find the feature that is most related to the procedure you want to perform or the cmdlet you want to run.
2. Next, look at the permissions required for the feature. You must be assigned one of those role groups, an equivalent custom role group, or an equivalent management role. You can also click on a role group to see its management roles. If a feature lists more than one role group, you only need to be assigned one of the role groups to use the feature. For more information about role groups and management roles, see Understanding Role Based Access Control.
3. Now, run the Get-ManagementRoleAssignment cmdlet to look at the role groups or management roles assigned to you to see if you have the permissions that are necessary to manage the feature.

Note:
You must be assigned the Role Management management role to run the

Get-ManagementRoleAssignment cmdlet. If you don't have permissions to run the **Get-ManagementRoleAssignment** cmdlet, ask your Exchange administrator to retrieve the role groups or management roles assigned to you.

If you want to delegate the ability to manage a feature to another user, see Delegate Role Assignments.

Note:
Some features that you want to manage might exist on Edge Transport servers. To manage features on Edge Transport servers, you need to become a member of the Local Administrators group on the Edge Transport server you want to manage. Edge Transport servers don't use Role Based Access Control (RBAC). Features that can be managed on Edge Transport servers have Edge Transport Local Administrator in the "Permissions required" column in the table below. For more information about Edge Transport permissions, see Setting Administrator Permissions for the Edge Transport Server Role.

Messaging Policy and Compliance Permissions

You can use the features in the following table to configure messaging policy and compliance features. The role groups that are required to configure each feature are listed.

Users who are assigned the View-Only Management role group can view the configuration of the features in the following table. For more information, see View-Only Organization Management.

Feature	Permissions required
Applying retention policies	Organization Management Recipient Management Records Management
Creating discovery mailboxes	Organization Management Recipient Management
Delete mailbox content (using the Search-Mailbox cmdlet with the *DeleteContent* switch)	Mailbox Import Export role. **Note:** By default, the Mailbox Import Export role isn't assigned to any role group. For more information, see Add a Role to a User or USG.
Journaling	Organization Management Records Management
Litigation hold	Discovery Management Organization Management Records Management
Mailbox audit logging	Organization Management

	Records Management
Message classifications	Organization Management
Messaging records management	Organization Management Records Management
Multi-Mailbox Search	Discovery Management **Note:** By default, the Discovery Management role group doesn't have any members. No users, including administrators, have the required permissions to search mailboxes.
Personal archive	Organization Management Recipient Management
Rights protection	Organization Management
Transport rules	Organization Management Records Management

1.3.3 Managing Permissions

Managing Permissions

Exchange Server 2010 > Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-09*

Managing Administrator and Specialist Users

Managing End Users

View Effective Permissions

Setting Administrator Permissions for the Edge Transport Server Role

Managing Advanced Permissions

Permissions Cmdlets

1.3.3.1 Managing Administrator and Specialist Users

Managing Administrator and Specialist Users

Exchange Server 2010 > Permissions > Managing Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-06*

1.3.3.1.1 Add Members to a Role Group

Add Members to a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

To give a user the permissions that are granted by a management role group, you need to add the user, or a universal security group (USG), or another role group that the user is a member of, as a member of the role group. For more information about role groups in Microsoft Exchange Server 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Use the ECP to add members to a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. In the Exchange Management Console (EMC), navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. Select the role group you want to add members to and, then click **Details**.
6. In the **Members** section, click **Add**.
7. Select the users, USGs, or other role groups you want to add to the role group, and then click **OK**.
8. Click **Save** to save the changes to the role group.

Use the Shell to add a mailbox as a member of a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

To add a mailbox as a member of a role group, use the following syntax.

```
Add-RoleGroupMember <role group name> -Member <member>
```

This example adds the mailbox Robert to the Seattle Administrators role group.

```
Add-RoleGroupMember "Seattle Administrators" -Member Robert
```

For detailed syntax and parameter information, see Add-RoleGroupMember.

Use the Shell to use a filter to add a group of similar users as members of a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

You can use the **Get-User** cmdlet to add members to a role group if the mailboxes match the criteria you specify in a filter. The **Add-RoleGroupMembers** cmdlet doesn't accept the object type provided by the **Get-User** cmdlet, so you need to pass the data through the **ForEach** statement first.

This procedure makes use of pipelining, variables, recipient filters, and the **ForEach** statement. For more information about these concepts, see the following topics:

- Pipelining
- User-Defined Variables
- Creating Filters in Recipient Commands

To add mailboxes that meet the criteria you specify as members of a role group, do the following.

1. Collect the mailboxes that match the criteria you specify using the **Get-User** command with the *Filter* parameter and store the mailboxes in a variable.

```
$Mailboxes = Get-User -Filter { RecipientType -Eq "UserMailbox" -and <
```

2. This is an optional step. View the list of mailboxes stored in the $Mailboxes variable.

```
$Mailboxes
```

3. Pass the mailboxes stored in the $Mailbox variable to the **Add-RoleGroupMember** cmdlet that's running in a **ForEach** statement.

```
$Mailboxes | ForEach { Add-RoleGroupMember <role group name> -Member $
```

This example adds all the mailboxes that are in the Sales IT Staff department to the Sales Help Desk role group.

```
$Mailboxes = Get-User -Filter { RecipientType -Eq "UserMailbox" -and Department -
$Mailboxes | ForEach { Add-RoleGroupMember "Sales Help Desk" -Member $_.Name }
```

For detailed syntax and parameter information, see Add-RoleGroupMember.

Other Tasks

After you add a member to a role group, you may also want to:

- View the Members of a Role Group
- Remove Members from a Role Group
- Add a Role to a Role Group
- Remove a Role from a Role Group

1.3.3.1.2 Remove Members from a Role Group

Remove Members from a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

To remove the permissions granted by a management role group from a user, you need to remove the user, or the universal security group (USG) the user is a member of, from the role group's membership. For more information about role groups in Microsoft Exchange Server 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Use the ECP to remove members from a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. In the Exchange Managdment Console (EMC), navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an

account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. Select the role group you want to remove members from, and then click **Details**.
6. In the **Members** section, select one or more members to remove, and then click **Remove**.
7. Click **Save** to save the changes to the role group.

Use the Shell to remove a mailbox as a member of a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

To remove a mailbox as a member of a role group, use the following syntax.

```
Remove-RoleGroupMember <role group name> -Member <member>
```

This example removes the mailbox Robert from the Seattle Administrators role group.

```
Remove-RoleGroupMember "Seattle Administrators" -Member Robert
```

For detailed syntax and parameter information, see Remove-RoleGroupMember.

Other Tasks

After you remove a member from a role group, you may also want to:

- View the Members of a Role Group
- Add Members to a Role Group
- Add a Role to a Role Group
- Remove a Role from a Role Group

1.3.3.1.3 View the Members of a Role Group

View the Members of a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The members of a management role group are granted the permissions provided by the management roles assigned to the role group. You can view the members of a role group to see which users, universal security groups (USG), or other role groups are granted permissions by the role group you specify. For more information about role groups in Microsoft Exchange Server 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Use the ECP to view the members of a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

To view the members of a role group, do the following:

1. In the Exchange Management Console (EMC), navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. To view the members of a role group, select the role group you want to view. The members of the role group are displayed in the details pane.

Use the Shell to view the members of a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

To view the members of a role group, you must specify the name of the role group with the **Get-RoleGroupMember** cmdlet.

1. To find the names of the role groups in your organization, use the following command:

```
Get-RoleGroup
```

2. Find the name of the role group whose members you want to list.
3. To list the members of the role group, use the following syntax:

```
Get-RoleGroupMember <role group name>
```

For example, to list all of the members of the "Organization Management" role group, use the following command:

```
Get-RoleGroupMember "Organization Management"
```

Note:

A maximum of 1,000 role group members are displayed by default. If you want to display more than 1,000 members, you must use the *ResultSize* parameter to override the maximum number of members to return. You can type in either an integer value or the value `unlimited`. The value `unlimited` returns all members of the role group.

Other Tasks

After you view a list of role group members, you may also want to:

- Add Members to a Role Group
- Remove Members from a Role Group

1.3.3.1.4 Create a Role Group

Create a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you want to customize the permissions that you can assign to a group of users, create a new custom management role group. For more information about role groups in Microsoft Exchange Server 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Prerequisites

To create a new role group, you need to know the management roles you want to assign to it.

If you're using the Exchange Management Shell to create a new role group, all other properties on a role group are optional and can be added after the role is created. For a role to be functional, you must add at least one management role and at least one member.

For a list of built-in roles, see Built-in Management Roles.

Use the ECP to create a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. In the Exchange Management Console (EMC), navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. Click **New** under **Role Groups**.
6. In the **Name** field, enter the name of the new role group.
7. In the **Description** field, provide a short description of the purpose for the role group.
8. Select one of the two following **Write scope** options:
   - A write scope from the drop-down box. In this box, you can select either the default write scope or a custom write scope.
   - **Organizational unit** Select this option and provide an organizational unit (OU) if you want to scope this role group to an OU.
9. In the **Roles** section, do the following:
   - To add one or more management roles to the role group, click **Add** and select the roles you want to add. You can select multiple roles at one time. Then click **OK**.
   - To remove one or more roles from the role group, select the roles you want to remove, and click **Remove**.
10. In the **Members** section, do the following:
    - To add one or more members to the role group, click **Add** and select the

mailboxes, role groups or universal security groups (USGs) you want to add. You can select multiple items at one time. Then click **OK**.
- To remove one or more members, select the members you want to remove, and click **Remove**.

11. When you're done, click **Save** to create the new role group.

Use the Shell to create a role group with no scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

To create a role group, add members to the role group and also specify the users who can delegate the role group to other users, use the following syntax.

```
New-RoleGroup -Name <role group name> -Roles <roles to assign> -Members <member1,
```

This example creates a role group that's assigned to the Transport Rules and Journaling management roles, is assigned to Joe, John, and David, and can be delegated by David and Chris.

```
New-RoleGroup -Name "Compliance Role Group" -Roles "Transport Rules", "Journaling
```

For detailed syntax and parameter information, see New-RoleGroup.

Use the Shell to create a role group with a custom recipient scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

You can create role groups with custom recipient management scopes, custom configuration management scopes, or both. To create a new role group that uses a custom management scope that you created, use the following syntax.

```
New-RoleGroup -Name <role group name> -Roles <roles to assign> -CustomRecipientWr
```

This example creates a new role group that's assigned the Transport Rules and Journaling management roles and uses the Seattle Recipients recipient scope.

```
New-RoleGroup -Name "Seattle Compliance Group" -Roles "Transport Rules", "Journal
```

You can also add members to the role group when you create it by using the *Members* parameter as shown in Use the Shell to create a role group with no scope earlier in this topic. For more information about management scopes, see Understanding Management Role Scopes.

For detailed syntax and parameter information, see New-RoleGroup.

Use the Shell to create a role group with an OU scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions

topic.

To create a role group that's scoped to a specific OU, use the following syntax.

```
New-RoleGroup -Name <role group name> -Roles <roles to assign> -RecipientOrganiza
```

This example creates a role group that allows management only of recipients in the Vancouver Office OU.

```
New-RoleGroup -Name "Vancouver Office Recipients Group" -Roles "Mail Recipients"
```

You can also add members to the role group when you create it by using the *Members* parameter as shown in Use the Shell to create a role group with no scope earlier in this topic. For more information about management scopes, see Understanding Management Role Scopes.

For detailed syntax and parameter information, see New-RoleGroup.

Other Tasks

After you create a new role group, you may also want to:

- View a List of Role Groups
- Add Members to a Role Group
- Remove Members from a Role Group
- Add a Role to a Role Group
- Remove a Role from a Role Group
- Change the Scope of Role Assignments to a Role Group
- Add or Remove a Role Group Delegate
- View the Members of a Role Group
- Change a Linked Foreign USG on a Linked Role Group

1.3.3.1.5 Copy a Role Group

Copy a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you have a management role group that contains the permissions you want to grant to users, but you want to apply a different management scope, or remove or add one or two management roles without having to add all the other roles manually, you can copy the existing role group. For more information about role groups in Microsoft Exchange Server 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Use the ECP to copy a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions

topic.

Important:

You can't use the Exchange Control Panel (ECP) to copy a role group if you've used the Exchange Management Shell to configure multiple management role scopes or exclusive scopes on the role group. If you've configured multiple scopes or exclusive scopes on the role group, you must use the Shell procedures later in this topic to copy the role group. For more information about management role scopes, see Understanding Management Role Scopes.

1. In the EMC, navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. Select the role group you want to copy, and then click **Copy**.
6. In the **Name** field, enter the name of the new role group.
7. In the **Description** field, provide a short description of the purpose for the role group.
8. Select one of the two following **Write scope** options:
   - A write scope from the drop-down box. In this box, you can select either the default write scope or a custom write scope.
   - **Organizational unit** Select this option and provide an organizational unit (OU) if you want to scope this role group to an OU.
9. In the **Roles** section, do the following:
   - To add one or more management roles to the role group, click **Add** and select the roles you want to add. You can select multiple roles at one time. Then click **OK**.
   - To remove one or more roles from the role group, select the roles you want to remove, and click **Remove**.
10. In the **Members** section, do the following:
    - To add one or more members to the role group, click **Add** and select the mailboxes, role groups or universal security groups (USGs) you want to add. You can select multiple items at one time. Then click **OK**.
    - To remove one or more members, select the members you want to remove, and click **Remove**.
11. When you're done, click **Save** to create the new role group.

Use the Shell to copy a role group with no scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. Store the role group that you want to copy in a variable using the following syntax:

```
$RoleGroup = Get-RoleGroup <name of role group to copy>
```

2. Create the new role group, and also add members to the role group and specify who can delegate the new role group to other users, using the following syntax:

```
New-RoleGroup <name of new role group> -Roles $RoleGroup.Roles -Member
```

For example, the following commands copy the Organization Management role group, and name the new role group "Limited Organization Management". It adds the members Isabelle, Carter, and Lukas and can be delegated by Jenny and Katie.

```
$RoleGroup = Get-RoleGroup "Organization Management"
New-RoleGroup "Limited Organization Management" -Roles $RoleGroup.Roles -Members
```

After the new role group is created, you can add or remove roles, change the scope of role assignments on the role, and more. For more information, see the Other Tasks section later in this topic.

For detailed syntax and parameter information, see Get-RoleGroup and New-RoleGroup.

Use the Shell to copy a role group with a custom scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

To copy a role group and add a custom scope to the new role group, do the following:

1. Store the role group that you want to copy in a variable using the following syntax:

   ```
   $RoleGroup = Get-RoleGroup <name of role group to copy>
   ```

2. Create the new role group with a custom scope using the following syntax:

   ```
   New-RoleGroup <name of new role group> -Roles $RoleGroup.Roles -Custom
   ```

For example, the following commands copy the Organization Management role group and create a new role group called Vancouver Organization Management with the Vancouver Users recipient scope and Vancouver Servers configuration scope.

```
$RoleGroup = Get-RoleGroup "Organization Management"
New-RoleGroup "Vancouver Organization Management" -Roles $RoleGroup.Roles -Custom
```

You can also add members to the role group when you create it by using the *Members* parameter as shown in Use the Shell to copy a role group with no scope earlier in this topic. For more information about management scopes, see Understanding Management Role Scopes.

After the new role group is created, you can add or remove roles, change the scope of role assignments on the role, and perform other tasks. For more information, see the Other Tasks section later in this topic.

For detailed syntax and parameter information, see Get-RoleGroup and New-RoleGroup.

Use the Shell to copy a role group with an OU scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. Store the role group that you want to copy in a variable using the following syntax:

   ```
   $RoleGroup = Get-RoleGroup <name of role group to copy>
   ```

2. Create the new role group with a custom scope using the following syntax:

   ```
   New-RoleGroup <name of new role group> -Roles $RoleGroup.Roles -Recipi
   ```

For example, the following commands copy the Recipient Management role group and create a new role group called Toronto Recipient Management that allows management of only users in the Toronto Users OU.

```
$RoleGroup = Get-RoleGroup "Recipient Management"
New-RoleGroup "Toronto Recipient Management" -Roles $RoleGroup.Roles -RecipientOr
```

You can also add members to the role group when you create it by using the *Members* parameter as shown in Use the Shell to copy a role group with no scope earlier in this topic. For more information about management scopes, see Understanding Management Role Scopes.

After the new role group is created, you can add or remove roles, change the scope of role assignments on the role, and more. For more information, see the Other Tasks section later in this topic.

For detailed syntax and parameter information, see Get-RoleGroup and New-RoleGroup.

Other Tasks

After you copy a role group, you may also want to:

- View a List of Role Groups
- Add Members to a Role Group
- Remove Members from a Role Group
- Add a Role to a Role Group
- Remove a Role from a Role Group
- Change the Scope of Role Assignments to a Role Group
- Add or Remove a Role Group Delegate
- View the Members of a Role Group
- Change a Linked Foreign USG on a Linked Role Group

1.3.3.1.6 Remove a Role Group

Remove a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you no longer need a role group you created, you can remove it. When you remove a role group, the management role assignments between the role group and the management roles are deleted. The management roles aren't deleted. If a user depended on the role group for access to a feature, the user will no longer have access to the feature. You can't remove built-in role groups. For more information about role groups in Microsoft Exchange Server 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Use the ECP to remove a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. In the EMC, navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. Select one or more role groups you want to remove, and then click ✕.

Important:
You can't remove built-in role groups or any role group that is assigned the last delegating role assignment to a role.

Use the Shell to remove a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

To remove a role group, use the following syntax.

```
Remove-RoleGroup <role group name>
```

This example removes the Seattle Recipients Group role group.

```
Remove-RoleGroup "Seattle Recipients Group"
```

For detailed syntax and parameter information, see Remove-RoleGroup.

1.3.3.1.7 Add a Role to a Role Group

Add a Role to a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Adding a management role to a management role group is the best and simplest way to grant permissions to a group of administrators or specialist users in Microsoft Exchange Server 2010. If you want to give users that are members of a role group the ability to manage a feature, you add the management role that manages the feature to the role group. After the role is added, the members of the role group are granted the permissions provided by the role.

For more information about role groups, in Exchange 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Use the ECP to add a management role to

a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Important:

You can't use the Exchange Control Panel (ECP) to add roles to a role group if you've used the Exchange Management Shell to configure multiple management role scopes or exclusive scopes on the role group. If you've configured multiple scopes or exclusive scopes on the role group, you must use the Shell procedures later in this topic to add roles to the role group. For more information about management role scopes, see Understanding Management Role Scopes.

1. In the EMC, navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. Select the role group you want to add one or more roles to, and then click **Details**.
6. In the **Roles** section, click **Add**.
7. Select one or more roles to add to the role group, and then click **OK**.
8. Click **Save** to save the changes to the role group.

Use the Shell to create a role assignment with no scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

You can create a role assignment with no scope between a role and a role group. When you do this, the implicit read and implicit write scopes of the role apply.

Use the following syntax to assign a role without any scope to a role group. A role assignment name is created automatically if you don't specify one.

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role name>
```

This example assigns the Transport Rules management role to the Seattle Compliance role group.

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Compliance" -Role "Transport
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Use the Shell to create a role assignment with a predefined scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

If a predefined scope meets your business requirements, you can apply that scope to the

role assignment rather than create a new one. For a list of predefined scopes and their descriptions, see Understanding Management Role Scopes.

For more information about role assignments, see Understanding Management Role Assignments.

Use the following syntax to assign a role to a role group with a predefined scope. A role assignment name is created automatically if you don't specify one.

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role name> -
```

This example assigns the Message Tracking role to the Enterprise Support role group and applies the Organization predefined scope.

```
New-ManagementRoleAssignment -SecurityGroup "Enterprise Support" -Role "Message T
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Use the Shell to create a role assignment with a recipient filter-based scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

If you created a recipient filter-based scope, you need to include the scope in the command used to assign the role to a role group by using the *CustomRecipientWriteScope* parameter.

You can also include a configuration write scope when you create a role assignment that has a recipient write scope.

For more information about role assignments and scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Use the following syntax to assign a role to a role group with a recipient filter-based scope. A role assignment name is created automatically if you don't specify one.

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role name> -
```

This example assigns the Message Tracking role to the Seattle Recipient Admins role group and applies the Seattle Recipients scope.

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Recipient Admins" -Role "Mes
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Use the Shell to create a role assignment with a configuration scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

If you created a server or database configuration filter or list-based scope, you need to

include the scope in the command used to assign the role to a role group by using the *CustomConfigWriteScope* parameter.

You can also include a recipient write scope when you create a role assignment that has a configuration write scope.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Use the following syntax to assign a role to a role group with a configuration scope. A role assignment name is created automatically if you don't specify one.

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role name> -
```

This example assigns the Databases role to the Seattle Server Admins role group and applies the Seattle Servers scope.

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Server Admins" -Role "Databa
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Use the Shell to create a role assignment with an OU scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

If you want to scope a role's write scope to an OU, you can specify the OU in the *RecipientOrganizationalUnitScope* parameter directly.

For more information about role assignments and management scopes, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Use the following command to assign a role to a role group and restrict the write scope of a role to a specific OU. A role assignment name is created automatically if you don't specify one.

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role name> -
```

This example assigns the Mail Recipients role to the Seattle Recipient Admins role group and scopes the assignment to the Sales\Users OU in the Contoso.com domain.

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Recipient Admins" -Role "Mai
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Other Tasks

After you add a role to a role group, you may also want to:

- View a List of Roles on a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group

- View the Members of a Role Group
- Add or Remove a Role Group Delegate
- Change the Scope of Role Assignments to a Role Group

1.3.3.1.8 Remove a Role from a Role Group

Remove a Role from a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Removing a management role from a management role group is the best and simplest way to revoke permissions granted to a group of administrators or specialist users in Microsoft Exchange Server 2010. If you don't want administrators or specialist users to have permissions to manage a feature, you remove the management role from the management role group that manages the permissions. After the role is removed, the members of the role group will no longer have permissions to manage the feature.

For more information about role groups in Exchange 2010, see Understanding Management Role Groups.

Note:

Some role groups, such as the Organization Management role group, restrict what roles can be removed from a role group. For more information, see Understanding Management Role Groups.
If an administrator is a member of another role group that contains management roles that grants permissions to manage the feature, you need to either remove the administrator from the other role groups, or remove the role that grants permissions to manage the feature from the other role groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Use the ECP to remove a management role from a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Important:

You can't use the Exchange Control Panel (ECP) to remove roles from a role group if you've used the Exchange Management Shell to configure multiple scopes or exclusive scopes on the role group. If you've configured multiple scopes or exclusive scopes on the role group, you must use the Shell procedures later in this topic to remove roles from the role group. For more information about management role scopes, see Understanding Management Role Scopes.

1. In the EMC, navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an

account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. Select the role group you want to remove roles from, and then click **Details**.
6. In the **Roles** section, select one or more roles that you want to remove, and then click **Remove**.
7. Click **Save** to save changes to the role group.

Use the Shell to remove a role from a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

You can remove roles from role groups by retrieving the associated management role assignment using the **Get-ManagementRoleAssignment** cmdlet and then piping the role assignment returned to the **Remove-ManagementRoleAssignment** cmdlet. Unless you want to remove both delegating and regular role assignments at the same time, specify the Delegating parameter to specify whether you want to remove regular or delegating role assignments.

For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

This procedure uses pipelining. For more information about pipelining, see Pipelining.

To remove a role from a role group, use the following syntax.

```
Get-ManagementRoleAssignment -RoleAssignee <role group name> -Role <role name> -D
```

This example removes the Distribution Groups role, which enables administrators to manage distribution groups, from the Seattle Recipient Administrators role group. Because we want to remove the role assignment that provides permissions to manage distribution groups, the *Delegating* parameter is set to `$False`, which returns only regular role assignments.

```
Get-ManagementRoleAssignment -RoleAssignee "Seattle Recipient Administrators" -Ro
```

For detailed syntax and parameter information, see Remove-ManagementRoleAssignment.

Other Tasks

After you remove a role from a role group, you may also want to:

- Add a Role to a Role Group
- View a List of Roles on a Role Group

1.3.3.1.9 View a List of Role Groups

View a List of Role Groups

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can view either a list of management role groups or the detailed information about a specific role group that exists in your organization. For more information about role groups in Microsoft Exchange Server 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Use the ECP to view a list of role groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. In the EMC, navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. To view the details of a specific role group, select the role group you want to view. The role group description, its members and the roles assigned to it are displayed in the details pane.

Use the Shell to view a list of role groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

This procedure makes use of pipelining and the **Format-Table** cmdlet. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output

You can view a list of all the role groups in your organization by not specifying any role groups when you run the **Get-RoleGroup** cmdlet.

This example returns a list of all role groups in your organization.

```
Get-RoleGroup
```

To return a list of specific properties for all the role groups in your organization, you can pipe the results of the **Format-Table** cmdlet and specify the properties you want in the list of results. Use the following syntax.

```
Get-RoleGroup | Format-Table <property 1>, <property 2...>
```

This example returns a list of all the role groups in your organization and includes the **Name** and **Roles** properties.

```
Get-RoleGroup | Format-Table Name, Roles
```

For detailed syntax and parameter information, see Get-RoleGroup.

Use the Shell to view the details of a

single role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

This procedure makes use of pipelining and the **Format-List** cmdlet. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output

You can view the details of a specific role group by using the **Get-RoleGroup** cmdlet and piping the output to the **Format-List** cmdlet.

To view the details of a specific role group, use the following syntax.

```
Get-RoleGroup <role group name> | Format-List
```

This example gets the details about the Organization Management role group.

```
Get-RoleGroup "Organization Management" | Format-List
```

For detailed syntax and parameter information, see Get-RoleGroup.

Other Tasks

After you view a list of role groups, you may also want to:

- View the Members of a Role Group

1.3.3.1.10 View a List of Roles on a Role Group

View a List of Roles on a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The management roles assigned to a management role group determine what tasks can be performed by the members of the role group. You can view the roles on a role group to see what the members of the role group can do. For more information about role groups in Microsoft Exchange Server 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Use the ECP to view a list of roles on a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions

topic.

1. In the EMC, navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. To view the list of roles on a role group, select the role group you want to view. The roles assigned to the role group are displayed in the details pane.

Use the Shell to view a basic list of roles assigned to a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

You can use the **Get-RoleGroup** cmdlet to view a basic list of roles assigned to a role group. If you want to view more detailed information about the role assignments that assign a role to a role group, such as what management scopes are associated with the assignments, see "View a more detailed list of roles assigned to a role group" later in this topic.

1. To find the names of the role groups in your organization, use the following command.

```
Get-RoleGroup
```

2. Find the name of the role group whose roles you want to list.
3. To list the roles on a role group, use the following syntax.

```
(Get-RoleGroup <role group name>).Roles
```

This example lists all of the roles assigned to the Organization Management role group.

```
(Get-RoleGroup "Organization Management").Roles
```

For detailed syntax and parameter information, see Get-RoleGroup.

Use the Shell to view a more detailed list of roles assigned to a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

You can use the **Get-ManagementRoleAssignment** cmdlet to view more detailed information about the role assignments that assign a role to a role group. If you want to view only a basic list of roles assigned to a role group, see "View a basic list of roles assigned to a role group" earlier in this topic.

1. To find the names of the role groups in your organization, use the following command.

```
Get-RoleGroup
```

2. Find the name of the role group whose roles you want to list.
3. To list the roles on a role group, use the following syntax.

```
Get-ManagementRoleAssignment -RoleAssignee <role group name>
```

This example lists all of the roles assigned to the Organization Management role group.

```
Get-ManagementRoleAssignment -RoleAssignee "Organization Management"
```

This command displays the default information about the role assignment between the role group and the roles assigned to it. If you want to view other, more advanced, information about the role assignments on a role group, such as which role assignments are delegating or exclusive, see View Role Assignments.

For detailed syntax and parameter information, see Get-RoleGroup or Get-ManagementRoleAssignment.

Other Tasks

After you view the list of roles on a role group, you may also want to:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Change the Scope of Role Assignments to a Role Group
- View the Members of a Role Group

1.3.3.1.11 Add or Remove a Role Group Delegate

Add or Remove a Role Group Delegate

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role group delegates are users or universal security groups (USGs) that can add or remove members from a role group or change the properties of a role group. By adding or removing role group delegates, you can control who is allowed to manage a role group. For more information about role groups in Microsoft Exchange Server 2010, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Important:

After you add a delegate to a role group, the role group can only be managed by the delegates on the role group, or by users who are assigned, either directly or indirectly, the Role Management management role.
If a user is assigned, either directly or indirectly, the Role Management role and isn't added as a delegate of the role group, the user must use the *BypassSecurityGroupManagerCheck* switch on the **Add-RoleGroupMember**, **Remove-RoleGroupMember**, **Update-RoleGroupMember**, and **Set-RoleGroup** cmdlets to manage a role group.

Use the Shell to add a delegate to a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to add a delegate to a role group.

To change the list of delegates on a role group, you use the *ManagedBy* parameter on the **Set-RoleGroup** cmdlet. The *ManagedBy* parameter overwrites the entire delegate list on the role group. If you want to add delegates to the role group rather than replace the entire list of delegates, use the following steps:

1. Store the role group in a variable using the following command.

```
$RoleGroup = Get-RoleGroup <role group name>
```

2. Add the delegate to the role group stored in the variable using the following command.

```
$RoleGroup.ManagedBy += (Get-User <user to add>).Identity
```

Note:
Use the **Get-Group** cmdlet if you want to add a USG.

3. Repeat Step 2 for each delegate you want to add.
4. Apply the new list of delegates to the actual role group using the following command.

```
Set-RoleGroup <role group name> -ManagedBy $RoleGroup.ManagedBy
```

This example adds the user David Strome as a delegate on the Organization Management role group.

```
$RoleGroup = Get-RoleGroup "Organization Management"
$RoleGroup.ManagedBy += (Get-User "David Strome").Identity
Set-RoleGroup "Organization Management" -ManagedBy $RoleGroup.ManagedBy
```

For detailed syntax and parameter information, see Set-RoleGroup.

Use the Shell to remove a delegate from a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to remove a delegate from a role group.

To change the list of delegates on a role group, you use the *ManagedBy* parameter on the **Set-RoleGroup** cmdlet. The *ManagedBy* parameter overwrites the entire delegate list on the role group. If you want to remove delegates from the role group rather than replace the entire list of delegates, use the following steps:

1. Store the role group in a variable using the following command.

```
$RoleGroup = Get-RoleGroup <role group name>
```

2. Remove the delegate from the role group stored in the variable using the following command.

```
$RoleGroup.ManagedBy -= (Get-User <user to remove>).Identity
```

Note:
Use the **Get-Group** cmdlet if you want to remove a USG.

3. Repeat Step 2 for each delegate you want to remove.
4. Apply the new list of delegates to the actual role group using the following command.

```
Set-RoleGroup <role group name> -ManagedBy $RoleGroup.ManagedBy
```

This example removes the user David Strome as a delegate on the Organization Management role group.

```
$RoleGroup = Get-RoleGroup "Organization Management"
$RoleGroup.ManagedBy -= (Get-User "David Strome").Identity
Set-RoleGroup "Organization Management" -ManagedBy $RoleGroup.ManagedBy
```

For detailed syntax and parameter information, see Set-RoleGroup.

Other Tasks

After you add a delegate to a role group, you may also want to:

- Add Members to a Role Group
- Remove Members from a Role Group
- Add a Role to a Role Group
- Remove a Role from a Role Group

1.3.3.1.12 Change the Scope of Role Assignments to a Role Group

Change the Scope of Role Assignments to a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role groups are assigned management roles. The management role assignments between a role group and a role contain management scopes, which determine what objects are made available to members of that role group. By changing the write scope on a role group, you can change what objects are made available to role group members to create, change, or remove. You can't change the read scope on a role group.

Microsoft Exchange Server 2010 includes scopes that are applied by default to role assignments when no custom scopes are created. If you want to use a custom scope with a role assignment on a role group, you must create one first. For more information about creating custom scopes, which is an advanced task, see Create a Regular or Exclusive Scope.

For more information about management role scopes and assignments in Exchange 2010, see the following topics:

- Understanding Management Role Scopes
- Understanding Management Role Assignments

Looking for other management tasks related to role groups? Check out Managing Administrator and Specialist Users.

Use the ECP to change the scope on a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

When you use the Exchange Control Panel (ECP) to change the scope on a role group, you're actually changing the scope on all the role assignments between the role group and each of the management roles assigned to the role group. If you want to change the scope on specific role assignments, you must use the Exchange Management Shell procedures later in this topic.

Important:

You can't use the ECP to manage scopes on role assignments between roles and a role group if you've used the Shell to configure multiple scopes or exclusive scopes on those role assignments. If you've configured multiple scopes or exclusive scopes on those role assignments, you must use the Shell procedures later in this topic to manage scopes. For more information about management role scopes, see Understanding Management Role Scopes.

1. In the EMC, navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **Administrator Roles** tab.
5. Select the role group you want to change the scope on, and then click **Details**.
6. Select one of the two following **Write scope** options:
   - A write scope from the drop-down box. In this box, you can select either the default write scope or a custom write scope.
   - **Organizational unit** Select this option and provide an organizational unit (OU) if you want to scope this role group to an OU.
7. Click **Save** to save the changes to the role group.

Use the Shell to change the scope of all role assignments on a role group at the same time

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Role assignments between the role group and the roles assigned to it can use the implicit scope obtained from the roles themselves, the same custom scope, or different custom scopes. For more information about role assignments, see Understanding Management Role Assignments.

The scopes on the role assignments are managed using the **Set-ManagementRoleAssignment** cmdlet. You can't manage scopes using the **Set-RoleGroup** cmdlet.

To change the scope of all the role assignments between a role group and a set of management roles at the same time, you need to first retrieve the role assignments on

the role group, and then set the new scope on each of the assignments. You can do this by using the **Get-ManagementRoleAssignment** cmdlet to retrieve the role assignments, and then pipe them to the **Set-ManagementRoleAssignment** cmdlet.

This procedure uses the concepts of pipelining and the *WhatIf* switch. For more information, see the following topics:

- Pipelining
- WhatIf, Confirm, and ValidateOnly Switches

To set the scope on all of the role assignments on a role group at the same time, use the following syntax.

```
Get-ManagementRoleAssignment -RoleAssignee <name of role group> | Set-ManagementR
```

You use only the parameters you need to configure the scope you want to use. For example, if you want to change the recipient scope for all role assignments on the Sales Recipient Management role group to Direct Sales Employees, use the following command.

```
Get-ManagementRoleAssignment -RoleAssignee "Sales Recipient Management" | Set-Man
```

Note:

You can use the *WhatIf* switch to verify that only the role assignments you want to change are changed. Run the preceding command with the *WhatIf* switch to verify the results, and then remove the *WhatIf* switch to apply the changes.

For more information about changing management role assignments, see Change a Role Assignment.

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

Use the Shell to change the scope of individual role assignments on a role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Role assignments between the role group and the roles assigned to it can use the implicit scope obtained from the roles themselves, the same custom scope, or different custom scopes. For more information about role assignments, see Understanding Management Role Assignments.

The scopes on the role assignments are managed using the **Set-ManagementRoleAssignment** cmdlet. You can't manage scopes using the **Set-RoleGroup** cmdlet.

This procedure uses the concepts of pipelining and the **Format-List** cmdlet. For more information, see the following topics:

- Pipelining
- Working with Command Output

To change the scope on a role assignment between a role group and a management role, you first find the name of the role assignment, and then set the scope on the role assignment.

1. To find the names of all the role assignments on a role group, use the

following command. By piping the management role assignments to the **Format-List** cmdlet, you can view the full name of the assignment.

```
Get-ManagementRoleAssignment -RoleAssignee <role group name> | Format-
```

2. Find the name of the role assignment you want to change. Use the name of the assignment in the next step.
3. To set the scope on an individual assignment, use the following syntax.

```
Set-ManagementRoleAssignment <role assignment name> -CustomRecipientWr
```

You use only the parameters you need to configure the scope you want to use. For example, if you want to change the recipient scope for the Mail Recipients_Sales Recipient Management role assignment to All Sales Employees, use the following command.

```
Set-ManagementRoleAssignment "Mail Recipients_Sales Recipient Management" -Custom
```

For more information about changing management role assignments, see Change a Role Assignment.

For detailed syntax and parameter information, see Set-ManagementRoleAssignment.

Other Tasks

After you change the scope of role assignments on a role group, you may also want to:

- Add Members to a Role Group
- Remove Members from a Role Group
- Add a Role to a Role Group
- Remove a Role from a Role Group

1.3.3.1.13 Create a Linked Role Group

Create a Linked Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A linked management role group can be used to enable members of a universal security group (USG) in a foreign Active Directory forest to manage a Microsoft Exchange Server 2010 organization in a resource Active Directory forest. By associating a USG in a foreign forest with a linked role group, the members of that USG are granted the permissions provided by the management roles assigned to the linked role group. For more information about linked role groups, see Understanding Management Role Groups.

Important:

To add or remove users on a linked role group, you must add or remove members in the USG in the foreign Active Directory forest. You can't use the **Add-RoleGroupMember**, **Remove-RoleGroupMember**, or **Update-RoleGroupMember** cmdlets to change the membership of a linked role group.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Prerequisites

- Configuring a linked role group requires that, at a minimum, a one-way trust is established between the resource Active Directory forest in which the linked role group will reside, and the foreign Active Directory forest where the users or USGs reside. The resource forest must trust the foreign forest.
- You must have the following information about the foreign Active Directory forest:
  - **Credentials** You must have a user name and password that can access the foreign Active Directory forest. This information is used with the *LinkedCredential* parameter on the **New-RoleGroup** cmdlet.
  - **Domain controller** You must have the fully qualified domain name (FQDN) of an Active Directory domain controller in the foreign Active Directory forest. This information is used with the *LinkedDomainController* parameter on the **New-RoleGroup** cmdlet.
  - **Foreign USG** You must have the full name of a USG in the foreign Active Directory forest that contains the members you want to associate with the linked role group. This information is used with the *LinkedForeignGroup* parameter on the **New-RoleGroup** cmdlet.

Use the Shell to create a linked role group with no scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a linked role group with no scope.

To create a linked role group and assign management roles to the linked role group, do the following:

1. Store the foreign Active Directory forest credentials in a variable.

```
$ForeignCredential = Get-Credential
```

2. Create the linked role group using the following syntax.

```
New-RoleGroup <role group name> -LinkedForeignGroup <name of foreign U
```

3. Add or remove members to or from the foreign USG using Active Directory Users and Computers on a computer in the foreign Active Directory forest.

This example does the following:

- Retrieves the credentials for the users.contoso.com foreign Active Directory forest. These credentials are used to connect to the DC01.users.contoso.com domain controller in the foreign forest.
- Creates a linked role group called Compliance Role Group in the resource forest where Exchange 2010 is installed.
- Links the new role group to the Compliance Administrators USG in the users.contoso.com foreign Active Directory forest.
- Assigns the Transport Rules and Journaling management roles to the new linked role group.

```
$ForeignCredential = Get-Credential
New-RoleGroup "Compliance Role Group" -LinkedForeignGroup "Compliance Administrat
```

For detailed syntax and parameter information, see New-RoleGroup.

Use the Shell to create a linked role group with a custom management scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a linked role group with a custom management scope.

You can create linked role groups with custom recipient management scopes, custom configuration management scopes, or both. To create a linked role group and assign management roles with custom scopes to it, do the following:

1. Store the foreign Active Directory forest credentials in a variable.

```
$ForeignCredential = Get-Credential
```

2. Create the linked role group using the following syntax.

```
New-RoleGroup <role group name> -LinkedForeignGroup <name of foreign U
```

3. Add or remove members to or from the foreign USG using Active Directory Users and Computers on a computer in the foreign Active Directory forest.

This example does the following:

- Retrieves the credentials for the users.contoso.com foreign Active Directory forest. These credentials are used to connect to the DC01.users.contoso.com domain controller in the foreign forest.
- Creates a linked role group called Seattle Compliance Role Group in the resource forest where Exchange 2010 is installed.
- Links the new role group to the Seattle Compliance Administrators USG in the users.contoso.com foreign Active Directory forest.
- Assigns the Transport Rules and Journaling management roles to the new linked role group with the Seattle Recipients custom recipient scope.

```
$ForeignCredential = Get-Credential
New-RoleGroup "Seattle Compliance Role Group" -LinkedForeignGroup "Seattle Compli
```

For more information about management scopes, see Understanding Management Role Scopes.

For detailed syntax and parameter information, see New-RoleGroup.

Use the Shell to create a linked role group with an OU scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a linked role group with an organizational unit (OU) scope.

You can create linked role groups that use an OU recipient scope. To create a linked role group and assign management roles to it with an OU scope, do the following:

1. Store the foreign Active Directory forest credentials in a variable.

```
$ForeignCredential = Get-Credential
```

2. Create the linked role group using the following syntax.

```
New-RoleGroup <role group name> -LinkedForeignGroup <name of foreign U
```

3. Add or remove members to or from the foreign USG using Active Directory Users and Computers on a computer in the foreign Active Directory forest.

This example does the following:

- Retrieves the credentials for the users.contoso.com foreign Active Directory forest. These credentials are used to connect to the DC01.users.contoso.com domain controller in the foreign forest.
- Creates a linked role group called Executives Compliance Role Group in the resource forest where Exchange 2010 is installed.
- Links the new role group to the Executives Compliance Administrators USG in the users.contoso.com foreign Active Directory forest.
- Assigns the Transport Rules and Journaling management roles to the new linked role group with the OU recipient scope Executives OU.

```
$ForeignCredential = Get-Credential
New-RoleGroup "Executives Compliance Role Group" -LinkedForeignGroup "Executives
```

For more information about management scopes, see Understanding Management Role Scopes.

For detailed syntax and parameter information, see New-RoleGroup.

Other Tasks

After you create a linked role group, you may also want to:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Change the Scope of Role Assignments to a Role Group

1.3.3.1.14 Change a Linked Foreign USG on a Linked Role Group

Change a Linked Foreign USG on a Linked Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can change the universal security group (USG), which is located in a foreign Active Directory forest associated with a linked management role group. This can be useful if the original foreign USG is being removed, and you need to transition to a new USG. For more information about linked role groups, see Understanding Management Role Groups.

Looking for other management tasks related to administrators and specialist users? Check out Managing Administrator and Specialist Users.

Prerequisites

- **Credentials** You must have a user name and password that can access the foreign Active Directory forest. This information is used with the *LinkedCredential* parameter on the **Set-RoleGroup** cmdlet.

- **Domain controller** You must have the fully qualified domain name (FQDN) of an Active Directory domain controller in the foreign Active Directory forest. This information is used with the *LinkedDomainController* parameter on the **Set-RoleGroup** cmdlet.
- **Foreign USG** You must have the full name of a USG in the foreign Active Directory forest that contains the members you want to associate with the linked role group. This information is used with the *LinkedForeignGroup* parameter on the **Set-RoleGroup** cmdlet.

Use the Shell to change the foreign USG on a linked role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change the foreign USG on a linked role group.

To change the foreign USG associated with a linked role group, do the following:

1. Store the foreign Active Directory forest credentials in a variable.

```
$ForeignCredential = Get-Credential
```

2. Create the new linked role group using the following syntax.

```
Set-RoleGroup <role group name> -LinkedForeignGroup <name of foreign U
```

This example does the following:

- Retrieves the credentials for the users.contoso.com foreign Active Directory forest. These credentials are used to connect to the DC01.users.contoso.com domain controller in the foreign forest.
- Changes the foreign USG on the Compliance Role Group role group to Regulatory Compliance Officers.

```
$ForeignCredential = Get-Credential
Set-RoleGroup "Compliance Role Group" -LinkedForeignGroup "Regulatory Compliance
```

For detailed syntax and parameter information, see Set-RoleGroup.

Other Tasks

After you change the foreign USG on a linked role group, you may also want to:

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Change the Scope of Role Assignments to a Role Group

1.3.3.1.15 Create Linked Role Groups that Mirror Built-in Role Groups

Create Linked Role Groups that Mirror Built-in Role Groups

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Using linked management role groups in Microsoft Exchange Server 2010, you can link a role group in an Exchange 2010 resource forest with a universal security group (USG) in a foreign user forest. This is useful when you want administrators with accounts in the user forest to manage the servers running Exchange in the resource forest. For more information about linked role groups, see Understanding Management Role Groups.

By default, Exchange 2010 includes a number of built-in role groups that provide you with permissions to manage a variety of features and job functions. Each role group is tailored to provide specific permissions for each feature and job function. However, these role groups can't be linked to USGs in a foreign forest. They can only contain users and USGs from the local resource forest. Fortunately, it's possible to replicate these built-in role groups using linked role groups.

You can re-create each built-in role group as a linked role group. All of the management roles and management scopes assigned to each role group are added to the new linked role group. For more information about management roles and scopes, see the following topics:

- Understanding Management Roles
- Understanding Management Role Scopes

Looking for other management tasks related to role groups? Check out Managing Administrator and Specialist Users.

Prerequisites

- Configuring a linked role group requires a one-way trust between the resource Active Directory forest in which the linked role group will reside, and the foreign Active Directory forest where the users or USGs reside. The resource forest must trust the foreign forest.
- You must have the following information about the foreign Active Directory forest:
  - **Credentials** You must have a user name and password that can access the foreign Active Directory forest. This information is used with the *LinkedCredential* parameter on the **New-RoleGroup** cmdlet. This information is obtained by running the **Get-Credential** cmdlet. The format of the user name is *domain**username*.
  - **Domain controller** You must have the fully qualified domain name (FQDN) of an Active Directory domain controller in the foreign Active Directory forest. This information is used with the *LinkedDomainController* parameter on the **New-RoleGroup** cmdlet.
  - **Foreign USG** You must have the full name of a USG in the foreign Active Directory forest that contains the members you want to associate with the linked role group. This information is used with the *LinkedForeignGroup* parameter on the **New-RoleGroup** cmdlet.

Use the Shell to create linked role groups that replicate built-in role groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:

You can't use the EMC to create linked role groups that replicate built-in role groups.

Each of the following sections shows you how to re-create each role group as a linked role group. Complete the procedures in each section to re-create all of the built-in role groups as linked role groups.

Create the Organization Management linked role group

To re-create the Organization Management role group as a linked role group, you perform a procedure that's different than the procedure used to re-create other built-in role groups. This is because the Organization Management role group has delegating role assignments between it and all of the management roles. Re-creating the delegating role assignments requires an additional step.

1. Create a USG in the foreign forest that will be linked to the Organization Management role group.
2. Store the foreign Active Directory forest credentials in a variable.

```
$ForeignCredential = Get-Credential
```

3. Store all of the roles assigned to the Organization Management role group in a variable.

```
$OrgMgmt  = Get-RoleGroup "Organization Management"
```

4. Create the Organization Management linked role group and add the roles assigned to the built-in Organization Management role group.

```
New-RoleGroup "Organization Management - Linked" -LinkedForeignGroup <
```

5. Remove all of the regular assignments between the new Organization Management linked role group and the My* end-user roles.

```
Get-ManagementRoleAssignment -RoleAssignee "Organization Management -
```

6. Add delegating role assignments between the new Organization Management linked role group and all management roles.

```
Get-ManagementRole | New-ManagementRoleAssignment -SecurityGroup "Orga
```

This example assumes the following values are used for each parameter:

- **LinkedForeignGroup** `Organization Management Administrators`
- **LinkedDomainController** `DC01.users.contoso.com`

Using the preceding values, this example re-creates the Organization Management role group as a linked role group.

```
$ForeignCredential = Get-Credential
$OrgMgmt  = Get-RoleGroup "Organization Management"
New-RoleGroup "Organization Management - Linked" -LinkedForeignGroup "Organizatio
Get-ManagementRoleAssignment -RoleAssignee "Organization Management - Linked" -Ro
Get-ManagementRole | New-ManagementRoleAssignment -SecurityGroup "Organization Ma
```

Create all other linked role groups

To re-create the built-in role groups (other than the Organization Management role group) as linked role groups, use the following procedure for each group.

1. Create a USG in the foreign forest for each role group that will be linked to each new role group.
2. Store the foreign Active Directory forest credentials in a variable. You only need to do this once.

```
$ForeignCredential = Get-Credential
```

3. Retrieve a list of role groups using the following cmdlet.

```
Get-RoleGroup
```

4. For each role group, other than the Organization Management role group, do the following.

```
$RoleGroup = Get-RoleGroup <name of role group to re-create>
New-RoleGroup "<role group name> - Linked" -LinkedForeignGroup <name o
```

5. Repeat the preceding step for each built-in role group you want to re-create

as a linked role group.

This example assumes the following values are used for each parameter:

- **LinkedDomainController** `DC01.users.contoso.com`
- **Built-in role groups to be re-created as linked role groups** `Recipient Management, Server Management`
- **Foreign group for Recipient Management linked role group** `Recipient Management Administrators`
- **Foreign group for Server Management linked role group** `Server Management Administrators`

Using the preceding values, this example re-creates the Recipient Management and Server Management role groups as linked role groups.

```
$ForeignCredential = Get-Credential
Get-RoleGroup
$RoleGroup = Get-RoleGroup "Recipient Management"
New-RoleGroup "Recipient Management - Linked" -LinkedForeignGroup "Recipient Mana
$RoleGroup = Get-RoleGroup "Server Management"
New-RoleGroup "Server Management - Linked" -LinkedForeignGroup "Server Management
```

Other Tasks

After you create linked role groups, you may also want to:

- Add members to the foreign USGs using Active Directory Users and Computers in the foreign forest.
- Remove members of built-in role groups. For more information, see Remove Members from a Role Group.
- Add additional roles to the new linked role groups. For more information, see Add a Role to a Role Group.
- Remove roles from the new linked role groups. For more information, see Remove a Role from a Role Group.
- Change the scopes of role assignments between the new linked role groups and management roles. For more information, see Change the Scope of Role Assignments to a Role Group.
- Create additional linked role groups. For more information, see Create a Linked Role Group.

1.3.3.2 Managing End Users

Managing End Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-06-04*

Add an Assignment Policy

Remove an Assignment Policy

View a List of Assignment Policies

Change the Assignment Policy on a Mailbox

Change the Default Assignment Policy

Add a Role to an Assignment Policy

Remove a Role from an Assignment Policy

View a List of Roles on an Assignment Policy

1.3.3.2.1 Add an Assignment Policy

Add an Assignment Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you want to customize the permissions that you assign to a group of end users, create a new custom management role assignment policy. The assignment policy you create can be customized to suit your end user's specific requirements. For more information about assignment policies in Microsoft Exchange Server 2010, see Understanding Management Role Assignment Policies.

After you've created the new assignment policy, you assign users to it. For more information, see Change the Assignment Policy on a Mailbox.

Looking for other management tasks related to end users? Check out Managing End Users.

Use the ECP to create a new assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

Note:

You can only create explicit assignment policies using the Exchange Control Panel (ECP). If you want to create a new default assignment policy, you must use the Exchange Management Shell. For more information, see the "Use the Shell to create a default assignment policy" section later in this topic.

1. In the EMC, navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **User Roles** tab.
5. Click New under Role Assignment Policies.
6. In the **Name** field, enter the name of the new assignment policy.
7. In the **Description** field, provide a short description of the purpose for the assignment policy.
8. Select the check box next to the role or roles you want to add to the assignment policy. You can select multiple roles, including end-user roles you've added. If you select a role that has child roles, the child roles are

automatically selected.

9. Click **Save** to save the changes to the assignment policy.

Use the Shell to create an explicit assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

To create an explicit assignment policy that can be manually assigned to mailboxes, use the following syntax.

```
New-RoleAssignmentPolicy <assignment policy name> -Roles <roles to assign>
```

This example creates the explicit assignment policy Limited Mailbox Configuration and assigns the `MyBaseOptions`, `MyAddressInformation`, and `MyDisplayName` roles to it.

```
New-RoleAssignmentPolicy "Limited Mailbox Configuration" -Roles MyBaseOptions, My
```

For detailed syntax and parameter information, see New-RoleAssignmentPolicy.

Use the Shell to create a default assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

To create a default assignment policy assigned to new mailboxes, use the following syntax.

```
New-RoleAssignmentPolicy <assignment policy name> -Roles <roles to assign> -IsDef
```

This example creates the default assignment policy Limited Mailbox Configuration and assigns the `MyBaseOptions`, `MyAddressInformation`, and `MyDisplayName` roles to it.

```
New-RoleAssignmentPolicy "Limited Mailbox Configuration" -Roles MyBaseOptions, My
```

For detailed syntax and parameter information, see New-RoleAssignmentPolicy.

Other Tasks

After you create a new assignment policy, you may also want to:

- Change the Assignment Policy on a Mailbox
- Add a Role to an Assignment Policy
- Remove a Role from an Assignment Policy
- View a List of Assignment Policies
- Change the Default Assignment Policy

1.3.3.2.2 Remove an Assignment Policy

Remove an Assignment Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you no longer need a management role assignment policy, you can remove it. For more information about assignment policies in Microsoft Exchange Server 2010, see Understanding Management Role Assignment Policies.

Looking for other management tasks related to end users? Check out Managing End Users.

Prerequisites

- All users assigned the assignment policy must be changed to another assignment policy. For more information about how to change an assignment policy on a mailbox, see Change the Assignment Policy on a Mailbox.
- All the management role assignments between the assignment policy and the assigned management roles must be removed. For more information about how to remove a role assignment from an assignment policy, see Remove a Role from an Assignment Policy.
- If you want to remove a default assignment policy, it must be the last assignment policy in the Exchange 2010 organization.

Use the ECP to remove an assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

1. In the Exchange Management Console (EMC), navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **User Roles** tab.
5. Select the assignment policy you want to remove, and then click  .

Use the Shell to remove an assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

To remove an assignment policy, use the following syntax.

```
Remove-RoleAssignmentPolicy <role assignment policy>
```

This example removes the New York Temporary Users assignment policy.

```
Remove-RoleAssignmentPolicy "New York Temporary Users"
```

For detailed syntax and parameter information, see Remove-RoleAssignmentPolicy.

Other Tasks

After you remove an assignment policy, you may also want to:

- Add an Assignment Policy
- View a List of Assignment Policies

1.3.3.2.3 View a List of Assignment Policies

View a List of Assignment Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can view management role assignment policies in a variety of ways, depending on the information you want and whether you're using the Exchange Control Panel (ECP) or the Exchange Management Shell.

In the ECP, you can view the list of assignment policies and the roles assigned to them. In the Shell, you can view all the assignment policies in your organization, list the mailboxes assigned a specific policy, and more.

For more information about assignment policies in Microsoft Exchange Server 2010, see Understanding Management Role Assignment Policies.

Looking for other management tasks related to end users? Check out Managing End Users.

Use the ECP to view a list of assignment policies

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

1. In the Exchange Management Console (EMC), navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **User Roles** tab.
5. To view the details of a specific assignment policy, select the assignment policy you want to view. The description and the roles assigned to the assignment policy are displayed in the details pane.

Use the Shell to view a list of assignment policies

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

You can view a list of all the assignment policies in your organization by not specifying any assignment policies when you run the **Get-RoleAssignmentPolicy** cmdlet.

This procedure makes use of pipelining and the **Format-Table** cmdlet. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output

To return a list of all assignment policies in your organization, use the following command.

```
Get-RoleAssignmentPolicy
```

To return a list of specific properties for all the assignment policies in your organization, you can pipe the results to the **Format-Table** cmdlet and specify the properties you want in the list of results. Use the following syntax.

```
Get-RoleAssignmentPolicy | Format-Table <property 1>, <property 2...>
```

This example returns a list of all the assignment policies in your organization and includes the **Name** and **IsDefault** properties.

```
Get-RoleAssignmentPolicy | Format-Table Name, IsDefault
```

For detailed syntax and parameter information, see Get-Mailbox or Get-RoleAssignmentPolicy.

Use the Shell to view the details of a single assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

You can view the details of a specific assignment policy by using the **Get-RoleAssignmentPolicy** cmdlet and piping the output to the **Format-List** cmdlet.

This procedure makes use of pipelining and the **Format-List** cmdlet. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output

To view the details of a specific assignment policy, use the following syntax.

```
Get-RoleAssignmentPolicy <assignment policy name> | Format-List
```

This example views the details about the Redmond Users - no Text Messaging assignment policy.

```
Get-RoleAssignmentPolicy "Redmond Users - no Text Messaging" | Format-List
```

For detailed syntax and parameter information, see Get-Mailbox or Get-RoleAssignmentPolicy.

Use the Shell to find the default assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

You can find the default assignment policy by piping the output of the **Get-RoleAssignmentPolicy** cmdlet to the **Where** cmdlet. With the **Where** cmdlet, filter the data returned to display only the assignment policy that has its *IsDefault* property set to `$True`.

This procedure makes use of pipelining and the **Where** cmdlet. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output

This example returns the default assignment policy.

```
Get-RoleAssignmentPolicy | Where { $_.IsDefault -eq $True }
```

For detailed syntax and parameter information, see Get-Mailbox or Get-RoleAssignmentPolicy.

Use the Shell to view mailboxes that are assigned a specific policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

You can find all of the mailboxes assigned a specific assignment policy by piping the output of the **Get-Mailbox** cmdlet to the **Where** cmdlet. With the **Where** cmdlet, filter the data returned to display only the mailboxes that have their *RoleAssignmentPolicy* property set to the assignment policy name you specify.

This procedure makes use of pipelining and the **Where** cmdlet. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output

Use the following syntax.

```
Get-Mailbox | Where { $_.RoleAssignmentPolicy -Eq "<role assignment policy>" }
```

This example finds all the mailboxes assigned the policy Vancouver End Users.

```
Get-Mailbox | Where { $_.RoleAssignmentPolicy -Eq "Vancouver End Users" }
```

For detailed syntax and parameter information, see Get-Mailbox or Get-RoleAssignmentPolicy.

Other Tasks

After you view a list of assignment policies, you may also want to:

- Change the Assignment Policy on a Mailbox

1.3.3.2.4 Change the Assignment Policy on a Mailbox

Change the Assignment Policy on a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can change the management role assignment policy assigned to a mailbox. When you change a mailbox's assignment policy, the change takes effect as soon as the user refreshes the connection, such as the next time they log into their mailbox or open your mailbox options page. For more information about assignment policies in Microsoft Exchange Server 2010, see Understanding Management Role Assignment Policies.

Looking for other management tasks related to end users? Check out Managing End Users.

Use the EMC to change the assignment policy on a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the user or resource mailbox you want to change the assignment policy on.
3. In the action pane, click **Properties**.
4. Select the **Mailbox Settings** tab.
5. Click **Role Assignment Policy**, and then click **Properties**.
6. Click **Browse** next to the **Apply role assignment policy** text box to see a list of available assignment policies. Select the role assignment you want to configure on this user or resource mailbox, and then click **OK**.

Use the Shell to change the assignment policy on a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

To change the assignment policy that's assigned to a mailbox, use the following syntax.

```
Set-Mailbox <mailbox alias or name> -RoleAssignmentPolicy <assignment policy>
```

This example sets the assignment policy to Unified Messaging Users on the mailbox Brian.

```
Set-Mailbox Brian -RoleAssignmentPolicy "Unified Messaging Users"
```

Use the Shell to change the assignment policy on a group of mailboxes assigned a specific assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

Note:
You can't use the Exchange Management Console (EMC) to change the assignment policy on a group of mailboxes all at once.

This procedure makes use of pipelining, the **Where** cmdlet, and the *WhatIf* parameter. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output
- WhatIf, Confirm, and ValidateOnly Switches

If you want to change the assignment policy for a group of mailboxes that are assigned a specific policy, use the following syntax.

```
Get-Mailbox | Where { $_.RoleAssignmentPolicy -Eq "<assignment policy to find>" }
```

This example finds all the mailboxes assigned to the Redmond Users - No Voicemail assignment policy and changes the assignment policy to Redmond Users - Voicemail Enabled.

```
Get-Mailbox | Where { $_.RoleAssignmentPolicy -Eq "Redmond Users - No Voicemail"
```

This example includes the *WhatIf* parameter so that you can see all the mailboxes that would be changed without committing any changes.

```
Get-Mailbox | Where { $_.RoleAssignmentPolicy -Eq "Redmond Users - No Voicemail"
```

For detailed syntax and parameter information, see Get-Mailbox or Set-Mailbox.

Other Tasks

After you change the assignment policy on a mailbox, you may also want to:

- Add a Role to an Assignment Policy
- Remove a Role from an Assignment Policy
- Add an Assignment Policy
- View a List of Assignment Policies

Change the Default Assignment Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can change the management role assignment policy assigned to new mailboxes that are created. For more information about assignment policies in Microsoft Exchange Server 2010, see Understanding Management Role Assignment Policies.

Looking for other management tasks related to end users? Check out Managing End Users.

Use the Shell to change the default assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change the default assignment policy.

To change the default assignment policy, use the following syntax.

```
Set-RoleAssignmentPolicy <assignment policy name> -IsDefault
```

This example sets the Vancouver End Users assignment policy as the default assignment policy.

```
Set-RoleAssignmentPolicy "Vancouver End Users" -IsDefault
```

Important:
New mailboxes are assigned the default assignment policy even if the policy hasn't been assigned management roles. Mailboxes assigned assignment policies with no assigned management roles can't access any mailbox configuration features in the Exchange 2010 Web interface. For more information about assigning management roles, see Other Tasks later in this topic.

For detailed syntax and parameter information, see Set-RoleAssignmentPolicy.

Other Tasks

After you change the default assignment policy, you may also want to:

- Add a Role to an Assignment Policy
- Remove a Role from an Assignment Policy
- Change the Assignment Policy on a Mailbox
- View a List of Assignment Policies

Add a Role to an Assignment Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you want to enable users to manage a feature on their mailboxes, you can add a management role to the management role assignment policy they're assigned to. If more than one user is assigned an assignment policy, all the users gain the ability to manage that feature. For more information about assignment policies in Microsoft Exchange Server 2010, see Understanding Management Role Assignment Policies.

Looking for other management tasks related to end users? Check out Managing End Users.

Use the ECP to add a role to an assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

1. In the Exchange Management Console (EMC), navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **User Roles** tab.
5. Select the assignment policy you want to add one or more roles to, and then click **Details**.
6. Select the check box next to the role or roles you want to add to the assignment policy. You can select multiple roles, including end-user roles you've added. If you select a role that has child roles, the child roles are automatically selected.
7. Click **Save** to save the changes to the assignment policy.

Use the Shell to add a role to an assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

To create a management role assignment between a role and an assignment policy, use the following syntax.

```
New-ManagementRoleAssignment -Name <role assignment name> -Role <role name> -Poli
```

This example creates the role assignment Seattle Users - Voicemail between the MyVoicemail role and the Seattle Users assignment policy.

```
New-ManagementRoleAssignment -Name "Seattle Users - Voicemail" -Role MyVoicemail
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Other Tasks

After you add a role to an assignment policy, you may also want to:

- Change the Assignment Policy on a Mailbox
- Change the Default Assignment Policy
- View a List of Roles on an Assignment Policy

1.3.3.2.7 Remove a Role from an Assignment Policy

Remove a Role from an Assignment Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you don't want end users to have permissions to manage certain features of their mailbox or distribution group, you can remove the management role that grants the permissions from the management role assignment policy the user is assigned. If other users are assigned the same assignment policy, they also lose the ability to manage that feature. For more information about assignment policies in Microsoft Exchange Server 2010, see Understanding Management Role Assignment Policies.

Looking for other management tasks related to end users? Check out Managing End Users.

Use the ECP to remove a role from an assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

1. In the Exchange Management Console (EMC), navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **User Roles** tab.
5. Select the assignment policy you want to remove one or more roles from, and then click **Details**.
6. Clear the check box next to the role or roles you want to remove from the assignment policy. If you clear the check box for a role that has child roles, the check boxes for the child roles are also cleared.
7. Click **Save** to save the changes to the assignment policy.

Use the Shell to remove a role from an

assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

You can remove roles from assignment policies by retrieving the associated management role assignment using the **Get-ManagementRoleAssignment** cmdlet and then piping the role assignment returned to the **Remove-ManagementRoleAssignment** cmdlet.

For more information about regular and delegating role assignments, see Understanding Management Role Assignments.

This procedure uses pipelining. For more information about pipelining, see Pipelining.

To remove a role from an assignment policy, use the following syntax.

```
Get-ManagementRoleAssignment -RoleAssignee <assignment policy name> -Role <role n
```

This example removes the MyVoicemail management role, which enables users to manage their voice mail options, from the Seattle Users assignment policy.

```
Get-ManagementRoleAssignment -RoleAssignee "Seattle Users" -Role MyVoicemail | Re
```

For detailed syntax and parameter information, see Remove-ManagementRoleAssignment.

Other Tasks

After you remove a role from an assignment policy, you may also want to:

- Add a Role to an Assignment Policy
- View a List of Roles on an Assignment Policy

1.3.3.2.8 View a List of Roles on an Assignment Policy

View a List of Roles on an Assignment Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The management roles assigned to an assignment policy determine what actions the end users who are assigned the assignment policy can perform. By viewing the list of roles assigned to an assignment policy, you can see what actions the users assigned that assignment policy can perform. For more information about role assignment policies, see Understanding Management Role Assignment Policies.

Looking for other management tasks related to end users? Check out Managing End Users.

Use the ECP to view a list of roles on an

assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. In the Exchange Management Console (EMC), navigate to **Toolbox** in the console tree.
2. In the work pane, double-click **Role Based Access Control (RBAC) User Editor** to open the user editor in the Exchange Control Panel (ECP).
3. Provide credentials in the **Domain\user name** and **Password** fields for an account that has the permissions needed to open the user editor in the ECP. Click **Sign in**.
4. Click the **User Roles** tab.
5. To view the list of roles on an assignment policy, select the assignment policy you want to view. The roles assigned to the assignment policy are displayed in the details pane.

Use the Shell to view a list of roles on an assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Assignment policies" entry in the Role Management Permissions topic.

You can use the **Get-ManagementRoleAssignment** cmdlet to view the list of roles assigned to an assignment policy.

1. To find the names of the assignment policies in your organization, use the following command.

```
Get-RoleAssignmentPolicy
```

2. Find the name of the assignment policy whose roles you want to list.
3. To list the roles on an assignment policy, use the following syntax.

```
Get-ManagementRoleAssignment -RoleAssignee <assignment policy name>
```

This example lists all of the roles assigned to the Default Role Assignment Policy assignment policy.

```
Get-ManagementRoleAssignment -RoleAssignee "Default Role Assignment Policy"
```

For detailed syntax and parameter information, see Get-RoleAssignmentPolicy or Get-ManagementRoleAssignment.

Other Tasks

After you view the list of roles assigned to an assignment policy, you may also want to:

- Add a Role to an Assignment Policy
- Remove a Role from an Assignment Policy
- Add an Assignment Policy
- Change the Assignment Policy on a Mailbox

1.3.3.3 View Effective Permissions

View Effective Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Permissions in Microsoft Exchange Server 2010 are granted using management roles that are assigned to management role groups, management role assignment policies, universal security groups (USGs), or directly to users. Users are granted the permissions if they're members of the role groups or USGs, or are assigned role assignment policies.

Most permissions are granted based on role group membership or the assignment of assignment policies to end users. Although using role groups and assignment policies makes it easy to grant permissions to large numbers of users, you may not be aware of who is a member of a role group, or who has been assigned an assignment policy. This is where the *GetEffectiveUsers* switch on the **Get-ManagementRoleAssignment** cmdlet is useful. It shows you what users are granted the permissions given by a management role through the role groups, assignment policies, and USGs that are assigned to them.

The *GetEffectiveUsers* switch is used with the **Get-ManagementRoleAssignment** cmdlet when the *Role* parameter is used. By specifying this switch with a particular role, the **Get-ManagementRoleAssignment** cmdlet examines all of the role assignees assigned to the role, such as role groups, assignment policies, and USGs, and lists the members of each.

Note:

The *GetEffectiveUser* switch doesn't list users that are members of a linked foreign role group. Instead of a list of users, if a linked role group is found, **All Linked Group Members** is displayed. For more information about permissions in multiple forests, see Understanding Multiple-Forest Permissions.

For more information about management roles, role groups, and assignment policies, see Understanding Role Based Access Control.

For more information about management role assignments, see Understanding Management Role Assignments.

Looking for other management tasks related to managing permissions? Check out Managing Permissions.

Use the Shell to list all effective users

Note:

You can't use the EMC to list all effective users.

To list all of the users that are granted the permissions provided by a management role, use the following syntax.

```
Get-ManagementRoleAssignment -Role <role name> -GetEffectiveUsers
```

This example lists all the users that are granted permissions provided by the Mail Recipients role.

```
Get-ManagementRoleAssignment -Role "Mail Recipients" -GetEffectiveUsers
```

If you want to change what properties are returned in the list or export the list to a

comma-separated value (CSV) file, see Customize output and display it later in this topic.

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

Use the Shell to find a specific user on a role

Note:
You can't use the EMC to find a specific user on a role.

To find a specific user that's been granted permissions by a management role, you must use the **Get-ManagementRoleAssignment** cmdlet to retrieve a list of all effective users, and then pipe the output of the cmdlet to the **Where** cmdlet. The **Where** cmdlet filters the output and returns only the user you specified. Use the following syntax.

```
Get-ManagementRoleAssignment -Role <role name> -GetEffectiveUsers | Where { $_.Ef
```

This example finds the user David Strome on the Journaling role.

```
Get-ManagementRoleAssignment -Role Journaling -GetEffectiveUsers | Where { $_.Eff
```

If you want to change what properties are returned in the list or export the list to a CSV file, see Customize output and display it later in this topic.

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

Use the Shell to find a specific user on all roles

Note:
You can't use the EMC to find a specific user on all roles.

To know every role that a user receives permissions from, you must use the **Get-ManagementRoleAssignment** cmdlet to retrieve all effective users on all management roles and then pipe the output of the cmdlet to the **Where** cmdlet. The **Where** cmdlet filters the output and returns only the role assignments that grant the user permissions.

```
Get-ManagementRoleAssignment -GetEffectiveUsers | Where { $_.EffectiveUserName -E
```

This example finds all the role assignments that grant permissions to the user Kim Akers.

```
Get-ManagementRoleAssignment -GetEffectiveUsers | Where { $_.EffectiveUserName -E
```

If you want to change what properties are returned in the list or export the list to a CSV file, see Customize output and display it later in this topic.

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

Use the Shell to customize output and display it

Note:
You can't use the EMC to customize output and display it.

The default output of the **Get-ManagementRoleAssignment** cmdlet might not have the information you want. The output of the cmdlet contains many more properties that you can access. The following are some of the properties that could be useful:

- **EffectiveUserName** This is the name of the user.
- **Role** This indicates the role that's granting the permissions.
- **RoleAssigneeName** This is the role group, assignment policy, or USG that's assigned to the role and contains the user in the `EffectiveUserName` property.
- **RoleAssigneeType** This indicates whether the role assignment is to a role group, assignment policy, USG, or user.
- **AssignmentMethod** This indicates whether the assignment between the role and the role assignee is direct or indirect.
- **CustomRecipientWriteScope** This indicates the custom recipient write scope, if any, that was applied to the role assignment when it was created. The scope specified in this property overrides the implicit recipient write scope specified in the `RecipientWriteScope` property.
- **CustomConfigWriteScope** This indicates the custom configuration write scope, if any, that was applied to the role assignment when it was created. The scope specified in this property overrides the implicit configuration write scope specified in the `ConfigWriteScope` property.
- **RecipientReadScope** This indicates the implicit recipient read scope that's applied to the role.
- **RecipientWriteScope** This indicates the implicit recipient write scope that's applied to the role.
- **ConfigReadScope** This indicates the implicit configuration read scope that's applied to the role.
- **ConfigWriteScope** This indicates the implicit configuration write scope that's applied to the role.

To select the properties you want to display in your list, you use nearly the same commands that are used in the Use the Shell to list all effective users, Use the Shell to find a specific user on a role, and Use the Shell to find a specific user on all roles sections. The difference is that you pipe the results of those commands to the **Format-Table** or **Select-Object** cmdlets. The **Format-Table** cmdlet is useful to output the list of results to your screen. The **Select-Object** cmdlet is useful to output the list of your results to a CSV file.

Both cmdlets let you specify the properties you want to see and in the order you want to see them. The **Format-Table** cmdlet gives you more options when you list results to a screen while **Select-Object** doesn't modify the output in any way, which is useful when piping the list to a CSV file.

For more information about the **Format-Table** and **Select-Object** cmdlets, see Working with Command Output.

Output a customized list to your screen

First, choose the information you want to see and find the associated command from one of the following procedures:

- Use the Shell to list all effective users
- Use the Shell to find a specific user a role
- Use the Shell to find a specific user on all roles

Then, choose the properties you want to see in your list. Finally, use the following syntax to view the list.

```
<command to retrieve list > | Format-Table <property 1>, <property 2>, <property
```

This example finds the user David Strome on all roles, and displays the `EffectiveUserName`, `Role`, `CustomRecipientWriteScope`, and `CustomConfigWriteScope` properties.

```
Get-ManagementRoleAssignment -GetEffectiveUsers | Where { $_.EffectiveUserName -E
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

Output a customized list to a CSV file

To export a list to a CSV file, you need to pipe the results of the **Get-ManagementRoleAssignment** command from the appropriate procedure listed previously to the **Select-Object** cmdlet. The output of the **Select-Object** cmdlet is then piped to the **Export-CSV** cmdlet, which saves the CSV output to a file name you specify.

First, choose the information you want to see and find the associated command from one of the following procedures:

- Use the Shell to list all effective users
- Use the Shell to find a specific user a role
- Use the Shell to find a specific user on all roles

Then, choose the properties you want to see in your list. Finally, use the following syntax to export the list to a CSV file.

```
<command to retrieve list > | Select-Object <property 1>, <property 2>, <property
```

This example finds the user David Strome on all roles, and displays the `EffectiveUserName`, `Role`, `CustomRecipientWriteScope`, and `CustomConfigWriteScope` properties.

```
Get-ManagementRoleAssignment -GetEffectiveUsers | Where { $_.EffectiveUserName -E
```

You can now view the CSV file in a viewer of your choice.

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

1.3.3.4 Setting Administrator Permissions for the Edge Transport Server Role

Setting Administrator Permissions for the Edge Transport Server Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-07-19*

This topic provides an overview of the permissions that a user must have to administer a computer that has the Microsoft Exchange Server 2010 Edge Transport server role installed.

Edge Transport Server Role Permissions

The Edge Transport server role is deployed in an organization's perimeter network, which is also known as the boundary network or screened subnet. The Edge Transport server can be deployed as a stand-alone server or as a member of a perimeter Active Directory domain.

When the Exchange 2010 Edge Transport server role is installed, no Exchange-specific groups are created. The Administrators local group is granted full control of the Edge Transport server. The Administrators local group control includes the instance of Active Directory Lightweight Directory Services (AD LDS) on the Edge Transport server. When you log on by using an account that has Administrators local group membership, you can modify the server configuration, the status of queues and messages in transit, the security configuration of the server, and AD LDS data.

You perform remote administration of Edge Transport servers by using Microsoft Windows Terminal Services. The Administrators local group is automatically granted remote logon permissions. Other user accounts must have membership in the Remote Desktop Users local group to log on to the server by using a remote desktop connection. We recommend that you create a specific user account for each user who administers an Edge Transport server. You must add these user accounts to the Administrators local group to make sure that the correct access level is granted.

Permissions That Are Required to Administer the Edge Transport Server

The following table lists the common administrative tasks that are performed on the Edge Transport server and the group memberships that are required to complete each task successfully. You can use this information to delegate server administration.

Administrative tasks and group membership requirements

Task	Required group membership
Backup and restore	Backup Operators
Enable and disable agents	Administrators
Configure connectors	Administrators
Configure anti-spam policies	Administrators
Configure IP Block lists and IP Allow lists	Administrators
View queues and messages	Users
Manage queues and messages	Administrators
Create an Edge Subscription file	Administrators

1.3.3.5 Managing Advanced Permissions

Managing Advanced Permissions

Exchange Server 2010 > Permissions > Managing Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-21*

The procedures in the following sections enable you to configure advanced permissions models for your organization. You should have an in-depth knowledge of Role Based Access Control (RBAC) before performing advanced customization of your permissions model.

Management Roles and Role Entries

Management Role Scopes

Management Role Assignments

Managing Split Permissions

We recommend you manage your permissions using management role groups and management role assignment policies. For more information, see the following topics:

Managing Administrator and Specialist Users

Managing End Users

For more information about RBAC, see Understanding Role Based Access Control.

1.3.3.5.1 Management Roles and Role Entries

Management Roles and Role Entries

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-11*

The following procedures enable you to perform advanced permissions management. You should only use these procedures if management role groups and management role assignment policies don't meet the needs of your organization.

Create a Role

View a Role

Remove a Role

Add a Role Entry to a Role

Change a Role Entry

View Role Entries

Remove a Role Entry from a Role

Create an Unscoped Role

Change a Role Entry on an Unscoped Top-Level Role

Add a Role Entry to an Unscoped Top-Level Role

For more information about managing role groups and role assignment policies, see the following topics:

Managing Administrator and Specialist Users

Managing End Users

Create a Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can create a management role, change the management role entries, add a scope if needed, and then assign the role to a role assignee. You should rarely need to perform this procedure. We recommend that you check whether a built-in management role can be used instead of creating a management role. For a list of built-in management roles, see Built-in Management Roles.

For more information about management roles in Microsoft Exchange Server 2010, see Understanding Management Roles.

You must use the Shell to create management roles.

Note:
This topic doesn't discuss how to create an unscoped management role. For information about how to create an unscoped management role, see Create an Unscoped Role.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Steps

Here are the basic steps needed to create a management role. Each of these steps includes links to more detailed procedures:

Step 1: Use the Shell to create the management role.

Step 2: Use the Shell to change the new role's management role entries.

Step 3: Use the Shell to create a custom management role scope, if required.

Step 4: Use the Shell to assign the new management role.

Note:
You can't use the EMC to create a management role.

Step 1: Create the management role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

New management roles are based on existing roles. When you create a role, an existing role and its management role entries are copied to the new role. The existing role becomes the parent to the new child role. You must always choose a role that contains all the cmdlets and parameters you need to use, and then remove the ones you don't want. Child roles can't have management role entries that don’t exist in the parent role.

Use the following syntax to create the new role.

```
New-ManagementRole -Parent <existing role to copy> -Name <name of new role>
```

This example copies the Mail Recipients role and its management role entries to the Seattle Mail Recipients role.

```
New-ManagementRole -Parent "Mail Recipients" -Name "Seattle Mail Recipients"
```

For detailed syntax and parameter information, see New-ManagementRole.

Step 2: Change the new role's management role entries

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

After you create your role, you need to change the role's entries. You can remove an entire role entry, which removes access to the associated cmdlet completely. Or, you can remove parameters from a role entry to remove access to those specific parameters on the associated cmdlet.

You can't add new role entries or parameters on role entries unless they exist in the parent role. Because you just created a role from a parent role in Step 1, you can't add any additional role entries or parameters on role entries because they don't exist in the parent role.

When you change a role entry on a role, you can do one of the following:

- Remove a single, entire role entry.
- Remove multiple, entire role entries.
- Remove parameters from a role entry.

To remove role entries from your new role, see Remove a Role Entry from a Role.

Step 3: Create a custom management role scope, if required

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

Management role scopes determine the objects made available to a user to view or change using the role entries configured in Step 2. New management roles inherit the read and write management role scopes of their parent role. These are called *implicit scopes*. However, there may be cases where you want to change the write scope of the new role to match your business needs. When you create a custom scope, you override the implicit write scope of the role. The implicit read scope of the role doesn't change. For more information about management role scopes, see Understanding Management Role Scopes.

You can create a custom scope, create an exclusive scope, use a predefined scope, or scope an assignment to an organizational unit (OU). The new scope must be within the implicit read scope of the role. To use a predefined scope or to specify an organizational unit, skip to Step 4.

To add a custom scope to your new role, see Create a Regular or Exclusive Scope.

Step 4: Assign the new management role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

The final step when you create and configure a role is to assign it to a role assignee.

When you create a role assignment, you can choose to do one of the following:

- Create the role assignment with no scope.
- Create the role assignment with a predefined scope.
- Create the role assignment with an OU without a domain restriction filter.
- Create the role assignment with the custom or exclusive scope you created in Step 3.

Note:
You can't specify a scope when you create an assignment between a role and a management role assignment policy.

You can assign the new role to a role group, a role assignment policy, a user, or a universal security group (USG). For more information, see the following topics:

- Add a Role to a Role Group
- Add a Role to an Assignment Policy
- Add a Role to a User or USG

1.3.3.5.1.2 View a Role

View a Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Management roles can be listed in a variety of ways, depending on the information you want. For example, you can choose to return only roles of a specific role type, roles that contain only specific cmdlets and parameters, or view the details of a specific management role. For more information about management roles in Microsoft Exchange Server 2010, see Understanding Management Roles.

If you want to view a list of all management role entries on a role, see View Role Entries.

You must use the Shell to view management roles.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Prerequisites

This topic makes use of pipelining and the **Format-List** and **Format-Table** cmdlets. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output

What Do You Want To Do?

- View a specific management role
- List all management roles
- List management roles that contain a specific cmdlet
- List management roles that contain a specific parameter
- List management roles of a specific role type
- List the immediate child roles of a parent role
- List all child roles below a parent role

Note:
You can't use the EMC to view roles.

View a specific management role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

You can view the details of a specific role by retrieving a specific role using the **Get-ManagementRole** cmdlet and piping the output to the **Format-List** cmdlet.

To view the details of a specific role, use the following syntax.

```
Get-ManagementRole <role name> | Format-List
```

This example retrieves the details about the Mail Recipients management role.

```
Get-ManagementRole "Mail Recipients" | Format-List
```

For detailed syntax and parameter information, see Get-ManagementRole.

List all management roles

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

You can view a list of all the management roles in your organization by not specifying any roles when you run the **Get-ManagementRole** cmdlet. By default, the role name and role type of each role are included in the results.

This example returns a list of all roles in your organization.

```
Get-ManagementRole
```

To return a list of specific properties for all the roles in your organization, you can pipe the results of the **Format-Table** cmdlet and specify the properties you want in the list of results. Use the following syntax.

```
Get-ManagementRole | Format-Table <property 1>, <property 2...>
```

This example returns a list of all the roles in your organization and includes the **Name** property and any property with the word **Implicit** at the beginning of the property name.

```
Get-ManagementRole | Format-Table Name, Implicit*
```

For detailed syntax and parameter information, see Get-ManagementRole.

List management roles that contain a specific cmdlet

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

You can return a list of roles that contain a cmdlet that you specify by using the *Cmdlet* parameter on the **Get-ManagementRole** cmdlet.

To return a list of roles that contain the cmdlet you specify, use the following syntax.

```
Get-ManagementRole -Cmdlet <cmdlet>
```

This example returns a list of roles that contain the **New-Mailbox** cmdlet.

```
Get-ManagementRole -Cmdlet New-Mailbox
```

For detailed syntax and parameter information, see Get-ManagementRole.

List management roles that contain a specific parameter

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

You can return a list of roles that contain one or more specified parameters by using the *CmdletParameters* parameter on the **Get-ManagementRole** cmdlet. Only roles that contain all the parameters you specify are returned.

When you use the *CmdletParameters* parameter, you can choose to include the *Cmdlet* parameter. If you include the *Cmdlet* parameter, only roles that contain the parameters you specify on the cmdlet you specify are returned. If you don't include the *Cmdlet* parameter, roles that contain the parameters you specify, regardless of the cmdlet they're on, are returned.

To return a list of roles that contain the parameters you specify, use the following syntax.

```
Get-ManagementRole [-Cmdlet <cmdlet>] -CmdletParameters <parameter 1>, <parameter
```

This example returns a list of roles that contain the *Database* and *Server* parameters, regardless of the cmdlets they exist on.

```
Get-ManagementRole -CmdletParameters Database, Server
```

This example returns a list of roles where the *EmailAddresses* parameter exists only on the **Set-Mailbox** cmdlet.

```
Get-ManagementRole -Cmdlet Set-Mailbox -CmdletParameters EmailAddresses
```

You can also use the wildcard character (*) with either the *Cmdlet* or *CmdletParameters* parameters to match partial cmdlet or parameter names.

For detailed syntax and parameter information, see Get-ManagementRole.

List management roles of a specific role type

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

You can return a list of roles based on a specified role type by using the *RoleType* parameter on the **Get-ManagementRole** cmdlet.

To return a list of roles that match the role type you specify, use the following syntax.

```
Get-ManagementRole -RoleType <roletype>
```

This example returns a list of roles based on the `UmMailboxes` role type.

```
Get-ManagementRole -RoleType UmMailboxes
```

For detailed syntax and parameter information, see Get-ManagementRole.

List the immediate child roles of a parent role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

You can return a list of roles that are the immediate children of the specified parent role by using the *GetChildren* parameter on the **Get-ManagementRole** cmdlet. Only roles that contain the role you specify as the parent role are returned.

To return a list of the immediate children roles of a parent role, use the following syntax.

```
Get-ManagementRole <parent role name> -GetChildren
```

This example returns a list of immediate children of the Disaster Recovery role.

```
Get-ManagementRole "Disaster Recovery" -GetChildren
```

For detailed syntax and parameter information, see Get-ManagementRole.

List all child roles below a parent role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

You can return a list of the entire chain of roles from a specified parent role to the last child role by using the *Recurse* parameter on the **Get-ManagementRole** cmdlet. The *Recurse* parameter tells the **Get-ManagementRole** cmdlet to recurse down through every parent and child relationship it finds until it reaches the last child role. The parent role is included in the list that's returned.

This example returns a list of all the child roles of a parent role.

```
Get-ManagementRole <parent role name> -Recurse
```

This example returns all the child roles of the Mail Recipients role.

```
Get-ManagementRole "Mail Recipients" -Recurse
```

For detailed syntax and parameter information, see Get-ManagementRole.

1.3.3.5.1.3 Remove a Role

Remove a Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Management roles that are no longer required can be removed from your organization. You can only remove management roles that you created. Built-in management roles can't be removed. For more information about management roles in Microsoft Exchange Server 2010, see Understanding Management Roles.

You must use the Shell to remove management roles.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Prerequisites

Before you can remove a management role, you must remove all its management role assignments. For more information about how to remove a role assignment, see Remove a Role from a User or USG.

What Do You Want to Do?

- Use the Shell to remove a management role with no child roles
- Use the Shell to remove a management role with child roles
- Use the Shell to remove an unscoped management role

Note:
You can't use the EMC to remove a management role.

Remove a management role with no child roles

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

To remove a role with no child roles, use the following syntax.

```
Remove-ManagementRole <role name>
```

This example removes the Seattle Server Administrators role.

```
Remove-ManagementRole "Seattle Server Administrators"
```

For detailed syntax and parameter information, see Remove-ManagementRole.

Remove a management role with child roles

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

If a role that you want to remove has child roles, you must remove all the child roles also. You receive an error message if you try to remove a role that has child roles unless you use the *Recurse* switch. If you use the *Recurse* switch when you remove a role, the role you specify and all its child roles are removed.

Caution:

If you use the *Recurse* switch, all child roles of the specified role you want to remove are also removed. Make sure that you're aware of what roles will be removed before you run this command.

To make sure that you remove only the roles that you want to remove, use the *WhatIf* switch with your command to verify that it's correct. Use the following syntax.

```
Remove-ManagementRole <role name> -Recurse -WhatIf
```

The *WhatIf* switch performs the command without committing any changes and reports which roles it would have removed. For more information about the *WhatIf* switch, see WhatIf, Confirm, and ValidateOnly Switches.

After you confirm that only the roles you want to remove will be removed, run the same command without the *WhatIf* switch. This example removes the London Administrators role and all its child roles.

```
Remove-ManagementRole "London Administrators" -Recurse
```

For detailed syntax and parameter information, see Remove-ManagementRole.

Remove an unscoped management role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Unscoped management roles" entry in the Role Management Permissions topic.

To remove an unscoped role, the same procedures provided in Remove a management role with no child roles and Remove a management role with child roles earlier in this topic can be used. The only difference is that when you remove an unscoped role, you must specify the *UnScopedTopLevel* switch when you run the command. This example removes an unscoped role and all its child roles.

```
Remove-ManagementRole "Custom IT Scripts" -Recurse -UnScopedTopLevel
```

As with removing other roles, you should use the *WhatIf* switch to verify that you're removing the correct roles.

For detailed syntax and parameter information, see Remove-ManagementRole.

Add a Role Entry to a Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

If you want to grant access to a cmdlet, you need to add the associated management role entry to a management role. After you add the role entry to a role, the users assigned the role will be able to access that cmdlet. For more information about management role entries in Microsoft Exchange Server 2010, see Understanding Management Roles.

You can't add role entries to built-in roles. If you want to customize roles, you must create a new role. For more information about how to create a new role, see Create a Role.

You must use the Shell to add role entries to a role.

Note:
This topic doesn't discuss how to add unscoped management role entries to an unscoped management role. For more information about how to add unscoped role entries, see Add a Role Entry to an Unscoped Top-Level Role.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Prerequisites

- A role entry that you want to add to a management role must exist in that role's immediate parent management role.
- This topic makes use of pipelining. For more information about pipelining, see Pipelining.

What Do You Want to Do?

- Use the Shell to add a single role entry from a parent role
- Use the Shell to add a single role entry from a parent role and include only specific parameters
- Use the Shell to add multiple role entries from a parent role

Note:
You can't use the EMC to add a role entry to a role.

Add a single role entry from a parent role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

You can add a role entry to a role exactly as it appears on the parent role by using the following syntax.

```
Add-ManagementRoleEntry <child role name>\<cmdlet>
```

This example adds the **Set-Mailbox** cmdlet to the Recipient Administrators role.

```
Add-ManagementRoleEntry "Recipient Administrators\Set-Mailbox"
```

This command checks the parent role, and if the role entry exists, adds it to the child role. If the role entry already exists on the child role, you can include the *Overwrite* parameter to overwrite the existing role entry.

For detailed syntax and parameter information, see Add-ManagementRoleEntry.

Add a single role entry from a parent role and include only specific parameters

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

If you want to add a role entry from a parent role, but you want to include only specific parameters in the role entry on the child role, use the following syntax.

```
Add-ManagementRoleEntry <child role name>\<cmdlet> -Parameters <parameter 1>, <pa
```

This example adds the **Set-Mailbox** cmdlet to the Help Desk role, but includes only the *DisplayName* and *EmailAddresses* parameters in the entry on the child role.

```
Add-ManagementRoleEntry "Help Desk\Set-Mailbox" -Parameters DisplayName, EmailAdd
```

This command checks the parent role, and if the role entry exists, adds it to the child role. If the role entry already exists on the child role, you can include the *Overwrite* parameter to overwrite the existing role entry.

For detailed syntax and parameter information, see Add-ManagementRoleEntry.

Add multiple role entries from a parent role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

If you want to add more than one role entry to a role, you need to retrieve a list of role entries that exist on the parent role that you want to add to the child role, and then add them to the child role. To do this, you retrieve the list of role entries on a parent role by using the **Get-ManagementRoleEntry** cmdlet. Then you pipe the output of the **Get-ManagementRoleEntry** cmdlet to the **Add-ManagementRoleEntry** cmdlet. To retrieve multiple role entries, you need to use the wildcard character (*).

To add multiple entries from a parent role to a child role, use the following syntax.

```
Get-ManagementRoleEntry <parent role name>\*<partial cmdlet name>* | Add-Manageme
```

This example adds all the role entries that contain the string `Mailbox` in the cmdlet name on the Mail Recipients parent role to the Seattle Mail Recipients child role.

```
Get-ManagementRoleEntry "Mail Recipients\*Mailbox*" | Add-ManagementRoleEntry -Ro
```

If the role entries already exist on the child role, you can include the *Overwrite* parameter to overwrite the existing role entries.

For more information about retrieving a list of management role entries, see View Role Entries.

For detailed syntax and parameter information, see Get-ManagementRoleEntry and Add-ManagementRoleEntry.

1.3.3.5.1.5 Change a Role Entry

Change a Role Entry

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Each management role entry on a management role represents a single cmdlet. By adding parameters to or removing parameters from a role entry, which is then added to a management role, you control whether those parameters are available on that cmdlet. For more information about management role entries in Microsoft Exchange Server 2010, see Understanding Management Roles.

You can't modify the role entries on built-in management roles.

You must use the Shell to add or remove parameters from a role entry.

Note:
This topic doesn't discuss how to modify unscoped management role entries on an unscoped management role. For more information about how to modify unscoped role entries, see Create a Role.

Caution:
To add or remove parameters from a role entry, you must use the *AddParameter* or *RemoveParameter* parameters. If you omit the *AddParameter* or *RemoveParameter* parameter when you run the **Set-ManagementRoleEntry** cmdlet, only the parameters you specify using the *Parameters* parameter will be included in the role entry. All other parameters on the role entry will be removed.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Prerequisites

- If you want to add parameters to a role entry, the parameters you add must exist in the role entry in the parent role.
- The parameters must also exist on the cmdlet you specify.
- If you want to remove parameters from a role entry, the parameters you remove can't exist in the role entries of any child roles. You must remove the parameters from the role entries of the child roles. Use the "Use the Shell to remove one or more parameters from a role entry" procedure later in this topic to remove the parameters from the role entries of all child roles.

What Do You Want to Do?

- Use the Shell to add one or more parameters to a role entry
- Use the Shell to remove one or more parameters from a role entry

- Use the Shell to remove all parameters from a role entry
- Use the Shell to apply a specific set of parameters

Note:
You can't use the EMC to change a role entry.

Use the Shell to add one or more parameters to a role entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

To add parameters to a role entry, you need to specify the parameters you want to add using the *Parameters* parameter. You then need to specify the *AddParameter* parameter to indicate that you want to perform an add operation.

To add parameters to a role entry, use the following syntax.

```
Set-ManagementRoleEntry <role name>\<cmdlet> -Parameters <parameter 1>, <paramete
```

This example adds the *EmailAddresses* and *Type* parameters to the **Set-Mailbox** cmdlet on the Recipient Administrators role.

```
Set-ManagementRoleEntry "Recipient Administrators\Set-Mailbox" -Parameters EmailA
```

For detailed syntax and parameter information, see Set-ManagementRoleEntry.

Use the Shell to remove one or more parameters from a role entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

To remove parameters from a role entry, you need to specify the parameters you want to remove using the *Parameters* parameter. You then need to specify the *RemoveParameter* parameter to indicate that you want to perform a remove operation.

To remove parameters from a role entry, use the following syntax.

```
Set-ManagementRoleEntry <role name>\<cmdlet> -Parameters <parameter 1>, <paramete
```

This example removes the *Port*, *ProtocolLoggingLevel*, and *SmartHostAuthMechanism* parameters from the **Set-SendConnector** cmdlet on the Tier 1 Server Administrators role.

```
Set-ManagementRoleEntry "Tier 1 Server Administrators\Set-SendConnector" -Paramet
```

For detailed syntax and parameter information, see Set-ManagementRoleEntry.

Use the Shell to remove all parameters from a role entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

To remove all the parameters from a role entry, you need to specify the value $Null on the *Parameters* parameter. You don't need to include the *RemoveParameters* parameter.

Removing all the parameters from a role entry is most useful when you want to make only a few parameters available on a cmdlet and exclude all of the other parameters. If you don't want the role to have access to a cmdlet, remove the associated role entry from the role completely instead of just removing the parameters. For more information about how to remove a role entry from a role, see Remove a Role Entry from a Role.

Caution:
You can't undo remove operations. If you mistakenly remove all the parameters from a role entry, you must add them again manually.

To remove all the parameters from a role entry, use the following syntax.

```
Set-ManagementRoleEntry <role name>\<cmdlet> -Parameters $Null
```

This example removes all the parameters from the **Set-CasMailbox** cmdlet on the Recipient Administrators role.

```
Set-ManagementRoleEntry "Recipient Administrators\Set-CasMailbox" -Parameters $Nu
```

For detailed syntax and parameter information, see Set-ManagementRoleEntry.

Use the Shell to apply a specific set of parameters

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

If you want only a specific set of parameters to be included on a role entry, specify the *Parameters* parameter only. Don't include the *AddParameter* or *RemoveParameter* parameters. When you specify only the *Parameters* parameter, only the parameters you specify in the command are included on the role entry. All other parameters are removed.

To specify a specific set of parameters, use the following syntax.

```
Set-ManagementRoleEntry <role name>\<cmdlet> -Parameters <parameter 1>, <paramete
```

This example includes only the *Identity*, *DisplayName*, *MissedCallNotificationEnabled*, and *PersonalAuthAttendantEnabled* parameters on the **Set-UMMailbox** cmdlet on the Seattle Mail Recipients role.

```
Set-ManagementRoleEntry "Seattle Mail Recipients\Set-UMMailbox" -Parameters Ident
```

For detailed syntax and parameter information, see Set-ManagementRoleEntry.

1.3.3.5.1.6 View Role Entries

View Role Entries

Managing Permissions > Managing Advanced Permissions > Management Roles and Role Entries >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Each management role entry represents a single cmdlet or script. The parameters included on a role entry determine what parameters on the cmdlet or script a user can access.

The identity of role entries consists of the management role name that the role entry is associated with, and the cmdlet or script that the role entry refers to. For more information about role entries in Microsoft Exchange Server 2010, see Understanding Management Roles.

You must use the Shell to view role entries.

Looking for other management tasks related to role entries? Check out Managing Advanced Permissions.

Prerequisites

This topic makes use of pipelining, the **Format-List** cmdlet, objects, and properties. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output
- Structured Data

What Do You Want To Do?

- View a list of role entries
  - View a list of all role entries on a role
  - View a list of roles that contain a specific role entry
  - View a targeted list of roles that contain similar role entries
- View a single role entry
- View the parameters on a single role entry

View a list of role entries

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

You can use the **Get-ManagementRoleEntry** cmdlet to retrieve a list of role entries. When you use the **Get-ManagementRoleEntry** cmdlet, you must specify a value that contains both the role name that contains the role entries you want to list and also the cmdlet name of the role entry you want to list. By combining the role name and cmdlet name with the wildcard character (*), you can return specific or broad lists of role entries.

For detailed syntax and parameter information, see Get-ManagementRoleEntry.

View a list of all role entries on a role

To view a list of role entries on a specific role, use the following syntax.

```
Get-ManagementRoleEntry <role name>\*
```

This examples retrieves all the role entries on the `Recipient Administrators` role.

```
Get-ManagementRole "Recipient Administrators\*"
```

For detailed syntax and parameter information, see Get-ManagementRoleEntry.

View a list of roles that contain a specific role entry

To view a list of all the roles that contain a specific role entry, use the following syntax.

```
Get-ManagementRoleEntry *\<cmdlet name>
```

This example retrieves all the roles that contain the **Set-Mailbox** role entry.

```
Get-ManagementRoleEntry *\Set-Mailbox
```

For detailed syntax and parameter information, see Get-ManagementRoleEntry.

View a targeted list of roles that contain similar role entries

To view a list of targeted roles that contain cmdlets with similar names, use the following syntax.

```
Get-ManagementRoleEntry *<partial role name>*\*<partial cmdlet name>*
```

This example returns a list of role entries that contain the string `Mailbox` that are on roles that contain the string `Tier 1` in their names.

```
Get-ManagementRoleEntry "*Tier 1*\*Mailbox*"
```

For detailed syntax and parameter information, see Get-ManagementRoleEntry.

View a single role entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

To view the details of a single role entry, use the following syntax.

```
Get-ManagementRoleEntry <role name>\<cmdlet name> | Format-List
```

This example retrieves the details of the **Set-Mailbox** role entry on the `Recipient Administrators` role.

```
Get-ManagementRoleEntry "Recipient Administrators\Set-Mailbox" | Format-List
```

If the role entry you view has too many parameters to list using the **Format-List** cmdlet, see "View the parameters on a single role entry" later in this topic.

For detailed syntax and parameter information, see Get-ManagementRoleEntry.

View the parameters on a single role entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

Some role entries have more parameters than can be viewed by piping the results of the **Get-ManagementRoleEntry** cmdlet to the **Format-List** cmdlet. If you need to view all the parameters on a role entry, you need to directly access the **Parameters** property of the role entry object.

To view parameters stored in the **Parameters** property of a role entry object, use the following syntax.

```
(Get-ManagementRoleEntry <role name>\<cmdlet name>).Parameters
```

This example retrieves the parameters on the **Set-Mailbox** role entry on the Mail Recipients role.

```
(Get-ManagementRoleEntry "Mail Recipients\Set-Mailbox").Parameters
```

For detailed syntax and parameter information, see Get-ManagementRoleEntry.

1.3.3.5.1.7 Remove a Role Entry from a Role

Remove a Role Entry from a Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Management role entries on a management role determine what cmdlets and parameters are available on a management role. By removing role entries or parameters on a role entry, you can restrict what users assigned the management role can perform. For more information about management role entries in Microsoft Exchange Server 2010, see Understanding Management Roles.

You must use the Shell to remove role entries from a role.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

What Do You Want to Do?

- Use the Shell to remove a single entire role entry from a role
- Use the Shell to remove multiple entire role entries from a role
- Use the Shell to remove parameters from a role entry on a role

Note:
You can't use the EMC to remove a role entry from a role.

Remove a single entire role entry from a role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

When you remove a role entry from a role, you remove the ability for users assigned that role to access the associated cmdlet or script.

Use the following syntax to remove an entire management role entry from a role.

```
Remove-ManagementRoleEntry <management role>\<management role entry>
```

This example removes the **Enable-MailUser** cmdlet from the Seattle Server Administrators role.

```
Remove-ManagementRoleEntry "Seattle Server Administrators\Enable-MailUser"
```

For detailed syntax and parameter information, see Remove-ManagementRoleEntry.

Remove multiple entire role entries from a role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

When you remove multiple role entries from a role, you remove the ability for users assigned that role to access the associated cmdlets or scripts.

To remove multiple role entries from a role, you need to retrieve the list of role entries to remove using the **Get-ManagementRoleEntry** cmdlet. Then you need to pipe the output to the **Remove-ManagementRoleEntry** cmdlet. You can use wildcard characters with the **Get-ManagementRoleEntry** cmdlet to match multiple role entries. It's a good idea to use the *WhatIf* switch to verify that you're removing the correct role entries. Use the following syntax.

```
Get-ManagementRoleEntry <management role>\<role entry with wildcard character> |
```

This example removes all the role entries that contain the word journal from the Seattle Server Administrators role.

```
Get-ManagementRoleEntry "Seattle Server Administrators\*Journal*" | Remove-Manage
```

When you run the command with the *WhatIf* switch, the cmdlet returns a list of all the role entries that would be removed. If the list looks correct, run the command again without the *WhatIf* switch to remove the role entries.

```
Get-ManagementRoleEntry "Seattle Server Administrators\*Journal*" | Remove-Manage
```

For detailed syntax and parameter information, see Get-ManagementRoleEntry and Remove-ManagementRoleEntry.

Remove parameters from a role entry on a role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management role entries" entry in the Role Management Permissions topic.

When you remove parameters from a role entry on a role, those parameters are no longer available to users assigned the role.

Use the following syntax to remove parameters from a role entry.

```
Set-ManagementRoleEntry <management role>\<role entry> -Parameters <parameter 1>,
```

This example removes the *MaxSafeSenders*, *MaxSendSize*, *SecondaryAddress*, and *UseDatabaseQuotaDefaults* parameters from the **Set-Mailbox** role entry on the Seattle Server Administrators role.

```
Set-ManagementRoleEntry "Seattle Server Adminstrators\Set-Mailbox" -Parameters Ma
```

For detailed syntax and parameter information, see Set-ManagementRoleEntry.

1.3.3.5.1.8 Create an Unscoped Role

Create an Unscoped Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

An unscoped management role can be used to provide administrators and specialist users access to Windows PowerShell scripts and non-Exchange cmdlets. You can either create an unscoped top-level role and add scripts or non-Exchange cmdlets to that role, or create a role that's based on an existing, unscoped top-level role. After an unscoped role has been created and customized, the role can be assigned to management role groups, users, and universal security groups (USGs). Unscoped roles can't be assigned to management role assignment policies. For more information about unscoped roles, see Understanding Management Roles.

Caution:
Unscoped roles can be powerful because, as their name implies, no management scopes are applied to them. This means that the scripts and non-Exchange cmdlets that they contain can be run against any object in your Exchange organization. Consider this when adding scripts or non-Exchange cmdlets to an unscoped role and when assigning the unscoped role.

Note:
If you want to create a role that contains Exchange cmdlets, you must create a role that's based on an existing management role. For more information about creating roles with Exchange cmdlets, see Create a Role.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Prerequisites

The ability to create unscoped roles isn't included in any management role group by default. You must first assign the Unscoped Role Management role to a user, or to a USG or role group of which the user is a member, before the user is able to create a role group. For more information about adding a role to a user, USG, or role group, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

What Do You Want to Do?

- Create an unscoped top-level management role
- Create an unscoped role based on another unscoped role

Create an unscoped top-level management role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Unscoped management roles" entry in the Role Management Permissions topic.

If you want to make scripts or non-Exchange cmdlets available to administrators or specialists in your organization, you need to create an unscoped top-level role. Scripts and non-Exchange cmdlets can only be added to an unscoped role that's created as a top-level role, because the initial unscoped role doesn't inherit from other roles. The new, unscoped top-level role can then be a parent to other unscoped roles that can also use the added scripts and non-Exchange cmdlets.

Here are the steps to create an unscoped top-level role:

- Step 1: Create the unscoped top-level role
- Step 2a: Add script management role entries
- Step 2b: Add non-Exchange cmdlet role entries
- Step 3: Assign the management role

Step 1: Create the unscoped top-level role

Unscoped top-level roles don't have a parent role. You need to specify the *UnscopedTopLevel* switch to create a role without a parent. Use the following syntax to create the new role.

```
New-ManagementRole <name of new role> -UnscopedTopLevel
```

This example creates the IT Scripts unscoped top-level role.

```
New-ManagementRole "IT Scripts" -UnscopedTopLevel
```

After it's created, the role is empty until you add scripts or non-Exchange cmdlets to it.

For detailed syntax and parameter information, see New-ManagementRole.

Step 2a: Add script management role entries

If you want to add a script to the new unscoped role, use this step. If you want to add a non-Exchange cmdlet to the new unscoped role, use Step 2b.

To add a Windows PowerShell script to an unscoped top-level role, you must add a management role entry to the role. The role entry contains the script's name and the parameters on the script that you want to make available to the role.

The script must reside in the Scripts directory in the Microsoft Exchange Server 2010 installation path on every server running Exchange 2010 where users might connect to run the script. If a user has access to run a script, but the script isn't located on the Exchange 2010 server the user is connected to, an error occurs. By default, the path to the Scripts directory is C:\Program Files\Microsoft\Exchange Server\V14\Scripts.

After you copy the script to the appropriate Exchange 2010 servers and you decide what script parameters should be used, create the role entry using the following syntax.

```
Add-ManagementRoleEntry <unscoped top-level role name>\<script filename> -Paramet
```

This example adds the BulkProvisionUsers.ps1 script to the IT Scripts role with the *Name* and *Location* parameters.

```
Add-ManagementRoleEntry "IT Scripts\BulkProvisionUsers.ps1" -Parameters Name, Loc
```

Note:

The **Add-ManagementRoleEntry** cmdlet performs basic validation to make sure that you add only the parameters that exist in the script. However, no further validation is done after the role entry is added. If parameters are later added or removed, you must manually update the role entries that contain the script.

Step 2b: Add non-Exchange cmdlet role entries

If you want to add a non-Exchange cmdlet to the new unscoped role, use this step. If you want to add a script to the new unscoped role, use Step 2a.

To add a non-Exchange cmdlet to an unscoped top-level role, you must add a management role entry to the role. The role entry contains the cmdlet snap-in, cmdlet name, and the parameters on the cmdlet that you want to make available to the role.

If you add non-Exchange cmdlets to the new role, the cmdlets must be installed on every Exchange 2010 server where users might connect to run the cmdlets. To learn how to properly install and register the Windows PowerShell snap-ins that contain the cmdlets you want to use, refer to the documentation for your product.

After you install the Windows PowerShell snap-in that contains the cmdlets on the appropriate Exchange 2010 servers and you decide what cmdlet parameters should be used, create the role entry using the following syntax.

```
Add-ManagementRoleEntry <unscoped top-level role name>\<cmdlet name> -PSSnapinNam
```

This example adds the **Set-WidgetConfiguration** cmdlet in the Contoso.Admin.Cmdlets snap-in to the Widget Cmdlets role with the *Database* and *Size* parameters.

```
Add-ManagementRoleEntry "Widget Cmdlets\Set-WidgetConfiguration" -PSSnapinName Co
```

Note:

The **Add-ManagementRoleEntry** cmdlet performs basic validation to make sure that you add only the parameters that exist in the cmdlet. However, no further validation is done after the role entry is added. If the cmdlet is later changed, and parameters are added or removed, you must manually update the role entries that contain the cmdlet.

Step 3: Assign the management role

The final step when you create and configure a role is to assign it to a role assignee.

Important:

Management scopes can't be configured on role assignments that assign an unscoped role. Whether you choose to create a role assignment for a role group, user, or USG, you must choose the option to create a role assignment without a management scope.

You can assign the new role to a role group, user, or USG. For more information, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Create an unscoped role based on another unscoped role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

If you have an existing, unscoped top-level role or other unscoped roles that you want to base new unscoped roles on, you can create child unscoped roles. The child unscoped roles can contain a subset of the scripts and cmdlets that exist on the parent unscoped roles. This is useful, for example, if you want to give only a subset of the scripts or cmdlets available on a parent unscoped role to a less experienced administrator.

Here are the steps to create an unscoped child role:

- Step 1: Create the unscoped child role
- Step 2: Change the role's management role entries
- Step 3: Assign the management role

Step 1: Create the unscoped child role

New, unscoped child roles can be based on existing unscoped roles. When you create a role, an existing role and its management role entries are copied to the new role. The existing role becomes the parent to the new child role. If you create an unscoped role that's based on another unscoped role, you must choose a role that contains all the cmdlets and parameters you need to use, and then remove the ones you don't want. Child unscoped roles can't have management role entries that don't exist in the parent role.

Note:

If you need to create an unscoped role that contains scripts or non-Exchange cmdlets that don't exist in any other unscoped role, create an unscoped top-level role. For more information, see Create an unscoped top-level management role earlier in this topic.

Use the following syntax to create the new role.

```
New-ManagementRole -Parent <existing unscoped role to copy> -Name <name of new un
```

This example copies the IT Global Scripts role and its management role entries to the Diagnostic IT Scripts role.

```
New-ManagementRole -Parent "IT Global Scripts" -Name "Diagnostic IT Scripts"
```

For detailed syntax and parameter information, see New-ManagementRole.

Step 2: Change the role's management role entries

After you create your role, you need to change the role's entries. You can remove an entire role entry, which removes access to the associated script or non-Exchange cmdlet completely. Or, you can remove parameters from a role entry to remove access to those specific parameters on the associated script or non-Exchange cmdlet.

You can't add role entries or parameters on role entries unless they exist in the parent role. Because you just created a role from a parent role in Step 1, you can't add any additional role entries or parameters on role entries because they don't exist in the parent role.

When you change a role entry on a role, you can do one of the following:

- Remove a single, entire role entry.
- Remove multiple, entire role entries.
- Remove parameters from a role entry.

To remove role entries from your new role, see Remove a Role Entry from a Role.

Step 3: Assign the management role

The final step when you create and configure a role is to assign it to a role assignee.

Important:

Management scopes can't be configured on role assignments that assign an unscoped role. Whether you choose to create a role assignment for a role group, user, or USG, you must choose the option to create a role assignment without a management scope.

You can assign the new role to a role group, user, or USG. For more information, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

1.3.3.5.1.9 Change a Role Entry on an Unscoped Top-Level Role

Change a Role Entry on an Unscoped Top-Level Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role entries on unscoped top-level management roles refer to the scripts and non-Exchange cmdlets, and their parameters, that you want to make available to those assigned the role. By changing the parameters available on a role entry, you control what those assigned the role can do with the script or non-Exchange cmdlet. For more information about unscoped role entries, see Understanding Management Roles.

Note:
If you want to change a role entry on a management role that contains Exchange cmdlets, see Change a Role Entry.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Prerequisites

The ability to change a role entry on an unscoped top-level role isn't included in any management role group by default. You must first assign the Unscoped Role Management role to a user, or to a universal security group (USG) or role group of which the user is a member, before the user is able to add or change an unscoped top-level role entry. For more information about adding a role to a user, USG, or role group, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Note:
You can't use the EMC to change a role entry.

Use the Shell to add one or more parameters to a role entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Unscoped management roles" entry in the Role Management Permissions topic.

To add parameters to an unscoped top-level role entry, you need to do the following:

- Specify the parameters you want to add using the *Parameters* parameter.
- Specify the *AddParameter* parameter to indicate that you want to perform an add operation.
- Specify the *UnscopedTopLevel* parameter to indicate that you're changing a role entry on an unscoped top-level role. If you don't specify this parameter when you change a role entry on an unscoped role, an error occurs.

To add parameters to a role entry, use the following syntax.

```
Set-ManagementRoleEntry <role name>\<script or non-Exchange cmdlet> -Parameters <
```

This example adds the *EmailAddress* and *City* parameters to the **CreateUsers.ps1** script on the Recipient Administrators unscoped role.

```
Set-ManagementRoleEntry "Recipient Administrators\CreateUsers.ps1" -Parameters Em
```

For detailed syntax and parameter information, see Set-ManagementRoleEntry.

Use the Shell to remove one or more parameters from a role entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Unscoped management roles" entry in the Role Management Permissions topic.

To remove parameters from a role entry, you need to do the following:

- Specify the parameters you want to remove using the *Parameters* parameter.
- Specify the *RemoveParameter* parameter to indicate that you want to perform a remove operation.
- Specify the *UnscopedTopLevel* parameter to indicate that you're changing a role entry on an unscoped top-level role. If you don't specify this parameter when you change a role entry on an unscoped role, an error occurs.

Caution:

You can't undo remove operations. If you mistakenly remove a parameter from a role entry, you must add it again manually.

To remove parameters from a role entry, use the following syntax.

```
Set-ManagementRoleEntry <role name>\<script or non-Exchange cmdlet> -Parameters <
```

This example removes the *Delay*, *Force*, and *Credential* parameters from the **Start-Widget** non-Exchange cmdlet on the Tier 1 Server Administrators role.

```
Set-ManagementRoleEntry "Tier 1 Server Administrators\Start-Widget" -Parameters D
```

For detailed syntax and parameter information, see Set-ManagementRoleEntry.

Use the Shell to remove all parameters from a role entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Unscoped management roles" entry in the Role Management Permissions topic.

To remove all of the parameters from a role entry, you need to do the following:

- Specify the value `$Null` on the *Parameters* parameter. You don't need to include the *RemoveParameter* parameter.
- Specify the *UnscopedTopLevel* parameter to indicate that you're changing a role entry on an unscoped top-level role. If you don't specify this parameter when you change a role entry on an unscoped role, an error occurs.

Removing all the parameters from a role entry is most useful when you want to make only a few parameters available on a script or non-Exchange cmdlet and exclude all of the

other parameters.

If you don't want the role to have access to a script or non-Exchange cmdlet, remove the associated role entry from the role completely instead of just removing the parameters. For more information about how to remove a role entry from a role, see Remove a Role Entry from a Role.

Caution:
You can't undo remove operations. If you mistakenly remove all the parameters from a role entry, you must add them again manually.

To remove all the parameters from a role entry, use the following syntax.

```
Set-ManagementRoleEntry <role name>\<script or non-Exchange cmdlet> -Parameters $
```

This example removes all the parameters from the FindMailboxesOverQuota.ps1 script on the Recipient Administrators role.

```
Set-ManagementRoleEntry "Recipient Administrators\FindMailboxesOverQuota.ps1" -Pa
```

For detailed syntax and parameter information, see Set-ManagementRoleEntry.

Use the Shell to apply a specific set of parameters

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Unscoped management roles" entry in the Role Management Permissions topic.

If you want only a specific set of parameters to be included on a role entry, you need to do the following:

- Specify the *Parameters* parameter only. Don't include the *AddParameter* or *RemoveParameter* parameters.
- Specify the *UnscopedTopLevel* parameter to indicate that you're changing a role entry on an unscoped role. If you don't specify this parameter when you change a role entry on an unscoped top-level role, an error occurs.

Caution:
When you specify only the *Parameters* parameter, only the parameters you specify in the command are included on the role entry. All other parameters are removed.

To specify a specific set of parameters, use the following syntax.

```
Set-ManagementRoleEntry <role name>\<script or non-Exchange cmdlet> -Parameters <
```

This example includes only the *Alias*, *DisplayName*, *WidgetConfig*, and *Enabled* parameters on the **Set-Widget** cmdlet on the Seattle Mail Recipient Admins role.

```
Set-ManagementRoleEntry "Seattle Mail Recipient Admins\Set-UMMailbox" -Parameters
```

For detailed syntax and parameter information, see Set-ManagementRoleEntry.

Other Tasks

After you change a role entry on an unscoped top-level role, you may also want to:

- Add a Role Entry to a Role

- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

1.3.3.5.1.10 Add a Role Entry to an Unscoped Top-Level Role

Add a Role Entry to an Unscoped Top-Level Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can add scripts and non-Exchange cmdlets to unscoped top-level management roles if you want to make new scripts or non-Exchange cmdlets available to existing unscoped roles. These scripts and non-Exchange cmdlets are added as management role entries to unscoped top-level management roles. They can then be used by those unscoped top-level role entries or any unscoped roles derived from the top-level roles. For more information about unscoped role entries, see Understanding Management Roles.

Note:
If you want to change a role entry on a management role that contains Exchange cmdlets, see Change a Role Entry.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Prerequisites

The ability to add a role entry on an unscoped top-level role isn't included in any management role group by default. You must first assign the Unscoped Role Management role to a user, or to a universal security group (USG) or role group of which the user is a member, before the user is able to add an unscoped top-level role entry. For more information about adding a role to a role group, user, or USG, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Add a script role entry to an unscoped top-level role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Unscoped management roles" entry in the Role Management Permissions topic.

If you want to add a script to an existing unscoped role, use this procedure. If you want to add a non-Exchange cmdlet to an existing unscoped role, see "Add a non-Exchange cmdlet role entry to an unscoped top-level role" later in this topic.

To add a Windows PowerShell script to an unscoped top-level role, you must add a management role entry to the role. The role entry contains the script's name and the

parameters on the script that you want to make available to the role.

The script must reside in the Scripts directory in the Microsoft Exchange Server 2010 installation path on every server running Exchange 2010 where users might connect to run the script. If a user has access to run a script, but the script isn't located on the Exchange 2010 server the user is connected to, an error occurs. By default, the path to the Scripts directory is C:\Program Files\Microsoft\Exchange Server\V14\Scripts.

After you copy the script to the appropriate Exchange 2010 servers and you decide what script parameters should be used, create the role entry using the following syntax.

```
Add-ManagementRoleEntry <unscoped top-level role name>\<script filename> -Paramet
```

This example adds the BulkProvisionUsers.ps1 script to the IT Scripts role with the *Name* and *Location* parameters.

```
Add-ManagementRoleEntry "IT Scripts\BulkProvisionUsers.ps1" -Parameters Name, Loc
```

Note:

The **Add-ManagementRoleEntry** cmdlet performs basic validation to make sure that you add only the parameters that exist in the script. However, no further validation is done after the role entry is added. If parameters are later added or removed, you must manually update the role entries that contain the script.

Add a non-Exchange cmdlet role entry to an unscoped top-level role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Unscoped management roles" entry in the Role Management Permissions topic.

If you want to add a non-Exchange cmdlet to an existing unscoped role, use this procedure. If you want to add a script cmdlet to an existing unscoped role, see "Add a script role entry to an unscoped top-level role" earlier in this topic.

To add a non-Exchange cmdlet to an unscoped top-level role, you must add a management role entry to the role. The role entry contains the cmdlet snap-in, cmdlet name, and the parameters on the cmdlet that you want to make available to the role.

If you add non-Exchange cmdlets to the new role, the cmdlets must be installed on every Exchange 2010 server where users might connect to run the cmdlets. To learn how to properly install and register the Windows PowerShell snap-ins that contain the cmdlets you want to use, refer to the documentation for your product.

After you install the Windows PowerShell snap-in that contains the cmdlets on the appropriate the Exchange 2010 servers and you decide what cmdlet parameters should be used, create the role entry using the following syntax.

```
Add-ManagementRoleEntry <unscoped top-level role name>\<cmdlet name> -PSSnapinNam
```

This example adds the **Set-WidgetConfiguration** cmdlet in the Contoso.Admin.Cmdlets snap-in to the Widget Cmdlets role with the *Database* and *Size* parameters.

```
Add-ManagementRoleEntry "Widget Cmdlets\Set-WidgetConfiguration" -PSSnapinName Co
```

Note:

The **Add-ManagementRoleEntry** cmdlet performs basic validation to make sure that you add only the parameters that exist in the cmdlet. However, no further validation is done after the role entry is added. If the cmdlet is later changed, and parameters are added or

removed, you must manually update the role entries that contain the cmdlet.

Other Tasks

After you add a role entry or an unscoped top-level role, you may also want to:

- Add a Role Entry to a Role
- Add a Role to a Role Group
- Remove a Role from a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group
- Add a Role to a User or USG
- Remove a Role from a User or USG

1.3.3.5.2 Management Role Scopes

Management Role Scopes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-05*

The following procedures enable you to perform advanced permissions management. You should only use these procedures if management role groups and management role assignment policies don't meet the needs of your organization.

Create a Regular or Exclusive Scope

Change a Role Scope

View Role Scopes

Remove a Role Scope

Control Automatic Mailbox Distribution Using Database Scopes

For more information about managing role groups and role assignment policies, see the following topics:

Managing Administrator and Specialist Users

Managing End Users

1.3.3.5.2.1 Create a Regular or Exclusive Scope

Create a Regular or Exclusive Scope

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role scopes determine what objects are made available to a user so that the objects can be changed using the cmdlets and parameters assigned to them. By adding a management scope, you can configure management role assignments so users can administer specific servers, databases, recipients, and other objects in your organization while being restricted from changing other objects.

Important:
When you create a regular or exclusive scope, you override the write scope that's defined on the management role you're assigning. You can't override the read scope that's configured on the management role.

You can create a custom management scope and add or change a management role assignment. If you want to create a management role assignment with a prebuilt or organizational unit (OU) management scope, see Add a Role to a User or USG.

For more information about management role scopes and assignments in Microsoft Exchange Server 2010, see the following topics:

- Understanding Management Role Scopes
- Understanding Management Role Assignments

Looking for other management tasks related to scopes? Check out Managing Advanced Permissions.

Step 1: Create a custom scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a custom scope.

To create a custom scope, choose one of the following types of scopes.

Recipient filter scope

Recipient filter-based scopes are created by using the *RecipientRestrictionFilter* parameter on the **New-ManagementScope** cmdlet. When you create a recipient filter, in addition to the recipient properties to filter, you can specify the OU in which the filter query runs. When you specify a base OU, you further restrict the write scope of the role.

For more information about management scope filters, see Understanding Management Role Scope Filters.

Use the following syntax to create a domain restriction filter scope with a base OU.

```
New-ManagementScope -Name <scope name> -RecipientRestrictionFilter <filter query>
```

This example creates a scope that includes all mailboxes within the contoso.com/Sales OU.

```
New-ManagementScope -Name "Mailboxes in Sales OU" -RecipientRestrictionFilter { R
```

Note:
You can omit the *RecipientRoot* parameter if you want the filter to apply to the entire implicit read scope of the management role and not just within a specific OU.

For detailed syntax and parameter information, see New-ManagementScope.

Server filter configuration scope

Server filter-based configuration scopes are created by using the *ServerRestrictionFilter* parameter on the **New-ManagementScope** cmdlet. A server filter enables you to create a scope that applies only to the servers that match the filter you specify.

For more information about management scope filters and for a list of filterable server properties, see Understanding Management Role Scope Filters.

Use the following syntax to create a server filter scope.

```
New-ManagementScope -Name <scope name> -ServerRestrictionFilter <filter query>
```

This example creates a scope that includes all the servers within the 'CN=Redmond,CN=Sites,CN=Configuration,DC=contoso,DC=com' AD (Active Directory) site.

```
New-ManagementScope -Name "Servers in Seattle AD site" -ServerRestrictionFilter {
```

For detailed syntax and parameter information, see New-ManagementScope.

Server list configuration scope

Server list-based configuration scopes are created by using the *ServerList* parameter on the **New-ManagementScope** cmdlet. A server list scope enables you to create a scope that applies only to the servers you specify in a list.

Use the following syntax to create a server list scope.

```
New-ManagementScope -Name <scope name> -ServerList <server 1>, <server 2...>
```

This example creates a scope that applies only to MBX1, MBX3, and MBX5.

```
New-ManagementScope -Name "Mailbox servers" -ServerList MBX1,MBX3,MBX5
```

For detailed syntax and parameter information, see New-ManagementScope.

Database filter configuration scope

Database filter-based configuration scopes are created by using the *DatabaseRestrictionFilter* parameter on the **New-ManagementScope** cmdlet. A database filter enables you to create a scope that applies only to the databases that match the filter you specify.

Important:

Role assignments associated with database scopes are applied only to users who connect to servers running Microsoft Exchange Server 2010 Service Pack 1 (SP1). If a user assigned a role assignment associated with a database scope connects to a release to manufacturing (RTM) version of Exchange 2010, the role assignment isn't applied to the user, and the user won't be granted any permissions provided by the role assignment.

For more information about management scope filters and for a list of filterable database properties, see Understanding Management Role Scope Filters.

Use the following syntax to create a database restriction filter.

```
New-ManagementScope -Name <scope name> -DatabaseRestrictionFilter <filter query>
```

This example creates a scope that includes all the databases that contain the string "Executive" in the **Name** property of the database.

```
New-ManagementScope -Name "Executive Databases" -DatabaseRestrictionFilter { Name
```

For detailed syntax and parameter information, see New-ManagementScope.

Database list configuration scope

Database list-based configuration scopes are created by using the *DatabaseList* parameter on the **New-ManagementScope** cmdlet. A database list scope enables you to create a scope that applies only to the databases you specify in a list.

Important:

Role assignments associated with database scopes are applied only to users who connect to servers running Microsoft Exchange Server 2010 Service Pack 1 (SP1). If a user assigned a role assignment associated with a database scope connects to a release to manufacturing (RTM) version of Exchange 2010, the role assignment isn't applied to the user, and the user won't be granted any permissions provided by the role assignment.

Use the following syntax to create a database list scope.

```
New-ManagementScope -Name <scope name> -DatabaseList <database 1>, <database 2...
```

This example creates a scope that applies only to the databases Database 1, Database 2, and Database 3.

```
New-ManagementScope -Name "Primary databases" -DatabaseList "Database 1", "Databa
```

For detailed syntax and parameter information, see New-ManagementScope.

Exclusive scope

Any scope that you create with the **New-ManagementScope** cmdlet can be designated as an exclusive scope. To create an exclusive scope, you use the same commands in one of the preceding sections to create a recipient filter-based scope, server filter-based scope, server list-based scope, database filter-based scope, or database list-based scope, and then add the *Exclusive* switch to the command.

Caution:

When you create exclusive management scopes, only the role assignees assigned exclusive scopes that contain objects to be modified can access those objects. Only those administrators assigned a role with the exclusive scope can access these exclusive, or protected, objects.

This example creates an exclusive recipient filter-based scope that matches any user in the Executives department.

```
New-ManagementScope "Executive Users Exclusive Scope" -RecipientRestrictionFilter
```

By default, when an exclusive scope is created, you're required to acknowledge that you created an exclusive scope and that you're aware of the impact that an exclusive scope has on existing role assignments that aren't exclusive. If you want to suppress the warning, you can use the *Force* switch. This example creates the same scope as the previous example, but without a warning.

```
New-ManagementScope "Executive Users Exclusive Scope" -RecipientRestrictionFilter
```

For detailed syntax and parameter information, see New-ManagementScope.

Step 2: Add or change a management role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to add or change a management role assignment.

After you create the scope, you must add it to a new or existing management role assignment.

If you create a management scope and want to add it to a new management role assignment that you're going to create, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

If you create a management role scope and want to add it to an existing management role assignment, see the following topics:

- Change the Scope of Role Assignments to a Role Group
- Change a Role Assignment

1.3.3.5.2.2 Change a Role Scope

Change a Role Scope

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role scopes determine what objects are made available to a user so that the objects can be changed using the cmdlets and parameters assigned to them. By changing a scope, you can change what objects are made available to users to create, change, or remove.

You can change a custom management scope. You can change either exclusive or regular scopes. If you change an exclusive scope, the new scope takes effect immediately. If you want to change a management role assignment with a predefined or organizational unit (OU) management scope, see Change a Role Assignment.

For more information about management role scopes and assignments in Microsoft Exchange Server 2010, see the following topics:

- Understanding Management Role Scopes
- Understanding Management Role Assignments

You must use the Shell to change scopes.

Looking for other management tasks related to role scopes? Check out Managing Advanced Permissions.

Change the name of a scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change the name of a scope.

To change the name of a scope, use the following syntax.

```
Set-ManagementScope <current scope name> -Name <new scope name>
```

This example changes the Seattle Servers scope to Seattle Exchange Servers.

```
Set-ManagementScope "Seattle Servers" -Name "Seattle Exchange Servers"
```

For detailed syntax and parameter information, see Set-ManagementScope.

Change a recipient filter on a scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change a recipient filter on a scope.

To change the recipient filter on a scope, use the following syntax.

```
Set-ManagementScope <scope name> -RecipientRestrictionFilter { <new recipient fil
```

This example changes the recipient filter to match all the recipient objects where the **Company** property is set to contoso.

```
Set-ManagementScope "Company Scope" -RecipientRestrictionFilter { Company -eq 'co
```

For detailed syntax and parameter information, see Set-ManagementScope.

For more information about recipient filters and to see a list of filterable recipient properties, see Understanding Management Role Scope Filters.

Change the organizational unit root on a scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change the organizational unit root on a scope.

To change the OU root on a scope, use the following syntax.

```
Set-ManagementScope <scope name> -RecipientRoot <OU>
```

This example changes the OU root to the North America/Sales Sales Users OU under the contoso.com domain.

```
Set-ManagementScope "Sales Users" -RecipientRoot "contoso.com/North America/Sales
```

For detailed syntax and parameter information, see Set-ManagementScope.

Change a server filter on a scope

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change a server filter on a scope.

To change the server filter on a scope, use the following syntax.

```
Set-ManagementScope <scope name> -ServerRestrictionFilter { <new server filter> }
```

This example changes the server filter to match all the server objects where the **ServerSite** property is set to 'CN=Redmond,CN=Sites,CN=Configuration,DC=contoso,DC=com'.

```
Set-ManagementScope "Company Scope" -ServerRestrictionFilter { ServerSite -eq 'CN
```

For detailed syntax and parameter information, see Set-ManagementScope.

For more information about server filters and to see a list of filterable server properties, see Understanding Management Role Scope Filters.

Change the server list on a scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

You can't change the list of servers on a scope. If you need to change the server list, you need to do the following:

1. If needed, retrieve the current server list in the scope to be replaced by using the "View a specific scope" procedure in the View Role Scopes topic.
2. Create a scope with the new server list by using the "Step 1: Create a custom scope" procedure in the Create a Regular or Exclusive Scope topic.
3. Change all the management role assignments that use the old scope to use the new scope by using the "Use the Shell to change the server filter or list-based scope on a role assignment" procedure in the Change a Role Assignment topic.
4. Remove the old scope by using the procedure in the Remove a Role Scope topic.

Change a database filter on a scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change a database filter on a scope.

To change the database filter on a scope, use the following syntax.

```
Set-ManagementScope <scope name> -DatabaseRestrictionFilter { <new database filte
```

This example changes the database filter to match all the database objects where the **Name** property contains the string "Executive".

```
Set-ManagementScope "Database Executive Scope" -DatabaseRestrictionFilter { Name
```

For detailed syntax and parameter information, see Set-ManagementScope.

For more information about database filters and to see a list of filterable database properties, see Understanding Management Role Scope Filters.

Change the database list on a scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

You can't change the list of databases on a scope. If you need to change the database list, you need to do the following:

1. If needed, retrieve the current database list in the scope to be replaced by using the "View a specific scope" procedure in the View Role Scopes topic.
2. Create a scope with the new database list by using the "Step 1: Create a custom scope" procedure in the Create a Regular or Exclusive Scope topic.
3. Change all the management role assignments that use the old scope to use the new scope by using the "Use the Shell to change the database filter or list-based scope on a role assignment" procedure in the Change a Role Assignment topic.
4. Remove the old scope by using the procedure in the Remove a Role Scope topic.

1.3.3.5.2.3 View Role Scopes

View Role Scopes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role scopes determine what objects are made available to a user so that the objects can be changed using the cmdlets and parameters assigned to them. You can view scopes to determine what scopes have been added to your organization, the configuration of a specific scope, or what scopes are orphans.

For more information about management role scopes in Microsoft Exchange Server 2010, see Understanding Management Role Scopes.

You must use the Shell to view scopes; you can't use the EMC to view role scopes.

Looking for other management tasks related to role scopes? Check out Managing Advanced Permissions.

Prerequisites

This topic makes use of pipelining and the **Format-List** cmdlet. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output

View a specific scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

You can view the details of a scope by piping the output of the **Get-ManagementScope** cmdlet to the **Format-List** cmdlet.

To view the details of a specific scope, use the following syntax.

```
Get-ManagementScope <scope name> | Format-List
```

This example retrieves the details of the Seattle Servers scope.

```
Get-ManagementScope "Seattle Servers" | Format-List
```

For detailed syntax and parameter information, see Get-ManagementScope.

List all scopes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

This example retrieves a list of scopes in your organization.

```
Get-ManagementScope
```

This cmdlet retrieves both exclusive and regular scopes. If you only want to return exclusive scopes or regular scopes, see "List all exclusive or regular scopes only" later in this topic.

For detailed syntax and parameter information, see Get-ManagementScope.

List all orphaned scopes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

Orphaned scopes are scopes that haven't been associated with any management role assignments.

This examples retrieves a list of orphaned scopes.

```
Get-ManagementScope -Orphan
```

For detailed syntax and parameter information, see Get-ManagementScope.

List all exclusive or regular scopes only

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

By default, the **Get-ManagementScope** cmdlet returns a list of scopes that contains both

exclusive and regular scopes. If you want to return only exclusive scopes or only regular scopes use the following syntax.

```
Get-ManagementScope -Exclusive < $true | $false >
```

This example returns only exclusive scopes.

```
Get-ManagementScope -Exclusive $true
```

This example returns a list of regular scopes only.

```
Get-ManagementScope -Exclusive $false
```

For detailed syntax and parameter information, see Get-ManagementScope.

1.3.3.5.2.4 Remove a Role Scope

Remove a Role Scope

Managing Permissions > Managing Advanced Permissions > Management Role Scopes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Management role scopes determine what objects are made available to a user who can then change the objects using the cmdlets and parameters assigned to the user. If you're no longer using a scope, it can be removed. For more information about management role scopes in Microsoft Exchange Server 2010, see Understanding Management Role Scopes.

You must use the Shell to remove scopes.

Prerequisites

Before you can remove a scope, you must remove the scope from any management role assignments that might be using it. For more information about how to remove a scope from a role assignment, see Change a Role Assignment.

Use the Shell to remove a scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topics.

To remove a scope, use the following syntax:

```
Remove-ManagementScope <scope name>
```

For example, to remove the "Dublin Servers" scope, use the following command:

```
Remove-ManagementScope "Dublin Servers"
```

Control Automatic Mailbox Distribution Using Database Scopes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Automatic mailbox distribution is a feature in Microsoft Exchange Server 2010 that randomly selects a mailbox database to store a new or moved mailbox when you don't specify a database explicitly. This feature can be helpful when you want to allow junior administrators or help desk staff to create mailboxes without needing to know which mailbox databases mailboxes should be created on.

You can use database management scopes to control which mailbox databases can be selected by automatic mailbox distribution. When you apply database scopes to an administrator, only the databases that match the defined database scope are available to the administrator. Because automatic mailbox distribution uses the context of the current user, it's also constrained by the database scopes applied to the administrator.

For more information about automatic mailbox distribution, database scopes, and role assignments, see the following topics:

- Understanding Automatic Mailbox Distribution
- Understanding Management Role Scopes
- Understanding Management Role Assignments

Looking for other management tasks related to scopes? Check out Managing Advanced Permissions.

Step 1: Create a database scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management scopes" entry in the Role Management Permissions topic.

Note:

You can't use the EMC to create a database scope.

In this step, decide which databases you want to include in the database scope. Also, decide whether you want to specify a static list of databases, or whether you want to create a database filter that includes only the databases that match the criteria you specify.

Important:

Role assignments associated with database scopes are applied only to users who connect to servers running Exchange 2010 Service Pack 1 (SP1). If a user assigned a role assignment associated with a database scope connects to a release to manufacturing (RTM) version of Exchange 2010, the role assignment isn't applied to the user, and the user won't be granted any permissions provided by the role assignment.

Use a database list scope

Use a database list if you want to define a static list of mailbox databases that should be included in this scope. Use the following syntax to create a database list scope.

```
New-ManagementScope -Name <scope name> -DatabaseList <database 1>, <database 2...
```

This example creates a scope that applies only to the databases Database 1, Database 2, and Database 3.

```
New-ManagementScope -Name "Accounting databases" -DatabaseList "Database 1", "Dat
```

For detailed syntax and parameter information, see New-ManagementScope.

Use a database filter scope

Use a database filter if you want to create a dynamic database scope that includes only the databases that match the criteria you specify. This can be useful if you don't want to manage the database scope after it's created and you've defined standard values for your organization that can identify specific sets of mailbox databases.

For a list of filterable database properties, see Understanding Management Role Scope Filters.

Use the following syntax to create a database filter scope.

```
New-ManagementScope -Name <scope name> -DatabaseRestrictionFilter <filter query>
```

This example creates a scope that includes all the databases that contain the string "ACCT" in the **Name** property of the database.

```
New-ManagementScope -Name "Accounting Databases" -DatabaseRestrictionFilter { Nam
```

For detailed syntax and parameter information, see New-ManagementScope.

Step 2: Add the database scope to a management role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

Note:

You can't use the EMC to add the database scope to a management role assignment.

After you create the scope, you must add it to a new or existing management role assignment. We recommend that you use management role groups to control administrative permissions, so the examples in this step use an example role group called Accounting Administrators. For more information about how to create a role group, see Create a Role Group.

After you assign the role to a role group with the database scope, the members of the role group will only be able to create mailboxes on, and move mailboxes to, the databases included in the scope.

For a list of built-in roles that you can assign to role groups, see Built-in Management Roles.

Add a new role assignment

Use this procedure if you've just created a role group and you need to add roles to it.

Use the following syntax to create a role assignment between the management role you want to assign and the new role group, with the new database scope.

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role name> -
```

This example creates a role assignment between the Mail Recipients and Mail Recipient Creation roles and the Accounting Administrators role group, using the Accounting Databases database scope.

```
New-ManagementRoleAssignment -SecurityGroup "Accounting Administrators" -Role "Ma
New-ManagementRoleAssignment -SecurityGroup "Accounting Administrators" -Role "Ma
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Modify an existing role assignment

Use this procedure if you have an existing role group that already has role assignments between it and the roles you want to apply the new database scope to.

This procedure uses pipelining. For more information, see Pipelining.

Use the following syntax to modify a role assignment between the management role that you want to apply the database scope to, and an existing role group.

```
Get-ManagementRoleAssignment -RoleAssignee <role group name> -Role <role name> |
```

This example adds the Accounting Databases database scope to the Mail Recipients and Mail Recipient Creation roles assigned to the Accounting Administrators role group.

```
Get-ManagementRoleAssignment -RoleAssignee "Accounting Administrators" -Role "Mai
Get-ManagementRoleAssignment -RoleAssignee "Accounting Administrators" -Role "Mai
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment or Set-ManagementRoleAssignment.

Step 3: Add members to a role group (if applicable)

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

Note:

You can't use the EMC to add members to a role group.

If you want to add members to a role group, see Add Members to a Role Group.

Important:

If you add members to this role group to restrict what databases they can create users on, or move mailboxes to, make sure they aren't members of other role groups that could grant extra permissions.

Step 4: Remove members from a role group (if applicable)

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

Note:

You can't use the EMC to remove members from a role group.

If you've added members to a new role group that restricts what databases they can create mailbox on, or move mailboxes to, and they're members of another role group that has additional permissions, remove them from the old role group. For more information, see Remove Members from a Role Group.

1.3.3.5.3 Management Role Assignments

Management Role Assignments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-06-09*

The following procedures enable you to perform advanced permissions management. You should only use these procedures if management role groups and management role assignment policies don't meet the needs of your organization.

Add a Role to a User or USG

Change a Role Assignment

View Role Assignments

Remove a Role from a User or USG

Delegate Role Assignments

For more information about managing role groups and role assignment policies, see the following topics:

Managing Administrator and Specialist Users

Managing End Users

1.3.3.5.3.1 Add a Role to a User or USG

Add a Role to a User or USG

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role assignments can assign a management role to a user or universal security group (USG). By assigning a role to a user or USG, you enable those users to perform tasks dependent on cmdlets or scripts and their parameters defined on the management role.

Although you can assign roles directly to users and USGs, the recommended method of granting permissions to administrators and end users is to use management role groups and management role assignment policies. When you use role groups and assignment policies, you simplify your permissions model.

If you want to assign roles to a management role group or a management role assignment policy, see the following topics:

- Add a Role to a Role Group
- Add a Role to an Assignment Policy

If you want to add members to a role group or assign a role assignment policy to an end user, see the following topics:

- Add Members to a Role Group
- Change the Assignment Policy on a Mailbox

For more information, see Understanding Role Based Access Control.

Note:
Role assignments are additive. This means that all the roles are added together when they are evaluated. If two roles are assigned to a user and one role contains a cmdlet but the other doesn't, the cmdlet will still be available to the user.
By default, role assignments don't grant the ability to assign roles to other users. To enable a user to assign roles to other users or USGs, see Delegate Role Assignments.

You must use the Shell to add a role assignment.

If you create an assignment with a scope, the scope overrides the role's implicit write scope. However, the role's implicit read scope still applies. The new scope can't return objects outside of the role's implicit read scope. For more information, see Understanding Management Role Scopes.

All the procedures in this topic use the *SecurityGroup* parameter to assign roles to a USG. If you want to assign the role to a specific user, use the *User* parameter instead of the *SecurityGroup* parameter. All other syntax for each command is the same.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Create a role assignment with no scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a role assignment with no scope.

You can create a role assignment with no scope. When you do this, the implicit read and implicit write scopes of the role apply.

Use the following syntax to assign a role to a USG without any scope.

```
New-ManagementRoleAssignment -Name <assignment name> -SecurityGroup <USG> -Role <
```

This example assigns the Exchange Servers role to the SeattleAdmins USG.

```
New-ManagementRoleAssignment -Name "Exchange Servers_SeattleAdmins" -SecurityGrou
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Create a role assignment with a predefined relative scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a role assignment with a predefined relative scope.

If a predefined relative scope meets your business requirements, you can apply that scope to the role assignment rather than create a custom scope. For a list of predefined scopes and their descriptions, see Understanding Management Role Scopes.

Use the following syntax to assign a role to a USG with a predefined scope.

```
New-ManagementRoleAssignment -Name <assignment name> -SecurityGroup < USG> -Role
```

This example assigns the Exchange Servers role to the SeattleAdmins USG and applies the Organization predefined scope.

```
New-ManagementRoleAssignment -Name "Exchange Servers_SeattleAdmins" -SecurityGrou
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Create a role assignment with a recipient filter-based scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a role assignment with a recipient filter-based scope.

If you created a recipient filter-based scope and want to use it with a role assignment, you need to include the scope in the command used to assign the role to a USG by using the *CustomRecipientWriteScope* parameter. If you use the *CustomRecipientWriteScope* parameter, you can't use the *RecipientOrganizationalUnitScope* parameter.

Before you can add a scope to a role assignment, you need to create one. For more information, see Create a Regular or Exclusive Scope.

Use the following syntax to assign a role to a USG with a recipient filter-based scope.

```
New-ManagementRoleAssignment -Name <assignment name> -SecurityGroup < USG> -Role
```

This example assigns the Mail Recipients role to the Seattle Recipient Admins USG and applies the Seattle Recipients scope.

```
New-ManagementRoleAssignment -Name "Mail Recipients_Seattle Recipient Admins" -Se
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Create a role assignment with a server or database filter or list-based configuration scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a role assignment with a server or database filter or list-based configuration scope.

If you created a server or database filter or list-based configuration scope and want to use it with a role assignment, you need to include the scope in the command used to assign the role to a USG by using the *CustomConfigWriteScope* parameter.

Before you can add a scope to a role assignment, you need to create one. For more information, see Create a Regular or Exclusive Scope.

Use the following syntax to assign a role to a USG with a configuration scope.

```
New-ManagementRoleAssignment -Name <assignment name> -SecurityGroup <USG> -Role <
```

This example assigns the Exchange Servers role to the MailboxAdmins USG and applies the Mailbox Servers scope.

```
New-ManagementRoleAssignment -Name "Exchange Servers_MailboxAdmins" -SecurityGrou
```

The preceding example shows you how to add a role assignment with a server configuration scope. The syntax to add a database configuration scope is the same. You specify the name of a database scope instead of a server scope.

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Create a role assignment with an OU scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a role assignment with an organization unit (OU) scope.

If you want to scope a role's write scope to an OU, you can specify the OU in the *RecipientOrganizationalUnitScope* parameter directly. If you use the *RecipientOrganizationalUnitScope* parameter, you can't use the *CustomRecipientWriteScope* parameter.

Use the following syntax to assign a role to a USG and restrict the write scope of a role to a specific OU.

```
New-ManagementRoleAssignment -Name <assignment name> -SecurityGroup <USG> -Role <
```

This example assigns the Mail Recipients role to the SalesRecipientAdmins USG and scopes the assignment to the sales/users OU in the contoso.com domain.

```
New-ManagementRoleAssignment -Name "Mail Recipients_SalesRecipientAdmins" -Securi
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Create a role assignment with an exclusive recipient or configuration scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a role assignment with an exclusive recipient or configuration scope.

To create an exclusive role assignment with an exclusive recipient or configuration scope, the same procedures provided in the Create a role assignment with a recipient filter-based scope and Create a role assignment with a server or database filter or list-based configuration scope sections can be used. The only difference is that when you create a role assignment with an exclusive scope, you must specify the following exclusive parameters depending on whether you're using an exclusive recipient scope or an exclusive configuration scope:

- **Exclusive recipient scopes** Use the *ExclusiveRecipientWriteScope* parameter instead of the *CustomRecipientWriteScope* parameter.
- **Exclusive configuration scopes** Use the *ExclusiveConfigWriteScope* parameter instead of the *CustomConfigWriteScope* parameter.

When you perform this procedure, the role assignees assigned the role can perform actions against the objects included in the exclusive scope. For more information about exclusive scopes, see Understanding Exclusive Scopes.

You can't create a role assignment with both exclusive and regular scopes.

This example assigns the Mail Recipients role to the Protected User Admins USG and applies the Protected Users exclusive scope.

```
New-ManagementRoleAssignment -Name "Mail Recipients_Protected User Admins" -Secur
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

1.3.3.5.3.2 Change a Role Assignment

Change a Role Assignment

Managing Permissions > Managing Advanced Permissions > Management Role Assignments >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role assignments assign a management role to a role assignee. By changing the role assignment, you can control what objects role assignees assigned a role can change. Management role scopes applied to role assignments override the role's implicit write scope. However, the role's implicit read scope still applies. Scopes that you apply can't return objects outside of the role's implicit read scope.

For more information about management role scopes and assignments in Microsoft Exchange Server 2010, see the following topics:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

You must use the Shell to change role assignments. Looking for other management tasks related to role assignments? Check out Managing Advanced Permissions.

Use the Shell to enable or disable a role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to enable or disable a role assignment.

Role assignments are enabled by default, meaning that the associated role is applied to the role assignee to which the role is assigned. If a role assignment is disabled, the associated role isn't applied to the role assignee.

To enable a role assignment, use the following syntax.

```
Set-ManagementRoleAssignment <role assignment> -Enabled $true
```

To disable a role assignment, use the following syntax.

```
Set-ManagementRoleAssignment <role assignment> -Enabled $false
```

This example disables the Help Desk Assignment role assignment.

```
Set-ManagementRoleAssignment "Help Desk Assignment" -Enabled $false
```

For detailed syntax and parameter information, see Set-ManagementRoleAssignment.

Use the Shell to change a management role or role assignee on a role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change a management role or role assignee on a role assignment.

You can't change the management role or role assignee specified on a role assignment. If you want a role assignment to be associated with another role or role assignee, you must create a new role assignment, and then delete the old role assignment. For more information about how to add and remove role assignments, see the following topics:

- Add a Role to a User or USG
- Remove a Role from a User or USG

If you've created assignments directly to a user or universal security group (USG), we recommend that you consider using management role groups and management role assignment policies. Role groups and assignment policies enable you to simplify your permissions model and reduce the number of role assignments you need to manage. For more information, see Understanding Role Based Access Control.

Use the Shell to change a predefined

relative scope on a role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change a predefined relative scope on a role assignment.

You can change or add a predefined relative scope on a role assignment. If you add or change a predefined scope, any previously specified recipient scopes are removed from the role assignment. For a list of predefined scopes and their descriptions, see Understanding Management Role Scopes.

To change or add a predefined scope on a role assignment, use the following syntax.

```
Set-ManagementRoleAssignment <assignment name> -RecipientRelativeWriteScope < MyD
```

This example changes the predefined scope on the John's Assignment role assignment to MyDistributionGroups.

```
Set-ManagementRoleAssignment "John's Assignment" - RecipientRelativeWriteScope My
```

For detailed syntax and parameter information, see Set-ManagementRoleAssignment.

Use the Shell to change a recipient filter scope on a role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change a recipient filter scope on a role assignment.

You can either specify a new recipient filter-based scope or change the recipient filter-based scope that's already applied to the role assignment. If you add a recipient filter scope, any previously defined recipient scopes are removed from the role assignment.

To specify a new recipient filter-based scope or replace an existing one, use the following syntax.

```
Set-ManagementRoleAssignment <assignment name> -CustomRecipientWriteScope <role s
```

This example adds or changes the recipient filter-based scope to Redmond Recipients.

```
Set-ManagementRoleAssignment "Redmond Recipient Administrators Assignment" -Custo
```

If you want to keep the same recipient filter-based scope that's applied to the role assignment but change the recipient filter used to match recipient objects, you need to change the recipient filter on the scope itself. For more information about how to change scopes, see Change a Role Scope.

For detailed syntax and parameter information, see Set-ManagementRoleAssignment.

Use the Shell to change the server filter or

list-based configuration scope on a role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change the server filter or list-based configuration scope on a role assignment.

You can either specify a new server filter or list-based configuration scope, or change the scope that's already applied to the role assignment. If you add or change the configuration scope, any previously specified configuration scopes are removed from the role assignment.

To specify a new configuration scope or replace an existing one, use the following syntax.

```
Set-ManagementRoleAssignment <assignment name> -CustomConfigWriteScope <role scop
```

This example adds or changes the configuration scope to Redmond Servers.

```
Set-ManagementRoleAssignment "Redmond Administrators Assignment" -CustomConfigWri
```

If you want to keep the same configuration scope that's applied to the role assignment but change the server filter or server list on the scope, you need to change the configuration scope itself. For more information about how to change scopes, see Change a Role Scope.

For detailed syntax and parameter information, see Set-ManagementRoleAssignment.

Use the Shell to change the database filter or list-based configuration scope on a role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change the database filter or list-based configuration scope on a role assignment.

You can either specify a new database filter or list-based configuration scope, or change the scope that's already applied to the role assignment. If you add or change the configuration scope, any previously specified configuration scopes are removed from the role assignment.

To specify a new configuration scope or replace an existing one, use the following syntax.

```
Set-ManagementRoleAssignment <assignment name> -CustomConfigWriteScope <role scop
```

This example adds or changes the configuration scope to Redmond Databases.

```
Set-ManagementRoleAssignment "Redmond Database Admins" -CustomConfigWriteScope "R
```

If you want to keep the same configuration scope that's applied to the role assignment but change the database filter or database list on the scope, you need to change the configuration scope itself. For more information about how to change scopes, see Change a Role Scope.

For detailed syntax and parameter information, see Set-ManagementRoleAssignment.

Use the Shell to change the organizational unit on a role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change the organizational unit (OU) on a role assignment.

You can either add a new OU or change an OU that's already applied to the role assignment. If you specify a new OU, any previously specified recipient scopes are removed from the role assignment.

To change or add a new OU on a role assignment, use the following syntax.

```
Set-ManagementRoleAssignment <assignment name> -RecipientOrganizationalUnitScope
```

This example adds the Engineering\Users OU in the contoso.com domain to the Engineering Help Desk role assignment.

```
Set-ManagementRoleAssignment "Engineering Help Desk" -RecipientOrganizationalUnit
```

For detailed syntax and parameter information, see Set-ManagementRoleAssignment.

Use the Shell to change an exclusive recipient or configuration scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to change an exclusive recipient or configuration scope.

To change exclusive recipient or exclusive configuration scopes, you can use the procedures provided in the "Use the Shell to change a recipient filter scope on a role assignment," "Use the Shell to change the server filter or list-based configuration scope on a role assignment," and "Use the Shell to change the database filter or list-based configuration scope on a role assignment" sections earlier in this topic. The only difference is that when you change an exclusive scope, you must specify the following exclusive parameters depending on whether you're changing an exclusive recipient scope or an exclusive configuration scope:

- **Exclusive recipient scopes** Use the *ExclusiveRecipientWriteScope* parameter instead of the *CustomRecipientWriteScope* parameter.
- **Exclusive server and database configuration scopes** Use the *ExclusiveConfigWriteScope* parameter instead of the *CustomConfigWriteScope* parameter.

As with regular recipient and configuration scopes, if you add or change an exclusive scope, any previously defined recipient or configuration scopes are replaced.

This example changes an exclusive recipient write scope.

```
Set-ManagementRoleAssignment "Exclusive Executive Users" -ExclusiveRecipientWrite
```

For detailed syntax and parameter information, see Set-ManagementRoleAssignment.

1.3.3.5.3.3 View Role Assignments

View Role Assignments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Management role assignments assign a management role to a role assignee. For more information about management role assignments in Microsoft Exchange Server 2010, see Understanding Management Role Assignments.

You must use the Shell to view role assignments.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Prerequisites

This topic makes use of pipelining and the **Format-List** cmdlet. For more information about these concepts, see the following topics:

- Pipelining
- Working with Command Output

Note:
You can't use the EMC to view role assignments.

View a list of all role assignments

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

You can view a list of all role assignments configured in your organization by running the **Get-ManagementRoleAssignment** cmdlet. If you want to retrieve a list of role assignments that match a partial string that you specify, use wildcard characters (*). This example retrieves a list of all the role assignments that start with the string "Tier 1".

```
Get-ManagementRoleAssignment "Tier 1*"
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View the details of a specific role

assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

You can view the details of a role assignment by piping the results of the **Get-ManagementRoleAssignment** cmdlet to the **Format-List** cmdlet. Use the following syntax.

```
Get-ManagementRoleAssignment <assignment name> | Format-List
```

This example retrieves the details of the Help Desk Assignment role assignment.

```
Get-ManagementRoleAssignment "Help Desk Assignment" | Format-List
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View the list of role assignments assigned to a specific role assignee

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

To view a list of role assignments associated with a management role group, role, or role assignment policy, or associated with a user or universal security group (USG), use the following syntax.

```
Get-ManagementRoleAssignment -RoleAssignee <role assignee name>
```

This example retrieves all of the role assignments associated with the Server Management role group.

```
Get-ManagementRoleAssignment -RoleAssignee "Server Management"
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View the role assignments associated with a specific role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

Each role can have multiple role assignments. You can use the **Get-ManagementRoleAssigment** cmdlet to view a list of role assignments associated with a specified role.

To view a list of role assignments associated with a specified role, use the following syntax.

```
Get-ManagementRoleAssignment -Role <role name>
```

This example retrieves all of the role assignments associated with the Mail Recipients role.

```
Get-ManagementRoleAssignment -Role "Mail Recipients"
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View a list of role assignments that use a specific predefined scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

To view a list of role assignments that use a specific predefined scope, use the following syntax.

```
Get-ManagementRoleAssignment -RecipientWriteScope < MyGAL | MyDistributionGroups
```

This example retrieves all of the role assignments that use the Organization predefined scope.

```
Get-ManagementRoleAssignment -RecipientWriteScope Organization
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View a list of role assignments that have been scoped to a specific OU

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

To view a list of role assignments that have been scoped to a specific organizational unit (OU), use the following syntax.

```
Get-ManagementRoleAssignment -RecipientOrganizationalUnitScope <OU>
```

This example retrieves all of the role assignments that have been scoped to the North America\Engineering\Users OU in the contoso.com domain.

```
Get-ManagementRoleAssignment -RecipientOrganizationalUnitScope "contoso.com/North
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View a list of assignments that use a specific custom scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

To view a list of role assignments that use a specific custom scope, you need to first determine whether the scope is a recipient scope, configuration scope, exclusive recipient scope, or exclusive configuration scope. Each type of scope uses a different parameter on the **Get-ManagementRoleAssignment** cmdlet. The following lists each scope and its associated parameter:

- **Recipient scopes** *CustomRecipientWriteScope*
- **Configuration scopes** *CustomConfigWriteScope*

- **Exclusive recipient scopes** *ExclusiveRecipientWriteScope*
- **Exclusive configuration scopes** *ExclusiveConfigWriteScope*

The syntax for each parameter is the same. Specify the name of the scope with the parameter that matches the type of scope it is.

This example retrieves all of the role assignments that use the Vancouver Recipients recipient scope.

```
Get-ManagementRoleAssignment -CustomRecipientWriteScope "Vancouver Recipients"
```

This example retrieves all of the role assignments that use the Seattle AD Site exclusive configuration scope.

```
Get-ManagementRoleAssignment -ExclusiveConfigWriteScope "Seattle AD Site"
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View a list of exclusive or regular scopes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

To view a list of exclusive or regular role assignments, use the following syntax.

```
Get-ManagementRoleAssignment -Exclusive < $True | $False >
```

For example, to view a list of exclusive scopes, run the following command:

```
Get-ManagementRoleAssignment -Exclusive $True
```

This example retrieves a list of regular scopes without any exclusive scopes.

```
Get-ManagementRoleAssignment -Exclusive $False
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View who can modify a specific recipient or server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

To view a list of role assignments that can modify a specific recipient or server, use the *WritableRecipient* and *WritableServer* parameters. Specify the name of the recipient with the *WritableRecipient* parameter, and the name of the server with the *WritableServer* parameter.

This example retrieves a list of role assignments that can modify the recipient Brian.

```
Get-ManagementRoleAssignment -WritableRecipient "Brian"
```

You can combine the *WritableRecipient* and *WritableServer* parameters with other parameters, such as the *RoleAssignee* parameter and the *GetEffectiveUsers* switch to refine your query and expand any role groups or USGs. This example retrieves all of the users who can modify the server EX02 and who are assigned the Server Management role group.

```
Get-ManagementRoleAssignment -WritableServer EX02 -RoleAssignee "Server Managemen
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View the users who receive permissions from an assignment via a role group or USG

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

To view a list of users that receive permissions from a role assignment, use the following syntax.

```
Get-ManagementRoleAssignment <assignment name> -GetEffectiveUsers
```

This example retrieves a list of users in the Help Desk Assignment role assigment.

```
Get-ManagementRoleAssignment "Help Desk Assignment" -GetEffectiveUsers
```

You can also combine the *GetEffectiveUsers* switch with several other parameters on the **Get-ManagementRoleAssignment** cmdlet to expand the role groups and USGs that the role assignments are assigned to. For an example of how the *GetEffectiveUsers* switch is used with other parameters, see "View who can modify a specific recipient or server" earlier in this topic.

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

View a list of role assignments that are enabled or disabled

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

To view a list of role assignments that are enabled or disabled, use the following syntax.

```
Get-ManagementRoleAssignment -Enabled < $True | $False >
```

This example retrieves a list of role assignments that are disabled.

```
Get-ManagementRoleAssignment -Enabled $False
```

For detailed syntax and parameter information, see Get-ManagementRoleAssignment.

1.3.3.5.3.4 Remove a Role from a User or USG

Remove a Role from a User or USG

Managing Permissions > Managing Advanced Permissions > Management Role Assignments >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Management role assignments assign a management role to a user or universal security group (USG). If you remove a role assignment, the users assigned the role will no longer have access to the cmdlets available on that role. For more information about management role assignments in Microsoft Exchange Server 2010, see Understanding Management Role Assignments.

You must use the Shell to remove role assignments.

Looking for other management tasks related to roles? Check out Managing Advanced Permissions.

Remove a management role assignment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role assignments" entry in the Role Management Permissions topic.

If you know the name of the role assignment you want to remove, use the following syntax:

```
Remove-ManagementRoleAssignment <assignment name>
```

For example, to remove the "Tier 2 Help Desk Assignment" role assignment, use the following command:

```
Remove-ManagementRoleAssignment "Tier 2 Help Desk Assignment"
```

If you don't know the name of the role assignment, you can use the following syntax:

```
Get-ManagementRoleAssignment -RoleAssignee <user or USG> -Role <role name> -Deleg
```

For example, if you want to remove the Mail Recipients regular role assignment from the user davids, use the following command:

```
Get-ManagementRoleAssignment -RoleAssignee davids -Role "Mail Recipients" -Delega
```


1.3.3.5.3.5 Delegate Role Assignments

Delegate Role Assignments

Managing Permissions > Managing Advanced Permissions > Management Role Assignments >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Management role delegation enables role assignees to assign a specified management role to other management role groups, management role assignment policies, users, or universal security groups (USG). By default, only members of the Organization Management management role group can delegate role assignments. When a new installation of Microsoft Exchange Server 2010 is deployed, only the user account that installed Exchange 2010 is a member of the Organization Management role group.

If you assign a delegating role assignment to a role group, any member of the role group can delegate the associated management role to other role assignees.

Important:

Delegating role assignments doesn't give the role assignee the permissions granted by the role, only the ability to assign the role to others. If you want to also give the permissions granted by the role to the role assignee, you must also create a regular role assignment. To create a regular role assignment, see the following topics:
Add a Role to a Role Group
Add a Role to an Assignment Policy
Add a Role to a User or USG

Note:
This topic discusses management role assignment delegation. If you want to delegate who can add members to or remove members from role groups, which is the recommended method of delegation, see Add or Remove a Role Group Delegate.

For more information about regular role assignments and delegating management role assignments, see Understanding Management Role Assignments.

Looking for other management tasks related to managing permissions? Check out Managing Advanced Permissions.

Use the Shell to delegate a management role

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Management roles" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to delegate a role assignment.

You can create delegating role assignments using the same predefined scopes, recipient filter or server-filter-based scopes, server list-based scopes, and organizational unit (OU) scopes that can be used to create regular or exclusive scopes. The only difference between creating a regular role assignment and a delegating role assignment is the addition of the *Delegating* switch to the command. For more information about how to create role assignments, see the following topics:

- Add a Role to a Role Group
- Add a Role to a User or USG

Note:
You can't create a delegating role assignment to a management role assignment policy.

This example creates a delegating role assignment to enable members of the Senior Admins role group to assign the Mail Recipients role to any role assignee in the Exchange organization.

```
New-ManagementRoleAssignment -Role "Mail Recipients" -SecurityGroup "Senior Admin
```

This example creates a delegating role assignment to enable members of the Senior Admins role group to assign the Mail Recipients role only to users in the Sales/Users OU in the contoso.com domain.

```
New-ManagementRoleAssignment -Role "Mail Recipients" -SecurityGroup "Senior Admin
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

1.3.3.5.4 Managing Split Permissions

Managing Split Permissions

Permissions > Managing Permissions > Managing Advanced Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-06-25*

The following procedures enable you to perform advanced permissions management. You should only use these procedures if management role groups and management role assignment policies don't meet the needs of your organization.

Configure Exchange 2010 for Split Permissions

Configure Exchange 2010 for Shared Permissions

For more information about managing role groups and role assignment policies, see the following topics:

Managing Administrator and Specialist Users

Managing End Users

1.3.3.5.4.1 Configure Exchange 2010 for Split Permissions

Configure Exchange 2010 for Split Permissions

Managing Permissions > Managing Advanced Permissions > Managing Split Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Split permissions enable two separate groups, such as Active Directory administrators and Microsoft Exchange Server 2010 administrators, to manage their respective services, objects, and attributes. Active Directory administrators manage security principals, such as users, that provide permissions to access an Active Directory forest. Exchange administrators manage the Exchange-related attributes on Active Directory objects and Exchange-specific object creation and management.

Microsoft Exchange Server 2010 Service Pack 1 (SP1) offers the following types of split permissions models:

- **RBAC split permissions** Permissions to create security principals in the Active Directory domain partition are controlled by Role Based Access Control (RBAC). Only those who are members of the appropriate role groups can create security principals.
- **Active Directory split permissions** Permissions to create security principals in the Active Directory domain partition are completely removed from any Exchange user, service, or server. No option is provided in RBAC to create security principals. Creation of security principals in Active Directory must be performed using Active Directory management tools.

Note:

Active Directory split permissions are available beginning with Exchange 2010 SP1.

The model that you choose depends on the structure and needs of your organization. Choose the procedure that follows that's applicable to the model you want to configure. We recommend that you use the RBAC split permissions model. The RBAC split permissions model provides significantly more flexibility while providing the same administration separation as Active Directory split permissions.

For more information about shared and split permissions, see Understanding Split Permissions.

For more information about management role groups, management roles, and regular and delegating management role assignments, see the following topics:

- Understanding Role Based Access Control
- Understanding Management Role Groups
- Understanding Management Roles
- Understanding Management Role Assignments

Looking for other management tasks related to permissions? Check out Managing Advanced Permissions.

Switch to RBAC split permissions

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Active Directory split permissions" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to switch to RBAC split permissions.

You can configure your Exchange 2010 organization for RBAC split permissions. When you are done, only Active Directory administrators will be able to create Active Directory security principals. This means that Exchange administrators won't be able to use the following cmdlets:

- **New-Mailbox**
- **New-MailContact**
- **New-MailUser**
- **New-RemoteMailbox**
- **Remove-Mailbox**
- **Remove-MailContact**
- **Remove-MailUser**
- **Remove-RemoteMailbox**

Exchange administrators will only be able to manage the Exchange attributes on existing Active Directory security principals. However, They will be able to create and manage Exchange-specific objects, such as transport rules and distribution groups. For more information, see the "RBAC Split Permissions" section in Understanding Split Permissions.

To configure Exchange 2010 for split permissions, you must assign the Mail Recipient Creation role and the Security Group Creation and Membership role to a role group that contains members that are Active Directory administrators. You must then remove the assignments between those roles and any role group or universal security group (USG) that contains Exchange administrators.

To configure RBAC split permissions, do the following:

1. If your organization is currently configured for Active Directory split permissions, do the following from a Windows command shell prompt:
   1.a. Disable Active Directory split permissions by running the following command from the Exchange 2010 SP1 installation media.

```
setup.com /PrepareAD /ActiveDirectorySplitPermissions:false
```

1.b.Restart the Exchange 2010 servers in your organization or wait for the Active Directory access token to replicate to all of your Exchange 2010 servers.

2. Do the following from the Exchange Management Shell:

2.a.Create a role group for the Active Directory administrators. In addition to creating the role group, the command creates regular role assignments between the new role group and the Mail Recipient Creation role and the Security Group Creation and Membership role.

```
New-RoleGroup "Active Directory Administrators" -Roles "Mai
```

Note:

If you want members of this role group to be able to create role assignments, include the Role Management role. You don't have to add this role now. However, if you ever want to assign either the Mail Recipient Creation role or Security Group Creation and Membership role to other role assignees, the Role Management role must be assigned to this new role group. The steps that follow configure the Active Directory Administrators role group as the only role group that can delegate these roles.

2.b.Create delegating role assignments between the new role group and the Mail Recipient Creation role and Security Group Creation and Membership role using the following commands.

```
New-ManagementRoleAssignment -Role "Mail Recipient Creation
New-ManagementRoleAssignment -Role "Security Group Creation
```

2.c.Add members to the new role group using the following command.

```
Add-RoleGroupMember "Active Directory Administrators" -Memb
```

2.d.Replace the delegate list on the new role group so that only members of the role group can add or remove members.

```
Set-RoleGroup "Active Directory Administrators" -ManagedBy
```

Important:

Members of the Organization Management role group, or those who are assigned the Role Management role, either directly or through another role group or USG, can bypass this delegate security check. If you want to prevent any Exchange administrator from adding himself or herself to the new role group, you must remove the role assignment between the Role Management role and any Exchange administrator and assign it to another role group.

2.e.Find all of the regular and delegating role assignments to the Mail Recipient Creation role using the following command. The command displays only the **Name**, **Role**, and **RoleAssigneeName** properties.

```
Get-ManagementRoleAssignment -Role "Mail Recipient Creation
```

2.f.Remove all of the regular and delegating role assignments to the Mail Recipient Creation role that aren't associated with the new role group or any other role groups, USGs, or direct assignments you want to keep using the following command.

```
Remove-ManagementRoleAssignment <Mail Recipient Creation rc
```

Note:
If you want to remove all of the regular and delegating role assignments to the Mail Recipient Creation role on any role assignee other than the Active Directory Administrators role group, use the following command. The *WhatIf* switch lets you see what role assignments will be removed. Remove the *WhatIf* switch and run the command again to remove the role assignments.

```
Get-ManagementRoleAssignment -Role "Mail Recipient Creation
```

2.g.Find all of the regular and delegating role assignments to the Security Group Creation and Membership role using the following command. The command displays only the **Name**, **Role**, and **RoleAssigneeName** properties.

```
Get-ManagementRoleAssignment -Role "Security Group Creation
```

2.h.Remove all of the regular and delegating role assignments to the Security Group Creation and Membership role that aren't associated with the new role group or any other role groups, USGs, or direct assignments you want to keep using the following command.

```
Remove-ManagementRoleAssignment <Security Group Creation ar
```

Note:
You can use the same command in the preceding Note to remove all of the regular and delegating role assignments to the Security Group Creation and Membership role on any role assignee other than the Active Directory Administrators role group, as shown in this example.

```
Get-ManagementRoleAssignment -Role "Security Group Creation
```

For detailed syntax and parameter information, see the following topics:

- New-RoleGroup
- New-ManagementRoleAssignment
- Add-RoleGroupMember
- Set-RoleGroup
- Get-ManagementRoleAssignment
- Remove-ManagementRoleAssignment

Switch to Active Directory split permissions

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Active Directory split permissions" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to switch to Active Directory split permissions.

You can configure your Exchange 2010 organization for Active Directory split permissions.

Active Directory split permissions completely remove the permissions that allow Exchange administrators and servers from creating security principals in Active Directory or modifying non-Exchange attributes on those objects. When you are done, only Active Directory administrators will be able to create Active Directory security principals. This means that Exchange administrators won't be able to use the following cmdlets:

- **Add-DistributionGroupMember**
- **New-DistributionGroup**
- **New-Mailbox**
- **New-MailContact**
- **New-MailUser**
- **New-RemoteMailbox**
- **Remove-DistributionGroup**
- **Remove-DistributionGroupMember**
- **Remove-Mailbox**
- **Remove-MailContact**
- **Remove-MailUser**
- **Remove-RemoteMailbox**
- **Update-DistributionGroupMember**

Exchange administrators and servers will only be able to manage the Exchange attributes on existing Active Directory security principals. They will, however, be able to create and manage Exchange-specific objects, such as transport rules and Unified Messaging dial plans.

Caution:

After you enable Active Directory split permissions, Exchange administrators and servers will no longer be able to create security principals in Active Directory, and they won't be able to manage distribution group membership. These tasks must be performed using Active Directory management tools with the required Active Directory permissions. Before you make this change, you should understand the impact it will have on your administration processes and third-party applications that integrate with Exchange 2010 and the RBAC permissions model.
For more information, see the "Active Directory Split Permissions" section in Understanding Split Permissions.

To switch from shared or RBAC split permissions to Active Directory split permissions, do the following:

1. From a Windows command shell, run the following command from the Exchange 2010 SP1 installation media to enable Active Directory split permissions.

```
setup.com /PrepareAD /ActiveDirectorySplitPermissions:true
```

2. Restart the Exchange 2010 servers in your organization or wait for the Active Directory access token to replicate to all of you Exchange 2010 servers.

1.3.3.5.4.2 Configure Exchange 2010 for Shared Permissions

Configure Exchange 2010 for Shared Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Shared permissions enable you, as an administrator of Microsoft Exchange Server 2010, to create Active Directory security principals, such as users, and then configure them as Exchange recipients. Unlike split permissions, which separate management tasks between groups of Exchange administrators and Active Directory administrators, there's no separation of tasks with shared permissions.

For more information about shared and split permissions, see Understanding Split Permissions.

You can configure your Exchange 2010 organization for shared permissions if you've previously set your organization for split permissions. The procedure to switch to shared permissions is different depending on whether you're currently using Role Based Access Control (RBAC) split permissions or Active Directory split permissions. Choose the procedure that follows that's applicable to your current configuration. If the following are true, your organization is using Active Directory split permissions:

- The Microsoft Exchange Protected Groups organizational unit (OU) exists.
- The Exchange Windows Permissions security group is located in the Microsoft Exchange Protected Groups OU.
- The Exchange Trusted Subsystem security group is a member of the Exchange Windows Permissions security group.
- There are no regular management role assignments to the Mail Recipient Creation role or Security Group Creation and Membership role.

If you've never configured your organization for split permissions, you don't need to perform this procedure. Exchange 2010 is configured for shared permissions by default.

For more information about management role groups, management roles, and regular and delegating management role assignments, see the following topics:

- Understanding Role Based Access Control
- Understanding Management Role Groups
- Understanding Management Roles
- Understanding Management Role Assignments

Looking for other management tasks related to permissions? Check out Managing Advanced Permissions.

Prerequisites

- The Exchange 2010 organization must currently be configured for RBAC or Active Directory split permissions.
- You must have permissions to delegate the Mail Recipient Creation management role and the Security Group Creation and Membership management role to the Organization Management management role group or another role group that's assigned the Mail Recipients role.

Switch from RBAC split permissions to shared permissions

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:

You can't use the EMC to switch from RBAC split permissions to shared permissions.

To switch from RBAC split permissions to Exchange 2010 shared permissions, you must assign the Mail Recipient Creation role and the Security Group Creation and Membership

role to a role group that's also assigned the Mail Recipients role and has Exchange 2010 administrators as members. In the default shared permissions configuration, the Organization Management role group contains each of these roles. Because of this, the Organization Management role group is in this procedure.

Configure shared permissions

To configure shared permissions on the Organization Management role group, do the following using an account that has permissions to delegate role assignments for the Mail Recipient Creation role and the Security Group Creation and Membership role:

1. Add delegating role assignments for the Mail Recipient Creation role and Security Group Creation and Membership role to the Organization Management role group using the following commands.

```
New-ManagementRoleAssignment -Role "Mail Recipient Creation" -Security
New-ManagementRoleAssignment -Role "Security Group Creation and Member
```

Note:

The role group (in this procedure, the Active Directory Administrators role group) that has delegating role assignments for the Mail Recipient Creation role and Security Group Creation and Membership role must be assigned the Role Management role to run the **New-ManagementRoleAssignment** cmdlet. The role assignee that can delegate the Role Management role must assign that role to the Active Directory Administrators role group.

2. Add regular role assignments for the Mail Recipient Creation role to the Organization Management and Recipient Management role groups using the following commands.

```
New-ManagementRoleAssignment -Role "Mail Recipient Creation" -Security
New-ManagementRoleAssignment -Role "Security Group Creation and Member
```

3. Add a regular role assignment for the Security Group Creation and Membership role to the Organization Management role group using the following command.

```
New-ManagementRoleAssignment -Role "Security Group Creation and Member
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Remove permissions from Active Directory administrators (Optional)

You can optionally remove the permissions granted to Active Directory administrators if you no longer want them to be able to create or manage Active Directory objects using the Exchange management tools. If you want to remove permissions from Active Directory administrators, perform this procedure.

Note:

Although you can remove permissions for Active Directory administrators to manage Active Directory objects using the Exchange management tools, Active Directory administrators can continue to manage Active Directory objects using Active Directory management tools, if their Active Directory permissions allow it. They won't, however, be able to manage Exchange-specific attributes on Active Directory objects. For more information, see Understanding Split Permissions.

To remove Exchange-related split permissions from Active Directory administrators, do the following:

1. Remove the regular and delegating role assignments that assign the Mail Recipient Creation role to the role group or universal security group (USG) that contains the Active Directory administrators as members using the following command. This command uses the Active Directory Administrators role group as an example. The *WhatIf* switch lets you see what role assignments will be removed. Remove the *WhatIf* switch, and run the

command again to remove the role assignments.

```
Get-ManagementRoleAssignment -Role "Mail Recipient Creation" | Where {
```

2. Remove the regular and delegating role assignments that assign the Security Group Creation and Membership role to the role group or USG that contains the Active Directory administrators as members using the following command. This command uses the Active Directory Administrators role group as an example. The *WhatIf* switch lets you see what role assignments will be removed. Remove the *WhatIf* switch, and run the command again to remove the role assignments.

```
Get-ManagementRoleAssignment -Role "Security Group Creation and Member
```

3. Optional. If you want to remove all Exchange permissions from the Active Directory administrators, you can remove the role group or USG in which they're members. For more information about how to remove a role group, see Remove a Role Group.

For detailed syntax and parameter information, see Get-ManagementRoleAssignment or Remove-ManagementRoleAssignment.

Switch from Active Directory split permissions to shared permissions

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Active Directory split permissions" entry in the Role Management Permissions topic.

Note:

You can't use the EMC to switch from Active Directory split permissions to shared permissions.

To switch from Active Directory split permissions to Exchange 2010 shared permissions, you must rerun Exchange Setup to disable Active Directory split permissions in the Exchange organization, and then create role assignments between a role group and the Mail Recipient Creation role and Security Group Creation and Membership role. In the default shared permissions configuration, the Organization Management role group contains each of these roles. Because of this, the Organization Management role group is in this procedure.

Important:

The setup.com command in this procedure makes changes to Active Directory. You must use an account that has the permissions required to make these changes. This account might not be the same account that has permissions to create role assignments using the **New-ManagementRoleAssignment** cmdlet. Use the account, or accounts, with the permissions necessary to successfully complete each step in this procedure.

To switch from Active Directory split permissions to shared permissions, do the following:

1. From a Windows command shell, run the following command from the Exchange 2010 SP1 installation media to disable Active Directory split permissions.

```
setup.com /PrepareAD /ActiveDirectorySplitPermissions:false
```

2. From the Exchange Management Shell, run the following commands to add regular role assignments between the Mail Recipient Creation role and Security Group Creation and Management role and the Organization Management and Recipient Management role groups.

```
New-ManagementRoleAssignment "Mail Recipient Creation_Organization Man
New-ManagementRoleAssignment "Security Group Creation and Membership_O
New-ManagementRoleAssignment "Mail Recipient Creation_Recipient Manage
```

3.Restart the Exchange 2010 servers in your organization.

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

1.4 Exchange Management Console

Exchange Management Console

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

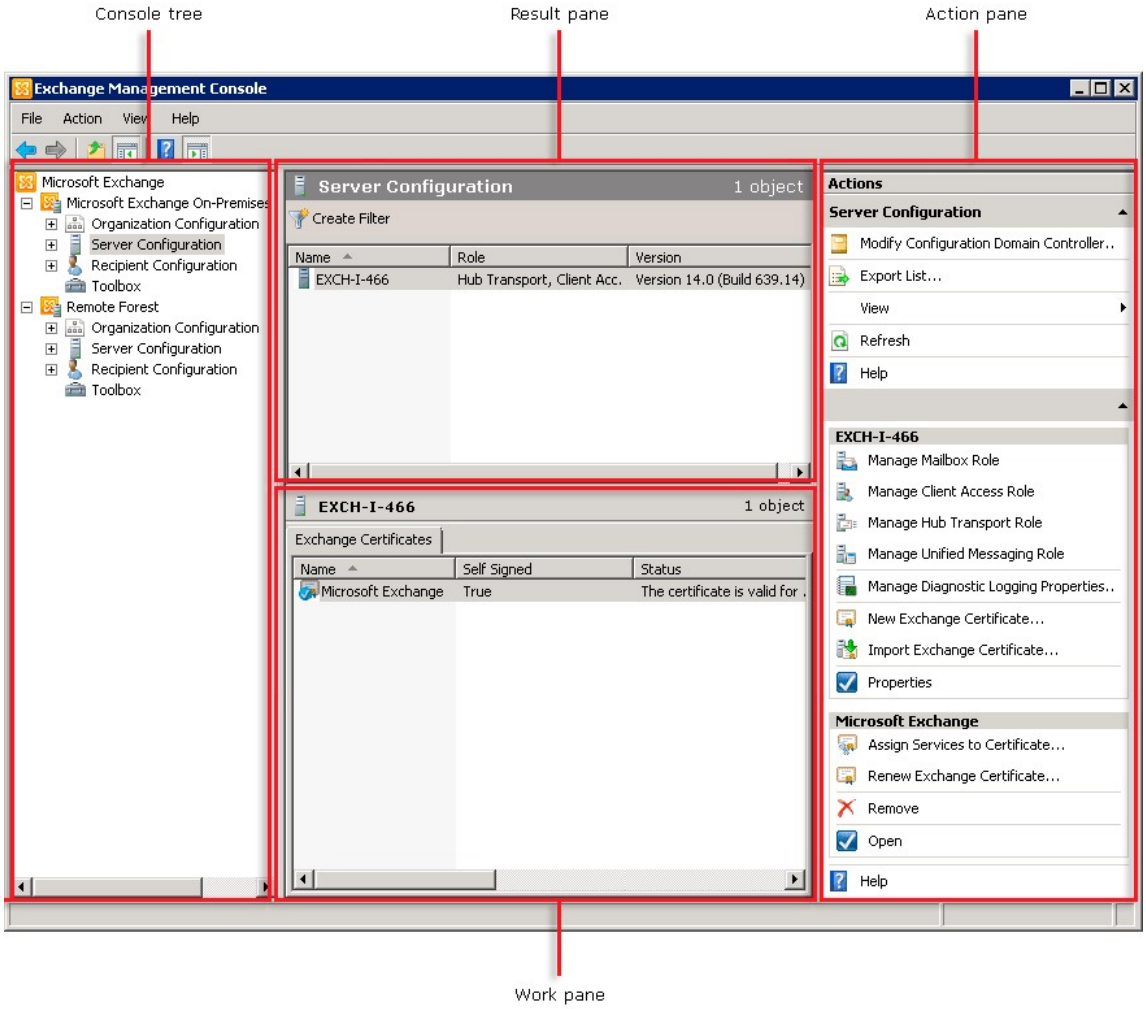
Topic Last Modified: *2011-04-28*

The Exchange Management Console (EMC) is a Microsoft Management Console (MMC) 3.0-based tool that provides Exchange administrators with a graphical user interface (GUI) to manage the configuration of Exchange organizations. You can also add the EMC snap-in to custom MMC-based tools.

For more information about improvements to the EMC, see New Administrative Functionality in the Exchange Management Console.

Common User Interface Elements in the Exchange Management Console

This section describes the user interface elements that are common across the EMC.



Console Tree

The console tree is located on the left side of the console and is organized by nodes that are based on the server roles you've installed. These server role-based nodes are described in greater detail later in this topic.

Result Pane

The result pane is located in the center of the console. This pane displays objects based on the node that's selected in the console tree. In addition, you can filter the information in the result pane. For more information, see Filter the Result Pane.

Work Pane

The work pane is located at the bottom of the result pane. This pane displays objects based on the server role that's selected in the **Server Configuration** node.

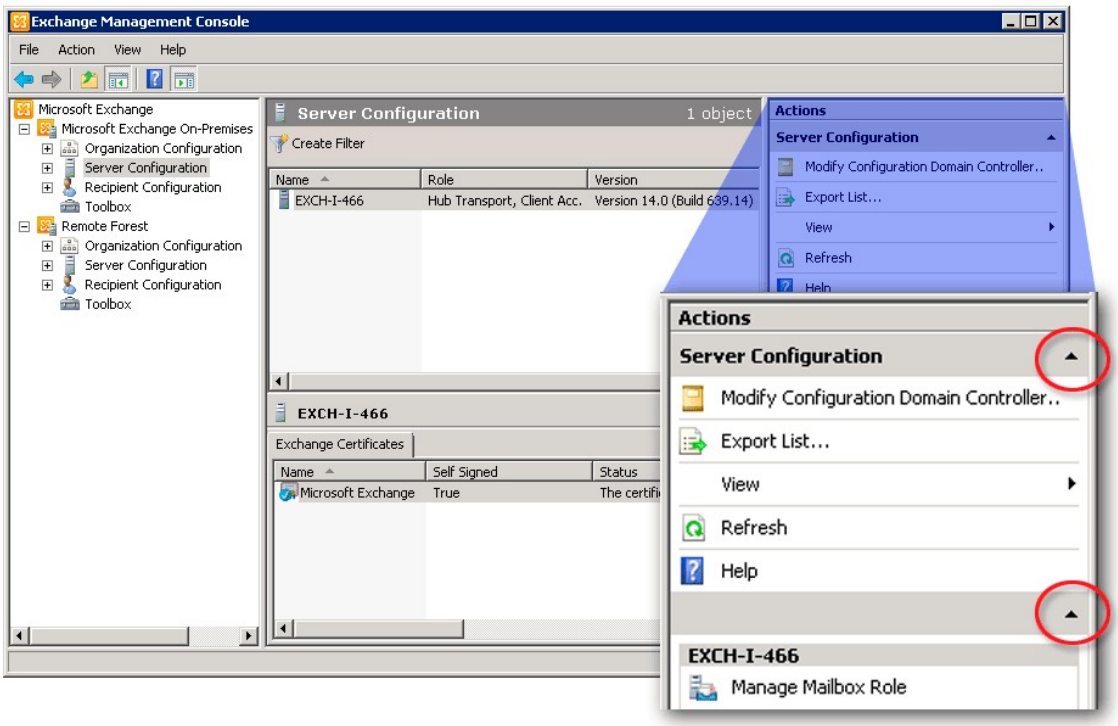
Note:

The work pane is available only when you select objects under the **Server Configuration** node, such as **Mailbox** or **Client Access**.

Action Pane

The action pane is located on the right side of the console. This pane lists the actions based on the object that's selected in the console tree, result pane, or work pane. The action pane is an extension of the shortcut menu, which is the menu that appears when you right-click an item. However, the shortcut menu is still available. To show or hide the

action pane, click the **Show/Hide Action Pane** arrow.



The following table lists common action pane options.

Action pane option	Description
Export List	Click **Export List** to open the **Export List** dialog box. You can use this dialog box to save the list of recipients in the result pane to a text file. For instructions about how to use the Export List feature, see Export Lists from the Exchange Management Console.
View	Click **View** in the action pane to modify how objects are displayed in the console and to record and view the Exchange Management Shell commands that run in the console. The following options may vary depending on your location in the console tree: • **View Exchange Management Shell Command Log** Click **View Exchange Management Shell Command Log** to view the Shell Command Log dialog box. The Command Log allows you to view all the Shell commands that have been executed in the console. For more information, see Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC. • **Add/Remove Columns** Click **Add/Remove Columns** to select which columns you want to display in the result pane and to change the

	order. The available columns depend on the node that you select. The MMC automatically saves your settings. To revert to the default column view, click **Restore Defaults** in the **Add/Remove Columns** dialog box. For more information, see Add or Remove Columns in the Exchange Management Console. • **Visual Effects** Click **Visual Effects** to set the visual effects to be never on or automatic. Use the visual effects setting to configure how Exchange wizards are displayed. If your connection is slow when running wizards, you can increase performance by turning off visual effects. Use the **Automatic** setting to have the console detect if your system should have visual effects turned on or off. • **Save Current Filter as Default** Click **Save Current Filter as Default** to make the existing filter the default filter for the servers listed in the result pane. • **Customize** Click **Customize** to select the console components and snap-ins to display or hide. These settings apply to the entire console. For more information, see Customize the Exchange Management Console.
Refresh	Click **Refresh** to refresh the information displayed in the result pane.
Help	Click **Help** to read the context-sensitive Help for the node or object selected.
Properties	Click **Properties** to view or edit the current configuration for the object selected in the result pane or work pane. **Note:** This option may not be available for all objects.
Remove	Click **Remove** to delete the selected object from the work pane. **Note:** This option may not be available for all objects. **Important:** When you remove a mailbox, not only is the Exchange data deleted, but the associated user account in Active Directory is deleted as well.
Enable or **Disable**	Click **Enable** or **Disable** to enable or disable the object selected in the result pane or work pane. Disabling an object doesn't delete it. **Note:**

	These options may not be available for all objects.

1.4.1 Microsoft Exchange On-Premises

Microsoft Exchange On-Premises

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-08-13*

The **Microsoft Exchange** On-Premises node in the Exchange Management Console allows you to manage your on-premises deployments of Exchange. When you select this node, the result pane displays these tabs:

- **Organizational Health** The Organizational Health report gives you a quick view of your organization and its operating characteristics. The service provides an organizational summary that includes health and licensing information plus a summary of the Exchange servers and recipients.

  Important:
  This report provides you with a quick overview of your Exchange organization that's representative of conditions only at the time the information was collected. In addition, this information may not be accurate because of errors that may have occurred while information was being collected.

  Exchange doesn't display the organizational information by default. To enable the report, you must use the Collect Organizational Health Data wizard to configure how frequently you want to collect data. For more information, see Collect Organizational Health Data.
- **Customer Feedback** The **Customer Feedback Options** section on this tab allows you to run the Customer Experience Improvement Program wizard, in which you can opt-in or out of CEIP. For more information, see Opt-in or Opt-out of the Customer Experience Improvement Program.
  The **Help and Feedback** section provides you with a link to the Exchange TechCenter and also allows you to submit feedback or report bugs directly to the Exchange team.

1.4.2 Organization Configuration Node

Organization Configuration Node

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the **Organization Configuration** node to manage federations and organization relationships. You can also modify the configuration domain controller from this node.

To focus on a set of items in the result pane that have specific attributes, you can use a variety of expressions to filter the list. For more information about filters, see Filter the

Result Pane.

The **Organization Configuration** node contains the following sub-nodes:

- **Mailbox** Use this node to manage Mailbox server role settings that apply to your entire organization. You can maintain existing or create new address lists, managed custom folders, messaging records management (MRM) mailbox policies, and offline address books (OABs).
- **Client Access** Use this node to manage Client Access server role settings that apply to your entire organization. You can maintain existing or create new Exchange ActiveSync mailbox policies and Outlook Web App mailbox policies.
- **Hub Transport** Use this node to manage Hub Transport server role settings that apply to your entire organization. You can maintain existing or create new remote domains, accepted domains, e-mail address policies, transport rules, journal rules, Send connectors, global settings, and Edge subscriptions.
- **Unified Messaging** Use this node to manage Unified Messaging (UM) server role settings that apply to your entire organization. You can maintain existing or create new UM dial plans, UM IP gateways, UM mailbox policies, and UM Auto Attendants.

When you select the **Organization Configuration** node, the following actions are available either by right-clicking **Organization Configuration** or by using the action pane.

Term	Definition
Modify Configuration Domain Controller	Click **Modify Configuration Domain Controller** to select the domain controller that you want to use for server and organization configuration. For more information, see Using the Configuration Domain Controller.
New Federation Trust	Use the **New Federation Trust** wizard to create a new federation trust. A federation trust establishes trust with Windows Live as a prerequisite for enabling sharing of calendar free/ busy information and contacts between two Exchange organizations, or allowing users to share with external recipients. For more information, see Create a Federation Trust.
Manage Federation	Use the **Manage Federation** wizard to configure the federation trust and federated organization identifier. The federated organization identifier specifies the accepted domains in an Exchange Server organization that are available for federation. Only users that have e-mail addresses with domains configured with the federated organization identifier can participate in federated sharing. The first domain specified with the organization identifier is called the *account namespace*. Additional domains can subsequently be added to the organization identifier. **Note:** This action is only available when a federation trust is selected in the result pane. For more information, see Manage Federation.

New Organization Relationship	Use the **New Organization Relationship** wizard to define a partnership for federated sharing with an external Exchange organization. The partnership is defined by specifying the domains configured for federated sharing in the external Exchange organization. Features can be enabled for an organization relationship, allowing you to control the information that is shared with the external organization.
Export List	Click **Export List** to open the **Export List** dialog box. You can use this dialog box to save the list of recipients in the result pane to a text file. For instructions about how to use the Export List feature, see Export Lists from the Exchange Management Console.
View	Click **View** in the action pane to modify how objects are displayed in the console and to record and view the Exchange Management Shell commands that run in the console. The following options may vary depending on your location in the console tree: • **View Exchange Management Shell Command Log** Click **View Exchange Management Shell Command Log** to view the Shell Command Log dialog box. The Command Log allows you to view all the Shell commands that have been executed in the console. For more information, see Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC. • **Add/Remove Columns** Click **Add/Remove Columns** to select which columns you want to display in the result pane and to change the order. The available columns depend on the node that you select. The MMC automatically saves your settings. To revert to the default column view, click **Restore Defaults** in the **Add/Remove Columns** dialog box. For more information, see Add or Remove Columns in the Exchange Management Console. • **Visual Effects** Click **Visual Effects** to set the visual effects to be never on or automatic. Use the visual effects setting to configure how Exchange wizards are displayed. If your connection is slow when running wizards, you can increase performance by turning off visual effects. Use the **Automatic** setting to have the console detect if your system should have visual effects turned on or off. • **Save Current Filter as Default**

	Click **Save Current Filter as Default** to make the existing filter the default filter for the servers listed in the result pane. • **Customize** Click **Customize** to select the console components and snap-ins to display or hide. These settings apply to the entire console. For more information, see Customize the Exchange Management Console.
Refresh	Click **Refresh** to refresh the information displayed in the result pane.

1.4.3 Server Configuration Node

Server Configuration Node

Exchange Server 2010 > Exchange Management Console >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Use the **Server Configuration** node to view a list of all the servers in your Exchange organization and perform server role-specific tasks, such as viewing the Exchange certificates in the work pane.

To focus on a set of items in the result pane that have specific attributes, you can use a variety of expressions to filter the list. For more information about filters, see Filter the Result Pane.

The nodes that appear under **Server Configuration** show only the Microsoft Exchange servers that have a specific server role installed. The **Server Configuration** node contains the following sub-nodes:

- **Mailbox** Use this node to manage the features of Mailbox servers, including viewing the properties of database copies.
- **Client Access** Use this node to manage the features of Client Access servers, including POP3 and IMAP4, Exchange ActiveSync, Outlook Web App, the Exchange Control Panel, and offline address book (OAB) distribution.
- **Hub Transport** Use this node to manage the features of Hub Transport server and receive connectors.
- **Unified Messaging** Use this node to manage the features of Unified Messaging (UM) servers, including enabling and disabling UM.

When you select the **Server Configuration** node, the following actions are available either by right-clicking **Server Configuration** or by using the action pane.

Modify Configuration Domain Controller

Click **Modify Configuration Domain Controller** to select the domain controller that you want to use for server and organization configuration.

Export List

Click **Export List** to open the **Export List** dialog box. You can use this dialog box to save the list of recipients in the result pane to a text file. For instructions about how to use the Export List feature, see Export Lists from the Exchange Management Console.

View

Click **View** in the action pane to modify how objects are displayed in the console and to record and view the Exchange Management Shell commands that run in the console. The following options may vary depending on your location in the console tree:

- **View Exchange Management Shell Command Log**
  Click **View Exchange Management Shell Command Log** to view the Shell Command Log dialog box. The Command Log allows you to view all the Shell commands that have been executed in the console. For more information, see Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC.
- **Add/Remove Columns**
  Click **Add/Remove Columns** to select which columns you want to display in the result pane and to change the order. The available columns depend on the node that you select. The MMC automatically saves your settings. To revert to the default column view, click **Restore Defaults** in the **Add/Remove Columns** dialog box. For more information, see Add or Remove Columns in the Exchange Management Console.
- **Visual Effects**
  Click **Visual Effects** to set the visual effects to be never on or automatic. Use the visual effects setting to configure how Exchange wizards are displayed. If your connection is slow when running wizards, you can increase performance by turning off visual effects. Use the **Automatic** setting to have the console detect if your system should have visual effects turned on or off.
- **Save Current Filter as Default**
  Click **Save Current Filter as Default** to make the existing filter the default filter for the servers listed in the result pane.
- **Customize**
  Click **Customize** to select the console components and snap-ins to display or hide. These settings apply to the entire console. For more information, see Customize the Exchange Management Console.

Refresh

Click **Refresh** to refresh the information displayed in the result pane.

1.4.4 Recipient Configuration Node

Recipient Configuration Node

Exchange Server 2010 > Exchange Management Console >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Use the **Recipient Configuration** node for several recipient management tasks. Specifically, you can view the recipients in your Microsoft Exchange Server 2010 organization, create new recipients, and manage existing mailboxes, mail contacts, mail users, and distribution groups.

To focus on a set of items in the result pane that have specific attributes, you can use a variety of expressions to filter the list. For more information about filters, see Filter the Result Pane.

The **Recipient Configuration** node contains the following sub-nodes:

- **Mailbox** Use this node to manage mailboxes, users, and resource mailboxes (resource mailboxes include room and equipment mailboxes). You can create new mailboxes and remove, disable, or move existing mailboxes. You can also

configure mailbox properties, enable and disable Unified Messaging (UM), and manage mobile devices.

- **Distribution Group** Use this node to manage mail-enabled distribution groups (which include security groups) and dynamic distribution groups. You can create new distribution groups, and remove, disable, or configure existing distribution groups.
- **Mail Contact** Use this node to manage mail contacts and mail users. You can create, delete, or configure mail contacts and mail users.
- **Disconnected Mailbox** Use this node to view and connect disconnected mailboxes.

Note:
Disconnected mailboxes are retained based on the configured mailbox database limits. You see only the mailboxes that have been disconnected within the retention period that is specified for the mailbox database.

- **Move Request** Use this node to manage mailbox move requests. For more information, see Understanding Move Requests.

When you select the **Recipient Configuration** node, the following actions are available either by right-clicking **Recipient Configuration** or by using the action pane.

Modify Recipient Scope

Click **Modify Recipient Scope** to open the **Recipient Scope** dialog box box.

- Changing the recipient scope changes the number of recipients that are displayed in the result pane. The recipient-specific dialog boxes within various wizards and property pages also work within the same scope.
- You can set the scope to include all recipients in the forest or limit it to all recipients in a specific organizational unit (OU). The recipient scope allows administrators to focus on all recipients that are in a specific location in Active Directory Domain Services (AD DS). Selecting a limited recipient scope reduces the number of recipients that are returned, and consequently improves the performance of the Exchange Management Console.

For more information, see Modify the Maximum Number of Recipients to Display in the Result Pane.

Modify the Maximum Number of Recipients to Display

Click **Modify Maximum Number of Recipients to Display** to open the **Maximum Number of Recipients to Display** dialog box. You can use this dialog box to set the maximum number of recipients to display in the result pane.

By default, a maximum of 1,000 recipients is displayed. Increasing this value can be beneficial in large environments. However, increasing the value also increases the time it takes to display the results. Depending on the size of your organization, it may also have a performance impact on the domain controller to which you are connected.

For more information, see Modify the Maximum Number of Recipients to Display in the Result Pane.

Find

Click **Find** to open the **Find** dialog box. You can use the **Find** dialog to search for recipients in your organization. For more information, see Using the Find Dialog Box.

New Mailbox

Click **New Mailbox** to open the New Mailbox wizard. This wizard helps you create a new user, room, equipment, or linked mailbox. For more information, see Managing User Mailboxes.

New Mail Contact

Click **New Mail Contact** to open the New Mail Contact wizard. Mail contacts are mail-enabled Active Directory objects that contain information about people or

organizations that exist outside your Exchange organization. For more information, see Managing Mail Contacts and Mail Users

New Mail User

Click **New Mail User** to open the New Mail User wizard. Mail users are mail-enabled Active Directory users that don't have a mailbox in your Exchange organization.

New Remote Mailbox

Click **New Remote Mailbox** to open the New Remote Mailbox wizard. Use this wizard to create a mail-enabled user in your Exchange 2010 on-premises organization with an associated mailbox in the cloud-based service.

For more information, see Create a Remote Mailbox.

New Distribution Group

Click **New Distribution Group** to open the New Distribution Group wizard. This wizard helps you create both distribution and security groups. Distribution groups are mail-enabled Active Directory objects that contain information about people within an Exchange organization. All distribution groups can be used for e-mail distribution. Security groups can also be used to assign permissions to shared resources. For more information, see Managing Distribution Groups.

New Dynamic Distribution Group

Click **New Dynamic Distribution Group** to open the New Dynamic Distribution Group wizard. This wizard helps you create a new dynamic distribution group.

In Exchange Server 2003, dynamic distribution groups were called query-based distribution groups. Dynamic distribution groups provide the same functionality as mail-enabled distribution groups. However, instead of containing a static group of recipients, the membership list for dynamic distribution groups is calculated based on their configuration each time they are used. When a message is sent to a dynamic distribution group, it's delivered to all recipients in the organization that match the criteria defined for that dynamic distribution group. For more information, see Managing Distribution Groups.

Export List

Click **Export List** to open the **Export List** dialog box. You can use this dialog box to save the list of recipients in the result pane to a text file. For instructions about how to use the Export List feature, see Export Lists from the Exchange Management Console.

View

Click **View** in the action pane to modify how objects are displayed in the console and to record and view the Exchange Management Shell commands that run in the console. The following options may vary depending on your location in the console tree:

- **View Exchange Management Shell Command Log**
  Click **View Exchange Management Shell Command Log** to view the Shell Command Log dialog box. The Command Log allows you to view all the Shell commands that have been executed in the console. For more information, see Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC.
- **Add/Remove Columns**
  Click **Add/Remove Columns** to select which columns you want to display in the result pane and to change the order. The available columns depend on the node that you select. The MMC automatically saves your settings. To revert to the default column view, click **Restore Defaults** in the **Add/Remove Columns** dialog box. For more information, see Add or Remove Columns in the Exchange Management Console.
- **Visual Effects**
  Click **Visual Effects** to set the visual effects to be never on or automatic.

Use the visual effects setting to configure how Exchange wizards are displayed. If your connection is slow when running wizards, you can increase performance by turning off visual effects. Use the **Automatic** setting to have the console detect if your system should have visual effects turned on or off.

- **Save Current Filter as Default**
  Click **Save Current Filter as Default** to make the existing filter the default filter for the servers listed in the result pane.
- **Customize**
  Click **Customize** to select the console components and snap-ins to display or hide. These settings apply to the entire console. For more information, see Customize the Exchange Management Console.

Refresh

Click **Refresh** to refresh the information displayed in the result pane.

1.4.5 View Local Forest Properties

View Local Forest Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Exchange Management Console to view the properties of a forest in Microsoft Exchange Server 2010.

Note:
You can't perform this procedure in the Exchange Management Shell.

Use the EMC to view the properties of an Exchange forest

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. In the console tree, right-click, select the forest in which you're interested, and then select **Properties**.
2. The **General** tab displays the following information about the forest:
   - **Administrator identity** The identity of the administrator of the forest. For example, Contoso\Adminstrator.
   - **Select a server to connect to for remote PowerShell** Select the server to connect to for remote PowerShell. Remote PowerShell is required to open the Exchange Management Shell or the Exchange Management Console on Mailbox, Hub Transport, Unified Messaging, and Client Access servers. You can choose to connect automatically to the selected server, or you can specify a server to connect to.

For More Information

Add an Exchange Forest

1.4.6 View Remote Exchange Forest

View Remote Exchange Forest

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Exchange Management Console to view the properties of a forest in Microsoft Exchange Server 2010.

Note:
You can't perform this procedure in the Exchange Management Shell.

Use the EMC to view the properties of an Exchange forest

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. In the console tree, select the remote Exchange forest in which you're interested, right-click, and then select **Properties**.
2. The **General** tab displays the following information about the forest:
   - **Administrator identity** The identity of the administrator of the source forest. For example, Contoso\Adminstrator.
   - **Remote PowerShell URL** The URL for the source forest's remote PowerShell connection. For example, https://server1.contoso.com/PowerShell/.

For More Information

Add an Exchange Forest

1.4.7 Microsoft Exchange Edge Transport Server

Microsoft Exchange Edge Transport Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-05-28*

The **Microsoft Exchange** node in the EMC is the starting point for managing Exchange. When you select this node, the result pane displays the following tabs:

- **Post-Installation Tasks** Use this tab to complete a variety of tasks that help you complete the deployment of the Edge Transport server role. The following post-installation tasks are available:
  - **Finalize Deployment Tasks** Required tasks that complete the deployment of your Edge Transport server. Examples of finalize deployment tasks are entering the product key, configuring Internet mail flow (either using the edge synchronization process or manual configuration) or configuring an external postmaster address.
  - **End-to-End Scenario Tasks** Recommended optional tasks that provide

end-to-end solutions. Examples of end-to-end scenarios are setting up monitoring options for your Edge Transport server or configuring anti-spam updates.

- **Additional Post-Installation Tasks** Optional tasks that you may want to perform depending on the needs of your organization. Examples are configuring administrator permissions or verifying your Microsoft Exchange Server 2010 installation.

- **Community and Feedback** This tab provides you with links to Exchange-related topics on Microsoft TechNet and new postings from the Exchange team blog. In addition, you can launch the Customer Experience Improvement Program (CEIP) wizard. For more information about CEIP, see Opt-in or Opt-out of the Customer Experience Improvement Program.

1.4.8 Managing Exchange Management Console Features

Managing Exchange Management Console Features

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-01*

Add an Exchange Forest

Add or Remove Columns in the Exchange Management Console

Collect Organizational Health Data

Connect to the Disconnected Mailbox Server

Customize the Exchange Management Console

Export Lists from the Exchange Management Console

Filter the Result Pane

Manage Diagnostic Logging Levels

Opt-in or Opt-out of the Customer Experience Improvement Program

Command Exposure in Exchange Management Console Property Pages

Using the Configuration Domain Controller

Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC

Using the Find Dialog Box

1.4.8.1 Add an Exchange Forest

Add an Exchange Forest

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the **Add Exchange Forest** dialog box to add an Exchange forest. When you add an Exchange forest, you can administer recipients in multiple forests from the Exchange Management Console (EMC). You can add up to 10 forests.

Note:
You can't perform this procedure in the Exchange Management Shell.

Prerequisites

You must establish a federated trust or an Active Directory trust to the target forest before you can add an Exchange forest. For more information, see the following topics:

- Deploy Exchange 2010 in a Cross-Forest Topology
- "Understanding Multiple Forest Administration" in Deploy Multiple Forest Topologies
- Configure Cross-Forest Connectors
- Federation

Use the EMC to add an Exchange forest

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

1. In the console tree, click the **Microsoft Exchange** node. This is the top-most node in the tree.
2. In the action pane, click **Add Exchange Forest**.
3. In the **Add Exchange Forest** dialog box, complete the following fields:
   - **Specify a friendly name for this Exchange forest** Type the name of the Exchange forest. This name will display in the console tree.
   - **Specify the FQDN or URL of the server running the Remote PowerShell instance** Type the FQDN or URL for the source forest's remote PowerShell connection. For example, https://server1.contoso.com/PowerShell/ for the URL connection. For an Online organization, select **Exchange Online**.
   - **Logon with default credential** If you select this check box, the default logged-on administrator password is used.

For More Information

View Local Forest Properties

View Remote Exchange Forest

Understanding Federation

What's New in Exchange 2010 SP1

1.4.8.2 Add or Remove Columns in the Exchange Management Console

Add or Remove Columns in the Exchange Management Console

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-08-21*

By default, the result pane or work pane in the EMC displays only a subset of the columns available. You can add or remove columns based on the type of information that you want to see.

The Microsoft Management Console (MMC) saves any changes you make to a snap-in as preferences in your user profile on the administrator computer. As a result, the next time you start the EMC on the same computer, any changes you've made to the columns will remain. However, if you use another computer or a different user account to run the EMC, you'll need to add or remove columns again. For more information about the MMC, see Microsoft Management Console.

Add or Remove Columns in the Results Pane or Work Pane

1. In the EMC, select an item in either the result pane or the work pane.
2. In the action pane or from the toolbar, navigate to **View** > **Add/Remove Columns**. You can perform the following tasks:
   - To add columns to your current view, select the column name in the **Available columns** box, and then click **Add**.
   - To remove columns from your current view, select the column name from the **Displayed columns** box, and then click **Remove**.
   - To change the position in which the columns display, select a column name from the **Displayed columns** box, and then click **Move Up** or **Move Down**.
   - To restore the EMC to its original configuration, click **Restore Defaults**.
3. Click **OK** to apply your changes and close the dialog box.

1.4.8.3 Collect Organizational Health Data

Collect Organizational Health Data

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-08-04*

The Collect Organizational Health Data wizard collects the information that is displayed on the **Organizational Health** tab in the EMC.

Use the EMC to gather organizational

health data

1. In the console tree, navigate to the appropriate forest.
2. In the action pane, click **Collect Organizational Health Data**.

3. On the **Introduction** page, select one of the following schedule settings:
   - **Immediately** Select this option to collect organizational health information immediately.
   - **At the following time** Select this option, and then use the corresponding drop-down lists to apply a date and time.
   - **Cancel tasks that are still running after (hours)** Select this check box, and then use the corresponding text box to specify how long the wizard will run. The default is 8 hours.

     Click **Next**.

4. On the **Collect Organizational Health Data** page, review your settings. Click **Collect** to collect the data or click **Back** to make configuration changes.

5. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

1.4.8.4 Connect to the Disconnected Mailbox Server

Connect to the Disconnected Mailbox Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Exchange Management Console (EMC) allows you to manage disconnected mailboxes on one server at a time. Use the **Connect to Server** dialog box to specify the Exchange server in your organization that you want to manage disconnected mailboxes.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Disconnected mailbox" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Disconnected Mailbox**.
2. In the action pane, click **Connect to Server**.
3. In **Connect to Server**, click **Browse** to open the **Select Exchange Server** dialog box. Use this dialog box to select the server from which you want to manage disconnected mailboxes.
4. Click **OK**.
5. In **Connect to Server**, you can set this server as the default server by selecting the **Set as default server** check box.
6. Click **OK** to close the dialog box and to save your settings.

For More Information

Connect or Restore a Disabled Mailbox

Understanding Disconnected Mailboxes

1.4.8.5 Customize the Exchange Management Console

Customize the Exchange Management Console

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-08-26*

You can customize the way the Exchange Management Console (EMC) looks.

The Microsoft Management Console (MMC) saves any changes you make to a snap-in as preferences in your user profile on the administrator computer. As a result, the next time you start the EMC on the same computer, the default any changes you've made to the columns will remain. However, if you use another computer or a different user account to run the EMC, you'll need to add or remove columns again. For more information about the MMC, see Microsoft Management Console.

Looking for other management tasks related to the EMC? Check out Exchange Management Console.

What Do You Want to Do?

- Turn visual effects on or off
- Show or hide console items

Turn visual effects on or off

Visual effects settings configure the way the Exchange wizards appear. By default, the visual effects are turned on. If you notice that your connection is slow when using wizards, you may want to turn off these effects.

In the action pane or from the toolbar, navigate to **View** > **Visual Effects**. Select from the following options:

- **Never** The wizards will display in a low-resolution mode.
- **Automatic** Based on your network connection, Exchange will decide whether to turn the effects on or off.

Show or hide console items

You can modify the EMC to show only the console items that you want to see.

1. In the action pane or from the toolbar, navigate to **View** > **Customize**.
2. In **Customize View**, select or clear the check boxes to show or hide items in the console window. Your changes will take effect immediately upon selecting or clearing the check boxes.
3. Click **OK**.

1.4.8.6 Export Lists from the Exchange Management Console

Export Lists from the Exchange Management Console

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the EMC, Public Folder Management Console, Details Templates Editor, or Queue Viewer to export lists from the result pane and the work pane.

You can export lists to the following file formats:

- Text (tab delimited)
- Text (comma delimited)
- Unicode text (tab delimited)
- Unicode text (comma delimited)

Note:
The result pane displays only the first 1,000 objects. For more information about how to filter results, see Filter the Result Pane.

Looking for other management tasks related to the EMC? Check out Managing Exchange Management Console Features.

Use the EMC to export a list from the result pane

Note:
You can't use the Shell to export a list from the result pane.

1. In the console tree, select the node or folder for which you want to display results. The list in the result pane is refreshed.

   Note:
   If the result pane doesn't refresh, in the action pane, click **Refresh**. Long lists may take several minutes to refresh.

2. In the action pane, click **Export List**. The **Export List** dialog box appears.
3. In **Export List**, type the name of the file in the **File name** box, and then select the file format from the **Save as type** list.
4. Click **Save**.

Use the EMC to export a list from the work pane

Note:
You can't use the Shell to export a list from the work pane.

1. In the console tree, expand **Server Configuration**, and then click **Mailbox**,

Client Access, or **Hub Transport**.
2. In the work pane, for any of the tabs displayed, right-click any empty space, and then click **Export List**. The **Export List** dialog box appears.
3. In **Export List**, type the name of the file in the **File name** box, and then select the file format from the **Save as type** list.
4. Click **Save**.

1.4.8.7 Filter the Result Pane

Filter the Result Pane

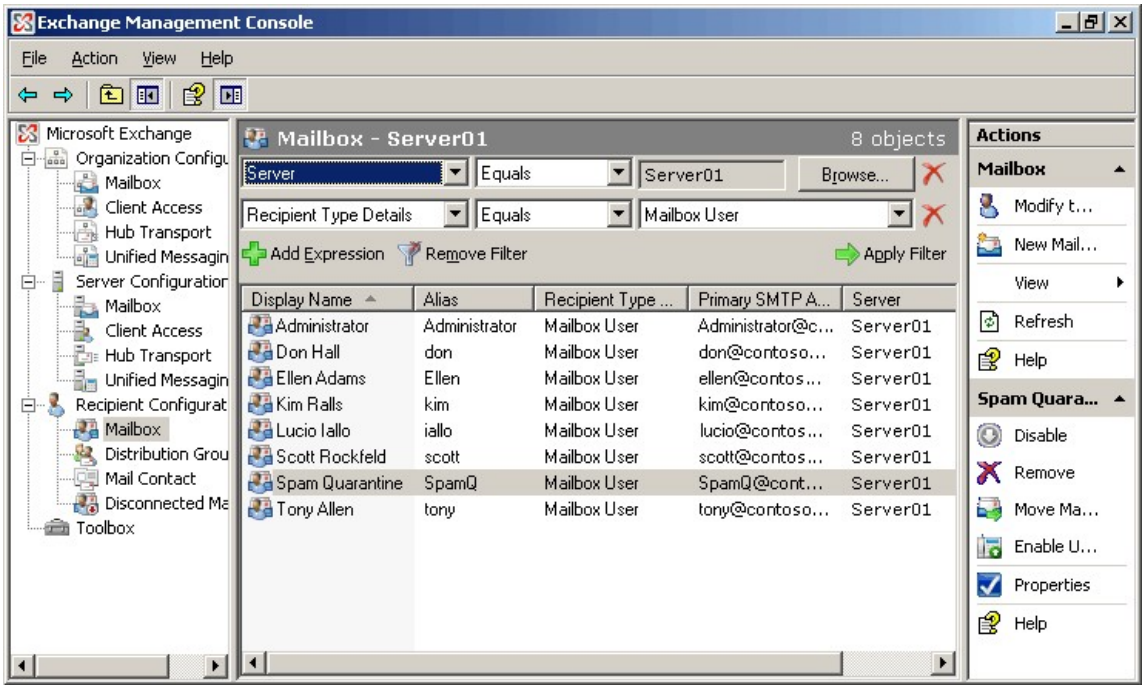
Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-19*

In addition to filtering the result pane for the EMC, you can create filters for the Queue Viewer, Details Templates Editor, and the Public Folder Management Console.

You can create filters for the result pane of the **Organization Configuration** node, **Server Configuration** node, **Recipient Configuration** node, and **Edge Transport** node.

The following figure illustrates a filter for the **Mailbox** node under **Recipient Configuration**. This filter displays all mailbox users for the server Server01.



Caution:

The result pane displays up to one thousand objects. We recommend that you create a default filter to allow the objects to display more quickly. For more information about how to set a default filter, see Step 6 of this procedure.

Looking for other management tasks related to the EMC? Check out Managing Exchange Management Console Features.

Prerequisites

- A filter contains one or more expressions. Each expression consists of an attribute, an operator, and a value. The attributes vary depending on the items for which you are creating the filter. For example, you can filter mailboxes based on attributes such as **Alias** and **Display Name**.
- The list of operators that are available is based on the attribute you select. For example, when you're filtering recipients, the **Display Name** attribute can have **Starts With** as an operator.
- The list of acceptable values is also based on the attribute you select. Acceptable values are selected from a drop-down list, such as the **Role** attribute for servers. In addition, you can type the values for some attributes in the **Value** field, such as the **Display Name** attribute.
- When you are building expressions for a filter, you can't specify what is an **AND** or an **OR** expression. However, the default behavior of the filter is as follows:
  - Multiple expressions that use the same attribute are considered an **OR** expression.
  - Expressions that use different attributes are considered an **AND** expression.

Use the EMC to filter the result pane

Note:
You can't use the Shell to filter the result pane.

1. In the result pane, click **Create Filter** to start defining your filter.
2. Using the drop-down list boxes, create the first filter expression.
3. To create a filter with more than one expression, click **Add Expression**. Additional expressions make the filter more restrictive, which allows you to focus more on the list of items. You can add up to 10 expressions.

   Note:
   You can modify any expression as you're creating it. You can also remove any expression from your filter definition by clicking  .
4. To view only the items that match the criteria defined by the expressions you created, click **Apply Filter**.
5. To remove all expressions and close the filter, click **Remove Filter**. The result pane then displays the full list of items in the Exchange organization.
6. To save the filter as the default filter, click **View** on the menu bar, and then click **Save Current Filter as Default**.

1.4.8.8 Manage Diagnostic Logging Levels

Manage Diagnostic Logging Levels

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Modifying logging levels may help you troubleshoot issues that may occur in an Exchange Server 2010 environment. This topic explains how to use the Exchange Management Console and the Exchange Management Shell to change the diagnostic logging level for processes used by Exchange 2010.

The logging level for each Exchange process determines which events are written to the Application event log in Event Viewer. Changing the process logging level for a given process may not yield additional events in the event log. Many variables affect whether a change to the process logging level setting will increase the number of events. These variables include, but are not limited to, the actions being performed by the process and the number of events implemented in the source code for the logging level selected.

You can use the information in the following table to configure settings for any of the Exchange server roles in your organization. The default logging level is 0 (Lowest). It's recommended that you return the logging level to the default setting after completing your troubleshooting activities.

Logging level	Description
Lowest	Only critical events, error events, and events with a logging level of zero (0) are logged. **Note:** This is the default level for all services on Exchange servers.
Low	Events with a logging level of 1 or lower are logged.
Medium	Events with a logging level of 3 or lower are logged.
High	Events with a logging level of 5 or lower are logged.
Expert	Events with a logging level of 7 or lower are logged.

What Do You Want to Do?

- Use the EMC to set logging levels
- Use the Shell to set logging levels

Use the EMC to set logging levels

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Shell infrastructure permissions" section in the Exchange and Shell Infrastructure Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Mailbox**.
2. In the Actions pane, select **Manage Diagnostic Logging Properties**.
3. On the **Manage Diagnostic Logging Properties** wizard page, click the Exchange service for which you want to change the logging level.
4. Select the logging level, and then click **Configure**.

   Note:
   You can return to the default logging levels by selecting **Reset all services to default logging levels** and then clicking **Configure**.

5. On the **Completion** page, confirm whether the process completed

successfully. A status of **Completed** indicates that the wizard completed the task successfully. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

6. Click **Finish** to complete the Manage Diagnostic Logging Level wizard.

Use the Shell to set logging levels

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Shell infrastructure permissions" section in the Exchange and Shell Infrastructure Permissions topic.

This example identifies all processes and their current logging level.

```
Get-EventLogLevel
```

This example changes the MSExchangeAl\Account Management logging level to High.

```
Set-EventLogLevel -Identity "MSExchangeAl\AccountManagement" -Level High
```

For more information on setting or viewing your logging levels, see the following:

- Set-EventLogLevel
- Get-EventLogLevel

1.4.8.9 Opt-in or Opt-out of the Customer Experience Improvement Program

Opt-in or Opt-out of the Customer Experience Improvement Program

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

The Customer Experience Improvement Program (CEIP) collects anonymous information about how you use Microsoft Exchange 2010 and the problems that you might encounter. You can choose a level of participation. For example, you can choose to opt-out either your entire organization or just specific servers. If you decide not to participate in the CEIP, the servers are opted-out automatically.

You can join the CEIP during installation of Exchange 2010, or you join and specify your participating servers after you've set up your organization. For more information about the program, see Microsoft Customer Experience Program FAQ.

What Do You Want to Do?

- Use EMC to opt-in or opt-out of CEIP
- Use the Shell to opt-in or opt-out of CEIP

Use the EMC to opt-in or opt-out of the CEIP

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange server configuration settings" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In the console tree, navigate to the **Microsoft Exchange On-Premises** node.
2. In the result pane, navigate to **Customer Feedback Options** > **Customer Experience Improvement Program**.
3. On the **Customer Experience Improvement Program** page, read the information about the CEIP and then complete the following settings:
   - **The industry that best represents your organization** Use the corresponding drop-down box to select the industry that best represents your organization.
   - **Join the Exchange Customer Experience Improvement Program** Select this option to join CEIP. If you select this option, select the participating servers later in this procedure.
   - **I don't want to join the program at this time** If you select this option, your organization will not participate in the program and the **Servers Opted in for the CEIP Program** list box will be disabled.
   - **Servers Opted in for the CEIP Program** Click **Add** to add servers to the program, or select servers from the list box and then click Remove (**X**) to remove servers from the program.
4. When you click **Add**, the **Select Exchange Server** dialog appears. Highlight each server that you want to add to the program, and then click **OK** for each server.
5. Click **Apply** on the **Customer Experience Improvement Program** page.
6. On the **Completion** page, the **Summary** states whether the operation was successful. The summary also displays the Exchange Management Shell command that was used to perform this procedure.
7. Click **Finish**.

Use the Shell to opt-in or opt-out of the CEIP

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange server configuration settings" entry in the Exchange and Shell Infrastructure Permissions topic.

This example joins your organization to the CEIP and identifies the industry that is relevant for your organization. In this example, the industry used is `Hospitality`.

```
Set-OrganizationConfig -Industry 'Hospitality' -CustomerFeedbackEnabled $true
```

This example opts-out your entire organization from the CEIP.

```
Set-OrganizationConfig -CustomerFeedbackEnabled $false
```

This example opts-in an Exchange server to the CEIP. In this example, the server name is SERVER01.

Note:
The organization must be joined to the CEIP before you can opt-in any servers.

```
Set-ExchangeServer -Identity 'SERVER01' -CustomerFeedbackEnabled $true
```

This example opts-out an Exchange server from the CEIP. In this example, the server name is SERVER01.

```
Set-ExchangeServer -Identity 'SERVER01' -CustomerFeedbackEnabled $false
```

For detailed syntax and parameter reference, see the following topics:

- Set-OrganizationConfig
- Set-ExchangeServer

1.4.8.10 Command Exposure in Exchange Management Console Property Pages

Command Exposure in Exchange Management Console Property Pages

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

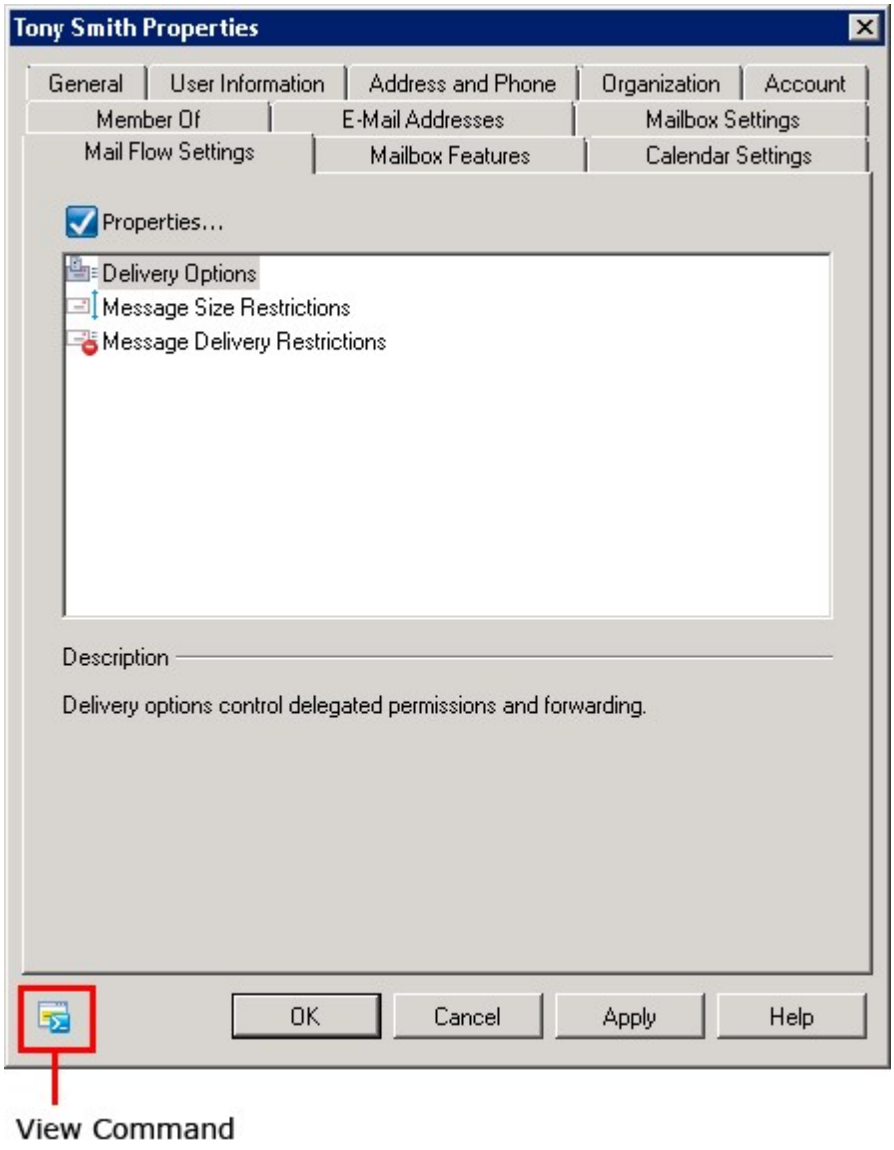
Topic Last Modified: *2009-10-21*

Command exposure in property pages is a new feature that allows you to view the Exchange Management Shell commands that are executed when you make changes to an object's properties.

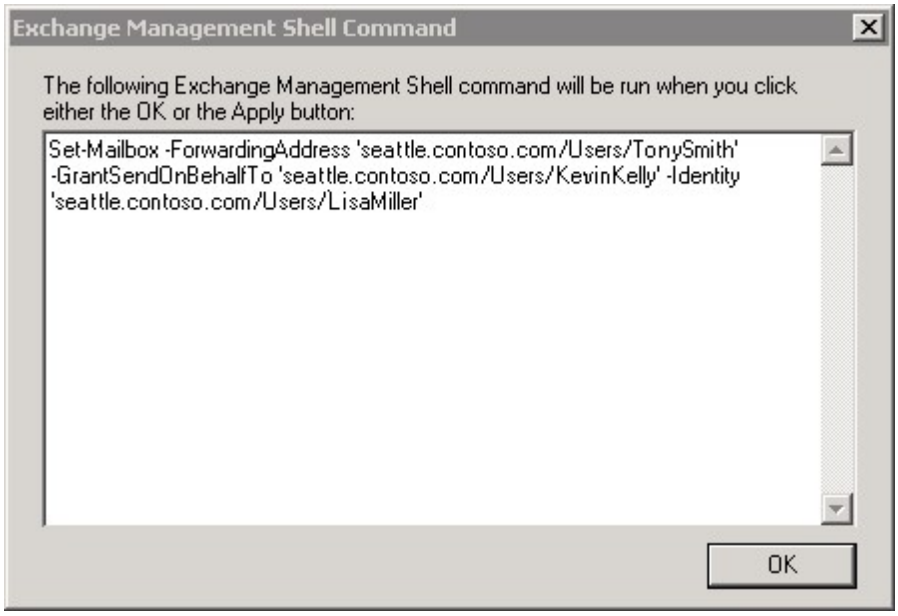
For example, the following figure shows the property page for the user mailbox Tony Smith. To view the Shell command that corresponds to any property changes, click the command-line icon that's located in the lower-left corner.

Note:

The icon is unavailable until you make a change to one of the settings.



When you click the command-line icon, the Exchange Management Shell Command dialog box displays the corresponding Shell command.



To copy the Shell command, highlight all of the text in the dialog box and press CTRL+C. You can then paste the command into a script or into the Shell.

1.4.8.11 Using the Configuration Domain Controller

Using the Configuration Domain Controller

Exchange Server 2010 > Exchange Management Console > Managing Exchange Management Console Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Use the **Configuration Domain Controller** dialog box to specify a domain controller to use to read and write to Active Directory if you modify any server or organization configuration.

To change the configuration domain controller click **Organization Configuration**, and then, in the action pane, click **Modify Configuration Domain Controller**.

Use a default domain controller

Click this button to use the default domain controller. The default domain controller is the domain controller to which the computer is currently connected.

Domain

If you want to specify a domain controller instead of using a default one, click **Browse** to open the **Select Domain** dialog box. Use this dialog box to select a domain in your Active Directory forest. You must select a domain before you can select a domain controller.

Configuration domain controller

This field isn't made available until you've specified a domain.

Click **Browse** to open the **Select Domain Controller** dialog box. Use this dialog box to select the domain controller you want to use when modifying server or organization

configuration.

1.4.8.12 Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC

Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Exchange Management Shell Command Log records the Shell commands that you run in the EMC. In addition, after you start command logging, you can view detailed information about the commands that have run by selecting an item in the result pane. The command that was run displays in the command display box.

Looking for other management tasks related to the EMC? Check out Exchange Management Console.

What Do You Want to Do?

- Turn on command logging
- Turn off command logging
- Export the command log
- Copy the command log to the Clipboard
- Modify the number of commands to log
- Clear the command log

Turn on command logging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Management Console configuration settings" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In the EMC, select **View** > **View Exchange Management Shell Command Log**.

   Note:

   You can't perform this action from the **Microsoft Exchange** node.

2. Select **Action** > **Start Command Logging**.
3. Select **File** > **Close** to close the Exchange Management Shell Command Log. The log will run in the background and continue to record all commands.

Turn off command logging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Management Console configuration settings" entry in the Exchange and Shell Infrastructure Permissions topic.

After you start command logging, the command log will run until you turn it off. Even if you close the program, the application will run in the background.

1. If the Exchange Management Shell Command Log is running in the background, in the EMC select **View** > **View Exchange Management Shell Command Log**.

2. In the Windows PowerShell Command Log, select **Action** > **Stop Command Logging**.

   Note:
   After you close the command log, all logged commands are cleared. The log will not be cleared until you close the EMC.

3. Select **File** > **Close** to close the Exchange Management Shell Command Log. The log will run in the background and continue to record all the commands.

Export the command log

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Management Console configuration settings" entry in the Exchange and Shell Infrastructure Permissions topic.

The command log doesn't save the log of the current EMC session. If you want to save the log, you can export it to a file.

1. If the Exchange Management Shell Command Log is running in the background, in the EMC select **View** > **View Exchange Management Shell Command Log**.
2. Select **Action** > **Export List**. You can save the file in the following formats:
   - Text (Tab Delimited) (*.txt)
   - Text (Comma Delimited) (*.csv)
   - Unicode Text (Tab Delimited) (*.txt)
   - Unicode Text (Comma Delimited) (*.csv)
3. Select **File** > **Close** to close the Exchange Management Shell Command Log. The log will run in the background and continue to record all the commands.

Copy the command log to the Clipboard

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Management Console configuration settings" entry in the Exchange and Shell Infrastructure Permissions topic.

The command log doesn't save the log of the current EMC session. If you want to save specific log entries, you can select them and then copy them to the Clipboard.

1. If the Exchange Management Shell Command Log is running in the background, in the EMC select **View** > **View Exchange Management Shell Command Log**.
2. Select an item or multiple items in the result pane, and then select **Action** | **Copy Commands**.
3. You can paste the command into a file, such as Notepad, by pressing CTRL+V.
4. Select **File** > **Close** to close the Exchange Management Shell Command Log. The log will run in the background and continue to record all the commands.

Modify the number of commands to log

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Management Console configuration settings" entry in the Exchange and Shell Infrastructure Permissions topic.

By default, the Exchange Management Shell Command Log tracks up to 2,048 entries.

1. If the Exchange Management Shell Command Log is running in the background, in the EMC select **View** > **View Exchange Management Shell Command Log**.
2. Select **Action** > **Modify the Maximum Number of Windows PowerShell Commands to log**.
3. Enter a number between 1 and 32767.
4. Click **OK** to save your changes and close the dialog box.

5. Select **File** > **Close** to close the Exchange Management Shell Command Log. The log will run in the background and continue to record all the commands.

Clear the command log

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Management Console configuration settings" entry in the Exchange and Shell Infrastructure Permissions topic.

Clearing the command log is a permanent action. After you clear it, you can't retrieve the log.

1. If the Exchange Management Shell Command Log is running in the background, in the EMC select **View** > **View Exchange Management Shell Command Log**.
2. Select **Action** > **Clear Log**.
3. A dialog box displays asking you to confirm that you want to clear the log. Click **Yes**.
4. Select **File** > **Close** to close the Exchange Management Shell Command Log. The log will run in the background and continue to record all the commands.

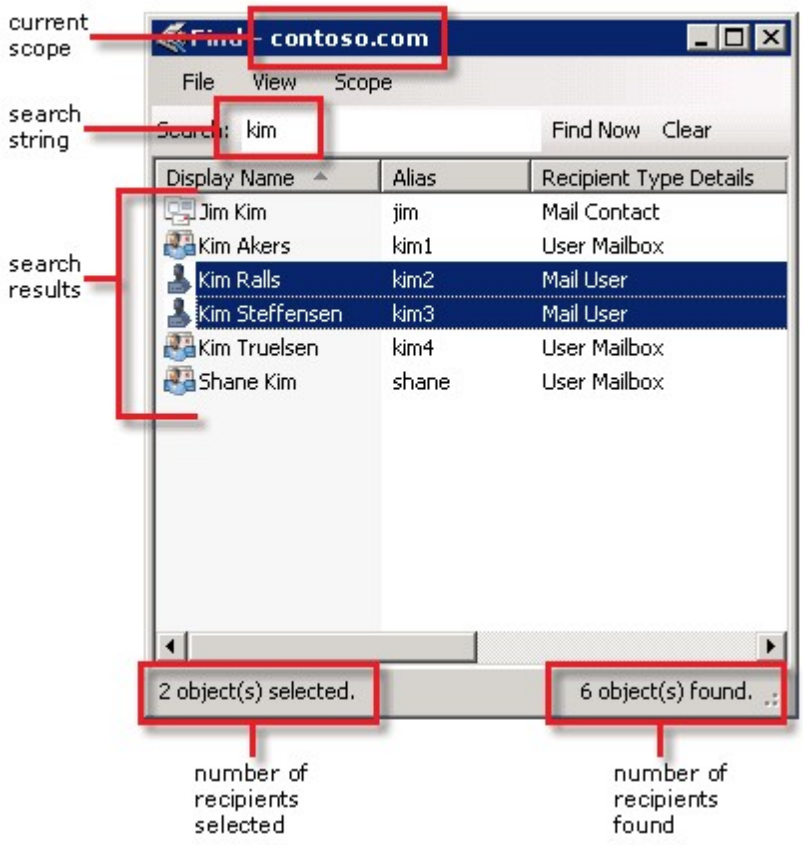
1.4.8.13 Using the Find Dialog Box

Using the Find Dialog Box

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Use the **Find** dialog box (a search feature) to help search for specific recipients by name. The following figure illustrates the components within the **Find** dialog box.



The **Find** dialog box is available in the **Recipient Configuration** node of the Exchange Management Console (EMC). To open the **Find** dialog box, click the **Recipient Configuration** node (or the **Mailbox**, **Distribution Group**, or **Mail Contact** sub-nodes), and then click **Find** in the action pane. Alternatively, you can right-click any blank area of the result pane, and then click **Find**.

Important:

While the **Find** dialog box is open, you can't perform other tasks in the EMC. Any wizard or property pages that are open will be inaccessible. To return to the EMC, you must close all dialog boxes and property pages that are associated with the **Find** dialog box, including the dialog box itself.

Components of the Find Dialog Box

The **Find** dialog box consists of the following four components:

- Menu bar
- Search toolbar
- Result pane
- Status bar

Expand the following sections to learn more about each of these components.

Menu Bar

The menu bar of the **Find** dialog box contains the following items.

File

- **Close** Click this menu item to close the **Find** dialog box.

View

- **Add/Remove Columns** Click this menu item to open the **Add/Remove Columns** dialog box. You can use the **Add**, **Remove**, and **Add All** buttons to change the columns that are displayed in the result pane. You can also use the **Move Up** and **Move Down** buttons to change the order of the columns. Click **OK** to return to the **Find** dialog box.
- **Modify the Maximum Number of Recipients to Display** Click this menu item to open the **Maximum Number of Recipients to Display** dialog box. You can use this dialog box to change the number of recipients that are displayed in the result pane when a search completes.

Note:
This setting applies only to the **Find** dialog box. It is independent of the **Maximum Number of Recipients to Display** setting in the **Recipient Configuration** node. The setting is preserved while the EMC is running. If you restart the EMC, the setting reverts to the default value of 1,000.

Scope

- **Modify Recipient Scope** Click this menu item to open the **Find Scope** dialog box. You can use this dialog box to change the scope of your search. You can view all recipients in the forest or in a specific organizational unit (OU).

Note:
This setting applies only to the **Find** dialog box. It is independent of the **Recipient Scope** setting in the **Recipient Configuration** node. The setting is preserved while the EMC is running. If you restart the EMC, the setting reverts to the default value, which is the domain of the computer that is running the EMC.

Search Toolbar

The search toolbar is directly below the menu bar. The search toolbar contains the following items.

Search

Use this text box to type the search string to use to find recipients.

Important:
The search string that you provide must be at least three characters long. Leading or trailing spaces are not included in the total.

Note:
You cannot use wildcard characters in the search string.

Find Now

Click this button to start the search. The search returns all recipients whose first name, last name, display name, user principal name (UPN), alias, or e-mail address begins with the specified search string. For example, if you search for the string **ter**, the search results include the recipient Terry Adams, but not Adam Carter.

The **Find Now** button is unavailable while a search is in progress. After the search completes or is cancelled, it is made available again.

Clear or **Stop**

Click **Clear** to clear the search results and the information that is displayed on the status bar.

Click **Stop** to stop the search that is in progress. Partial results may be displayed if matching recipients were found while the search was in progress.

Note:
While a search is in progress, the **Clear** button changes to **Stop**. If you stop the search, or the search completes, the button changes back to **Clear**.

Result Pane

The result pane is directly below the search toolbar. When a search completes, the

recipient objects that match your criteria are displayed in the result pane. If you double-click a recipient in the result pane, the property page for that recipient is displayed. If you right-click a recipient, the shortcut menu displays the actions you can perform for that recipient type.

Status Bar

The status bar, located directly below the result pane, displays the following information:

- While a search is in progress, a progress indicator is displayed on the right side of the status bar.
- After a search is complete or is stopped, the number of recipient objects found is displayed on the right side of the status bar. If the search is stopped before completion, the status bar displays the text **The query was cancelled** after the number of objects found.
- After a search is complete or is stopped, the number of recipient objects that are selected is displayed on the left side of the status bar.

1.4.9 Managing Tools in the Toolbox

Managing Tools in the Toolbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-30*

The Toolbox is a collection of diagnostic, troubleshooting, and recovery tools installed with Microsoft Exchange. The tools available in the Toolbox work center are divided into two categories:

- **Dedicated Microsoft Management Console (MMC) 3.0 tools** Some tools, such as Queue Viewer, are self-hosted in an MMC console. The Exchange Management Console (EMC) doesn't have to be running to use the MMC tools.
- **Independent tools** Independent tools, such as the Exchange Best Practices Analyzer, aren't integrated with the EMC and function as separate executable files when run from the Toolbox. These tools have their own Help file content. For more information about how to use the tools, refer to the Help file for each tool.

When you click the **Toolbox** node from the **Microsoft Exchange On-Premises** node, all the tools discussed in this topic are displayed in the result pane. You can open the tool by double-clicking the tool name, by clicking **Open Tool** from the action pane, or from the right-click menu.

When you click the **Toolbox** node from a remote forest node, only the following tools are displayed:

- Role Based Access Control (RBAC) User Editor
- Message Tracking
- Call Statistics
- User Call Logs

Configuration Management Tools

The following configuration management tools are available in the Toolbox:

- **Best Practices Analyzer** The Exchange Best Practices Analyzer automatically

examines an Exchange deployment and determines whether the configuration is in line with Microsoft best practices. We recommend running the Exchange Best Practices Analyzer after you install a new Exchange server, upgrade an existing Exchange server, or make configuration changes. For more information, see Microsoft Exchange Analyzers.

- **Details Templates Editor** The Details Templates Editor controls the appearance of the object properties accessed by using address lists in MAPI 32-bit client applications, such as Microsoft Outlook. For example, when a user opens an address list in Outlook, the properties of the recipients in that address list are displayed in accordance with the details template that exists in your Exchange organization. For more information, see Managing Details Templates.
- **Public Folder Management Console** The Public Folder Management Console is an MMC 3.0-based interface that provides you with a graphical user interface (GUI) for creating, configuring, and managing public folders. For more information, see Using the Public Folder Management Console.
- **Remote Connectivity Analyzer** The Exchange Remote Connectivity Analyzer is a Web-based tool that helps you troubleshoot connectivity issues. The tool simulates several client logon and mail flow scenarios. When a test fails, many of the errors have troubleshooting tips to assist you in correcting the problem. For more information, see Exchange Remote Connectivity Analyzer Tool.
- **Role Based Access Control (RBAC) User Editor** The RBAC User Editor allows you to add users to management role groups. When you open this tool, you need to sign in to Microsoft Office Outlook Web App as a user who has permission to perform this task. After you sign in, you are directed to the **Administrator Roles** tab. For more information, see Understanding Role Based Access Control.

Mail Flow Tools

The following mail flow tools are available in the Toolbox:

- **Mail Flow Troubleshooter** The Mail Flow Troubleshooter assists you in troubleshooting common mail flow problems. You can diagnose a problem by selecting the symptoms observed. Based on the symptoms, the tool walks you through the correct troubleshooting path. It shows an analysis of possible root causes and provides suggestions for corrective actions.
- **Message Tracking** The Message Tracking tool helps you access and configure delivery reports. When you open this tool, you need to sign in to Outlook Web App as a user who has permission to perform this task. After you sign in, you are directed to the **Delivery Reports** tab. For more information, see Understanding Message Tracking.
- **Queue Viewer** Queue Viewer helps you monitor mail flow, and inspect queues and messages. You can also perform actions to the queuing databases such as suspending or resuming a queue, or removing messages. For more information, see Using Queue Viewer.
- **Routing Log Viewer** Routing Log Viewer is a tool you can use to open a routing log file that contains information about the routing topology. You can also open a second routing log and compare it to the first log opened. The tool consists of a parser and a public user interface.
  To use the Routing Log Viewer to view logs of routing table configuration changes, you must connect to an Exchange server that has the Hub Transport server role or the Edge Transport server role installed. For more information, see Using the Routing Log Viewer.
- **Tracking Log Explorer** Tracking Log Explorer provides a detailed log of all message activity as messages are transferred to and from an Exchange server that has the Hub Transport server role, the Mailbox server role, or the Edge Transport server role installed. Exchange servers that have the Client Access server role or Unified Messaging (UM) server role installed don't have message tracking logs. Message tracking logs can be used for message forensics, mail

flow analysis, reporting, and troubleshooting.

Performance Tools

The following performance tools are available in the Toolbox:

- **Performance Monitor** Performance Monitor is a tool you can configure to collect information about the performance of your messaging system. Specifically, you can use it to monitor, create graphs, and log performance metrics for core system functions. You can also use Performance Monitor to monitor Exchange-specific parameters, such as the number of inbound or outbound messages per hour or the number of directory lookups performed by Exchange. Performance Monitor is commonly used to view key parameters while troubleshooting performance problems. It's also used to gather baseline performance data to perform historical trend analysis and measure the impact of changes to your Exchange environment.
- **Performance Troubleshooter** Performance Troubleshooter helps you to locate and identify performance-related issues that could affect an Exchange server. You can diagnose a problem by selecting the symptoms observed. Based on the symptoms, the tool walks you through the correct troubleshooting path. Performance Troubleshooter identifies possible bottlenecks and suggests corrective actions.

Unified Messaging Tools

The following Unified Messaging tools are available in the Toolbox:

- **Call Statistics** The Call Statistics tool provides aggregated statistical information about calls forwarded to or placed by Unified Messaging servers. This information can be used if you're interested in overall statistics for the Exchange 2010 Unified Messaging servers in your organization. When you open this tool, you need to sign in to Outlook Web App as a user who has permission to perform this task. After you sign in, you are directed to the **Call Statistics** page. For more information, see the following topics:
  - Review the UM Calls for Your Organization
  - Using Unified Messaging Tools
- **User Call Logs** The User Call Logs tool displays the call data records for a selected UM-enabled user. These logs are useful in Help desk situations where the Help desk employee must gather information about specific calls for a UM-enabled user to assist them in diagnosing and fixing issues. When you open this tool, you need to sign in to Outlook Web App as a user who has permission to perform this task. After you sign in, you are directed to the **User Call Logs** page. For more information, see the following topics:
  - Review the UM Calls for a User
  - Using Unified Messaging Tools

1.4.9.1 Using the Routing Log Viewer

Using the Routing Log Viewer

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Routing Log Viewer tool works on a server running Microsoft Exchange Server 2010

that has the Hub Transport or the Edge Transport server role installed. It is started from the Exchange Management Console (EMC).

In earlier versions of Exchange, you could connect to the Microsoft Exchange Routing Engine service on port 691 by using the WinRoute tool. In Exchange 2010, there's no routing engine, but you can use the Routing Log Viewer to open a routing log file that contains information about how the routing topology appears to the server. You can also open a second routing log, and then determine the changes that have occurred within the routing topology between two time periods. This is helpful when routing problems resolve themselves before troubleshooting begins, or for determining what changes have occurred in the topology over time. In these cases, if problems occurred because of changes in the routing topology, the tool can be used to compare the changes and help resolve any mail routing problems.

The Routing Log Viewer tool consists of a parser and a public graphical user interface to the parsing component.

There are four tabs in the Routing Log Viewer that present server information:

- Active Directory Sites & Routing Groups
- Servers
- Send Connectors
- Address Spaces

These tabs are described in the following sections.

Active Directory Sites & Routing Groups Tab

The **Active Directory Sites & Routing Groups** tab provides a listing of Active Directory sites and routing groups in the Exchange organization. For Active Directory sites, only those sites that have Exchange servers are listed.

If the site is enabled as a hub site, it can be verified on this tab. The local site where the routing table log was generated is also noted. All servers in each site are listed as is the total cost to deliver mail to the site from the local site, and the **Backoff path** that should be used if there are problems with delivering messages.

Note:

If the site is a hub site, all sites beyond it will have the **Next hop site** property pointing to the hub site. This indicates where the mail stops before it's relayed to the target site.

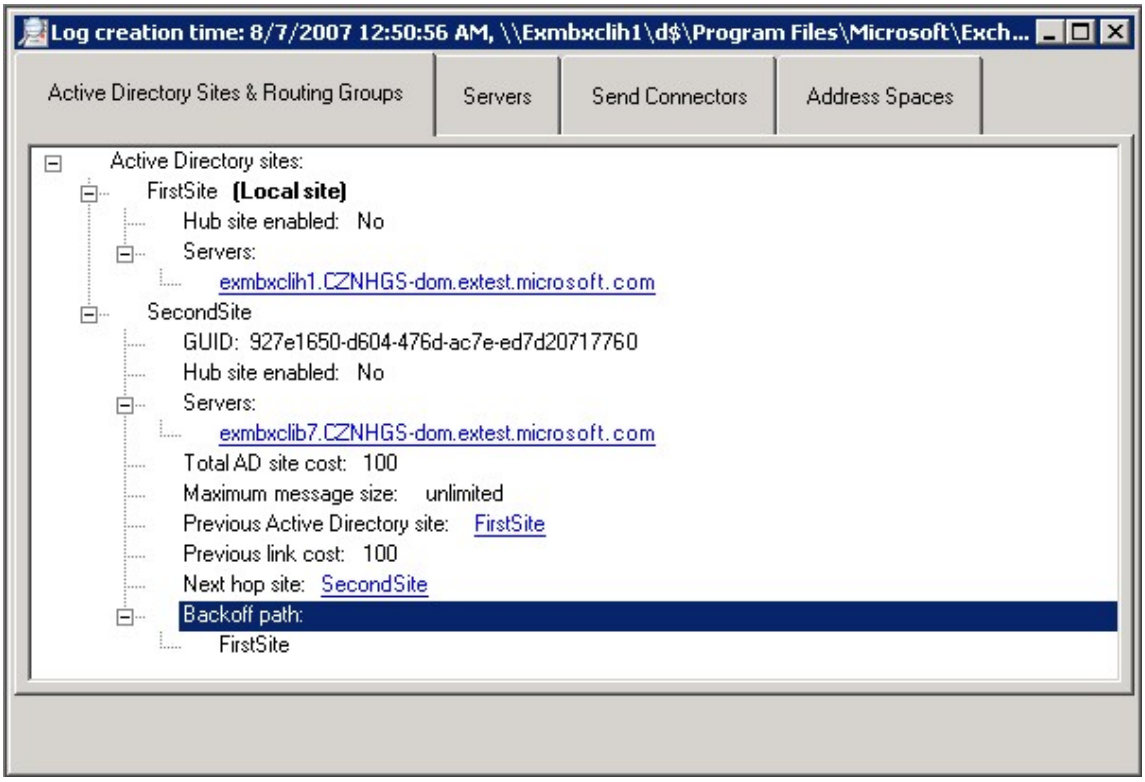
Note:

The **Backoff path** property refers to the full backoff path, instead of the binary backoff path. Routing will use the binary backoff path if the number of segments in the backoff path is greater than four.

For routing groups, although all Exchange 2010 servers are installed in their own routing group, only Exchange Server 2003 routing groups are listed. Exchange 2010 servers are listed under the Active Directory sites. Each server in each routing group is listed together with the first hop routing group connector used to reach that routing group.

All servers and connectors displayed on this page have hyperlinks that link to the appropriate object with either the **Servers** or **Send Connectors** tabs.

The following figure is an example of what is displayed when you double-click the **Active Directory Sites & Routing Groups** tab.



Servers Tab

The **Servers** tab contains a list of all Exchange servers in the Exchange organization. The local server where the routing logs were generated is indicated at the top level. The following information is generated when you use the **Servers** tab:

- Distinguished name (DN) of the server
- Proximity to the local server
- Active Directory site or routing group that the server belongs to
- Server roles installed such as Mailbox or Hub Transport
- Total cost
- Message databases (MDBs) available
- Legacy DN
- Whether you are using Exchange 2007 or a later version

Some properties have hyperlinks that link to their counterpart in related tabs. For example, Active Directory sites and routing groups have hyperlinks that link to their counterpart on the **Active Directory Sites & Routing Groups** tab. Routing group connectors have hyperlinks to the appropriate connector on the **Send Connectors** tab.

Send Connectors Tab

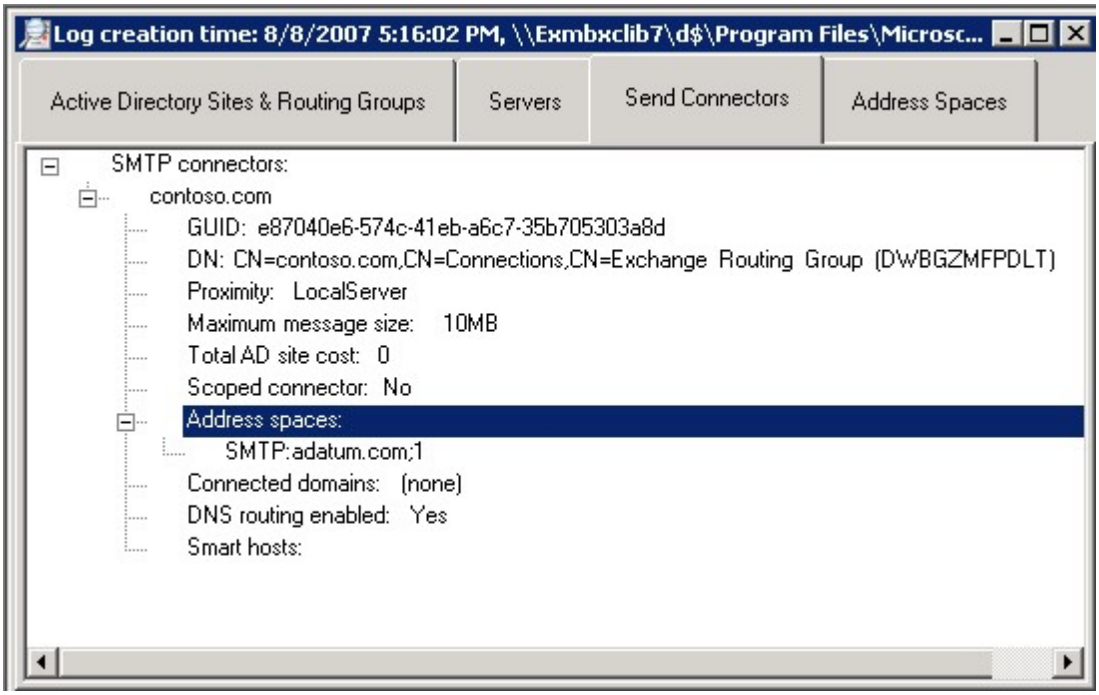
The **Send Connectors** tab provides a list of all SMTP connectors, foreign connectors, and routing group connectors available in the Exchange organization. Legacy gateway connectors homed on legacy servers are also listed.

Information for each connector type includes the following:

- Name
- GUID
- DN

- Proximity to the local server
- Maximum message size of a message that passes through a connector (default is unlimited)
- Total site cost to reach the connector
- Whether this is scoped connector
- Address spaces
- Whether DNS routing is enabled
- What smart hosts are defined

The following figure shows an example of the **Send Connectors** tab for SMTP connectors.



If the connector uses connected routing groups, that information is available on the **Connected domains** property. For **Foreign connectors**, the value specified by the drop directory is also provided.

Routing group connectors identify the targeted routing group and list all targeted Exchange servers except routing group connectors that target Exchange 2010. These connectors have a blank **Target routing group** property.

Address Spaces Tab

The **Address Spaces** tab provides a list of all address spaces in the Exchange organization, separated by the address type, such as SMTP. Each address space lists all the associated connectors with their cost. The list of connectors is ordered based on the connector selection algorithm for using that particular address space. Therefore, the first connector in the list is the connector that Exchange 2010 uses for delivery to that address space.

Note:
If the first connector can't meet the message size, one of the other connectors for that address space, or a less specific address space, can be used.

The connectors displayed on the **Address Spaces** tab have hyperlinks that link to their

properties on the **Send Connectors** tab.

Examples of How Routing Table Log Data Can Be Used

The following are examples of how you can use the Routing Log Viewer tool to examine the routing data.

Finding the Lowest Cost Path to a Site

After a routing log XML file is opened and parsed, the Routing Log Viewer displays all the information about each Active Directory site in the **Active Directory Sites & Routing Groups** tab on the **Routing Log Viewer** screen. To find the lowest cost path from the local site to another site, locate the destination site, expand it, find the **Previous Active Directory** site, and follow the chain until you reach the local site.

Finding the Preferred Connector for a Specific Address

After a routing log file is opened and parsed, the Routing Log Viewer displays all the information about each address space that can be routed by the local server. For a specific address space, all connectors that have the address space configured are listed in the priority order using the address selection algorithm used by Exchange 2010 routing. Unless the preferred connector has size restrictions, the preferred connector is listed first, is bold, and is always the connector used to route to the address space that it's listed under. If the preferred connector has size restrictions, the next best connector in the list that meets size restrictions, or a connector with a less specific address space match, is chosen.

1.4.9.1.1 Open a Log File by Using the Routing Log Viewer

Open a Log File by Using the Routing Log Viewer

Exchange Management Console > Managing Tools in the Toolbox > Using the Routing Log Viewer >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can open a log file by using the Routing Log Viewer. There are no logs available when the Routing Log Viewer first opens. You can either specify the name of a transport server, or you can browse through the files on a local server.

Important:

When you are using the Edge Transport server role, you must use the **Browse local files** button on the Edge Transport server. The **Browse server files** option from the **Open Routing Table Log File** dialog box doesn't work for browsing on the Edge Transport server role.

You can specify alternative credentials with which to access the remote routing table logs. The **Run As** dialog box enables you to provide credentials with which to access files from the remote servers. If all fields are blank in this dialog box, the Routing Log Viewer uses the local user's credentials for all file access operations.

Use the Routing Log Viewer to open a log

file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport logs" entry in the Transport Permissions topic.

1. In the EMC, click **Toolbox** > **Routing Log Viewer** > **Open Tool**.
2. On the **Routing Log Viewer** menu, click **File**, and then click **Open log file**.
3. In the **Name of transport server** box, enter the name of the transport server you want, or click **Browse server files** and then click the server that you want to use and click **Open**. On an Exchange Hub Transport server, you can leave the server name field blank to browse through the local server's log files.

   Note:
   When you click **Browse server files**, the Routing Log Viewer connects to Active Directory. The tool reads the Exchange server object, determines where the routing logs are stored, and then tries to open the directory.

4. Or, you can click **Browse local files** and then select the file of interest and click **Open**.
5. If you are browsing the files on a remote server, you need to supply administrator permissions to access the share on the remote server. To supply alternative credentials, click **Run As** to do remote browsing. Complete the following, and then click **OK**:
   - **Use Run As for remote browsing** This is selected by default.
   - **User name** Type the alternative user name.
   - **Domain** Type the domain for the alternative user name.
   - **Password** Type the password.

Use the Routing Log Viewer to change credentials to browse through files on a remote server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport logs" entry in the Transport Permissions topic.

1. In the EMC, click **Toolbox** > **Routing Log Viewer** > **Open Tool**.
2. On the **Routing Log Viewer** menu, click **Settings**, and then click **Run As**. Or, on the **Routing Log Viewer** menu, click **File**, and then click **Open log file**.
3. From **Open Routing Table Log File**, click **Run As**. In the **Run As** dialog box, complete the following, and then click **OK**:
   - **Use Run As for remote browsing** Click this check box to use the alternative credentials you provide in this dialog box when browsing through logs on remote computers. This is selected by default.
   - **User name** Type the alternative user name.
   - **Domain** Type the domain for the alternative user name.
   - **Password** Type the password.

Note:
Local administrator permissions are required on the remote server to access the administrative share used to access the log file directory. This is why you would want to change credentials to browse through files on remote servers.

1.4.9.1.2 Compare Routing Log Files

Compare Routing Log Files

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

With the Routing Log Viewer tool, you can load two routing table logs and then view the differences between them. This approach can help you discover changes that have occurred in the routing topology between different sets of logs. The log with the most recent timestamp is the log labeled with the change status Added, Removed, or Modified. As long as the timestamp is different, it's not important which log you open first. If the timestamps are the same, the comparison is performed from the perspective of the first log opened.

Looking for other management tasks related to tools? Check out Managing Tools in the Toolbox.

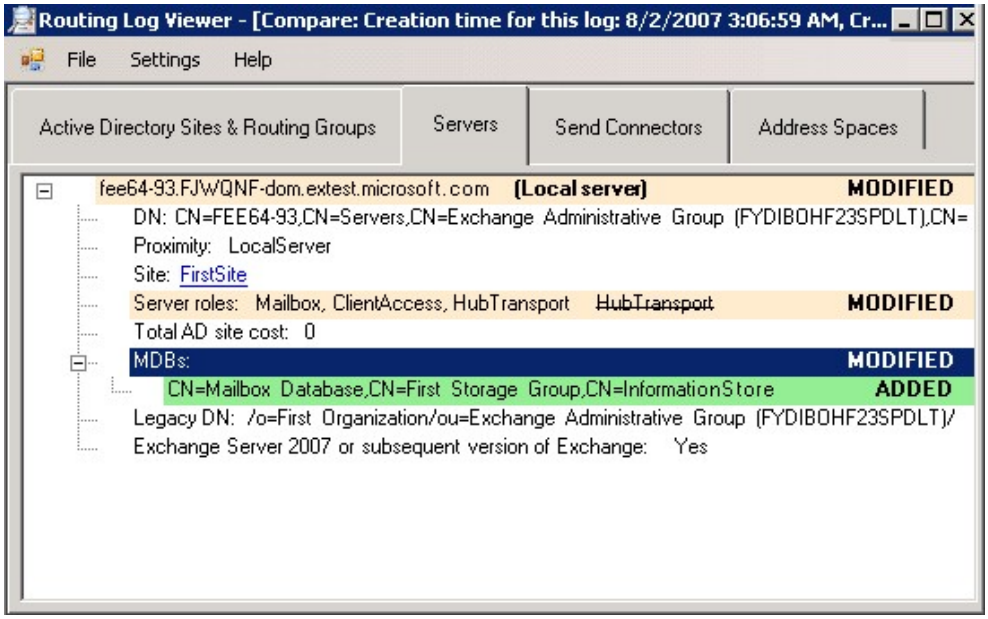
Use the Routing Log Viewer tool to compare log files

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport logs" entry in the Transport Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Routing Log Viewer**.
3. In the action pane, click **Open Tool**.
4. Open the first log by following the procedure in the topic Open a Log File by Using the Routing Log Viewer.
5. On the **File** menu, click **Compare log file**.

   Note:
   The **Compare log files** option on the **File** menu is available only when the window of a previously parsed log file has been left open.

6. Open a second log file by entering the applicable information in the **Open Routing Table Log file** dialog box.
7. An example of the report is shown in the following figure. Any changes that have been made to the topology are highlighted to indicate whether the item was **Added**, **Removed**, or **Modified**. If a value was modified, both the original value and the changed values are shown. In the following example, the report shows an addition and three modifications. The information is being displayed from the **Servers** tab.



1.4.9.2 Using the Public Folder Management Console

Using the Public Folder Management Console

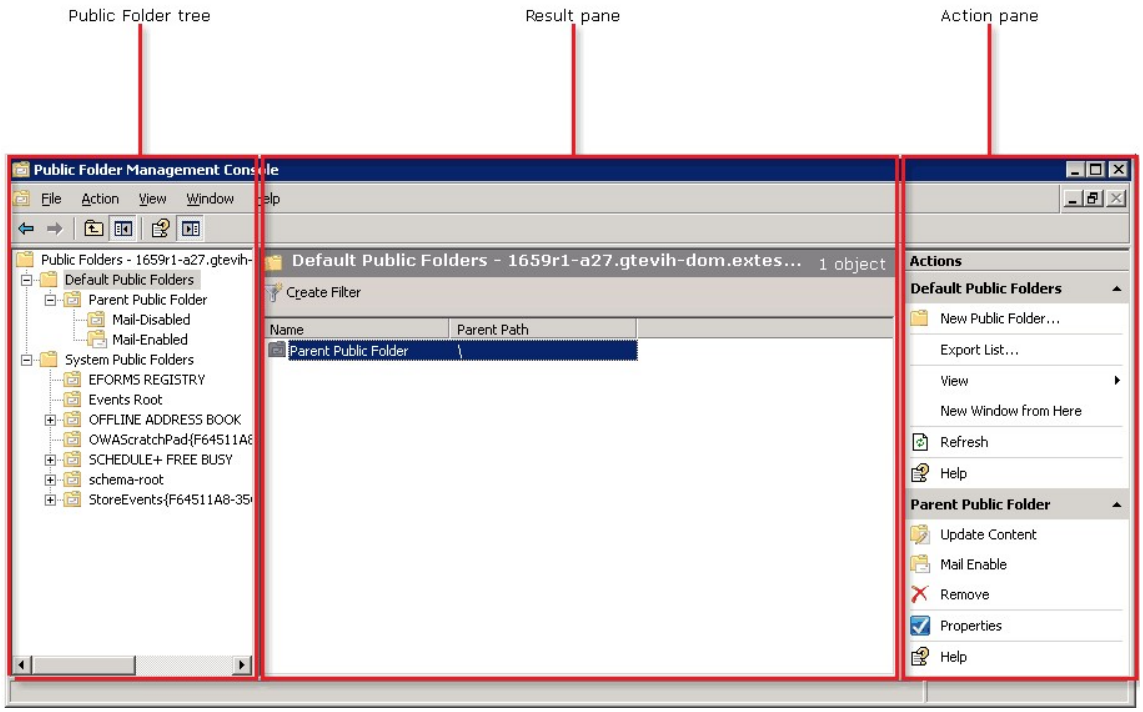
Exchange Server 2010 > Exchange Management Console > Managing Tools in the Toolbox >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Public Folder Management Console is a Microsoft Management Console (MMC) 3.0-based interface that provides you with a graphical user interface (GUI) to create, configure, and maintain public folders. You can access the Public Folder Management Console from the Toolbox in the Exchange Management Console (EMC). For more information about the Toolbox, see Managing Tools in the Toolbox.

Similar to the EMC, the Public Folder Management Console is organized into three panes. In the Public Folder Management Console, these panes are called the public folder tree, the result pane, and the action pane.



Mail-enabled public folders are represented in the user interface by this icon: 

System public folders and public folders that are not mail-enabled are represented in the user interface by this icon: 

Expand the following sections to learn more about each pane

Public Folder Tree

The public folder tree is located on the left side of the console and is organized by nodes that are based upon the public folder hierarchy. Exchange Server 2003 supports the use of a non-MAPI folder tree, otherwise known as an *Application* folder tree or *General Purpose* folder tree. Exchange 2007 and Exchange 2010 support only the default MAPI folder tree.

The MAPI folder tree is divided into the following subtrees:

- **Default Public Folders (also known as the IPM_Subtree)** Users can access these folders directly by using client applications such as Outlook.
- **System Public Folders (also known as the Non IPM_Subtree)** Users cannot access these folders directly by using conventional methods. Client applications such as Outlook use these folders to store information such as free and busy data, offline address books (OABs), and organizational forms. Other system folders contain configuration information that is used by custom applications or by Exchange itself. The public folder tree contains additional system folders, such as the EFORMS REGISTRY folder, that do not exist in general-purpose public folder trees. System folders include the following:
  - **EFORMS REGISTRY** By default, one content replica of each of these folders resides in the default public folder database on the first server that is installed in the first administrative group. This is the location where organizational forms are stored for legacy Outlook clients (clients that use an Outlook version earlier than Office Outlook 2007).

- **Offline Address Book** and **Schedule+ Free Busy** The Offline Address Book folder and the Schedule+ Free Busy folders automatically contain a subfolder for each administrative group (or site) in your topology. By default, a content replica of a specific administrative group folder resides on the first server that is installed in the administrative group. These folders are used to store legacy free and busy information and OAB data for legacy Outlook clients. Legacy Outlook clients do not support the Exchange Server 2007 or later features that manage free and busy information and OAB data. (These features include the Availability service, the Autodiscover service, and OAB distribution on Client Access servers).

Result Pane

The result pane is located in the center of the console. This pane displays public folders based upon the public folder that is selected in the public folder tree.

To focus on a set of items in the result pane that have specific attributes, you can use a variety of expressions to filter the list. For more information about filters, see Filter the Result Pane.

The following columns are displayed by default:

- **Name** This column lists the name of the public folder.
- **Parent Path** This column lists the public folder path to the parent public folder. If a backslash (****) is displayed, the parent public folder is the top-level public folder for that tree.

The following columns are hidden by default:

- **Mail Enabled** This column lists the mail-enabled status of the public folder.
- **Age Limit in Days** This column lists the age limit (in days) of the public folder.
- **Local Replica Age Limit in Days** This column lists the local replica age limit (in days) of the public folder.
- **Hidden From Address List** This column lists the true or false status of whether the public folder is hidden from address lists in your organization.
- **Replicas** This column lists the server name on which this public folder is replicated.

Action Pane

The action pane is located on the right side of the console. The action pane lists the actions based upon the object that is selected in the public folder tree or the result pane. The action pane is an extension of the shortcut menu, which is the menu that appears when you right-click an item.

Public Folder Node Actions

When you select the **Public Folders** node in the public folder tree, the following actions are available in the action pane.

Properties

Click **Properties** to view or configure the settings of the server that Remote Power Shell uses to perform the specified tasks in the Public Folder Management Console.

For more information, see View or Configure Remote PowerShell Connectivity.

Connect to Server

Click this button to connect the Public Folder Management Console to a Mailbox server on which a public folder database resides.

For more information, see Connect to Public Folder Server.

Update Hierarchy

Click this button to synchronize the public folder hierarchy from one server to the other servers on which public folder replicas exist.

For more information, see Update a Public Folder Hierarchy.

View

Click **View** in the action pane to modify how objects are displayed in the console and to record and view the Exchange Management Shell commands that run in the console. The following options may vary depending on your location in the console tree:

- **View Exchange Management Shell Command Log**
  Click **View Exchange Management Shell Command Log** to view the Shell Command Log dialog box. The Command Log allows you to view all the Shell commands that have been executed in the console. For more information, see Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC.
- **Add/Remove Columns**
  Click **Add/Remove Columns** to select which columns you want to display in the result pane and to change the order. The available columns depend on the node that you select. The MMC automatically saves your settings. To revert to the default column view, click **Restore Defaults** in the **Add/Remove Columns** dialog box. For more information, see Add or Remove Columns in the Exchange Management Console.
- **Visual Effects**
  Click **Visual Effects** to set the visual effects to be never on or automatic. Use the visual effects setting to configure how Exchange wizards are displayed. If your connection is slow when running wizards, you can increase performance by turning off visual effects. Use the **Automatic** setting to have the console detect if your system should have visual effects turned on or off.
- **Save Current Filter as Default**
  Click **Save Current Filter as Default** to make the existing filter the default filter for the servers listed in the result pane.
- **Customize**
  Click **Customize** to select the console components and snap-ins to display or hide. These settings apply to the entire console. For more information, see Customize the Exchange Management Console.

Refresh

Click **Refresh** to refresh the information displayed in the result pane.

Export List

Click **Export List** to open the **Export List** dialog box. You can use this dialog box to save the list of recipients in the result pane to a text file. For instructions about how to use the Export List feature, see Export Lists from the Exchange Management Console.

Public Folder Tree Actions

When you select a public folder in the public folder tree, the following actions are available in the action pane.

New Public Folder

Click New Public Folder to create a public folder child under the public folder that is selected in the public folder tree. For more information, see Create a Public Folder.

Export List

Click **Export List** to open the **Export List** dialog box. You can use this dialog box to save the list of recipients in the result pane to a text file. For instructions about how to use the Export List feature, see Export Lists from the Exchange Management Console.

View

Click **View** in the action pane to modify how objects are displayed in the console and to record and view the Exchange Management Shell commands that run in the console. The following options may vary depending on your location in the console tree:

- **View Exchange Management Shell Command Log**
  Click **View Exchange Management Shell Command Log** to view the Shell Command Log dialog box. The Command Log allows you to view all the Shell commands that have been executed in the console. For more information, see Using the Exchange Management Shell Command Log to

Track Tasks Performed in the EMC.

- **Add/Remove Columns**
  Click **Add/Remove Columns** to select which columns you want to display in the result pane and to change the order. The available columns depend on the node that you select. The MMC automatically saves your settings. To revert to the default column view, click **Restore Defaults** in the **Add/Remove Columns** dialog box. For more information, see Add or Remove Columns in the Exchange Management Console.
- **Visual Effects**
  Click **Visual Effects** to set the visual effects to be never on or automatic. Use the visual effects setting to configure how Exchange wizards are displayed. If your connection is slow when running wizards, you can increase performance by turning off visual effects. Use the **Automatic** setting to have the console detect if your system should have visual effects turned on or off.
- **Save Current Filter as Default**
  Click **Save Current Filter as Default** to make the existing filter the default filter for the servers listed in the result pane.
- **Customize**
  Click **Customize** to select the console components and snap-ins to display or hide. These settings apply to the entire console. For more information, see Customize the Exchange Management Console.

Refresh

Click **Refresh** to refresh the information displayed in the result pane.

Public Folder Actions

When you select a public folder in the result pane, the following actions are available for that public folder in the action pane:

Update Content

Click this button to synchronize the public folder content from one server to the other servers on which public folder replicas exist.

For more information, see Update Public Folders.

Mail Enable or Mail Disable

Click these buttons to mail-enable or mail-disable a public folder. For more information, see the following topics:

- Mail-Enable a Public Folder
- Mail-Disable a Public Folder

Remove

Click this button to remove a public folder. For more information, see Remove Public Folders.

Manage Settings

Click this button to open the Manage Public Folder Settings wizard. Use this wizard to manage client permissions for the current public folder and its subfolders.

For more information, see Use the Public Folder Management Console to Manage Public Folder Settings.

Manage Send As Permission

This button is available only for mail-enabled public folders.

Click this button to use the Manage Send As Permission wizard to grant Send As permissions to users or groups for the selected public folder. You can also use this wizard to remove Send As permissions from users or groups

For more information, see Manage Send As Permissions for Mail-Enabled Public Folders.

1.4.9.3 Connect to Public Folder Server

Connect to Public Folder Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Public Folder Management Console allows you to manage public folders on one server at a time. Use the **Connect to Server** dialog box to connect the Public Folder Management Console to a Mailbox server on which a public folder database resides.

Connect to a public folder server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the EMC console tree, click **Toolbox**.
2. In the result pane, click **Public Folder Management Console.**
3. In the action pane, click **Open Tool**. The Public Folder Management Console appears.
4. In console tree of the Public Folder Management Console, click the top-level node.
5. In the action pane, click **Connect to Server**.
6. In **Connect to server**, click **Browse** to view a list of the available Mailbox servers that contain a public folder database.
7. In **Select Public Folder Servers**, select a Mailbox server. To search for a Mailbox server to which to connect, perform one of the following steps:
   - In the **Search** box, type the exact name of the server (or the first few letters of the name), click **Find Now**, and then select a server from the result pane.
   - From the **View** menu, click **Show Filter**. In the **Name**, **Site**, or **Role** boxes, type the filter criteria, and then select a server from the result pane.
8. Click **OK** to close **Select Public Folder Servers**.
9. (Optional) After you select a server, in the **Connect to Server** dialog box, you can select the **Set as Default Server** check box to set the server you selected as the default Exchange server for managing public folders. By default, this is the server to which the Public Folder Management Console connects each time you open the console.

   Note:

   This setting is saved for the user on the computer that is running the Public Folder Management Console. If you open the Public Folder Management Console from another computer or by using a different user account, the default server may be different.

10. Click **Connect**.

1.4.9.4 View or Configure Remote PowerShell Connectivity

View or Configure Remote PowerShell Connectivity

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-10-19*

Use the Remote PowerShell Connectivity dialog box to view or configure the server to which remote Windows PowerShell connects.

Note:

Although the name of this dialog box appears in the user interface as **<Management Console Name> Properties**, it's more commonly referred to as the Remote PowerShell Connectivity dialog box.

This dialog box is available in the following management consoles:

- Exchange Management Console (EMC)
- Public Folder Management Console
- Queue Viewer
- Details Templates Editor

When you change the server to which remote Windows PowerShell connects, you're changing it only for that management console. Changing the remote Windows PowerShell server in one management console doesn't change it for other management consoles.

1. To open the Remote PowerShell Connectivity dialog box, perform one of the following steps:
   From the EMC
   1.a. In the console tree, click **Microsoft Exchange On-Premises**.
   1.b. In the action pane, click **Properties**.
   From the Public Folder Management Console, Queue Viewer, or Details Templates Editor
   1.c. To open the appropriate management console, in the EMC, click **Toolbox**, and then click the console you want.
   1.d. In the action pane, click **Open Tool**.
   1.e. In the action pane of the Public Folder Management Console, Queue Viewer, or Details Templates Editor, click **Properties**.
2. View or configure the following settings:
   2.a. **Administrator identity** This read-only field displays the administrator credentials of the selected Exchange forest.
   2.b. **Connect to the automatically selected server** Click this button if you want to connect to the default server.
   2.c. **Specify a server to connect to** Click this button if you want to use a different server to run remote Windows PowerShell. Click **Browse** to select a server.
3. Click **OK**.

1.4.9.5 Using Unified Messaging Tools

Using Unified Messaging Tools

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-05-24*

The new Unified Messaging (UM) reporting tools added in Microsoft Exchange Server 2010 Service Pack 1 (SP1) can be used to gather usage statistics for UM servers and call statistics for UM-enabled users in your organization. You can access Unified Messaging server statistic reports by using the **Call Statistics** tool and access call logs for UM-

enabled users by using the **User Call Logs** tool.

Both tools are found in the **Toolbox** node of the Exchange Management Console. These reports are displayed in the Exchange Control Panel.

Overview

The reports generated by the new tools in Exchange 2010 SP1 provide aggregated statistical information about calls for UM servers and calls for UM-enabled users in your organization. With the new tools, reports:

- Are more scalable than the reports available in Exchange Server 2007.
- Give tenant administrators, cross-premises administrators, and on-premises administrators the ability to gather statistics about the UM servers and UM-enabled users in their organizations.
- Provide summaries from the data that's gathered. This data can be stored for 90 days and to be archived for up to 2 years to meet retention requirements.

Administrators can use the new reports to:

- Verify how UM servers deployed in the organization are used over a given period of time.
- Plan for UM server capacity for their on-premises organization.
- Easily verify the availability of the voice mail system and UM servers in the organization for a given period of time.
- Verify the overall audio quality for incoming calls to UM servers that are deployed.

To support the UM reporting tools in the EMC, the following cmdlets have been added for SP1:

- **Get-UMCallSummaryReport**
- **Get-UMCallDataRecord**

In Exchange 2007, 3 reports related to the Unified Messaging server role were available to administrators who used System Center Operations Manager. These Unified Messaging reports were based on the values of performance counters on each UM server that was deployed in an organization. However, generating reports using performance counters on each UM server had limitations. When System Center and UM performance counters were used to create reports based on aggregated data from all the UM servers in an organization and a user's call data, the results weren't scalable and couldn't be used in cross-premises organizations.

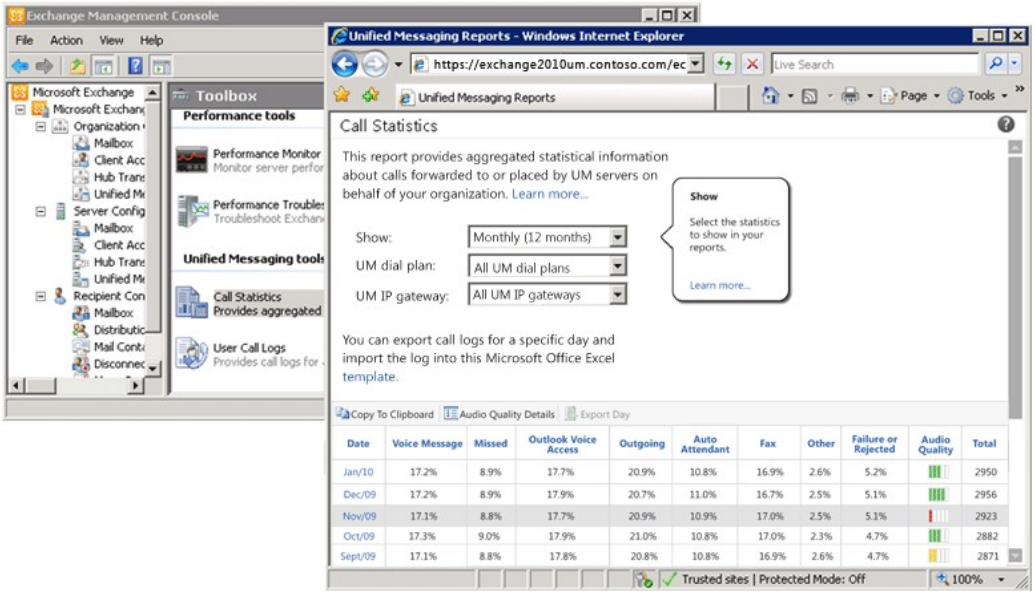
Without the ability to generate scalable reports or reports that could be used cross-premises, the administrator of an organization wouldn't be able to:

- Verify how UM servers deployed in the organization were used over a given period of time. This was a critical issue for a tenant administrator or an administrator in a cross-premises deployment, because no information, including performance counters from the UM server, would be available to them.
- Plan for UM server capacity for their on-premises organization.
- Easily verify the availability of the voice mail system and UM servers in the organization for a given period of time.
- Verify the overall audio quality of the UM servers that were deployed.

Call Statistics

The **Call Statistics** tool provides aggregated statistical information about calls forwarded to or placed by UM servers and can be used by administrators who are interested in overall statistics for the Exchange 2010 Unified Messaging servers in their organization.

Call statistics reports that you initiate in the EMC are displayed in the Exchange Control Panel user interface.



Reports can be filtered to show call statistics by month or by day for the past 90 days or since UM was deployed in your organization. You can then filter these results by UM dial plan and UM IP gateway within your organization.

Call statistics reports display:

- The total number of calls organized by type of call (for example, missed calls, Outlook Voice Access calls, or fax calls).
- Whether the call was accepted or rejected.
- The average audio quality.
- The day or the month covered in the report, or all calls.

You can export the call logs to a Microsoft Office Excel template, or copy the call statistics information to the Clipboard so that it can be pasted into another application. You can use the **Audio Quality Details** button to display more specific information about the call, including the information in the following table.

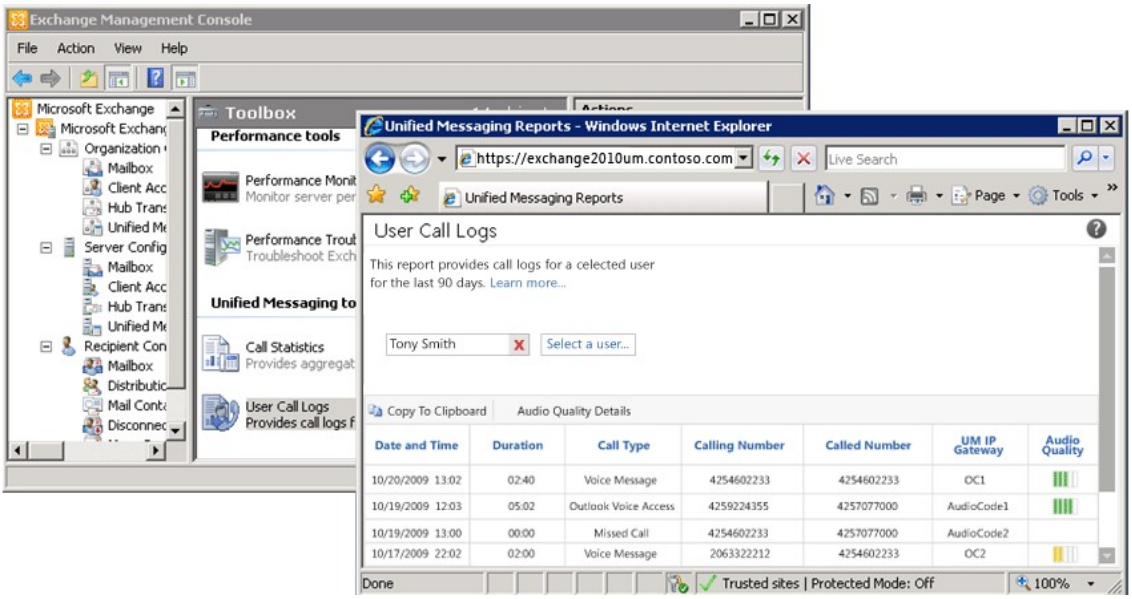
Data	Description
Date	The date and time of the incoming or outgoing call.
UM dial plan	The name of the UM dial plan that's associated with the UM IP gateway used for handling the incoming or outgoing call.
UM IP gateway	The name of the UM IP gateway used for the incoming or outgoing call.
Type of audio codec	The audio codec that's used when sending RTP or SRTP data across a network. The audio codec can be RTAudio (Wide band), RTAudio (Narrow band), G.711, or G.723.1, depending on the audio codec that's configured on the IP gateway or IP PBX or whether Microsoft Office Communications Server 2007 R2 or a later version is used.
NMOS	The mean opinion score for the audio across the network. The UM audio quality indicator will be

	calculated based on the Network MOS (NMOS) that's gathered from the RTP (and SRTP). "Mean opinion score" (MOS) is a number on a scale from 1 to 5 (5 being excellent) that indicates the audio quality of the call. MOS metrics are directly linked to the audio codec that's used. This means that users will get a different audio quality if they use different audio codecs. The following is the NMOS maximum for the audio codecs that are supported: • RTAudio (Wide band): 4.10 • RTAudio (Narrow band): 2.95 • G.711 a/u: 3.61 • G.723.1: 2.63
NMOS degradation	Total NMOS degradation is how far the reported NMOS value is from the top value for the audio codec that was used for the call.
Jitter	The average Jitter for the incoming or outgoing call. In data networks, the term jitter is used as a measure of the packet latency across a network. A network with constant latency has no variation (or jitter). Jitter is sometimes expressed as the average deviation from the network mean latency.
Pack loss	The average percentage of network packet loss during the call.
Round trip time	For the selected call, this is the time, in milliseconds, for a round trip (between the UM IP gateway and the UM server) of the audio packets that carried the voice data over the network.
Burst Loss Duration	The average duration of packet loss during burst losses for the incoming call.

User Call Logs

You can use the **User Call Logs** tool to display the call statistics for a selected UM-enabled user. The report is displayed in the Exchange Control Panel and is useful in helpdesk-type situations where you have to gather information about specific calls for a UM-enabled user to assist them in diagnosing and fixing issues. After you click the **Select a user** button and specify the user, the following information will be displayed for calls of the user you selected:

- Date and time
- Duration of the call
- Type of call
- The calling number
- The called number
- The UM IP gateway
- Audio quality



You can copy the user's call statistics to the Clipboard and then paste them into another application. You can use the **Audio Quality Details** button to display more specific information about the call, including the information in the following table.

Data	Description
Date	The date and time of the incoming or outgoing call.
UM dial plan	The name of the UM dial plan that's associated with the UM IP gateway used for handling the incoming or outgoing call.
UM IP gateway	The name of the UM IP gateway that was used for the incoming or outgoing call.
Type of audio codec	The audio codec that's used when sending RTP or SRTP data across a network. The audio codec can be RTAudio (Wide band), RTAudio (Narrow band), G.711, or G.723.1, depending on the audio codec that's configured on the IP gateway or IP PBX or whether Office Communications Server R2 or a later version is used.
NMOS	The mean opinion score for the audio across the network. The UM audio quality indicator will be calculated based on the Network MOS (NMOS) that's gathered from the RTP (and SRTP). "Mean opinion score" (MOS) is a number on a scale from 1 to 5 (5 being excellent) that indicates the audio quality of the call. MOS metrics are directly linked to the audio codec that's used. This means that users will get a different audio quality if they use different audio codecs. The following is the NMOS maximum for the audio codecs that are supported: • RTAudio (Wide band): 4.10 • RTAudio (Narrow band): 2.95 • G.711 a/u: 3.61

	• G.723.1: 2.63
NMOS degradation	Total NMOS degradation is how far the reported NMOS value is from the top value for the audio codec that was used for the call.
Jitter	The average Jitter for the incoming or outgoing call. In data networks, the term jitter is used as a measure of the packet latency across a network. A network with constant latency has no variation (or jitter). Jitter is sometimes expressed as the average deviation from the network mean latency.
Pack loss	The average percentage of network packet loss during the call.
Round trip time	For the calls within the selected time range, this is the average time, in milliseconds, for a round trip (between the UM IP gateway and the UM server) of the audio packets that carried the voice data over the network.
Burst Loss Duration	The average duration of packet loss during burst losses for the incoming call.
Number of calls sampled	This is the total number of incoming calls that were sampled to determine the audio quality for the call.

For detailed information about other tools in the EMC Toolbox, see Managing Tools in the Toolbox.

1.4.10 Troubleshooting the Exchange Management Console

Troubleshooting the Exchange Management Console

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

While using the Exchange Management Console (EMC), you may encounter problems. Most of these problems will be those associated with the remote Exchange Management Shell. For more information, see "Connection Issues" in Troubleshooting the Exchange Management Shell.

The EMC now checks a user's permissions before loading, so it may take several minutes to load. Use the progress bar located in the lower-left corner of the EMC to view the status of the EMC initialization or to troubleshoot connection issues.

1.5 Exchange Management Shell

Exchange Management Shell

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-10*

Overview of Exchange Management Shell

Learn about the different implementations of the Exchange Management Shell in Microsoft Exchange Server 2010.

Exchange Management Shell Basics

Get detailed information to help you learn how to use the Shell.

Managing Exchange Management Shell Connections

Get step-by-step guidance for managing the Shell, including how to enable and disable users for remote Shell and how to create a manual remote Shell connection.

Cmdlet Extension Agent

Learn about the cmdlet extension agents and how you can add custom scripts that run when Exchange cmdlets are run.

Administrator Audit Logging

Learn about administrator audit logging and how to use it to log the cmdlets that are run by the Shell, the Exchange Management Console, and Exchange Control Panel, and who ran them.

Troubleshooting the Exchange Management Shell

Get troubleshooting tips to help you correct problems that you might experience using the Shell.

Exchange 2010 Cmdlets

Refer to this section for a list of cmdlet Help topics, segmented by feature area.

1.5.1 Overview of Exchange Management Shell

Overview of Exchange Management Shell

Exchange Server 2010 > Exchange Management Shell >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

The Exchange Management Shell, built on Windows PowerShell technology, provides a powerful command-line interface for Microsoft Exchange Server 2010 that enables automation of administrative tasks. With the Shell, you can manage every aspect of Exchange. You can enable new e-mail accounts, configure SMTP connectors, store database properties, store transport agents, and more. The Shell can perform every task that can be performed by the Exchange Management Console and the Exchange Web interface in addition to tasks that can't be performed in those interfaces. In fact, when a task is performed in the console and the Web interface, those interfaces use the Shell to perform the task.

The Shell also provides a robust and flexible scripting platform that can reduce the

complexity of current Microsoft Visual Basic scripts. Tasks that previously required many lines in Visual Basic scripts can now be done by using as little as one line of code in the Shell. The Shell provides this flexibility because it doesn't use text as the basis for interaction with the system, but uses an object model based on the Microsoft .NET platform. This object model enables the Shell cmdlets to apply the output from one command to subsequent commands when they are run.

If you want to start using the Shell immediately, see Exchange Management Shell Basics. Otherwise, read this topic for more information about the Shell in Exchange 2010.

Local Shell and Remote Shell

The Shell in Exchange 2010 uses two methods, local Shell and remote Shell, to connect to servers running Exchange 2010. The following sections describe each of the concepts.

Local Shell

In Microsoft Exchange Server 2007, the Shell consists of a Windows PowerShell host; a Windows PowerShell snap-in, which contains all of the Exchange cmdlets; and some additional custom scripts. Loading all three components enables you to run Exchange cmdlets on the Exchange server you opened the Shell on.

When you open Windows PowerShell on a computer, you create a local session. In simple terms, a session is an environment in which Windows PowerShell runs. Cmdlets, variables, and other Windows PowerShell components within the same session can share data with each other. In Exchange 2007, cmdlets are always run in the local session on the local Exchange 2007 server. Even if you change an object that resides on a different server, the cmdlet is always run on the local Exchange server.

Except for the Edge Transport server role, Exchange 2010 doesn't use the local Shell. Instead, it uses a new concept called remote Shell, which is explained in the next section.

Remote Shell

With Exchange 2010, you can connect to a remote session on a remote Exchange 2010 computer to perform commands on that remote computer. Whether you use the Shell to administer a server you are physically connected to or administer a server across the country, remote Shell is used to perform the operation in Exchange 2010. Only the Edge Transport server role doesn't use remote Shell.

Remote Shell performs almost like the Shell in Exchange 2007. Other than feature changes that occurred between versions, you're likely to continue using the Shell as you did in Exchange 2007. If the Exchange management tools are installed and you want to use the Shell, follow the procedure in the Open the Shell topic.

In Exchange 2010, when you click the Shell shortcut, Windows PowerShell opens. Unlike in Exchange 2007, a Windows PowerShell snap-in for Exchange isn't loaded. Instead, Windows PowerShell connects to the closest Exchange 2010 server using a new required component called Windows Remote Management 2.0, performs authentication checks, and then creates a remote session for you to use. When the remote session is created, you're given access only to the cmdlets and the parameters associated with the management roles you've been assigned. For more information about management roles, see Understanding Role Based Access Control.

A benefit of remote Shell is that you don't need to install Exchange-specific tools on your computer. With just Windows PowerShell and Windows Remote Management installed on any client computer running the Windows Vista operating system with Service Pack 1 (SP1) or Windows Server 2008, you can connect to a remote Exchange 2010 computer to administer it. However, while it's possible to manage an Exchange 2010 server with just Windows PowerShell and Windows Remote Management, we recommend that you install the Exchange management tools on any computer that you use to manage Exchange

2010. Without the Exchange management tools installed, you need to connect to the remote Exchange 2010 server manually, and you don't have access to the additional capabilities that the Exchange management tools provide.

For more information about connecting to Exchange 2010 servers without the Exchange management tools installed, see Create a Manual Remote Shell Connection.

Edge Transport Server Role

Exchange 2010 uses the local Shell only on the Edge Transport server role. This is because each computer that runs the Edge Transport server role is administered individually and because the Edge Transport server role doesn't use Active Directory Domain Services (AD DS). You can open the Shell on an Edge Transport server using the procedure in Open the Shell.

1.5.1.1 Understanding Importing and Exporting Files in the Exchange Management Shell

Understanding Importing and Exporting Files in the Exchange Management Shell

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 uses Windows PowerShell command-line interface remoting to establish a connection between the server or workstation from which you're administering Exchange and the server running Exchange 2010 that you're administering. In Exchange 2010, this is called remote Exchange Management Shell, or remote Shell. Even if you're administering the local Exchange 2010 server, remote Shell is used to make the connection. For more information about local and remote Shell, see Overview of Exchange Management Shell.

How you import and export files to and from an Exchange server has changed in Exchange 2010 due to the implementation of remote Shell. This topic discusses why this new process is required and how to import and export files between a local server or workstation and a remote Exchange 2010 server.

Windows PowerShell Sessions

To understand why you need a special syntax to import and export files in remote Shell, you need to know how the Shell is implemented in Exchange 2010. The Shell uses Windows PowerShell sessions, which are the environments in which variables, cmdlets, and so on, can share information. Every time you open a new Shell window, you create a new session. The cmdlets that are run in each window can access variables and other information stored in that window, but can't access variables in other open Shell windows. This is because they're each contained within their own Windows PowerShell session. Windows PowerShell sessions can also be referred to as runspaces.

Remote Shell in Exchange 2010 has two sessions, the local session and the remote session. The local session is the Windows PowerShell session that's running on your local computer. This session contains all of the cmdlets that ship with Windows PowerShell. It also has access to your local file system.

The remote session is the Windows PowerShell session that's running on the remote Exchange server. This session is where all Exchange cmdlets are run. It has access to the Exchange server's file system.

When you connect to a remote Exchange server, a connection is made between your local session and the remote session on the Exchange server. This connection enables you to run Exchange cmdlets on the remote Exchange server in your local session even though your local computer doesn't have any Exchange cmdlets installed.

Important:

Even if you open the Shell on an Exchange 2010 server, the same connection process takes place and two sessions are created. This means that you must use the same new syntax to import and export files whether you're opening the Shell on an Exchange 2010 server or a remote client workstation.

The Exchange cmdlets that run in the remote session on the remote Exchange server don't have access to your local file system. This means that you can't use Exchange cmdlets, on their own, to import or export files from or to your local file system. Additional syntax needs to be used to transfer the files to and from your local file system so that the Exchange cmdlets running on the remote Exchange server can use the data. For more information about the required syntax, see "Importing and Exporting Files in Remote Shell" later in this topic.

Note:

Importing and exporting files on Edge Transport servers doesn't require any special syntax. For more information about the Edge Transport server role, see "Importing and Exporting Files on Edge Transport Servers" later in this topic.

Importing and Exporting Files in Remote Shell

Remote Shell is used on the Mailbox, Hub Transport, Unified Messaging, and Client Access server roles in Exchange 2010. Importing and exporting files require a specific syntax because they use remote Shell. The Edge Transport server role uses local Shell and uses a different syntax. For more information about the Edge Transport server role, see "Importing and Exporting Files on Edge Transport Servers" later in this topic.

Importing Files in Remote Shell

The syntax to import files in Exchange 2010 is used any time you want to send a file to a cmdlet running on an Exchange 2010 server from your local computer or server. Cmdlets that accept data from a file on your local computer will have a parameter called *FileData* (or something similar). To determine the correct parameter to use, see the Help information for the cmdlet you're using.

The Shell must know what file you want to send to the Exchange 2010 cmdlet, and what parameter will accept the data. To do so, use the following syntax.

```
<Cmdlet> -FileData ([Byte[]]$(Get-Content -Path <local path to file> -Encoding By
```

For example, the following command imports the file C:\MyData.dat into the *FileData* parameter on the **Import-SomeData** fictional cmdlet.

```
Import-SomeData -FileData (Byte[]]$(Get-Content -Path "C:\MyData.dat" -Encoding B
```

The following actions occur when the command is run:

1. The command is accepted by remote Shell.
2. Remote Shell evaluates the command and determines that there's an embedded command in the value being provided to the *FileData* parameter.
3. Remote Shell stops evaluating the **Import-SomeData** command and runs

the **Get-Content** command. The **Get-Content** command reads the data from the MyData.dat file.

4. Remote Shell temporarily stores the data from the **Get-Content** command as a `Byte[]` object so that it can be passed to the **Import-SomeData** cmdlet.
5. Execution of the **Import-SomeData** command resumes. Remote Shell sends the request to run the **Import-SomeData** cmdlet to the remote Exchange 2010 server, along with the object created by the **Get-Content** cmdlet.
6. On the remote Exchange 2010 server, the **Import-SomeData** cmdlet is run, and the data stored in the temporary object created by the **Get-Content** cmdlet is passed to the *FileData* parameter. The **Import-SomeData** cmdlet processes the input and performs whatever actions are required.

Some cmdlets use the following alternate syntax that accomplishes the same thing as the preceding syntax.

```
[Byte[]]$Data = Get-Content -Path <local path to file> -Encoding Byte -ReadCount
Import-SomeData -FileData $Data
```

The same process happens with this alternate syntax. The only difference is instead of performing the entire operation at once, the data retrieved from the local file is stored in a variable that can be referenced after it's created. The variable is then used in the import command to pass the contents of the local file to the **Import-SomeData** cmdlet. Using this two-step process is useful when you want to use the data from the local file in more than one command.

There are limitations that you must consider when importing files. For more information, see "Limitations on Importing Files" later in this topic.

For specific information about how to import data into Exchange 2010, see the Help topics for the feature you're managing.

Limitations on Importing Files

Limits must be set when importing data in remote Shell to preserve the integrity of the data that's being transferred. Transfers that are in progress can't be resumed if they're interrupted. Also, because data being transferred is stored in the remote server's memory, the server must be protected from memory exhaustion caused by excessively large amounts of data.

For these reasons, the amount of data that's transferred to a remote Exchange 2010 server from a local computer or server is limited to the following:

- 500 megabytes (MB) for each cmdlet that's run
- 75 MB for each object that's passed to a cmdlet

If you exceed either of the limits, the execution of the cmdlet and its associated pipeline will stop and you'll receive an error. Consider the examples in the following table to understand how these limits work.

Import data limit examples

Number of objects	Object size (MB)	Total size (MB)	Result of operation
10	40	400	The operation is successful because neither the size of the individual objects exceeds 75 MB nor the total amount of data passed to the cmdlet exceeds 500 MB.

5	80	400	The operation fails because, although the total amount of data passed to the cmdlet is only 400 MB, the size of each individual object exceeds the 75 MB limit.
120	5	600	The operation fails because, although each individual object is only 5 MB, the total amount of data passed to the cmdlet exceeds the 500 MB limit.

Due to the size limits that have been placed on the amount of data that can be transferred between a remote Exchange 2010 server and a local computer, not all cmdlets that once supported importing support this method of data transfer. To determine whether a specific cmdlet supports this method, see the Help information for the specific cmdlet.

These limits should accommodate the majority of typical operations that can be performed on an Exchange 2010 server. If the limits are lowered, you may find that some normal operations fail because they exceed the new limits. If the limits are raised, the data being transferred could take longer to transfer and become more at risk to transient conditions that interrupt the data transfer. Also, you may exhaust the memory on the remote server if you haven't installed enough memory to allow the server to store the entire block of data during transfer. Each possibility could result in data loss and therefore we recommend you don't change the default limits.

Exporting Files in Remote Shell

The syntax to export files in Exchange 2010 is used any time you want to accept data from a cmdlet running on a remote Exchange 2010 server and store the data on your local computer or server. Cmdlets that provide data that you can save to a local file will output an object that will contain the **FileData** property (or something similar). Depending on the cmdlet, the **FileData** property is only populated on the object that's output in specific situations. To determine the correct property to use and when it can be used, see the Help information for the cmdlet you're using.

The Shell must know that you want to save the data stored in the **FileData** property to your local computer. To do so, use the following syntax.

```
<cmdlet> | ForEach { $_.FileData | Add-Content <local path to file> -Encoding Byt
```

For example, the following command exports the data stored in the **FileData** property on the object created by the **Export-SomeData** fictional cmdlet. The exported data is stored in a file you specify on the local computer, in this case MyData.dat.

Note:

This procedure uses the **ForEach** cmdlet, objects, and pipelining. For more information about each, see:
Pipelining
Structured Data

```
Export-SomeData | ForEach { $_.FileData | Add-Content C:\MyData.dat -Encoding Byt
```

The following actions occur when the command is run:

1. The command is accepted by remote Shell.
2. Remote Shell calls the **Export-SomeData** cmdlet on the remote Exchange 2010 server.
3. The output object created by the **Export-SomeData** cmdlet is passed back to the local Shell session via the pipeline.
4. The output object is then piped to the **ForEach** cmdlet, which has a script block.
5. Within the script block, the **FileData** property on the current object in the pipeline is accessed. The data contained within the **FileData** property is piped to the **Add-Content** cmdlet.
6. The **Add-Content** cmdlet saves the data piped from the **FileData** property to the file MyData.dat on the local file system.

For specific information about how to export data from Exchange 2010, see the Help topics for the feature you're managing.

Importing and Exporting Files on Edge Transport Servers

The Edge Transport server role doesn't use remote Shell like the other Exchange 2010 server roles. It uses local Shell. This is because remote Shell requires Active Directory and Role Based Access Control (RBAC) to work. The Edge Transport server role uses Active Directory Lightweight Directory Services (AD LDS).

Because the Edge Transport server role doesn't use remote Shell, the new process for importing and exporting files doesn't apply to it. Cmdlets that are run on the Edge Transport server role can accept files directly without any additional syntax. To find the required syntax for importing and exporting files on Edge Transport servers, see the Help information for the cmdlet you're using.

1.5.2 Exchange Management Shell Basics

Exchange Management Shell Basics

Exchange Server 2010 > Exchange Management Shell >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-14*

WhatIf, Confirm, and ValidateOnly Switches

Modifying Multivalued Properties

Working with Command Output

Comparison Operators

Aliases

User-Defined Variables

Shell Variables

Structured Data

Arrays

Script Security

Scripting with the Exchange Management Shell

For More Information

Overview of Exchange Management Shell

Exchange 2010 Cmdlets

Create a Manual Remote Shell Connection

1.5.2.1 Open the Shell

Open the Shell

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-21*

When you open the Exchange Management Shell, you can perform administrative tasks against servers that run Microsoft Exchange Server 2010.

Are you looking for information about how to connect to an Exchange 2010 server without installing the Exchange management tools? If so, check out Create a Manual Remote Shell Connection.

Prerequisites

- The Exchange management tools have been installed on the computer you want to use to administer Exchange servers. For detailed steps, see Install the Exchange 2010 Management Tools.
- To connect to any server role other than the Edge Transport server role, the user must be enabled to connect to the Shell remotely. For detailed steps, see Enable Remote Exchange Management Shell for a User.
- To connect to any server role other than the Edge Transport server role, the

user must be assigned at least one management role. For detailed steps, see Managing Permissions.

Open the Shell

1. Click **Start** > **All Programs**, and then **Microsoft Exchange Server 2010**.
2. Click **Exchange Management Shell**.

1.5.2.2 Getting Help

Getting Help

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-14*

In Microsoft Exchange Server 2010, the Exchange Management Shell provides many Help resources so that you can use it to its fullest potential. This topic provides the following sections, which describe Help resources and functionality:

- Exchange 2010 Help Exchange 2010 Help contains all the cmdlet Help topics in a role-based and task-based hierarchy. The cmdlet Help topics also link to procedural topics that tell you how to perform specific tasks.
- Help Cmdlets The Shell has several Help cmdlets that enable you to find the appropriate information to accomplish your task.
- Help Views Help in the Shell contains extensive information about the cmdlets available to you. Help views enable you to access the information that you need about a cmdlet.
- Tab Completion You can use tab completion on cmdlet names and parameter names to reduce the amount of typing at a command prompt.

Exchange 2010 Help

Exchange 2010 Help contains the same cmdlet Help information available on each cmdlet in the Shell. However, in Exchange 2010 Help, the Help topics for all the cmdlets are organized by server role and administration task so that you can easily find specific cmdlets associated with the task that you want to perform. Also, cmdlet topics in Exchange 2010 Help are linked to topics that introduce you to the features that they manage, show you how to use the cmdlets to manage that feature, and provide specific details about the feature or common scenarios.

For more information about the cmdlet Help topics available in Exchange 2010 Help, see Exchange 2010 Cmdlets.

Help Cmdlets

The following tables provide examples of how to use the **Get-Help** and **Get-Command** cmdlets to access the Help information available for each cmdlet in the Shell.

Important:
To view a list of Exchange cmdlets that match a string that you specify, use the **Get-ExCommand** cmdlet. For more information, see the "Examples of how to use miscellaneous Help commands" table later in this section.

The following table provides examples of how the **Get-Help** cmdlet is used.

Examples of how to use the Get-Help cmdlet

Examples	Description
`Get-Help`	When you use the **Get-Help** cmdlet by itself, it gives you basic instructions on how to use the Shell Help system.
`Get-Help <cmdlet>`	When you give the **Get-Help** cmdlet a cmdlet as an argument, it displays the Help information for that cmdlet. For example, to retrieve the Help information for the **Get-SystemMessage** cmdlet, use the following command. `Get-Help Get-SystemMessage`
`Get-Help About_*`	The **Get-Help About_*** command provides a list of all general Shell Help topics to help you better understand and use the Shell. If you want to learn more about a topic in the list displayed, run the **Get-Help About_<*feature*>** command. For example, if you want to learn more about wildcards, use the following command. `Get-Help About_wildcards.`
`Get-Help <cmdlet> -Detailed`	For a description, see the Help Views section later in this topic.
`Get-Help <cmdlet> -Full`	For a description, see the Help Views section later in this topic.
`Get-Help <cmdlet> -Examples`	For a description, see the Help Views section later in this topic.
`Get-Help <cmdlet> -Parameter <parameter name>`	For a description, see the Parameters Filter section later in this topic.
`Get-Help <cmdlet> -Online`	For a description, see the Online Help section later in this topic.

The following table provides examples of how the **Get-Command** cmdlet is used.

Examples of how to use the Get-Command cmdlet

Examples	Description
`Get-Command`	The **Get-Command** cmdlet provides a list of all the cmdlets available to the Shell. The **Get-Command** cmdlet allows for wildcard character expansion.
`Get-Command *<string>*`	When you enclose a string with wildcard characters (*), the **Get-Command** cmdlet returns a list of all cmdlets and functions that are available to you that contain that string. For example, to find all cmdlets or functions that contain the string "`mailbox`",

	use the command `Get-Command *mailbox*`. Exchange 2010 cmdlets are shown as functions in the output of the **Get-Command** cmdlet.
`Get-Command -Noun <CmdletNoun>`	The **Get-Command -Noun <***CmdletNoun***>** command lists all the cmdlets that exist with the specified noun. This command is useful when you want to view a list of all cmdlets associated with a particular feature. For example, the **Get-Command -Noun SystemMessage** command returns all the cmdlets available for the SystemMessage feature.
`Get-Command -Verb <CmdletVerb>`	The **Get-Command -Verb <***CmdletVerb***>** command lists all the cmdlets that exist with the specified verb. This command is useful when you want to view a list of all cmdlets associated with a particular action. For example, the **Get-Command -Verb Enable** command returns all cmdlets available that perform the enable action.

The following table provides examples of how to use miscellaneous Help commands.

Examples of how to use miscellaneous Help commands

Examples	Description
`Get-ExCommand`	The Get-ExCommand command returns a list of all Exchange cmdlets available to you.
`Get-ExCommand *<string>*`	When you enclose a string with wildcard characters (*), the **Get-ExCommand** command returns a list of all Exchange cmdlets that are available to you that contain that string. For example, to find all Exchange cmdlets that contain the string "mailbox", use the command `Get-ExCommand *mailbox*`. Exchange 2010 cmdlets are shown as functions in the output of the **Get-ExCommand** command.
`QuickRef`	The **QuickRef** command opens a link to a printable HTML chart that lists the most frequently used Shell cmdlets. This command works only if the Exchange management tools are installed. To open this chart directly, see Exchange Management Shell Quick Reference for Exchange 2010.
`<Cmdlet> -?`	Use the **<Cmdlet> -?** command together with any cmdlet to find the same Help

	information available when you use the **Get-Help** cmdlet. For example, type `Get-SystemMessage -?` to display detailed Help for the **Get-SystemMessage** cmdlet.
`Get-Tip`	The **Get-Tip** cmdlet generates a new Exchange Management Shell Tip of the Day. This cmdlet works only if the Exchange management tools are installed.
`Get-ExBlog`	The **Get-ExBlog** cmdlet opens your default browser to display the Exchange Team blog. This cmdlet works only if the Exchange management tools are installed.

Help Views

When a cmdlet is specified as a parameter of the **Get-Help** cmdlet, the Help information for the specified cmdlet is displayed. In some cases, the information returned can be extensive, and you may only want to see specific information. Help views enable you to view specific information about a cmdlet without having to sort through information that you may not need.

The Shell has four views that present different types of information. You can also retrieve a specific parameter or set of similar parameters.

The following table shows the sections displayed in each view.

Help views in the Exchange Management Shell

Help view	Default	Detailed	Full	Examples
Synopsis	X	X	X	X
Syntax	X	X	X	
Description	X	X	X	
Parameters without metadata		X		
Parameters with metadata			X	
Inputs			X	
Outputs			X	
Errors			X	
Examples		X	X	X
Related links	X		X	
Remarks	X	X		

The following table describes each view and provides an example of a command that calls each view.

Examples of Exchange Management Shell Help views

Help view	Examples	Description
Default	`Get-Help Set-Mailbox`	The Default view is displayed when you use the command `Get-Help` *<cmdlet>*.
`Detailed`	`Get-Help Set-Mailbox -Detailed`	The `Detailed` view is displayed when you use the command `Get-Help` *<cmdlet>* `-Detailed`. The parameters returned in the `Parameters` section don't include parameter metadata. For more information, see Parameters.
`Full`	`Get-Help Set-Mailbox - Full`	The `Full` view is displayed when you use the command `Get-Help` *<cmdlet>* `-Full`. The parameters returned in the `Parameters` section include the following parameter metadata: • `Required?` • `Position?` • `Default value` • `Accept pipeline input?` • `Accept wildcard characters?` For more information, see Parameters.
`Examples`	`Get-Help Set-Mailbox -Examples`	The `Examples` view is displayed when you use the command `Get-Help` *<cmdlet>* `-Examples`.

Parameters Filter

In addition to these four Help views, you can also access the description and metadata about a specific parameter or set of similar parameters. You can specify the parameter together with the `Get-Help` *<cmdlet>* command. The following example shows how you can display the description of the *ForwardingAddress* parameter on the **Set-Mailbox** cmdlet:

```
Get-Help Set-Mailbox -Parameter ForwardingAddress
```

You can also display a set of similar parameters that exist on a specific cmdlet if you specify the partial name of a parameter together with a wildcard character (*). The following example shows how you can display all the parameters on the **Set-Mailbox** cmdlet that contain the word Quota.

```
Get-Help Set-Mailbox -Parameter *Quota*
```

Note:

When you use the *Parameter* parameter with the **Get-Help** cmdlet to retrieve Help information for a cmdlet that has only one parameter, the **Get-Help** cmdlet doesn't return any results, even if you use the wildcard character (*). This is a known issue in Microsoft Windows PowerShell.

Online Help

If a cmdlet has many parameters, it may be difficult to read the Help information for that cmdlet in the Shell. With Exchange 2010, the *Online* switch has been made available. The *Online* switch tells the Shell to open your default Web browser and browse to the online Help topic for the cmdlet. The online Help topic is the same as the Help for the cmdlet in the Shell with the additional benefits of being able to view the topic in a larger window, to

search the topic for terms, or to click related links embedded within the topic. For example, to view online Help for the **Set-Mailbox** cmdlet, use the following command:

```
Get-Help Set-Mailbox -Online
```

Using the *Online* switch requires that your computer has a connection to the Internet.

Tab Completion

You can use tab completion to reduce typing when you use the Shell. After you type a partial cmdlet name, and then press the TAB key, the Shell completes the cmdlet name if a matching cmdlet is found. If multiple matching cmdlet names are found, each cmdlet name cycles through after you press the TAB key. When you use tab completion with cmdlet names, you must supply at least the verb and the hyphen (-). The following examples show how you can use tab completion when you enter a cmdlet name:

```
Get-Transport<Tab>
Enable-<Tab>
```

Each time you press the TAB key in the first example, the Shell cycles through all the cmdlet names that start with **Get-Transport**. In the second example, the Shell cycles through all cmdlets with the verb **Enable**.

As with cmdlet names, you can also use tab completion when you want the Shell to complete the partial parameter name that you entered. When you use tab completion with parameter names, you must specify the full cmdlet name either by typing it or by using tab completion. The following examples show how you can use tab completion when you enter a parameter name:

```
Set-Mailbox -Email<Tab>
New-TransportRule -Cond<Tab>
```

Each time you press the TAB key in the first example, the Shell cycles through all the parameter names that start with *Email* on the **Set-Mailbox** cmdlet. In the second example, when you press the TAB key, the Shell completes the *Conditions* parameter on the **New-TransportRule** cmdlet.

1.5.2.3 Cmdlets

Cmdlets

Exchange Server 2010 > Exchange Management Shell > Exchange Management Shell Basics >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-11*

A *cmdlet*, pronounced "command-let", is the smallest unit of functionality in the Exchange Management Shell. Cmdlets resemble built-in commands in other shells, for example, the `dir` command found in `cmd.exe`. Like these familiar commands, cmdlets can be called directly from the command line in the Shell and run under the context of the Shell, not as a separate process.

Note:

Since Microsoft Exchange Server 2007, there have been changes to how Exchange 2010 uses cmdlets internally due to the use of Windows PowerShell remoting functionality. These changes have little to no impact on how you need to use cmdlets, but they may offer additional flexibility in how you manage your Exchange servers.

Cmdlets are usually designed around repetitive administrative tasks, and, in the Shell, several hundred cmdlets are provided for Exchange-specific management tasks. These cmdlets are available in addition to the non-Exchange system cmdlets included in the basic Windows PowerShell shell design. For information about how to open the Exchange Management Shell, see Open the Shell.

All cmdlets in the Shell are presented in verb-noun pairs. The verb-noun pair is always separated by a hyphen (-) without spaces, and the cmdlet nouns are always singular. Verbs refer to the action that the cmdlet takes. Nouns refer to the object on which the cmdlet takes action. For example, in the **Get-SystemMessage** cmdlet, the verb is **Get**, and the noun is **SystemMessage**. All Shell cmdlets that manage a specific feature share the same noun. The following table provides examples of some verbs available in the Shell.

Note:

By default, if the verb is omitted, the Shell assumes the **Get** verb. For example, when you call **Mailbox**, you retrieve the same results as when you call **Get-Mailbox**.

Examples of verbs in the Exchange Management Shell

Verb	Description
Disable	**Disable** cmdlets set the `Enabled` status of the specified Exchange 2010 object to `$False`. This prevents the object from processing data even though the object exists.
Enable	**Enable** cmdlets set the Enabled status of the specified Exchange 2010 object to `$True`. This enables the object to process data.
Get	**Get** cmdlets retrieve information about a specific Exchange 2010 object. **Note:** Most **Get** cmdlets only return summary information when you run them. To tell the **Get** cmdlet to return verbose information when you run a command, pipe the command to the **Format-List** cmdlet. For more information about the **Format-List** command, see Working with Command Output. For more information about pipelining, see Pipelining.
Install	**Install** cmdlets install a new object or feature on an Exchange 2010 server.
Move	**Move** cmdlets relocate the specified Exchange 2010 object from one container or server to another.
New	**New** cmdlets create new Exchange 2010 object.
Remove	**Remove** cmdlets delete the specified Exchange 2010 object.
Set	**Set** cmdlets modify the properties of an existing Exchange 2010 object.
Test	**Test** cmdlets test specific Exchange 2010 components and provide log files that you

	can examine.
Uninstall	**Uninstall** cmdlets remove an object or feature from an Exchange 2010 server.

The following list of cmdlets is an example of a complete cmdlet set. This cmdlet set is used to manage the delivery status notification (DSN) message and mailbox quota message features of Exchange 2010:

- **Get-SystemMessage**
- **New-SystemMessage**
- **Remove-SystemMessage**
- **Set-SystemMessage**

For More Information

Exchange Management Shell Basics

1.5.2.4 Parameters

Parameters

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-14*

Most cmdlets rely on parameters. Parameters are elements that provide information to the cmdlet, either identifying an object and its attributes to act upon, or controlling how the cmdlet performs its task. The name of the parameter is preceded by a hyphen (-) and followed by the value of the parameter as follows:

```
Verb-Noun -ParameterName <ParameterValue>
```

In this simple example, the hyphen in front of the parameter name tells the Exchange Management Shell that the word that immediately follows the hyphen is a parameter that is passed to the cmdlet and that the next separate word after the parameter is the value of the parameter.

This topic discusses the following parameters and their behavior in the Shell:

Positional Parameters

Boolean Parameters

Switch Parameters

Common Parameters

Positional Parameters

A positional parameter is a parameter that lets you specify the parameter's value without specifying the parameter's name. A parameter is a positional parameter if the `Parameter Position` attribute is an integer. This integer indicates the position on the command line where the cmdlet can find the parameter's value. For more information about the various attributes that make up a parameter, see the Parameter Details section later in this topic.

Most cmdlets only have one positional parameter, *Identity*. *Identity* is always in position 1 if it is available on a cmdlet. Some cmdlets have multiple positional parameters. With these cmdlets, you can specify the values for each positional parameter in the order specified by the `Parameter Position` attribute on each parameter. The values for each parameter must be in the correct position on the command line to work correctly.

If a parameter isn't a positional parameter, it's considered to be a `named` parameter. You must specify the parameter name and parameter value for `named` parameters.

The following two commands perform the same task of returning configuration information for a Receive connector that is named `"Contoso"`.

```
Get-ReceiveConnector -Identity "Contoso"
Get-ReceiveConnector "Contoso"
```

The following two commands perform the same task. The positional parameter values in the first command are placed in the exact order as required by the Parameter Position attribute on each parameter.

```
Set-ExampleCmdlet "Seattle Users" $True "Contoso.com"
Set-ExampleCmdlet -Name "Seattle Users" -Enabled $True -Domain "Contoso.com"
```

Parameter Details

Attributes, also called metadata, on each parameter are included in the PARAMETERS section of the Shell Help that is retrieved by the **Get-Help** cmdlet. The following example is from the **Get-Service** cmdlet.

```
PARAMETERS
    -ServiceName System.String[]
        Parameter required?           false
        Parameter position?           1
        Default value                 *
        Accept pipeline input?       true
        Accept wildcard characters?  True
```

This example from the **Get-Service** cmdlet includes some specific details about the value types that can be passed for the *ServiceName* parameter. Not all cmdlets include such details. However, most cmdlets do include some settings for each parameter as described in the following table.

Parameter settings

Setting	Description
Required?	Indicates whether the cmdlet will run if you don't supply the parameter. When *Required?* is set to `True`, the Shell prompts you for the value if the parameter isn't supplied on the command line.
Position?	Indicates whether you must put the parameter name in front of the parameter value. When *Position?* is set to `Named`, the parameter name is required. When *Position?* is set to an integer, the name isn't required, only the value.
Default value	Indicates the default value for this parameter if no other value is provided.

Accept pipeline input?	Indicates whether the parameter can receive its value as an input through a pipeline from another cmdlet.
Accept wildcard characters?	Indicates whether the parameter's value can contain wildcard characters and can be matched to multiple objects.

Boolean Parameters

Boolean parameters are used in the Shell to determine, among other things, whether a feature or option is enabled, `$True`, or disabled, `$False`. The value that you assign to a Boolean parameter is stored in the configuration of the object that you're modifying. When you supply a value to a Boolean parameter, you must use the values `$True` or `1`, or `$False` or `0`. The dollar sign ($) must be included with `$True` and `$False`. You may notice that some commands insert a colon (:) between the Boolean parameter name and Boolean value. On Boolean parameters, this colon is optional. The following example disables the Receive connector "Contoso.com":

```
Set-ReceiveConnector "Contoso.com" -Enabled $False
```

Switch Parameters

Switch parameters are commonly used to indicate whether the current command should proceed with additional prompting or to enable an alternate option for the command being run. This state isn't saved between commands. Switch parameters resemble Boolean parameters, but they serve different purposes and require different syntax. Switch parameters don't require a value. When you specify a switch parameter on a command line without a value, the parameter evaluates to `$True`.

On some cmdlets, the cmdlet may run as though the switch parameter was included on the command line, even if you didn't include it yourself. This behavior commonly occurs with the *Confirm* switch parameter on cmdlets that can cause data loss if they're inadvertently run. In the case of the *Confirm* switch parameter on such a cmdlet, the cmdlet will always prompt for confirmation before running unless you explicitly tell the cmdlet not to by overriding the switch parameter. You can override the switch parameter by including the *Confirm* switch parameter on the command line with a value of `:$False`. Unlike any other parameters, the colon character (`:`) is required between switch parameters and the value `$False`.

The first of the following examples instructs the **Start-EdgeSynchronization** cmdlet to display a confirmation prompt before it lets EdgeSync synchronization start. The second example instructs the **Remove-ReceiveConnector** cmdlet not to display a confirmation prompt before deleting the Receive connector "Contoso.com":

```
Start-EdgeSynchronization -Confirm
Remove-ReceiveConnector "Contoso.com" -Confirm:$False
```

Common Parameters

Common parameters are parameters that are automatically added to all commands by the Shell. These parameters perform functions that can be used with, or used by, the commands that they're run against. The following table lists all the common parameters that are available in the Shell. Three additional parameters, *WhatIf, Confirm*, and *ValidateOnly*, may also be added to cmdlets. For more information about these additional parameters, see WhatIf, Confirm, and ValidateOnly Switches.

Common parameters in the Exchange Management Shell

Parameter name	Required	Type	Description
Debug	Optional	System.Boolean	The *Debug* parameter instructs the command to provide programmer-level detail about the operation.
ErrorAction	Optional	System.Enum	The *ErrorAction* parameter controls the behavior of the command when an error occurs. Values are as follows: • `Continue`, which is the default value • `Stop` • `SilentContinue` • `Inquire`, which asks the user what to do
ErrorVariable	Optional	System.String	The *ErrorVariable* parameter specifies the name of the variable that the command uses to store errors that are encountered during processing. This variable is populated in addition to `$ERROR`.
OutVariable	Optional	System.String	The *OutVariable* parameter specifies the name of the variable that the command uses for objects that are output from this command. This is equivalent to piping the command to `Set-Variable <name> -Passthru:$true`
Verbose	Optional	System.Boolean	The *Verbose* parameter instructs the command to provide detailed information about the operation. **Note:** Most **Get** cmdlets only return summary information that contains the most commonly used properties when you run them. To tell the **Get** cmdlet to return all of the properties on an object, pipe the command to the **Format-List** cmdlet. For more information, see Pipelining and Working with Command Output.

For More Information

Exchange Management Shell Basics

1.5.2.5 Identity

Identity

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-03*

The *Identity* parameter is a special parameter that you can use with most cmdlets. The *Identity* parameter gives you access to the unique identifiers that refer to a specific object in Microsoft Exchange Server 2010. This capability lets you perform actions on a specific Exchange 2010 object.

The following sections describe the Identity parameter and provide examples of how you can use it effectively:

Characteristics of the Identity Parameter

The primary unique identifier of an object in Exchange 2010 is always a GUID. A GUID is a 128-bit identifier, such as `63d64005-42c5-4f8f-b310-14f6cb125bf3`. This GUID never repeats and is therefore always unique. However, you don't want to type such GUIDs regularly. Therefore the *Identity* parameter typically also consists of the values of other parameters, or combined set of values from multiple parameters on a single object. These values are also guaranteed to be unique across that set of objects. You can specify the values of these other parameters, such as *Name* and *DistinguishedName*, or they can be system-generated. The additional parameters that are used, if any, and how they are populated, depend on the object you refer to.

The *Identity* parameter is also considered a positional parameter. The first argument on a cmdlet is assumed to be the *Identity* parameter when no parameter label is specified. This reduces the number of keystrokes when you type commands. For more information about positional parameters, see Parameters.

The following example shows the use of the *Identity* parameter by using the Receive connector's unique *Name* parameter value. This example also shows how you can omit the *Identity* parameter name because *Identity* is a positional parameter.

```
Get-ReceiveConnector -Identity "From the Internet"
Get-ReceiveConnector "From the Internet"
```

Like all objects in Exchange 2010, this Receive connector can also be referred to by its unique GUID. For example, if the Receive connector named `"From the Internet"` is also assigned the GUID `63d64005-42c5-4f8f-b310-14f6cb125bf3`, you can also retrieve the Receive connector by using the following command:

```
Get-ReceiveConnector 63d64005-42c5-4f8f-b310-14f6cb125bf3
```

Return to top

Wildcard Characters in Identity

Some **Get** cmdlets can accept a wildcard character (*) as part of the value you submit to *Identity* when you run the cmdlet. By using a wildcard with the *Identity* parameter, you can specify a partial name and retrieve a list of objects that match that partial name. You can place a wildcard character at the beginning or the end of the *Identity* value, but you can't place the character in the middle of a string. For example, the commands `Get-Mailbox David*` and `Get-Mailbox *anders*` are valid, but `Get-Mailbox Reb*ca` isn't a valid command.

Some **Get** cmdlets retrieve objects in Exchange 2010 that are organized in a hierarchical or parent and children relationship. That is, there may be a collection of parent objects that also contain their own child objects. Objects that have a parent and child relationship may have an *Identity* with the syntax of `<parent>\<child>`.

When an *Identity* parameter has a syntax of `<parent>\<child>`, some cmdlets enable you to use a wildcard character (*) to replace all or some of the parent or child names. For example, if you want to find all of the child objects named "Contoso" in all parent objects, you could use the syntax `"*\Contoso"`. Likewise, if you want to find all of the child objects with a partial name of "Auth" that exist under the `"ServerA"` parent object, you could use the syntax `"ServerA\Auth*"`.

Some, but not all, cmdlets allow you to specify just the child portion of the Identity parameter when you run a command. When you do this, the cmdlets default to the current parent object being accessed. For example, two receive connectors named "Contoso Receive Connector" exist on both MBX1 and MBX2. If you run the command `Get-ReceiveConnector "Contoso Receive Connector"` on MBX2, only the receive connector on the server MBX2 is returned.

The specific behavior of the Identity parameter and wildcard characters is dependent on the cmdlet that's being run. For more information about the cmdlet you're running, see the feature-specific content for that cmdlet.

Return to top

Examples of the Identity Parameter

The examples described in this topic illustrate how the *Identity* parameter can accept different unique values to refer to specific objects in the Exchange 2010 organization. These examples also illustrate how the *Identity* parameter label can be omitted to reduce the number of keystrokes when you type commands.

DSN Messages

The examples in this section refer to the delivery status notification (DSN) messages that can be configured in an Exchange 2010 organization. The first example shows how to retrieve DSN 5.4.1 by using the **Get-SystemMessage** cmdlet. In the **Get-SystemMessage** cmdlet, the *Identity* parameter consists of several pieces of data that are configured on each DSN message object. These pieces of data include the language that the DSN is written in, whether the DSN is internal or external in scope, and the DSN message code as in the following example:

```
Get-SystemMessage en\internal\5.4.1
```

You can also retrieve this DSN message by using its GUID as in the following example, because all objects in Exchange 2010 have a GUID:

```
Get-SystemMessage 82ca7bde-1c2d-4aa1-97e1-f298a6f10222
```

For more information about the makeup of the *Identity* parameter when it's used with the **SystemMessage** cmdlets, see DSN Message Identity.

Management Role Entries

The examples in this section refer to management role entries that make up management roles in Exchange 2010. Management roles are used to control the permissions that are granted to administrators and end users. Management role entries are made up of two parts: the management role they're associated with and a cmdlet. The Identity parameter is likewise made up of both the management role name and the cmdlet name. For example, the following is the role entry for the **Set-Mailbox** cmdlet on the `Mail Recipients` role:

```
Mail Recipients\Set-Mailbox
```

The `Mail Recipients\Set-Mailbox` role entry is one of several entries on the `Mail Recipients` role. To view all the role entries on the `Mail Recipients` role, you can use the following command:

```
Get-ManagementRoleEntry "Mail Recipients\*"
```

To view all the role entries on the `Mail Recipients` role that contain the string "`Mailbox`", use the following command:

```
Get-ManagementRoleEntry "Mail Recipients\*Mailbox*"
```

To view all the management roles where **Set-Mailbox** is one of the role entries, use the following command:

```
Get-ManagementRoleEntry *\Set-Mailbox
```

With role entries you can use the wildcard character in a variety of ways to query Exchange 2010 for the information you're interested in.

For more information about management roles, see Understanding Permissions.

Return to top

For More Information

Exchange Management Shell Basics

1.5.2.6 Syntax

Syntax

Exchange Server 2010 > Exchange Management Shell > Exchange Management Shell Basics >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-07-09*

This topic explains how to read the Exchange Management Shell parameter sets and examples in the Exchange Help documentation and how to format a command so that the Shell can process the command. In the Shell and the Microsoft Exchange Server 2010 Help, parameter sets are displayed in the Syntax section of a cmdlet Help topic. For more information about cmdlet help, see Getting Help.

See the following sections:

Command Conventions in the Exchange Management Shell

The Shell follows several command conventions that help you understand what information is required or optional when you run a command and how you must present the parameters and their values. See the "Parameter Sets" section later in this topic for examples of how parameter sets are presented in the Shell Help and Exchange 2010 Help.

The following table lists these command conventions.

Exchange Management Shell command conventions

Symbol	Description
-	A hyphen indicates that the next word on the command line is a parameter. The most common parameter is *Identity*. For more information, see Parameters.
< >	Angle brackets are used to enclose parameter values. These values can be choices or names. For example, in `-Parameter1 <1 | 2 | 3>`, the numbers represent specific value choices. In `-Parameter2 <ServerName>`, `ServerName` represents the actual value.
[ ]	Square brackets are used to enclose an optional parameter and its value. A parameter and its value that are not enclosed in square brackets are required.
|	When the pipe symbol is used in a parameter value list, such as `-Parameter1 <1 | 2 | 3>`, it indicates a choice between available values. This convention applies to `System.Enum` parameters and `System.Boolean` parameters.

These command conventions help you understand how a command should be constructed. Don't type these conventions when you enter the command on the command line.

Parameter Sets

In the Exchange Help documentation, all cmdlets display their associated parameters in parameter sets. Parameter sets are groupings of parameters that can be used with each other. Parameters that exist in one parameter set, but not in another parameter set, are mutually exclusive. They can't be used together.

Although all cmdlets have parameter sets, many only have one set of parameters. This means that all the parameters on that cmdlet can be used with each other. Other cmdlets may have several parameter sets. The following example displays the parameter sets that are available on the **New-SystemMessage** cmdlet:

```
New-SystemMessage -DsnCode <EnhancedStatusCode> -Internal <$true | $false>
-Language <CultureInfo> -Text <String> [-DomainController <String>] [-Templ
ateInstance <MshObject>]
New-SystemMessage -Language <CultureInfo> -QuotaMessageType <WarningMailbox
UnlimitedSize | WarningPublicFolderUnlimitedSize | WarningMailbox | Warning
PublicFolder | ProhibitSendMailbox | ProhibitPostPublicFolder | ProhibitSen
dReceiveMailBox> -Text <String> [-DomainController <String>] [-TemplateInst
ance <MshObject>]
```

The **New-SystemMessage** cmdlet has two parameter sets. The first parameter set contains the *DsnCode* parameter and *Internal* parameter, and the second parameter set contains the *QuotaMessageType* parameter. This means that the *DsnCode* parameter and *Internal* parameter can be used with each other. But, they can't be used with the *QuotaMessageType* parameter. The remaining parameters, *Language*, *Text*, *DomainController*, and *TemplateInstance*, are listed in both parameter sets. This means that they can be used with the *DsnCode* parameter and *Internal* parameter and with the *QuotaMessageType* parameter.

Parameter sets can indicate that a single cmdlet may have multiple uses. For example, you can use the **New-SystemMessage** cmdlet to configure customized delivery status notification (DSN) messages or configure customized mailbox quota limit messages. However, cmdlets typically have multiple parameter sets because one parameter may perform a function that is incompatible with another parameter. For example, the following example displays the parameter sets for the **New-AddressList** cmdlet:

```
New-AddressList -Name <String> [-ConditionalCompany <MultiValuedProperty>]
[-ConditionalCustomAttribute1 <MultiValuedProperty>] [-ConditionalCustomAtt
ribute10 <MultiValuedProperty>] [-ConditionalCustomAttribute11 <MultiValued
Property>] [-ConditionalCustomAttribute12 <MultiValuedProperty>] [-Conditio
nalCustomAttribute13 <MultiValuedProperty>] [-ConditionalCustomAttribute14
<MultiValuedProperty>] [-ConditionalCustomAttribute15 <MultiValuedProperty>
] [-ConditionalCustomAttribute2 <MultiValuedProperty>] [-ConditionalCustomA
ttribute3 <MultiValuedProperty>] [-ConditionalCustomAttribute4 <MultiValued
Property>] [-ConditionalCustomAttribute5 <MultiValuedProperty>] [-Condition
alCustomAttribute6 <MultiValuedProperty>] [-ConditionalCustomAttribute7 <Mu
ltiValuedProperty>] [-ConditionalCustomAttribute8 <MultiValuedProperty>] [-
ConditionalCustomAttribute9 <MultiValuedProperty>] [-ConditionalDepartment
<MultiValuedProperty>] [-ConditionalStateOrProvince <MultiValuedProperty>]
[-Confirm [<SwitchParameter>]] [-Container <AddressListIdParameter>] [-Disp
layName <String>] [-DomainController <Fqdn>] [-IncludedRecipients <Nullable
>] [-Organization <OrganizationIdParameter>] [-RecipientContainer <Organiza
tionalUnitIdParameter>] [-WhatIf [<SwitchParameter>]] [<CommonParameters>]
New-AddressList -Name <String> [-Confirm [<SwitchParameter>]] [-Container <
AddressListIdParameter>] [-DisplayName <String>] [-DomainController <Fqdn>]
 [-Organization <OrganizationIdParameter>] [-RecipientContainer <Organizati
onalUnitIdParameter>] [-RecipientFilter <String>] [-WhatIf [<SwitchParamete
r>]] [<CommonParameters>]
```

In the **New-AddressList** cmdlet, the first parameter set lists parameters that let you create a new address list based on values supplied to the *Company*, *Department*, *IncludedRecipients*, and *StateOrProvice* parameters. However, you can also create a new address list by using a custom filter that is specified with the *RecipientFilter* parameter. When you create a new address list, a custom filter that was specified by using the *RecipientFilter* parameter overrides anything that was configured by using the parameters

that exist in the first parameter set. Therefore, the *RecipientFilter* parameter is put in its own parameter set. Exchange 2010 doesn't let you specify both parameters on the same command line. As with the **New-SystemMessage** cmdlet, the remaining parameters that exist in both parameters sets in the **New-AddressList** cmdlet can be used in any combination.

Use of Quotation Marks

Double quotation marks (") are most commonly used to enclose a value that has spaces when you pass that value to a parameter. For example, if you want to pass `Contoso Receive Connector` to the *Name* parameter of the **Set-ReceiveConnector** cmdlet, you must enclose `Contoso Receive Connector` in quotation marks as in the following example:

```
Set-ReceiveConnector -Name "Contoso Receive Connector"
```

If you don't enclose the string in quotation marks, the Shell tries to interpret each word in the string as a new argument on the command line and displays an error.

In the Shell, double quotation marks and single quotation marks (') have different meanings. When you enclose a string in double quotation marks, the Shell replaces any variables with a matching value. For example, assume the value `ServerName` is assigned to the variable `$Server`. Then, assume the following command is entered on the command line:

```
"$Server Example"
```

The following output is displayed:

```
ServerName Example
```

The variable `$Server` is replaced by the value `ServerName` in the output.

When you enclose a string in single quotation marks, the Shell doesn't try to replace variables with a matching value. Assume the variable `$Server` is still assigned the value `ServerName`. Then assume the following command is entered on the command line:

```
'$Server-Example'
```

The following output is displayed:

```
$Server-Example
```

The variable `$Server` has not been replaced with a value because the Shell doesn't interpret variables that are included in text that is enclosed in single quotation marks.

For more information about variables, see User-Defined Variables and Shell Variables.

Escape Character

You may also want to display some characters, such as the dollar sign ($), double or single quotation marks, or back quotation mark (` ). These characters have special meanings when you use them in the Shell. To instruct the Shell not to interpret these characters and to display them when they are included in a string that is enclosed with double quotation marks, you must use the back quotation mark escape character ( `). For example, type the following text on the command line:

```
"The price is `$23."
```

The following output is displayed:

```
The price is $23.
```

Because we used the back quotation escape character with the dollar sign ($), the Shell doesn't interpret the $ as the beginning of a variable.

If you enclose a string in single quotation marks, you don't have to escape any character unless you want to display a single quotation mark in a string. If you want to display a single quotation mark in a string that is enclosed in single quotation marks, you must use two single quotation marks (''). For example, type the following on the command line:

```
'Don''t confuse two single quotation marks with a double quotation mark!'
```

The following output is displayed:

```
Don't confuse two single quotation marks with a double quotation mark!
```

Command Operators in the Exchange Management Shell

Use the operators in the following table when you type commands in the Shell. Some of the operators may match some of the previously mentioned command conventions. However, they don't have the same meaning when they are typed on the command line. The following table shows the valid operators that you can use in a command.

Exchange Management Shell command operators

Operator	Description
=	The equal sign is used as an assignment character. The value on the right side of the equal sign is assigned to the variable on the left side of the equal sign. The following characters are also assignment characters: • **+=** Add the value on the right side of the equal sign to the current value that is contained in the variable on the left side of the equal sign. • **-=** Subtract the value on the right side of the equal sign from the current value that is contained in the variable on the left side of the equal sign. • ***=** Multiply the current value of the variable on the left side of the equal sign by the value that is specified on the right side of the equal sign. • **/=** Divide the current value of the variable on the left side of the equal sign by the value that is specified on the right side of the equal sign. • **%=** Modify the current value of the variable on the left side of the equal sign by the value that is specified on the right side of the equal sign.
:	A colon can be used to separate a parameter's name and the parameter's value, as in the following example: `-Enabled:$True`. The use of a colon is optional with all parameter types except switch parameters. For more information about

	switch parameters, see Parameters.
!	The exclamation point is a logical **NOT** operator. When it is used with the equal (**=**) sign, the combined pair means "not equal to."
[ ]	Brackets are used to specify the index value of an array position. For example, `$Red[9]` refers to the tenth index position in the array, `$Red`. It refers to the tenth index position because array indexes start at zero (0). Brackets can also be used to assign a type to a variable, as in the following example: `$A=[XML] "<Test><A>value</A></Test>"`. The following types are valid: `Array`, `Bool`, `Byte`, `Char`, `Char[]`, `Decimal`, `Double`, `Float`, `Int`, `Int[]`, `Long`, `Long []`, `RegEx`, `Single`, `ScriptBlock`, `String`, `Type`, and `XML`.
{ }	Braces are used to include an expression in a command, as in the following example: `Get-Process | Where { $_.HandleCount -gt 400 }`
|	The pipe symbol is used when one cmdlet pipes a result to another cmdlet. For example, the following command pipes the results from the Get-Mailbox cmdlet to the Set-Mailbox cmdlet: `Get-Mailbox -Server SRV1 | Set-Mailbox -ProhibitSendQuota 2GB`
>	The right-angle bracket is used to send the output of a command to a file, as in the following example: `Get-TransportRulePredicate > c:\out.txt`. The destination file is overwritten.
>>	Double right-angle brackets are used to append the output of a command to a file, if the file exists. If the file doesn't exist, a new file is created. The following is an example of how to use double right-angle brackets: `Get-TransportRulePredicate >>c:\out.txt`
" "	Quotation marks are used to enclose a string that contains spaces.
$	A dollar sign indicates a variable. For example, `$Blue = 10` assigns the value 10 to the variable `$Blue`.
@	The @ symbol references an associative array. For more information, see Arrays.
$( )	A dollar sign ($) with parentheses indicates command substitution. You can use command substitution when you want to use the output of one command as an argument in another command, as in the following example: `Get-ChildItem $(Read-Host -Prompt "Enter`

	`FileName: ")`
..	Double-periods indicate a value range. For example, if an array contains several indexes, you can specify the following command to return the values of all indexes between the second and fifth indexes, as in the following example: `$Blue [2..5]`
+	The **+** operator adds two values together. For example, `6 + 6` equals 12.
-	The **-** operator subtracts one value from another value. For example, `12 - 6` equals 6. The **-** operator can also be used to represent a negative number, such as -6. For example, `-6 * 6` equals -36.
*****	A wildcard character has several meanings. You can use wildcard characters to match strings, to multiply numeric values, or, if strings and numeric values are used together, to repeat the string value the number of times that is specified by the numeric value, as in the following example: `"Test" * 3` equals `TestTestTest`.
/	The **/** operator divides one value by another. For example, `6 / 6` equals 1.
%	When used in a numerical evaluation, the **%** operator returns the remainder from a division operator. For example, `6 % 4` equals 2. When used in a pipeline, the percent character (`%`) is shorthand for the `ForEach` cmdlet. For example, instead of the command `Import-Csv c:\MyFile.csv | ForEach { Set-Mailbox $_.Identity -Name $_.Name }`, you can use `Import-Csv c:\MyFile.csv | % { Set-Mailbox $_.Identity -Name $_.Name }`. For more information, see Pipelining.
?	The question mark character (?) is shorthand for the **Where** cmdlet. For example, instead of `Get-Alias | Where {$_.Definition -eq "Clear-Host"}`, you can use `Get-Alias \| ? {$_.Definition -eq "Clear-Host"}`.

For More Information

Exchange Management Shell Basics

1.5.2.7 Pipelining

Pipelining

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-02-23*

Pipelining in the Exchange Management Shell is the act of one cmdlet using the output of another cmdlet when it performs an operation. Pipelining is accomplished by using the pipe "|" symbol. All verbs in the same noun-cmdlet set can use piped information from another command. Some noun-cmdlet sets also let you pass data through the pipeline to another noun cmdlet set.

See the following sections for information and examples of using pipelining in the Shell:

Using Pipelining to Perform Multiple Actions

The use of pipelining to string together the actions of two or more cmdlets gives the Shell the power of composition, which lets you take smaller components and convert them into something more powerful. For example, you can use one cmdlet to gather data, pass that data to a second cmdlet to filter the data to a subset, and then pass that data to a third cmdlet to act on the subset only.

For example, the following command uses pipelining to move all the mailboxes on `Server1` to the `Executives` database on `Server2` by using the **Move-Mailbox** cmdlet, based on output that is piped from the **Get-Mailbox** cmdlet:

```
Get-Mailbox -Server Server1 | Move-Mailbox -TargetDatabase Executives
```

Using Pipelining to Process Data from Another Cmdlet

You can also use pipelining to process data that is output by a cmdlet. For example, for a list of all processes where the `HandleCount` property of the process is larger than 400, you can run the following command:

```
Get-Process | Where { $_.HandleCount -gt 400 } | Format-List
```

In this example, the **Get-Process** cmdlet passes objects to the **Where-Object** cmdlet. The **Where-Object** cmdlet picks out the objects that have a property called `HandleCount` with a value larger than 400.

Note:

Where is an alias for the **Where-Object** cmdlet. For more information, see Aliases.

In this example, the `HandleCount` property is preceded by the `$_` variable. This variable is created automatically by the Shell to store the current pipeline object. The **Where-Object** cmdlet then sends these objects to the **Format-List** cmdlet to be displayed.

The use of structured objects, instead of text, is one of the most exciting capabilities of the Shell. The use of structured objects forms the basis of a powerful compositional model of administration. For more information about structured objects, see Structured Data.

Using Pipelining to Pipe Data between Dissimilar Nouns

Piping data between dissimilar nouns is useful in cases where you want to use the data from one cmdlet with another cmdlet, but the preceding cmdlet in the pipeline doesn't output an object that the next cmdlet can use to identify the object to act upon. This situation typically happens if you're trying to pipe an object from a cmdlet with a noun that's different than the cmdlet that's expecting the object. For more information about cmdlets, see Cmdlets.

To pass data between cmdlets that haven't been optimized to pass objects directly between each other, you need to pass the object through the **ForEach** cmdlet. When you use the **ForEach** cmdlet, you can access the object directly using the `$_` special variable and associate its properties with the parameters on the second cmdlet.

In the following example, the **Get-Mailbox** cmdlet and the **New-InboxRule** cmdlet aren't optimized to send objects directly between each other. For the **New-InboxRule** cmdlet to take action on objects provided by the **Get-Mailbox** cmdlet, we need to manually associate the correct property on the mailbox object to the correct parameter on the **New-InboxRule** cmdlet. To do this, we use the following command:

```
Get-Mailbox | ForEach { New-InboxRule -Name "Mark as Read" -Mailbox $_.Name -From
```

In this example, we know that the **New-InboxRule** cmdlet requires that you specify the mailbox on which to create the new inbox rule. We also know that the **Get-Mailbox** cmdlet outputs an object that contains the name of each mailbox being returned. By using the **ForEach** cmdlet, which contains the command to be run on each object it receives, we gain access to the `$_` special variable, which contains the current object in the pipeline. We can access the *Name* property of the current mailbox object using the syntax `$_.Name`. We provide `$_.Name` as an argument on the *Mailbox* parameter of the **New-InboxRule** cmdlet which provides the cmdlet with the information it needs to create the new inbox rule.

Note:

ForEach is an alias for the **ForEach-Object** cmdlet. For more information, see Aliases.

Using Pipelining to Report Errors

To report errors, you can use the error pipeline. The error pipeline lets you report errors while a command runs. You don't have to wait until the command has finished running or to put the error information in the standard result pipeline. The **Write-Error** cmdlet writes its arguments to the error pipeline.

For more information about pipelining, run the following command in the Shell:

```
Get-Help About_Pipeline
```

For More Information

Exchange Management Shell Basics

1.5.2.8 WhatIf, Confirm, and ValidateOnly Switches

WhatIf, Confirm, and ValidateOnly Switches

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-02-20*

Both experienced administrators and script writers, and administrators who are new to Exchange and scripting, can benefit from using the *WhatIf*, *Confirm*, and *ValidateOnly* switches. These switches let you control how your commands run and indicate exactly what a command will do before it affects data. This functionality is quite valuable as you transition from your test environment into your production environment and as you roll out new scripts or commands.

The *WhatIf*, *Confirm*, and *ValidateOnly* switches are especially useful when you use them with commands that modify objects that are returned by using a filter or by using a **Get** command in a pipeline. This topic describes each switch and also provides an example command for each switch.

Important:

If you want to use the *WhatIf*, *Confirm*, and *ValidateOnly* switches with commands in a script, you must add the appropriate switch to each command in the script, and not on the command line that calls the script.

Note:

WhatIf, *Confirm*, and *ValidateOnly* are called switch parameters. For more information about switch parameters, see Parameters.

WhatIf Switch

The *WhatIf* switch instructs the command to which it is applied to run but only to display the objects that would be affected by running the command and what changes would be made to those objects. The switch does not actually change any of those objects. When you use the *WhatIf* switch, you can see whether the changes that would be made to those objects match your expectations, without the worry of modifying those objects.

When you run a command together with the *WhatIf* switch, you put the *WhatIf* switch at the end of the command, as in the following example:

```
New-AcceptedDomain -Name "Contoso Domain" -DomainName "contoso.com" -WhatIf
```

When you run this example command, the following text is returned by the Shell:

```
What if: Creating Accepted Domain "Contoso Domain" with domain name "contoso.com"
```

Confirm Switch

The *Confirm* switch instructs the command to which it is applied to stop processing before any changes are made. The command then prompts you to acknowledge each action before it continues. When you use the *Confirm* switch, you can step through changes to objects to make sure that changes are made only to the specific objects that you want to change. This functionality is useful when you apply changes to many objects and want precise control over the operation of the Shell. A confirmation prompt is displayed for each

object before the Shell modifies the object.

By default, the Shell automatically applies the *Confirm* switch to cmdlets that have the following verbs:

- **Clear**
- **Disable**
- **Dismount**
- **Move**
- **Remove**
- **Stop**
- **Suspend**
- **Uninstall**

When a cmdlet runs that has any of these verbs, the Shell automatically stops the command and waits for your acknowledgement before it continues to process.

If you want to manually apply the *Confirm* switch to a command, include the *Confirm* switch at the end of the command, as in the following example:

```
Get-JournalRule | Enable-JournalRule -Confirm
```

When you run this example command, the following confirmation prompt is returned by the Shell:

```
Confirm
Are you sure you want to perform this action?
Enabling journal rule "Litigation Journal Rule".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

The confirmation prompt gives you the following choices:

- **[Y] Yes** Type **Y** to instruct the command to continue the operation. The next operation will present another confirmation prompt. `[Y] Yes` is the default choice.
- **[A] Yes to All** Type **A** to instruct the command to continue the operation and all subsequent operations. You will not receive additional confirmation prompts for the duration of this command.
- **[N] No** Type **N** to instruct the command to skip this operation and continue with the next operation. The next operation will present another confirmation prompt.
- **[L] No to All** Type **L** to instruct the command to skip this operation and all subsequent operations.
- **[S] Suspend** Type **S** to pause the current pipeline and return to the command line. Type **Exit** to resume the pipeline.
- **[?] Help** Type **?** to display confirmation prompt Help on the command line.

If you want to override the default behavior of the Shell and suppress the confirmation prompt for cmdlets on which it is automatically applied, you can include the *Confirm* switch with a value of `$False`, as in the following example:

```
Get-JournalRule | Disable-JournalRule -Confirm:$False
```

In this case, no confirmation prompt is displayed.

Caution:

The default value of the *Confirm* switch is `$True`. The default behavior of the Shell is to automatically display a confirmation prompt. If you suppress this default behavior, you instruct the command to suppress all confirmation prompts for the duration of that command. The command will process all objects that meet the criteria for the command without confirmation.

ValidateOnly Switch

The *ValidateOnly* switch instructs the command to which it is applied to evaluate all the conditions and requirements that are needed to perform the operation before you apply any changes. The *ValidateOnly* switch is available on cmdlets that may take a long time to run, have several dependencies on multiple systems, or affect critical data, such as mailboxes.

When you apply the *ValidateOnly* switch to a command, the command runs through the whole process. The command performs each action as it would without the *ValidateOnly* switch. But the command doesn't change any objects. When the command completes its process, it displays a summary with the results of the validation. If the validation indicates that the command was successful, you can run the command again without the *ValidateOnly* switch.

When you run a command together with the *ValidateOnly* switch, you put the *ValidateOnly* switch at the end of the command, as in the following example:

```
Get-Mailbox "Kim Akers" | Move-Mailbox -TargetDatabase "Executive Database" -Vali
```

When you run this example command, the following text is returned by the Shell:

```
Identity                          : contoso.com/Users/Kim Akers
DistinguishedName                 : CN=Kim Akers,CN=Users,DC=contoso,DC=com
DisplayName                       : Kim Akers
Alias                             : kim
LegacyExchangeDN                  : /o=First Organization/ou=Exchange Administra
                                    tive Group (FYDIBOHF23SPDLT)/cn=Recipients/c
                                    n=Kim Akers
PrimarySmtpAddress                : kim@contoso.com
SourceServer                      : MBX.contoso.com
SourceDatabase                    : Mailbox Database 0896551697
SourceGlobalCatalog               : MBX
SourceDomainController            : MBX.contoso.com
TargetGlobalCatalog               : MBX
TargetDomainController            : MBX.contoso.com
TargetMailbox                     :
TargetServer                      : MBX.contoso.com
TargetDatabase                    : Executive Database
MailboxSize                       : 0 B (0 bytes)
IsResourceMailbox                 : False
SIDUsedInMatch                    :
SMTPProxies                       :
SourceManager                     :
SourceDirectReports               :
SourcePublicDelegates             :
SourcePublicDelegatesBL           :
SourceAltRecipient                :
SourceAltRecipientBL              :
SourceDeliverAndRedirect          :
MatchedTargetNTAccountDN          :
IsMatchedNTAccountMailboxEnabled  :
MatchedContactsDNList             :
TargetNTAccountDNToCreate         :
TargetManager                     :
TargetDirectReports               :
TargetPublicDelegates             :
TargetPublicDelegatesBL           :
TargetAltRecipient                :
TargetAltRecipientBL              :
TargetDeliverAndRedirect          :
Options                           : Default
SourceForestCredential            :
TargetForestCredential            :
TargetFolder                      :
PSTFilePath                       :
```

```
RecoveryMailboxGuid               :
RecoveryMailboxLegacyExchangeDN   :
RecoveryMailboxDisplayName        :
RecoveryDatabaseGuid              :
StandardMessagesDeleted           : 0
AssociatedMessagesDeleted         : 0
DumpsterMessagesDeleted           : 0
MoveType                          : IntraOrg
MoveStage                         : Validation
StartTime                         : 2/10/2009 12:20:04 PM
EndTime                           : 2/10/2009 12:20:04 PM
StatusCode                        : 0
StatusMessage                     : This mailbox can be moved to the target data
                                    base.
ReportFile                        : C:\Program Files\Microsoft\Exchange Server\V
                                    14\Logging\MigrationLogs\move-Mailbox2009021
                                    0-122003-8563750.xml
```

For More Information

Exchange Management Shell Basics

1.5.2.9 Modifying Multivalued Properties

Modifying Multivalued Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Shell to add values to and remove values from a multivalued property on an object.

Multivalued Property Overview

A multivalued property is a property that can contain more than one value. For example, the **BlockedRecipients** property on the **RecipientFilterConfig** object can accept multiple recipient addresses as in the following examples:

- john@contoso.com
- kim@northwindtraders.com
- david@adatum.com

Because the **BlockedRecipients** property can accept more than one value, it's called a multivalued property.

For more information about objects, see Structured Data.

Modifying a Multivalued Property vs. Modifying a Property That Accepts Only a Single Value

How you modify a multivalued property is slightly different from how you modify a property that accepts only one value. When you modify a property that accepts only a single value, you can assign a value directly to it, as in the following command.

```
Set-TransportConfig -MaxSendSize 12MB
```

When you use this command to provide a new value to the **MaxSendSize** property, the stored value is overwritten. This isn't a problem with properties that accept only one value. However, it becomes a problem with multivalued properties. For example, assume that the **BlockedRecipients** property on the **RecipientFilterConfig** object is configured to have the three values that are listed in the previous section. When you run the command `Get-RecipientFilterConfig | Format-List BlockedRecipients`, the following is displayed.

```
BlockedRecipients : {david@adatum.com, kim@northwindtraders.com, john@contoso.com
```

Now assume that you've received a request to add a new SMTP address to the blocked recipients list. You run the following command to add the new SMTP address.

```
Set-RecipientFilterConfig -BlockedRecipients chris@contoso.com
```

When you run the `Get-RecipientFilterConfig | Format-List BlockedRecipients` command again, you will see the following.

```
BlockedRecipients : {chris@contoso.com}
```

This isn't what you expected. You wanted to add the new SMTP address to the existing list of blocked recipients, but instead the existing list of blocked recipients was overwritten by the new SMTP address. This unintended result exemplifies how modifying a multivalued property differs from modifying a property that accepts only a single value. When you modify a multivalued property, you must make sure that you append or remove values instead of overwriting the whole list of values. The following sections show you how to do exactly that.

Note:

Some cmdlets, such as **Set-TransportRule**, don't support modifying properties on objects in the manner described in this topic. For more information about how to add values to and remove values from the multivalued properties of these cmdlets, see the topics for those cmdlets, such as Set-TransportRule.

Modifying Multivalued Properties

Modifying multivalued properties is similar to modifying single-valued properties. You just need to add some additional syntax to tell the Shell that you want to add or remove values to or from the multivalued property rather than replace everything that's stored in the property. The syntax is included, along with the value or values to add or remove to or from the property, as a value on a parameter when you run a cmdlet. The following table shows the syntax that you need to add to a parameter on a cmdlet to modify multivalued properties.

Multivalue property syntax

Action	Syntax
Add one or more values to a multivalued property	`@{Add="<value1>", "<value2>", "<value3>"}`
Remove one or more values from a multivalued property	`@{Remove="<value1>", "<value2>", "<value3>"}`

The syntax that you choose from the Multivalue property syntax table is specified as a

parameter value on a cmdlet. For example, the following command adds multiple values to a multivalued property:

```
Set-ExampleCmdlet -Parameter @{Add="Red", "Blue", "Green"}
```

When you use this syntax, the values that you specify are added or removed from the list of values already present on the property. Taking the **BlockedRecipients** example earlier in this topic, we can now add chris@contoso.com without overwriting the rest of the values on this property by using the following command:

```
Set-RecipientFilterConfig -BlockedRecipients @{Add="chris@contoso.com"}
```

If you wanted to remove david@adatum.com from the list of values, you would use this command:

```
Set-RecipientFilterConfig -BlockedRecipients @{Remove="david@adatum.com"}
```

More complex combinations can be used, such as adding or removing values to and from a property at the same time. To do so, insert a semicolon (`;`) between `Add` and `Remove` actions. For example:

```
Set-RecipientFilterConfig -BlockedRecipients @{Add="carter@contoso.com", "sam@nor
```

If we use the `Get-RecipientFilterConfig | Format-List BlockedRecipients` command again, we can see that the email addresses for Carter, Sam, and Brian have been added while the address for John has been removed.

```
BlockedRecipients : {brian@adatum.com, sam@northwindtraders.com, carter@contoso.c
```


1.5.2.10 Working with Command Output

Working with Command Output

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-18*

The Exchange Management Shell offers several methods that you can use to format command output. This topic discusses the following subjects:

- How to format data Control how the data that you see is formatted by using the **Format-List**, **Format-Table**, and **Format-Wide** cmdlets.
- How to output data Determine whether data is output to the Shell console window or to a file by using the **Out-Host** and **Out-File** cmdlets. Included in this topic is a sample script to output data to Microsoft Internet Explorer.
- How to filter data Filter data by using either of the following filtering methods:
  - Server-side filtering, available on certain cmdlets
  - Client-side filtering, available on all cmdlets by piping the results of a command to the **Where-Object** cmdlet

To use the functionality that is described in this topic, you must be familiar with the following concepts:

- Pipelining
- Shell Variables
- Comparison Operators

How to Format Data

If you call formatting cmdlets at the end of the pipeline, you can override the default formatting to control what data is displayed and how that data appears. The formatting cmdlets are **Format-List**, **Format-Table**, and **Format-Wide**. Each has its own distinct output style that differs from the other formatting cmdlets.

Format-List

The **Format-List** cmdlet takes input from the pipeline and outputs a vertical columned list of all the specified properties of each object. You can specify which properties you want to display by using the *Property* parameter. If the **Format-List** cmdlet is called without any parameters specified, all properties are output. The **Format-List** cmdlet wraps lines instead of truncating them. One of the best uses for the **Format-List** cmdlet is to override the default output of a cmdlet so that you can retrieve additional or more focused information.

For example, when you call the **Get-Mailbox** cmdlet, you only see a limited amount of information in table format. If you pipe the output of the **Get-Mailbox** cmdlet to the **Format-List** cmdlet and add parameters for the additional or more focused information that you want to view, you can retrieve the output that you want.

You can also specify a wildcard character "*" with a partial property name. If you include a wildcard character, you can match multiple properties without having to type each property name individually. For example, `Get-Mailbox | Format-List -Property Email*` returns all properties that begin with `Email`.

The following examples show the different ways that you can view the same data returned by the **Get-Mailbox** cmdlet.

```
Get-MailBox TestUser1
Name                    Alias                ServerName       ProhibitSendQuo
                                                              ta
----                    -----                ----------       ---------------
TestUser1               TestUser1            mbx              unlimited
```

In the first example, the **Get-Mailbox** cmdlet is called without specific formatting so the default output is in table format and contains a predetermined set of properties.

```
Get-Mailbox TestUser1 | Format-List -Property Name,Alias,EmailAddresses
Name           : TestUser1
Alias          : TestUser1
EmailAddresses : {SMTP:TestUser1@contoso.com}
```

In the second example, the output of the **Get-Mailbox** cmdlet is piped to the **Format-List** cmdlet, together with specific properties. As you can see, the format and content of the output is significantly different.

```
Get-Mailbox TestUser1 | Format-List -Property Name, Alias, Email*
Name                       : Test User
Alias                      : TestUser1
EmailAddresses             : {SMTP:TestUser1@contoso.com}
EmailAddressPolicyEnabled : True
```

In the last example, the output of the **Get-Mailbox** cmdlet is piped to the **Format-List** cmdlet as in the second example. However, in the last example, a wildcard character is used to match all properties that start with `Email`.

If more than one object is passed to the **Format-List** cmdlet, all specified properties for an object are displayed and grouped by object. The display order depends on the default parameter for the cmdlet. The default parameter is most frequently the *Name* parameter or the *Identity* parameter. For example, when the **Get-Childitem** cmdlet is called, the

default display order is file names in alphabetical order. To change this behavior, you must call the **Format-List** cmdlet, together with the *GroupBy* parameter, and the name of a property value by which you want to group the output. For example, the following command lists all files in a directory and then groups these files by extension.

```
Get-Childitem | Format-List Name,Length -GroupBy Extension
    Extension: .xml
Name   : Config_01.xml
Length : 5627
Name   : Config_02.xml
Length : 3901
    Extension: .bmp
Name   : Image_01.bmp
Length : 746550
Name   : Image_02.bmp
Length : 746550
    Extension: .txt
Name   : Text_01.txt
Length : 16822
Name   : Text_02.txt
Length : 9835
```

In this example, the **Format-List** cmdlet has grouped the items by the *Extension* property that is specified by the *GroupBy* parameter. You can use the *GroupBy* parameter with any valid property for the objects in the pipeline stream.

Format-Table

The **Format-Table** cmdlet lets you display items in a table format with label headers and columns of property data. By default, many cmdlets, such as the **Get-Process** and **Get-Service** cmdlets, use the table format for output. Parameters for the **Format-Table** cmdlet include the *Properties* and *GroupBy* parameters. These parameters work exactly as they do with **Format-List** cmdlet.

The **Format-Table** cmdlet also uses the *Wrap* parameter. This parameter enables long lines of property information to display completely instead of truncating at the end of a line. To see how the *Wrap* parameter is used to display returned information, compare the output of the **Get-Command** command in the following two examples.

In the first example, when the **Get-Command** cmdlet is used to display command information about the **Get-Process** cmdlet, the information for the *Definition* property is truncated.

```
Get-Command Get-Process | Format-Table Name,Definition
Name                                Definition
----                                ----------
get-process                         get-process [[-ProcessName] String[]...
```

In the second example, the *Wrap* parameter is added to the command to force the complete contents of the *Definition* property to display.

```
Get-Command Get-Process | Format-Table Name,Definition -Wrap
Get-Process                         Get-Process [[-Name] <String[]>] [-Comp
                                    uterName <String[]>] [-Module] [-FileVe
                                    rsionInfo] [-Verbose] [-Debug] [-ErrorA
                                    ction <ActionPreference>] [-WarningActi
                                    on <ActionPreference>] [-ErrorVariable
                                    <String>] [-WarningVariable <String>] [
                                    -OutVariable <String>] [-OutBuffer <Int
                                    32>]
                                    Get-Process -Id <Int32[]> [-ComputerNam
                                    e <String[]>] [-Module] [-FileVersionIn
                                    fo] [-Verbose] [-Debug] [-ErrorAction <
                                    ActionPreference>] [-WarningAction <Act
                                    ionPreference>] [-ErrorVariable <String
                                    >] [-WarningVariable <String>] [-OutVar
```

```
                                        iable <String>] [-OutBuffer <Int32>]
                                        Get-Process [-ComputerName <String[]>]
                                        [-Module] [-FileVersionInfo] -InputObje
                                        ct <Process[]> [-Verbose] [-Debug] [-Er
                                        rorAction <ActionPreference>] [-Warning
                                        Action <ActionPreference>] [-ErrorVaria
                                        ble <String>] [-WarningVariable <String
                                        >] [-OutVariable <String>] [-OutBuffer
                                        <Int32>]
```

As with the **Format-List** cmdlet, you can also specify a wildcard character "*" with a partial property name. By including a wildcard character, you can match multiple properties without typing each property name individually.

Format-Wide

The **Format-Wide** cmdlet provides a much simpler output control than the other format cmdlets. By default, the **Format-Wide** cmdlet tries to display as many columns of property values as possible on a line of output. By adding parameters, you can control the number of columns and how the output space is used.

In the most basic usage, calling the **Format-Wide** cmdlet without any parameters arranges the output in as many columns as will fit the page. For example, if you run the **Get-Childitem** cmdlet and pipe its output to the **Format-Wide** cmdlet, you will see the following display of information:

```
Get-ChildItem | Format-Wide
    Directory: FileSystem::C:\WorkingFolder
Config_01.xml                           Config_02.xml
Config_03.xml                           Config_04.xml
Config_05.xml                           Config_06.xml
Config_07.xml                           Config_08.xml
Config_09.xml                           Image_01.bmp
Image_02.bmp                            Image_03.bmp
Image_04.bmp                            Image_05.bmp
Image_06.bmp                            Text_01.txt
Text_02.txt                             Text_03.txt
Text_04.txt                             Text_05.txt
Text_06.txt                             Text_07.txt
Text_08.txt                             Text_09.txt
Text_10.txt                             Text_11.txt
Text_12.txt
```

Generally, calling the **Get-Childitem** cmdlet without any parameters displays the names of all files in the directory in a table of properties. In this example, by piping the output of the **Get-Childitem** cmdlet to the **Format-Wide** cmdlet, the output was displayed in two columns of names. Notice that only one property type can be displayed at a time, specified by a property name that follows the **Format-Wide** cmdlet. If you add the *Autosize* parameter, the output is changed from two columns to as many as can fit the screen width.

```
Get-ChildItem | Format-Wide -AutoSize
    Directory: FileSystem::C:\WorkingFolder
Config_01.xml   Config_02.xml   Config_03.xml   Config_04.xml   Config_05.xml
Config_06.xml   Config_07.xml   Config_08.xml   Config_09.xml   Image_01.bmp
Image_02.bmp    Image_03.bmp    Image_04.bmp    Image_05.bmp    Image_06.bmp
Text_01.txt     Text_02.txt     Text_03.txt     Text_04.txt     Text_05.txt
Text_06.txt     Text_07.txt     Text_08.txt     Text_09.txt     Text_10.txt
Text_11.txt     Text_12.txt
```

In this example, the table is arranged in five columns, instead of two columns. The *Column* parameter offers more control by letting you specify the maximum number of columns to display information as follows:

```
Get-ChildItem | Format-Wide -Column 4
    Directory: FileSystem::C:\WorkingFolder
```

```
Config_01.xml       Config_02.xml       Config_03.xml       Config_04.xml
Config_05.xml       Config_06.xml       Config_07.xml       Config_08.xml
Config_09.xml       Image_01.bmp        Image_02.bmp        Image_03.bmp
Image_04.bmp        Image_05.bmp        Image_06.bmp        Text_01.txt
Text_02.txt         Text_03.txt         Text_04.txt         Text_05.txt
Text_06.txt         Text_07.txt         Text_08.txt         Text_09.txt
Text_10.txt         Text_11.txt         Text_12.txt
```

In this example, the number of columns is forced to four by using the *Column* parameter.

How to Output Data

Out-Host and Out-File

The **Out-Host** cmdlet is an unseen default cmdlet at the end of the pipeline. After all formatting is applied, the **Out-Host** cmdlet sends the final output to the console window for display. You don't have to explicitly call the **Out-Host** cmdlet, because it is the default output. You can override sending the output to the console window by calling the **Out-File** cmdlet as the last cmdlet in the command. The **Out-File** cmdlet then writes the output to the file that you specify in the command as in the following example:

```
Get-ChildItem | Format-Wide -Column 4 | Out-File c:\OutputFile.txt
```

In this example, the **Out-File** cmdlet writes the information that is displayed in the **Get-ChildItem | Format-Wide -Column 4** command to a file that is named `OutputFile.txt`. You can also redirect pipeline output to a file by using the redirection operator, which is the right-angle bracket (>). To append pipeline output of a command to an existing file without replacing the original file, use the double right-angle brackets (>>), as in the following example:

```
Get-ChildItem | Format-Wide -Column 4 >> C:\OutputFile.txt
```

In this example, the output from the **Get-Childitem** cmdlet is piped to the **Format-Wide** cmdlet for formatting and then is written to the end of the `OutputFile.txt` file. Notice that if the `OutputFile.txt` file did not exist, use of the double right-angle brackets (>>) would create the file.

For more information about pipelines, see Pipelining.

For more information about the syntax used in the previous examples, see Syntax.

Viewing Data in Internet Explorer

Because of the flexibility and ease of scripting in the Exchange Management Shell, you can take the data that is returned by commands and format and output them in almost limitless ways.

The following example shows how you can use a simple script to output the data that is returned by a command and display it in Internet Explorer. This script takes the objects that are passed through the pipeline, opens an Internet Explorer window, and then displays the data in Internet Explorer:

```
$Ie = New-Object -Com InternetExplorer.Application
$Ie.Navigate("about:blank")
while ($Ie.Busy) { Sleep 1 }
$Ie.Visible = $True
$Ie.Document.Write("$Input")
# If the previous line doesn't work on your system, uncomment the line below.
# $Ie.Document.IHtmlDocument2_Write("$Input")
$Ie
```

To use this script, save it to the `C:\Program Files\Microsoft\Exchange Server`

\V14\Scripts directory on the computer where the script will be run. Name the file Out-Ie.ps1. After you save the file, you can then use the script as a regular cmdlet.

Note:
To run scripts in Exchange 2010, scripts must be added to an unscoped management role and you must be assigned the management role either directly or through a management role group. For more information, see Understanding Management Roles.

The Out-Ie script assumes that the data it receives is valid HTML. To convert the data that you want to view into HTML, you must pipe the results of your command to the **ConvertTo-Html** cmdlet. You can then pipe the results of that command to the Out-Ie script. The following example shows how to view a directory listing in an Internet Explorer window:

```
Get-ChildItem | Select Name,Length | ConvertTo-Html | Out-Ie
```

How to Filter Data

The Shell gives you access to a large quantity of information about your servers, mailboxes, Active Directory directory service, and other objects in your organization. Although access to this information helps you better understand your environment, this large quantity of information can be overwhelming. The Shell lets you control this information and return only the data that you want to see by using filtering. The following two types of filtering are available:

- **Server-side filtering** Server-side filtering takes the filter that you specify on the command line and submits it to the Exchange server that you query. That server processes the query and returns only the data that matches the filter that you specified.
  Server-side filtering is performed only on objects where tens or hundreds of thousands of results could be returned. Therefore, only the recipient management cmdlets, such as the **Get-Mailbox** cmdlet, and queue management cmdlets, such as the **Get-Queue** cmdlet, support server-side filtering. These cmdlets support the *Filter* parameter. This parameter takes the filter expression that you specify and submits it to the server for processing.
- **Client-side filtering** Client-side filtering is performed on the objects in the local console window in which you are currently working. When you use client-side filtering, the cmdlet retrieves all the objects that match the task that you are performing to the local console window. The Shell then takes all the returned results, applies the client-side filter to those results, and returns to you only the results that match your filter. All cmdlets support client-side filtering. This is invoked by piping the results of a command to the **Where-Object** cmdlet.

Server-Side Filtering

The implementation of server-side filtering is specific to the cmdlet on which it is supported. Server-side filtering is enabled only on specific properties on the objects that are returned.

For more information about how to manage recipients by using server-side filtering, see Creating Filters in Recipient Commands. For more information about how to manage queues by using server-side filtering, see Filter Queues.

Client-Side Filtering

Client-side filtering can be used with any cmdlet. This capability includes those cmdlets that also support server-side filtering. As described earlier in this topic, client-side filtering accepts all the data that is returned by a previous command in the pipeline, and in turn, returns only the results that match the filter that you specify. The **Where-Object** cmdlet performs this filtering. It can be shortened to **Where**.

As data passes through the pipeline, the **Where** cmdlet receives the data from the previous object and then filters the data before passing it on to the next object. The filtering is based on a script block that is defined in the **Where** command. The script block filters data based on the object's properties and values.

The **Clear-Host** cmdlet is used to clear the console window. In this example, you can find all the defined aliases for the **Clear-Host** cmdlet if you run the following command:

```
Get-Alias | Where {$_.Definition -eq "Clear-Host"}
CommandType     Name                            Definition
-----------     ----                            ----------
Alias           clear                           clear-host
Alias           cls                             clear-host
```

The **Get-Alias** cmdlet and the **Where** command work together to return the list of aliases that are defined for the **Clear-Host** cmdlet and no other cmdlets. The following table outlines each element of the **Where** command that is used in the example.

Elements of the Where command

Element	Description
`{ }`	Braces enclose the script block that defines the filter.
`$_`	This special variable automatically initiates and binds to the objects in the pipeline.
`Definition`	The `Definition` property is the property of the current pipeline objects that stores the name of the alias definition. When `Definition` is used with the `$_` variable, a period comes before the property name.
`-eq`	This comparison operator for "equal to" is used to specify that the results must exactly match the property value that is supplied in the expression.
"**Clear-Host**"	In this example, "**Clear-Host**" is the value for which the command is parsing.

In the example, the objects that are returned by the **Get-Alias** cmdlet represent all the defined aliases on the system. Even though you don't see them from the command line, the aliases are collected and passed to the **Where** cmdlet through the pipeline. The **Where** cmdlet uses the information in the script block to apply a filter to the alias objects.

The special variable $_represents the objects that are being passed. The $_variable is automatically initiated by the Shell and is bound to the current pipeline object. For more information about this special variable, see Shell Variables.

Using standard "dot" notation (object.property), the `Definition` property is added to define the exact property of the object to evaluate. The `-eq` comparison operator then compares the value of this property to `"Clear-Host"`. Only the objects that have the `Definition` property that match this criterion are passed to the console window for output. For more information about comparison operators, see Comparison Operators.

After the **Where** command has filtered the objects returned by the **Get-Alias** cmdlet, you can pipe the filtered objects to another command. The next command processes only the filtered objects returned by the Where command.

For More Information

Exchange Management Shell Basics

1.5.2.11 Comparison Operators

Comparison Operators

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-02-27*

The Exchange Management Shell has a rich set of operators that enables comparisons of one object with another object or one object with a set of objects. For more information about comparison operators, run the following command in the Shell:

```
Get-Help About_Comparison_Operators
```

The following table lists the comparison operators that are available in the Shell. Some comparison operators are case-sensitive. If a comparison operator is case-sensitive, the case that is used in the strings that are being compared must match. For example, the string "Test" does not match "test" when you use a comparison operator that is case-sensitive.

Comparison operators that are available in the Exchange Management Shell

Operator	Definition
-eq	Equals (not case-sensitive)
-ieq	Equals (not case-sensitive)
-ceq	Equals (case-sensitive)
-ne	Not equal (not case-sensitive)
-ine	Not equal (not case-sensitive)
-cne	Not equal (case-sensitive)
-lt	Less than (not case-sensitive)
-ilt	Less than (not case-sensitive)
-clt	Less than (case-sensitive)
-gt	Greater than (not case-sensitive)
-igt	Greater than (not case-sensitive)
-cgt	Greater than (case-sensitive)
-le	Less than or equal to (not case-sensitive)
-ile	Less than or equal to (not case-sensitive)
-cle	Less than or equal to (case-sensitive)

-ge	Greater than or equal to (not case-sensitive)
-ige	Greater than or equal to (not case-sensitive)
-cge	Greater than or equal to (case-sensitive)
-contains	The elements in the left operand that is equal to the right operand (not case-sensitive)
-icontains	The elements in the left operand that is equal to the right operand (not case-sensitive)
-ccontains	The elements in the left operand that is equal to the right operand (case-sensitive)
-notcontains	The elements in the left operand that is equal to the right operand (not case-sensitive)
-inotcontains	The elements in the left operand that is equal to the right operand (not case-sensitive)
-cnotcontains	The elements in the left operand that is equal to the right operand (case-sensitive)
-band	Bitwise And
-bor	Bitwise Or
-bnot	Bitwise NOT
-and	Logical and
-or	Logical or
-not	Logical not
-match	Compare strings by using regular expressions (not case-sensitive)
-notmatch	Compare strings by using regular expressions (not case-sensitive)
-imatch	Compare strings by using regular expressions (not case-sensitive)
-inotmatch	Compare strings by using regular expressions (not case-sensitive)
-cmatch	Compare strings by using regular expressions (case-sensitive)
-cnotmatch	Compare strings by using regular expressions (case-sensitive)
-like	Compare strings by using wildcard rules
-notlike	Compare strings by using wildcard rules

-ilike	Compare strings by using wildcard rules (not case-sensitive)
-inotlike	Compare strings by using wildcard rules (not case-sensitive)
-clike	Compare strings by using wildcard rules (case-sensitive)
-cnotlike	Compare strings by using wildcard rules (case-sensitive)

For More Information

Exchange Management Shell Basics

1.5.2.12 Aliases

Aliases

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-19*

You can assign an Exchange Management Shell cmdlet or Cmd.exe command to an administrator-defined and easy-to-remember alias in Microsoft Exchange Server 2010. Such aliases can be handy when you frequently use certain cmdlets and want to reduce the typing that you must do.

When an alias is called from the command line, the rules that apply to the cmdlet that is represented by the alias are enforced exactly as when the cmdlet is called. You must supply any required parameters and their values exactly as if you had called the cmdlet name.

See the following sections for more information about using aliases in the Shell:

Built-in Aliases

Creating Custom Aliases

Removing an Alias

Importing and Exporting Aliases

Alias Persistence

Alias Limitations

Built-in Aliases

Many cmdlets that are used regularly have default, or built-in, aliases assigned to them. These built-in aliases help reduce the typing that you have to do when you administer Exchange 2010 by using the Shell.

For example, the **Get-ChildItem** cmdlet resembles the MS-DOS `Dir` command. Because you are familiar with the `Dir` command, you might want to use the `Dir` alias when you use the Shell instead of typing **Get-ChildItem** every time that you want to view the contents of a directory. The output from the **Get-ChildItem** cmdlet and the `Dir` alias is the same and can be used interchangeably.

The following table shows the built-in aliases and their full names.

Built-in aliases

Alias	Cmdlet	Alias	Cmdlet	Alias	Cmdlet
%	ForEach-Object	gdr	Get-PSDrive	popd	Pop-Location
?	Where-Object	ghy	Get-History	ps	Get-Process
ac	Add-Content	gi	Get-Item	pushd	Push-Location
asnp	Add-PSSnapIn	gjb	Get-Job	pwd	Get-Location
cat	Get-Content	gl	Get-Location	r	Invoke-History
cd	Set-Location	gm	Get-Member	rbp	Remove-PSBreakpoint
chdir	Set-Location	gmo	Get-Module	rcjb	Receive-Job
clc	Clear-Content	gp	Get-ItemProperty	rd	Remove-Item
clear	Clear-Host	gps	Get-Process	rdr	Remove-PSDrive
clhy	Clear-History	grid	Out-GridView	ren	Rename-Item
cli	Clear-Item	group	Group-Object	ri	Remove-Item
clp	Clear-ItemProperty	gsn	Get-PSSession	rjb	Remove-Job
cls	Clear-Host	gsnp	Get-PSSnapIn	rm	Remove-Item
clv	Clear-Variable	gsv	Get-Service	rmdir	Remove-Item
compare	Compare-Object	gu	Get-Unique	rni	Rename-Item
copy	Copy-Item	gv	Get-Variable	rnp	Rename-ItemProperty
cp	Copy-Item	gwmi	Get-WmiObject	rp	Remove-ItemProperty
cpi	Copy-Item	h	Get-History	rsn	Remove-PSSession
cpp	Copy-	history	Get-History	rsnp	Remove-

	ItemProperty				PSSnapin
cvpa	Convert-Path	icm	Invoke-Command	rv	Remove-Variable
dbp	Disable-PSBreakpoint	iex	Invoke-Expression	rvpa	Resolve-Path
del	Remove-Item	ihy	Invoke-History	rwmi	Remove-WMIObject
diff	Compare-Object	ii	Invoke-Item	sajb	Start-Job
dir	Get-ChildItem	imo	Import-Module	sal	Set-Alias
ebp	Enable-PSBreakpoint	ipal	Import-Alias	sasv	Start-Service
echo	Write-Output	ipcsv	Import-Csv	sbp	Set-PSBreakpoint
emm	Export-ModuleMember	IPSN	Import-PSSession	sc	Set-Content
epal	Export-Alias	iwmi	Invoke-WMIMethod	select	Select-Object
epcsv	Export-Csv	kill	Stop-Process	set	Set-Variable
EPSN	Export-PSSession	list	format-list	si	Set-Item
erase	Remove-Item	lp	Out-Printer	sl	Set-Location
ETSN	Enter-PSSession	ls	Get-ChildItem	sleep	Start-Sleep
EXSN	Exit-PSSession	man	help	sort	Sort-Object
fc	Format-Custom	md	mkdir	sp	Set-ItemProperty
fl	Format-List	measure	Measure-Object	spjb	Stop-Job
foreach	ForEach-Object	mi	Move-Item	spps	Stop-Process
ft	Format-Table	mount	New-PSDrive	spsv	Stop-Service
fw	Format-Wide	move	Move-Item	start	Start-Process
gal	Get-Alias	mp	Move-ItemProperty	sv	Set-Variable
gbp	Get-PSBreakpoint	mv	Move-Item	swmi	Set-WMIInstance
gc	Get-Content	nal	New-Alias	table	format-table

gci	**Get-ChildItem**	**ndr**	**New-PSDrive**	**tee**	**Tee-Object**
gcm	**Get-Command**	**ni**	**New-Item**	**type**	**Get-Content**
gcs	**Get-PSCallStack**	**nmo**	**New-Module**	**where**	**Where-Object**
nv	**New-Variable**	**nsn**	**New-PSSession**	**wjb**	**Wait-Job**
ogv	**Out-GridView**	**oh**	**Out-Host**	**write**	**Write-Output**

For more information about aliases, run the following command in the Shell:

```
Get-Help About_Alias
```

Return to top

Creating Custom Aliases

In addition to the default, or built-in, aliases, you can define and use custom aliases instead of the names of cmdlets that you frequently use. You can use the **Set-Alias** cmdlet to associate cmdlets to familiar command names that have the equivalent functionality in Cmd.exe. You can assign multiple aliases to a single command. However, each alias can only be assigned to a single command. For example, you can have three aliases `Alias1`, `Alias2`, and `Alias3` that are assigned to the **New-Mailbox** cmdlet. You could then use any of the three aliases to run the **New-Mailbox** cmdlet. However, each alias that you create can only be assigned to the **New-Mailbox** cmdlet. You can't, for example, assign `Alias1` to both the **New-Mailbox** cmdlet and the **Get-Mailbox** cmdlet.

To create a new alias-cmdlet pairing, run the **Set-Alias** cmdlet and supply the name of the alias, together with the name of the cmdlet that you want to call when the alias is entered.

The following table shows several examples of how to create a new alias.

Examples of custom aliases

Alias description	Alias command
Retrieve the contents of a file.	`Set-Alias Type Get-Content`
Retrieve the listing of a directory.	`Set-Alias Dir Get-ChildItem`
Remo	`Set-Alias Erase Remove-Item`

ve a file.	
Set **pad** as an alias for Microsoft Word Pad.	`Set-Alias Pad "${env:programfiles}\Windows NT\Accessories\wordpad.exe"`
Display the list of all defined aliases.	`Set-Alias Aliases Get-Alias`

Return to top

Removing an Alias

To remove an alias, delete the alias from the alias drive. For example, an administrator creates the `Ls` alias by using the following command:

```
Set-Alias Ls Get-ChildItem
```

Later the administrator decides that the `Ls` alias is no longer needed and uses the following command to remove the `Ls` alias:

```
Remove-Item Alias Ls
```

Importing and Exporting Aliases

The **Export-Alias** cmdlet writes the current alias list to a file in comma-separated values (CSV) format. You can include the name of the file and its path in the command line. If the path doesn't exist, the cmdlet will create the path for you.

The **Import-Alias** cmdlet reads a text file that has CSV values and brings the list into the Shell as an object. By using the **Export-Alias** cmdlet and **Import-Alias** cmdlet, you can export a list of aliases from the Shell on one computer and import them to the Shell on another computer. Because existing predefined aliases exist on both computers, all alias name conflicts will be ignored and not imported.

Alias Persistence

Aliases that are created from the command line by using the **Set-Alias** cmdlet during a Shell session can be used when the session is active. After the session is closed, the alias definition is lost. To make a user-defined alias persistent and available every time that a new Shell session is opened, you must add the alias definition to your Shell profile. You can modify your Shell profile by running the command `Notepad $Profile`. If the profile directory doesn't exist, you might have to create it first. To find out the path of your

profile, run the command `$Profile`.

Alias Limitations

Although aliases can be defined for cmdlets and used instead of cmdlet names, you can't include parameters in the definition of the aliases that you define. You must provide parameters as needed when the alias is called, exactly as you would if you called the cmdlet.

Return to top

For More Information

Exchange Management Shell Basics

1.5.2.13 User-Defined Variables

User-Defined Variables

Exchange Server 2010 > Exchange Management Shell > Exchange Management Shell Basics >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-02-27*

A variable is a location to store information. Unlike in many programming environments, in the Exchange Management Shell, you don't have to declare a variable before you use it.

You designate a variable by prepending a string with a dollar sign ($). You must enclose the string in braces ({ }) if the string contains spaces or other special characters. By using the array reference notation ([ ]), you can address the elements of an array or hash table variable. For more information, see Arrays.

See the following sections for more information about user-defined variables in the Shell:

Using Variables to Store Values

Storing the Output of a Command in a Variable

Storing the Output of the Dir Command in a Variable

Using Variables to Store Values

Variables are very useful if you want to store a value. You can assign values to variables by using an assignment operator. For more information about operators, see Syntax.

For example, to assign a value of 8 to the variable `$Example`, use the following command:

```
$Example = 8
```

This command assigns the integer 8 to the variable `$Example`. You can then call the `$Example` variable later in another command to recall the value. The values that are specified in a variable are treated exactly as if the value that it contains was typed in the location that the variable is specified. For example, the following two commands are equivalent if `$Example2` is assigned the value `"Hello"`:

```
Write-Host $Example2
Write-Host "Hello"
```

Storing the Output of a Command in a Variable

You can also store the output of commands in a variable for later use. When you assign a command to a variable, the command is evaluated at the time that command is run. The output of that command is assigned to the variable. For example, if you run `$CurrentDate = Get-Date` on the command line and then call `$CurrentDate` repeatedly over several seconds, the value that is reported is the same every time that the variable is called.

When you assign the output of a command to a variable, you can also access the properties and methods of the underlying object. For example, to view the properties and methods that are available when you assign `Get-Date` to `$CurrentDate`, you can use the `$CurrentDate | Get-Member` command. When you use the `$CurrentDate | Get-Member -MemberType Property` command, the following properties are returned in a list:

```
Name        MemberType Definition
----        ---------- ----------
Date        Property   System.DateTime Date {get;}
Day         Property   System.Int32 Day {get;}
DayOfWeek   Property   System.DayOfWeek DayOfWeek {get;}
DayOfYear   Property   System.Int32 DayOfYear {get;}
Hour        Property   System.Int32 Hour {get;}
Kind        Property   System.DateTimeKind Kind {get;}
Millisecond Property   System.Int32 Millisecond {get;}
Minute      Property   System.Int32 Minute {get;}
Month       Property   System.Int32 Month {get;}
Second      Property   System.Int32 Second {get;}
Ticks       Property   System.Int64 Ticks {get;}
TimeOfDay   Property   System.TimeSpan TimeOfDay {get;}
Year        Property   System.Int32 Year {get;}
```

You can then call any of these properties by typing the variable, a period (`.`), and then the property that you want to view. For example, to view the year that is stored on a variable, use the following command:

```
$CurrentDate.Year
```

By accessing the properties of a variable, you can easily manipulate and use each piece of information that is stored in the variable without the use of text parsing.

Storing the Output of the Dir Command in a Variable

You can also store the output of the `Dir` command in a variable. Because the `Dir` command returns multiple rows when it runs, each row that is returned is stored in a variable as a new array element. You can then access each file object that is stored in the newly created array. For more information about arrays, see Arrays.

The following command assigns the output of the `Dir` command to the `$DirOutput` variable:

```
$DirOutput = Dir
```

You can then select a specific file object by specifying the array index that you want to

view as follows:

```
$DirOutput[1].Name
```

Or you can create a simple loop that cycles through the whole array and displays the name and file size of each file that is stored in the array as follows:

```
0..$DirOutput.Length | ForEach { $DirOutput[$_].Name + " is " + $DirOutput[$_].Le
```

The following list examines this example:

- The `0..$DirOutput.Length` command instructs the Shell to output an integer from 0 to the maximum length of the array that is stored in the `$DirOutput` variable.
- The output of the `0..$DirOutput.Length` command is piped to the `ForEach` command that loops through each element of the array until it reaches the end of the array. The `ForEach` command runs the commands that are enclosed in the braces " { } ".
- The $_ variable stores the current object that is in the pipeline. In this case, the object in the pipeline is an integer that is produced by the `0..$DirOutput.Length` command as it counts from 0 to the maximum length of the array. This variable is used in the `$DirOutput[$_].Name` command and `$DirOutput[$_].Length` command to select the array element to access.
- For more information about the $_ variable, see Shell Variables.
- The plus " + " signs concatenate the output of the `$DirOutput[$_].Name` command and `$DirOutput[$_].Length` command, together with the strings supplied, to create output similar to the following:

```
abv_dg.dll is 416144 bytes long.
addxa.dll is 285056 bytes long.
ASDat.MSI is 5626880 bytes long.
ASEntDat.MSI is 5626880 bytes long.
ASEntIRS.MSI is 910336 bytes long.
ASEntSig.MSI is 45056 bytes long.
BPA.Common.dll is 211848 bytes long.
BPA.ConfigCollector.dll is 101272 bytes long.
BPA.NetworkCollector.dll is 52128 bytes long.
```

These examples show that you can use the `Length` property more than one time to display different information about the same variable. You can do this because more than one type of data is stored in the `$DirOutput` variable. The first type of data is the directory object itself, and the second type of data is the file objects. When you run the `$DirObject.Length` command, without specifying an array index, you're accessing the directory parent object types that are stored in the array. When you specify an array index, such as `$DirObject[5].Length`, you're accessing the file child objects that are stored in the directory object.

This behavior exists on many objects. You can typically access many levels of object data that are contained in a single variable. The ability to access this data makes the Shell quite flexible.

For More Information

Exchange Management Shell Basics

1.5.2.14 Shell Variables

Shell Variables

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-02-16*

Shell variables are a set of variables that are created and declared automatically by the Exchange Management Shell. The variables are maintained throughout your session as part of the system state and are available to all commands, scripts, and applications that run in that session.

The Shell supports two types of shell variables:

- Automatic variables provide a mechanism for passing information to and from commands, scripts, and applications.
- Policy variables store information about the state of the Shell.

You can use shell variables as you would use any other type of variable. For example, the `$PSHome` shell variable stores the name of the directory where the Shell is installed, and the `$_` shell variable stores the current pipeline object. You can use these variables in a command to specify the location of the file and to call a property of the `Get-ChildItem` object, as shown in the following example:

```
Get-ChildItem $PSHome | Sort {$_.Name}
```

This command retrieves all items from the Shell installation directory, and it uses the name property of the object that is stored in the `$_` variable to sort the data when it is displayed.

Common Shell Variables

The following table lists several common automatic variables that are available for your use in the Shell.

Common automatic variables

Automatic variable	Description
`$$`	Contains the last token of the last line that is received by the Shell.
`$?`	Contains the success or fail status of the last operation.
`$^`	Contains the first token of the last line that is received by the Shell.
`$_`	Contains the current pipeline object that is used in script blocks, filters, and the `Where` statement.
`$Error`	Contains objects for which an error occurred when they are processed in a cmdlet.
`$ExBin`	Displays the full path of the Exchange Server\bin directory. This variable is only available if the Exchange management tools are installed.

$ExScripts	Displays the full path of the Exchange scripts directory. This variable is only available if the Exchange management tools are installed.
$ForEach	Refers to the enumerator in a ForEach loop.
$Home	Specifies the user's root directory. It is the equivalent of %HomeDrive%%HomePath%.
$MaximumHistoryCount	Specifies the maximum number of entries that can be saved in the command history.
$PSHome	Specifies the directory where the Shell is installed.

1.5.2.15 Structured Data

Structured Data

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-05-02*

Each action that you take in the Exchange Management Shell must be done within the context of objects. The Shell uses structured collections of information called objects. These objects represent items in hierarchical data sources. When you call a cmdlet, one or more strongly typed structured objects are returned. Objects carry information about an item and about the object's structure. The object also acts as a proxy for the real item. For example, when you access a file from the Shell, you work with the object that represents that file, and not with the file itself.

Using objects gives the Shell an advantage over other traditional command shells. Traditional command shells have always supported the redirection of the output of one command to another in the form of a textual stream. This method has its disadvantages because parsing text has to be carefully controlled, usually by some kind of encoding to prevent unexpected behavior. By using objects, the Shell enables you to more easily choose the data you want to work with and use predefined methods to utilize and manipulate that data. You spend less time retrieving the data and more time using it.

The Exchange Management Shell uses this object model to pass information from one command to another by using pipelining. This avoids the problems caused by textual parsing in other command shells because the data that the Shell uses has a definite structure and is interpreted according to the object model.

For more information about pipelining, see Pipelining.

Structure of an Object

An object consists of three types of data: the object's type, its properties, and its methods.

Object Type

The data type of an object provides details about what kind of object it is. For example, an object that represents a mailbox is a **Mailbox** object. An object that represents a file is a **FileInfo** object. All objects have a distinct predefined type and namespace that the

Shell can process.

To see what object types are accepted and returned by cmdlets, see Cmdlet Input and Output Types.

Object Properties

A property is data associated with an object that specifies a particular state of that object. For example, a **Mailbox** object includes the property **EmailAddresses**. This object property represents the value of the actual attribute **ProxyAddresses** on mailbox-enabled Active Directory user accounts. This is the actual item represented by the **Mailbox** object.

The information about properties included with an object includes the current state and the definition of each property. This includes its name and the type of data that the property can take, such as Integer, Boolean, String, and so on.

Object Methods

A method is a set of instructions that defines a particular action that you can take on an object. Methods are defined based on the object type. For example, an object that is of type System.String, or String, has several methods that enable you to manipulate the string. Using the **ToUpper()** method on a string enables you to raise all of the characters within the string to uppercase. Some methods don't take arguments and some require arguments. It depends on the particular method you're using.

To call the methods available to an object, specify the method you want to use after the variable that the object is stored in. The variable and the method are separated by a period. The following example stores a string in the *$Example* variable and then calls the **ToUpper()** method to raise the string to uppercase.

```
$Example = "This is a string"
$Example.ToUpper()
THIS IS A STRING.
```

Notice that if you run `$Example` again, the string itself hasn't been modified.

```
$Example
This is a string.
```

To update the variable with the output of the method, you need to assign the output to the variable as shown in the following example.

```
$Example = "This is a string"
$Example = $Example.ToUpper()
```

Now when you run `$Example`, the string has been changed to uppercase in the variable.

```
$Example
THIS IS A STRING.
```

If an object has properties, the properties can also have their own methods. As with objects, the type of the property defines what methods are available. The property type doesn't necessarily match the object type. To call a method on an object property, you use similar syntax to when you call an object method, but you include the property along with the object. For example, a Send connector object has a property called **MaxMessageSize**, which is of type ByteQuantifiedSize. One of the methods for the type ByteQuantifiedSize is **ToMB()**. The following command displays the value stored in **MaxMessageSize**.

```
$Connector = Get-ReceiveConnector "From Internet"
$Connector.MaxMessageSize
10 MB (10,485,760 bytes)
```

If you now call the **ToMB()** method, the value stored in **MaxMessageSize** is displayed in

megabytes.

```
$Connector.MaxMessageSize.ToMB()
10
```


1.5.2.16 Arrays

Arrays

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-02-16*

An array provides a data structure that can be used to store a collection of data elements of the same type. The Exchange Management Shell supports all kinds of data elements. See the following sections for information about:

Creating Arrays

Reading Arrays

Manipulating Arrays

Associative Arrays

For detailed information about how to use arrays, run the following command in the Shell:

```
Get-Help About_Array
```

Creating Arrays

You can create and initialize arrays by assigning multiple values to a variable. The values that are stored in the array are delimited by using a comma and are separated from the variable name by the **=** assignment operator. For example, suppose you want to create an array that is named `$Example` that contains the following seven integer values: `22, 5, 10, 8, 12, 9, 80`. To create the array, enter the following command:

```
$Example = 22,5,10,8,12,9,80
```

In the array, the first data element is at index position 0, the second is at position 1, and so on.

Reading Arrays

You can reference an array by its variable name, such as `$Example`. You can reference a specific value within the array by using the index number of the position in the array where the value is stored. For example, to reference the first data element in the `$Example` array, enter the following command:

```
Write-Host $Example[0]
```

The Shell will return the value 22 because that is stored in the first array element.

Manipulating Arrays

To change the value of a single item in an array, specify the array name, the index you want to modify, the **=** assignment operator, and the new value that you want to use instead of the existing value. For example, to change the value of the second item in the `$Example` array, index position 1, to 10, enter the following command:

```
$Example[1] = 10
```

You can also use the **SetValue** method to change a value. The following example changes the second value, index position 1, of an array named `$Example` to 500:

```
$Example.SetValue(500,1)
```

You can append a value to the end of an existing array. For example, to add an additional integer, such as 200, to the `$Example` array, enter the following command:

```
$Example += 200
```

Associative Arrays

Associative arrays are the same as regular arrays. However, they enable the assignment of key-value pairs to a variable. For example, you may want to assign values to keys in an array to be called on when a command is being processed. The following example creates an associative array:

```
$Example = @{blue = 1; red = 2,3}
```

When you enter `$Example` on the command line, you see the following output:

```
Key                            Value
---                            -----
red                            {2, 3}
blue                           1
```

You can retrieve the information that is stored in the array by calling the array as follows:

```
$Example.blue
```

The previous example returns a value 1.

Because multiple values were assigned to the `red` key, those values make up a nested array. You can reference the values in this nested array by using their index value. You can retrieve the information that is stored in the key's nested array by calling the associative array, `$Example`, with the `red` key and the index of the nested array location that you want to retrieve 1, as follows:

```
$Example.red[1]
```

The previous example returns the value 3.

For more information about associative arrays, run the following command in the Shell:

```
Get-Help About_Associative_Array
```

1.5.2.17 Script Security

Script Security

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Script security in the Exchange Management Shell helps prevent harmful or otherwise unwanted scripts from running in your organization. Options are available to modify script security to meet the requirements of your organization.

You typically encounter scripts from several sources: yourself, another person in your organization, and script writers from outside your organization, such as the Internet. If you write a script, you trust the script to do what it's designed to do. If you share the script with other administrators in your organization, they too may trust the script because they trust you.

When scripts come from other sources, such as the Internet, script security is a concern. The only way that you can trust scripts from sources unknown to your organization is to inspect the script code directly and test it in an isolated lab environment. Although this process can be time consuming and tedious, we recommend this practice to prevent unintentional execution of malicious or destructive code.

The Shell supports the recommended use of digital signatures to make sure a script isn't altered after the script is created. For more information about digital signatures, see "Code-Signing Basics" later in this topic.

Script Execution Modes

Four modes of script execution in the Shell control how scripts are used, depending on how they are signed and if they are from known or unknown sources. The following table describes each script execution mode.

Important:
The remote Shell requires that the script execution mode be set to `RemotedSigned` or `Unrestricted`. For more information about the remote Shell, see Overview of Exchange Management Shell.

Script execution modes

Mode	Description
`Restricted` mode	No scripts will run, even if they are signed by a trusted publisher. This is the default script execution mode.
`AllSigned` mode	All scripts must be digitally signed by a trusted publisher before they will run.
`RemoteSigned` mode	All scripts locally created will run. Scripts downloaded from remote locations, such as the Internet, that can't be trusted, won't run.
`Unrestricted` mode	All scripts, regardless of whether they are digitally signed or trusted, will run. We don't recommend the `Unrestricted` mode unless you're running the script in a controlled test environment and not in a production

	environment.

To change the script execution mode from the default `Restricted` script execution mode, use the **Set-ExecutionPolicy** cmdlet in the Shell. This example changes the execution policy to `RemotedSigned` mode.

```
Set-ExecutionPolicy RemotedSigned
```

The Shell recognizes the change to the policy immediately.

Note:
If you have user access control enabled, you must open the Shell with elevated permissions to set the execution policy. To open the Shell with elevated permissions, right-click the Shell icon and select **Run as administrator**.

Large organizations that want to set a consistent script execution mode for all computers running the Shell should apply the script execution mode setting by using an Active Directory Group Policy. You configure the Active Directory Group Policy to set the `ExecutionPolicy` value located under the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell** registry key to the desired script execution mode.

Caution:
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Code-Signing Basics

Digital signatures are created by using a public-key signature algorithm that uses two different cryptographic keys called a key pair: the public key and the private key. The private key is known only to its owner, and the public key is available to anyone. In digital signatures, the private key generates the signature, and the corresponding public key validates the signature.

A *certificate* is a digital document that's generally used for authentication and to help secure information on open networks. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing certification authority (CA). By using a code-signing certificate, the author of the script adds a digital signature to the script file. During this process, a one-way hash of the script is created and encrypted by using the private key. The encrypted hash is a digital signature string that's added to the script file. This digital signature string is commented out so that it doesn't interfere with script functionality.

When this script is run in a Shell environment where code signing is required, a new one-way hash of the script file is produced. The one-way hash is compared to the encrypted hash included with the script file after it's decrypted by using the public key. If the script wasn't altered in any way after it was signed, the hashes will match. The computer then tries to verify that the signature is from a trusted publisher by building a certificate chain to a trusted CA. If the trust is verified, the script runs.

Whether a script is from a trusted source depends on the origin of the code-signing certificate used to digitally sign the script. There are generally two types of certificates:

- **Certificates issued by a trusted CA** The CA verifies the identity of the requestor before it issues a code-signing certificate. The issuing authority can be an external, public third party that sells certificates or an internal CA hosted by your organization. If you sign a script by using this kind of certificate, you can share the script with users on other computers that recognize and trust

the CA that issued the certificate.

- **Self-signed certificates** For this kind of certificate, your computer is the authority that creates the certificate. The benefit of a self-signed certificate is you can write, sign, and run scripts on your computer. But you can't share your script to run on other computers because your computer isn't recognized as a trusted CA. If your computer isn't trusted, your self-signed signature can't be validated, and the script won't run.

Cmdlets for Managing Code Signing

The Shell includes two cmdlets for managing code signing. The **Set-AuthenticodeSignature** cmdlet is used to add digital signatures to script files. The **Set-AuthenticodeSignature** cmdlet takes the name of the file to be signed as its first positional parameter. If the file isn't in the current working directory, you must provide the path of the file. The second input parameter for this cmdlet is the certificate used for signing. This certificate is stored in the local certificate store. You must provide this parameter in the form of a string that references the certificate. The certificate can be accessed through the Cert: drive.

The other cmdlet for managing code signing is the **Get-AuthenticodeSignature** cmdlet. Use the **Get-AuthenticodeSignature** cmdlet to check and confirm the current code-signing status for the file provided as a parameter input. If a problem occurs when you use a code-signed script, the output from the **Get-AuthenticodeSignature** cmdlet will provide useful troubleshooting information.

If you want to run scripts from outside sources, such as Microsoft, you must adapt the scripts according to the script execution mode of your environment. You can receive scripts as basic .txt files, rename them as .ps1 script files, and then after you apply any required signing, run these scripts as if you had written the scripts yourself.

For more information about digital signing and script execution policies, in the Shell, run the following command: `Get-Help About_Signing`. This command returns information that includes detailed instructions for digitally signing scripts.

1.5.2.18 Scripting with the Exchange Management Shell

Scripting with the Exchange Management Shell

Exchange Server 2010 > Exchange Management Shell > Exchange Management Shell Basics >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

For most general tasks, running cmdlets one at a time or together through pipelines is sufficient. However, sometimes you may want to automate tasks. The Exchange Management Shell supports a rich scripting language, based on the Microsoft .NET Framework, which resembles the scripting language in other shells. The Shell lets you create scripts, from simple to complex. Language constructs for looping, conditional, flow control, and variable assignment are all supported.

Every organization has tasks that are in some way unique to that organization. With a library of script files to perform these tasks, you can save time by running these scripts on any computer that has the Shell installed.

For more information about how to use scripts, see Scripting with Windows PowerShell. Because the Shell is built on Microsoft Windows PowerShell technology, the scripting guidance for Windows PowerShell applies to the Exchange Management Shell.

Running a Script Inside the Exchange Management Shell

Those familiar with the Cmd.exe environment know how to run command shell scripts. These scripts are simply text files that have the .bat file name extension. Like batch files, you can create the Shell script files by using a text editor, such as Notepad. You can also use the Windows PowerShell Integrated Scripting Environment (ISE) to write scripts. The Windows PowerShell ISE provides a rich editing experience with debugging support, syntax coloring, selective execution, and more. The Shell script files use the .ps1 file name extension.

The Shell uses a root directory for script files when they are called. By default, the root directory is the *<root drive>*:\Program Files\Microsoft\Exchange Server\V14\bin directory. You can also verify the current PSHome directory on any computer running the Shell by running `$PSHome` at a command prompt. Both of these directories are in the PATH environment variable.

If a script file is saved to the root directory, you can call it by using the script name. If the script file is located somewhere other than the current location, the path and script name must be used. If the script file is located in the current location, the script name must be prefixed by the period backslash (.\) characters.

These examples show the command syntax requirements for calling three different scripts. These examples all use the **Get-Date** cmdlet, from three different locations.

```
[PS] C:\>Get-Date-Script-A.ps1
Friday, January 20, 2006 3:13:01 PM
```

The script file Get-Date-Script-A.ps1 is located in the directory specified by `$PSHhome` and requires only the script name to run.

```
[PS] C:\>c:\workingfolder\Get-Date-Script-B.ps1
Friday, January 20, 2006 3:13:25 PM
```

The script file Get-Date-Script-B.ps1 is located in the C:\workingfolder directory so the full path must be supplied to run.

```
[PS] C:\>.\Get-Date-Script-C.ps1
Friday, January 20, 2006 3:13:40 PM
```

The script file Get-Date-Script-C.ps1 is located in the current location, C:\. Therefore, it must be prefixed with .\ to run.

```
[PS] C:\>Get-Date-Script-C.ps1
The term 'Get-Date-Script-C.ps1' is not recognized as the name of a cmdlet, funct
of the name, or if a path was included, verify that the path is correct and try a
At line:1 char:22
+ Get-Date-Script-C.ps1 <<<<
    + CategoryInfo          : ObjectNotFound: (Get-Date-Script-C.ps1:String) [],
    + FullyQualifiedErrorId : CommandNotFoundException
```

In the last example, when this same script, Get-Date-Script-C.ps1, is called without the prefix .\, the expected results are shown.

As a best practice, always give script files a descriptive name and include comments in the script to describe its purpose and to identify each point of interest. Some information about the author should also be included in case someone running the script has questions about its use. Use the number sign (#) to start comment lines inside the script body.

Running a Script from Cmd.exe

If you want to run a script on a scheduled basis using the Windows Task Scheduler service, you can call the Shell and include the script that you want to run as a parameter. If you want to use Exchange cmdlets with your script, you must direct Windows PowerShell to connect to a server running Exchange and load the Exchange cmdlets you have access to. The shortcut you use to open the Shell does this automatically. To do this when you want to run a script that contains Exchange cmdlets, you must direct Windows PowerShell to run the scripts that make this connection. This syntax is required to open Windows PowerShell, connect to an Exchange server, and run your script from the Cmd.exe command.

```
PowerShell.exe -command ". 'D:\Program Files\Microsoft\Exchange Server\V14\bin\Re
```

This example runs the script RetrieveMailboxes.ps1 from C:\My Scripts.

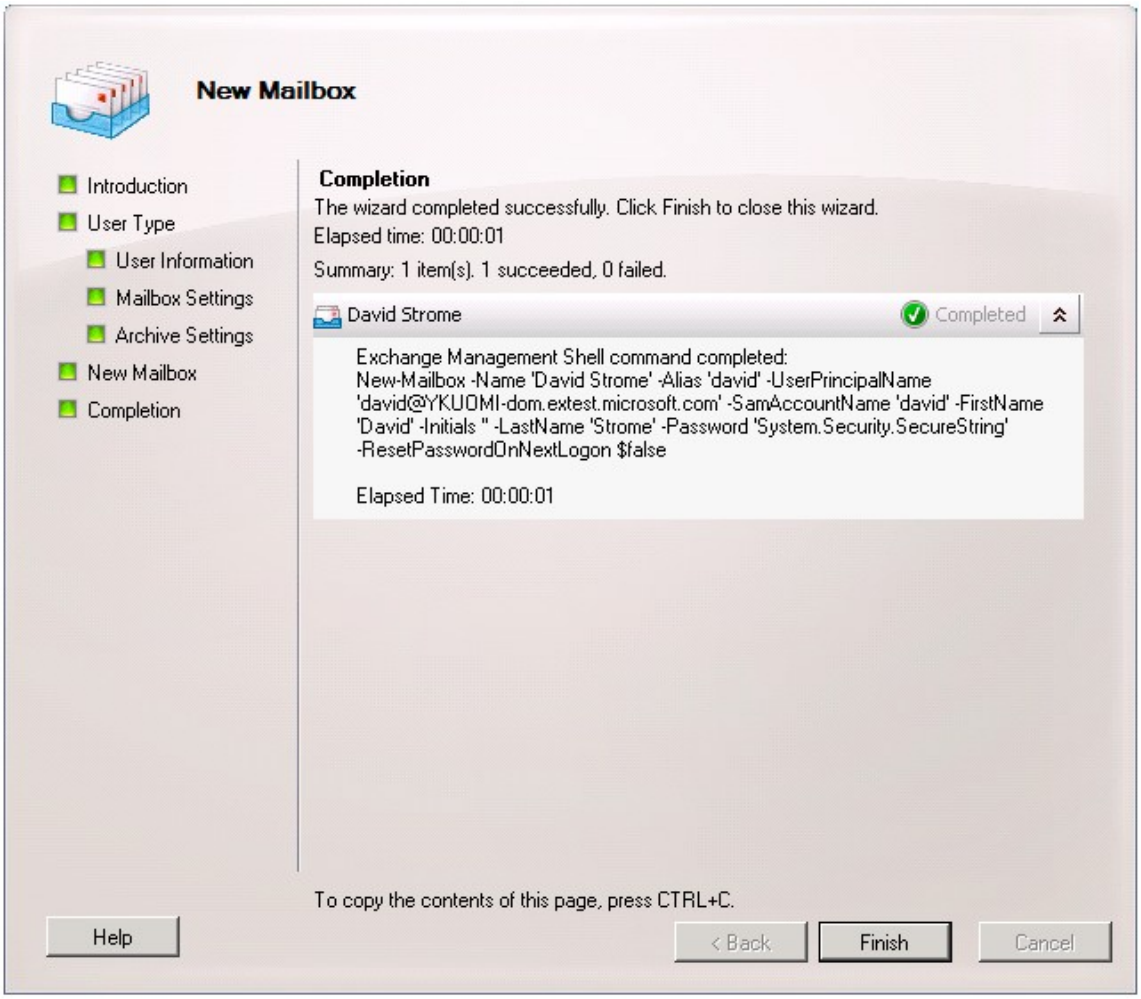
```
PowerShell.exe -command ". 'D:\Program Files\Microsoft\Exchange Server\V14\bin\Re
```

For additional options to use when you call the Shell from the Cmd.exe environment, type **PowerShell.exe /?**

Getting Hints from the Exchange Management Console

In Microsoft Exchange Server 2010, you can use the Exchange Management Console (EMC) to view detailed information about specific shell commands used to perform certain tasks. When you run a wizard in the EMC, the wizard takes the information that you entered and creates a shell command that is then run by the computer. You can copy and paste this command directly into the Shell or copy it into a text editor where you can modify it. If you examine how the EMC creates commands, you can obtain a better understanding of how to construct or modify those commands to suit your future needs.

For example, if you create a mailbox for the user David Strome, the following information is displayed on the **Completion** page of the New Mailbox wizard.



The information displayed on the **Completion** page gives you an idea of the information that you must have to make sure a similar command that you run in the Shell is completed successfully. On the **Completion** page, press CTRL+C to copy this information to the Clipboard. Then you can use a text editor to examine the command to determine what must be changed to add more mailboxes. You can also customize the command so that it can be used as part of a script that consumes a comma-separated values (CSV) file or another input source to automate creating many mailboxes.

In addition to the wizard **Completion** page, the EMC also provides the Exchange Management Shell Command Log, which when enabled, logs every command that the EMC runs. The output of this log can be saved so that you can study the commands the EMC uses as it retrieves and saves information. For more information, see Using the Exchange Management Shell Command Log to Track Tasks Performed in the EMC.

Testing Scripts

When you create scripts, you should always test them in a lab environment before you apply them in your production environment. As you test your scripts in your lab, and as you deploy them in your production environment, you can use the *WhatIf* parameter that's available on many cmdlets included in the Shell to verify that your script performs as expected. The *WhatIf* parameter instructs the command to which it is applied to run, but only to display which objects would be affected by running the command and what changes would be made to those objects, without actually changing any of those objects.

For more information about the *WhatIf* parameter, see WhatIf, Confirm, and ValidateOnly Switches.

Troubleshooting Scripts

Scripts may not work as expected for many reasons. It can be difficult to determine where the problem is and what's wrong. The Shell can help you locate general syntax errors by reporting the line and character at the point of failure. When the syntax of a script is correct but its behavior is unexpected, it can be much more difficult to diagnose the problem. The Shell includes simple debugging functionality to troubleshoot script files by examining each step that the script makes as it executes. This functionality is called *tracing*.

To enable tracing and examine each command step in a script, use the **Set-PSDebug** cmdlet with the *Trace* parameter set to a value of 1. To examine each step and each variable assignment as they are made, set the *Trace* parameter to a value of 2. To turn tracing off, set the value of the *Trace* parameter to 0 (zero).

To examine each command in a script line by line, use the **Set-PSDebug** cmdlet with the *Step* parameter. At each step, you will be prompted to continue the operation. The following choices are available in step mode.

```
[Y] Yes (continue to the next step)
[A] Yes to All (continue to the end of the script)
[N] No (stop this step)
[L] No to All (stop all remaining steps)
[S] Suspend (suspend at this point and drop to a prompt)
```

Suspend lets you exit to a prompt where you can run any command, for example, to check or set values on an object before the script can access it. When you are ready to resume script execution, type **Exit**, and control immediately returns to the point at which the script was suspended.

1.5.3 Managing Exchange Management Shell Connections

Managing Exchange Management Shell Connections

Exchange Server 2010 > Exchange Management Shell >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-21*

Enable Remote Exchange Management Shell for a User

Disable Remote Exchange Management Shell for a User

Create a Manual Remote Shell Connection

1.5.3.1 Enable Remote Exchange Management Shell for a User

Enable Remote Exchange Management Shell for a User

Exchange Server 2010 > Exchange Management Shell > Managing Exchange Management Shell

Connections >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Remote Shell in Microsoft Exchange Server 2010 enables you to manage your server running Exchange 2010 from a remote computer, either on your network or from the Internet. A user must be enabled for remote Shell before the user can use it. For more information about remote Shell, see Overview of Exchange Management Shell.

Looking for other management tasks related to remote Shell? Check out Managing Exchange Management Shell Connections.

Important:

To use remote Shell, users must be a member of a management role group or be directly assigned a management role that enables the user to run Exchange cmdlets. For more information about role groups and management roles, see Understanding Role Based Access Control.

Use the Shell to enable remote Shell for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote Shell" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:

You can't use the EMC to enable remote Shell for a user.

To enable remote Shell for a user, set the *RemotePowerShellEnabled* parameter to `$True` on the **Set-User** cmdlet. This example enables remote Shell for the user David.

```
Set-User David -RemotePowerShellEnabled $True
```

For detailed syntax and parameter information, see Set-User.

Other Tasks

After you enable remote Shell for a user, you may also want to:

- Add Members to a Role Group
- Open the Shell

1.5.3.2 Disable Remote Exchange Management Shell for a User

Disable Remote Exchange Management Shell for a User

Exchange Server 2010 > Exchange Management Shell > Managing Exchange Management Shell Connections >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Remote Shell in Microsoft Exchange Server 2010 enables you to manage your server running Exchange 2010 from a remote computer, either on your network or from the Internet. If remote Shell is disabled for a user, it can't be used by the user. For more information about remote Shell, see Overview of Exchange Management Shell.

Looking for other management tasks related to remote Shell? Check out Managing Exchange Management Shell Connections.

Use the Shell to disable remote Shell for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote Shell" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You can't use the EMC to disable remote Shell for a user.

To disable remote Shell for a user, set the *RemotePowerShellEnabled* parameter to `$False` on the **Set-User** cmdlet. This example disables remote Shell for the user David.

```
Set-User David -RemotePowerShellEnabled $False
```

For detailed syntax and parameter information, see Set-User.

1.5.3.3 Create a Manual Remote Shell Connection

Create a Manual Remote Shell Connection

Exchange Server 2010 > Exchange Management Shell > Managing Exchange Management Shell Connections >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-12*

The Exchange Management Shell is the administrative interface that enables you to manage your Microsoft Exchange Server 2010 organization from the command line. If you don't have the Exchange management tools installed but you still want to connect to, and administer, a server running Exchange 2010, this topic explains how you can create a manual remote Shell to connect to an Exchange 2010 server.

Note:
For ease of management and to receive the benefits that come with them, we recommend that you install the Exchange management tools on any computer that's used to administer an Exchange 2010 server. For more information, see the following topics:
Install the Exchange 2010 Management Tools
Open the Shell

For more information about the Exchange Management Shell, see Overview of Exchange Management Shell.

Administer Exchange 2010 Using the

Remote Shell

To administer Exchange 2010 using the remote Shell without the Exchange management tools installed, you'll need the following:

- Windows Management Framework installed

  Note:
  Windows Management Framework includes Windows PowerShell V2 and Windows Remote Management (WinRM) 2.0.

- The fully qualified domain name (FQDN) of an Exchange 2010 server in your organization
- TCP port 80 open between your client computer and the remote Exchange 2010 server
- A user that's enabled for remote Shell

Before you can connect using remote Shell, you need to install the Windows Management Framework. If you have previous versions of Windows PowerShell or WinRM, you need to uninstall them before installing the Windows Management Framework. Choose the option that matches your operating system:

- **Windows 7 or Windows Server 2008 R2** The correct version of the Windows Management Framework is already installed. You can continue on to connect remote Shell to an Exchange server.
- **Windows Vista, Windows Server 2008, Windows Server 2003, or Windows XP** Perform the steps in the following topics to install the Windows Management Framework:
  - Uninstall Previous Versions of Windows PowerShell and Windows Remote Management
  - Install Windows Management Framework

After you've installed the Windows Management Framework, see the following topics:

- Connect Remote Exchange Management Shell to an Exchange Server
- Disconnect Remote Exchange Management Shell from an Exchange Server
- Troubleshooting the Exchange Management Shell

1.5.3.3.1 Uninstall Previous Versions of Windows PowerShell and Windows Remote Management

Uninstall Previous Versions of Windows PowerShell and Windows Remote Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You need to uninstall previous versions of Windows PowerShell and Windows Remote Management (WinRM) before you can install Windows Management Framework, which includes Windows PowerShell 2.0 and WinRM 2.0. This procedure should be performed on computers running Windows Vista, Windows Server 2008, Windows Server 2003, or Windows XP.

You don't need to perform this procedure on computers running Windows 7 or Windows Server 2008 R2. The current version of Windows Management Framework is already

installed on these operating systems.

Looking for other management tasks related to Windows PowerShell and Windows Remote Management? Check out Managing Exchange Management Shell Connections.

Note:
If you want to run remote Shell on a computer that already has Microsoft Exchange Server 2010 installed, you don't need to perform this procedure. Instead, for more information about how to open the Shell with the Exchange management tools installed, see Open the Shell.

What Do You Want To Do?

- Remove Windows PowerShell on Windows Vista
- Remove Windows PowerShell on Windows Server 2008 with the built-in version of Windows PowerShell installed
- Remove Windows PowerShell on Windows Server 2008 with a pre-release version of Windows PowerShell V2 installed
- Remove WinRM on Windows Vista and Windows Server 2008
- Remove Windows PowerShell on Windows Server 2003 and Windows XP
- Remove WinRM on Windows Server 2003 and Windows XP

Remove Windows PowerShell on Windows Vista

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "PowerShell and WinRM installation" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In **Control Panel**, in **Programs**, open **Programs and Features**.
2. Uninstall any instances of Windows PowerShell that appear in the installed programs list or the installed updates list. Previous versions may appear as **Windows PowerShell(TM) V2** if you have installed the Community Technology Preview (CTP) versions of Windows PowerShell v2. If Windows PowerShell v1 is installed, it might be listed as a Windows update with one of the following Knowledge Base article numbers:
   - KB928439
   - KB923569

   Note:
   You might need to click the **View installed updates** link in the Tasks sidebar to view currently installed updates.

Remove Windows PowerShell on Windows Server 2008 with the built-in version of Windows PowerShell installed

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "PowerShell and WinRM installation" entry in the Exchange and Shell Infrastructure Permissions topic.

1. Start **Server Manager** and navigate to **Features**.
2. Click **Uninstall Features**.
3. Select **Windows PowerShell** and follow the directions to uninstall.

Remove Windows PowerShell on Windows Server 2008 with a pre-release version of Windows PowerShell 2.0 installed

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "PowerShell and WinRM installation" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In **Control Panel**, in **Programs**, open **Programs and Features**.
2. Uninstall any instances of Windows PowerShell that appear in the installed programs list or the installed updates list.

Note:
You might need to click the **View installed updates** link in the Tasks sidebar to view currently installed updates.

Remove WinRM on Windows Vista and Windows Server 2008

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "PowerShell and WinRM installation" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In **Control Panel**, in **Programs**, open **Programs and Features**.
2. Uninstall any instances of Windows Remote Management that appear in the installed programs list or the installed updates list. WinRM might be listed as a Windows update with one of the following Knowledge Base articles numbers:
   - KB936059
   - KB950099

Note:
You might need to click the **View installed updates** link in the Tasks sidebar to view currently installed updates.

Remove Windows PowerShell on Windows Server 2003 and Windows XP

1. In **Control Panel**, open **Add or Remove Programs**.
2. Uninstall any instances of Windows PowerShell that appear in the installed programs list or the installed updates list. Windows PowerShell might be listed as a Windows update with the Knowledge Base article number KB926139.

Note:
You might need to select the **Show updates** box to view currently installed updates.

Remove WinRM on Windows Server 2003 and Windows XP

1. In **Control Panel**, open **Add or Remove Programs**.

2. Uninstall any instances of Windows Remote Management that appear in the installed programs list or the installed updates list. WinRM might be listed as a Windows update with the Knowledge Base article number KB936059.

Note:
You might need to select the **Show updates** box to view currently installed updates.

Other Tasks

After you uninstall all previously installed versions of Windows PowerShell and WinRM, you need to install Windows Management Framework. For more information, see Install Windows Management Framework.

1.5.3.3.2 Install Windows Management Framework

Install Windows Management Framework

Exchange Management Shell > Managing Exchange Management Shell Connections > Create a Manual Remote Shell Connection >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Windows Management Framework, which contains Windows PowerShell 2.0 and Windows Remote Management (WinRM) 2.0, is a required component that enables you to use the EMC and the Shell. You can install Windows Management Framework on computers running Windows Vista, Windows Server 2008, Windows Server 2003, or Windows XP.

You don't need to perform this procedure on computers running Windows 7 or Windows Server 2008 R2. Windows Management Framework is already installed on these operating systems.

Looking for other management tasks related to Windows Management Framework? Check out Managing Exchange Management Shell Connections.

Note:
If you want to run the EMC or the remote Shell on a computer that already has Microsoft Exchange Server 2010 installed, you don't need to perform this procedure. Instead, for more information about how to open the EMC or the Shell with the Exchange management tools installed, see the following topics:
Exchange Management Console
Open the Shell

Prerequisites

- Before you install Windows Management Framework, you must uninstall all previous versions of Windows PowerShell and WinRM from the computer you are using. For instructions about how to uninstall Windows PowerShell and WinRM, see Uninstall Previous Versions of Windows PowerShell and Windows Remote Management.
- You must be running one of the following operating systems to install Windows Management Framework:
  - Windows Vista Service Pack 1 (SP1)
  - Windows Vista SP2
  - Windows Server 2008 SP1

- Windows Server 2008 SP2
- Windows Server 2003 SP2
- Windows XP SP3

Install Windows Management Framework

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "PowerShell and WinRM installation" entry in the Exchange and Shell Infrastructure Permissions topic.

1. Download Windows Management Framework to your local computer. See Microsoft Knowledge Base article 968930, Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0). Choose the version that includes the Windows PowerShell and WinRM components, and applies to your operating system, system architecture, and language.

   Note:
   Before you install Windows Management Framework, verify that your computer meets all of the requirements listed on the download page for the package. For more information, see the installation instructions available from the Windows Management Framework download Web site.

2. Install Windows Management Framework. Follow the wizard to install the Windows PowerShell and WinRM components.
3. Set the Windows PowerShell script execution policy to allow unsigned scripts you created and signed scripts obtained from the Internet to run by doing the following:
   3.a. Click **Start**, point to **All Programs**, point to **Accessories**, point to **Windows PowerShell**, and then click **Windows PowerShell**.
   If you're running Windows Vista, Windows 7, or Windows Server 2008 R2 and you have User Account Control (UAC) enabled, right-click **Windows PowerShell**, and then select **Run as administrator**.
   If you receive a prompt stating Windows needs your permission to continue, click **Continue**.

   Note:
   This is the only time you should need to run Windows PowerShell as the administrator. When using Windows PowerShell to connect to an Exchange 2010 server, you don't need to select **Run as administrator**.

   3.b. In Windows PowerShell, type **Set-ExecutionPolicy RemoteSigned**, and then press Enter.
4. Close Windows PowerShell.

Other Tasks

After you install Windows Management Framework, you may want to connect to a remote Exchange 2010 server. For more information, see Connect Remote Exchange Management Shell to an Exchange Server.

If you want to use the EMC, see Exchange Management Console.

1.5.3.3.3 Connect Remote Exchange Management Shell to an Exchange Server

Connect Remote Exchange Management Shell to an Exchange Server

Exchange Management Shell > Managing Exchange Management Shell Connections > Create a

Manual Remote Shell Connection >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Using the remote Shell, you can connect to a remote server running Microsoft Exchange Server 2010 to perform administration without the need to have any Exchange administration tools installed on your local computer. The remote Shell uses Windows PowerShell 2.0 and Windows Remote Management (WinRM) 2.0 to enable you to connect to remote Exchange 2010 servers.

After you connect the remote Shell to an Exchange server, the Exchange 2010 cmdlets that you have access to are made available to you in your local PowerShell session. When you run a cmdlet on your computer, the requests are sent to the remote Exchange 2010 server. The remote Exchange 2010 server then returns the results, if any, to your computer. Use the **Get-Help** cmdlet to access Help for individual cmdlets.

For more information about the remote Shell, see Create a Manual Remote Shell Connection.

Looking for other management tasks related to the remote Shell? Check out Managing Exchange Management Shell Connections.

Note:

If you want to use the Shell on an Exchange server or on a computer that has Exchange management tools installed, see Open the Shell. Use the procedure in this topic only on computers that don't have the Exchange management tools installed.

Prerequisites

- **Install Windows Management Framework** Windows Management Framework contains Windows PowerShell and WinRM. For more information, see Install Windows Management Framework.
- **Join your computer to a Windows domain** If you want to use your current network credentials, the domain you're joined to must be trusted by the domain where the Exchange server resides. Your domain doesn't need to be trusted if you manually specify credentials that are valid in the remote domain.
- **Open TCP port 80** TCP port 80 must be open between your computer and the remote Exchange 2010 server, and the port must be allowed through Windows Firewall on the Exchange 2010 server.

Use your network logon account to connect to a remote Exchange 2010 server

To connect to a remote Exchange 2010 server using the remote Shell, the user you connect as must be enabled for the remote Shell. This is enabled by default for the account used to install the first Exchange 2010 server in your organization. For more information about how to enable the remote Shell for other users, see Enable Remote Exchange Management Shell for a User.

To perform administrative tasks on a remote Exchange 2010 server, the account you use must be assigned the management roles that allow that feature to be managed. To determine the required management roles, see the Help topic for each feature. For more information about permissions, assigning management roles and management role scopes, and the rights required to administer Exchange 2010, see Understanding

Permissions.

If you want to connect to a remote Exchange server using your current network logon account, use the following procedure. You don't need to specify your user name or password. This procedure can be used even if there are no Exchange 2010 management tools installed.

1. Click **Start**, point to **All Programs**, point to **Windows PowerShell**, and then click **Windows PowerShell** or **Windows PowerShell ISE**.

   Note:
   Windows PowerShell Integrated Scripting Environment (ISE) is the new Windows PowerShell graphical console and can be used instead of the traditional text-based PowerShell console.

2. Open the connection to Exchange 2010 by running the following command.

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -Connec
```

3. Import the server-side PowerShell session into your client-side session by running the following command.

```
Import-PSSession $Session
```

After you perform this procedure, you can run Exchange cmdlets in the remote Shell.

Use a user account that you specify to connect to a remote Exchange 2010 server

To connect to a remote Exchange 2010 server using the remote Shell, the user you connect as must be enabled for the remote Shell. This is enabled by default for the account used to install the first Exchange 2010 server in your organization. For more information about how to enable the remote Shell for other users, see Enable Remote Exchange Management Shell for a User.

To perform administrative tasks on a remote Exchange 2010 server, the account you use must be assigned the management roles that allow that feature to be managed. To determine the required management roles, see the Help topic for each feature. For more information about permissions, assigning management roles and management role scopes, and the rights required to administer Exchange 2010, see Understanding Permissions.

When you connect to a remote Exchange 2010 server using a user name and password you specify, you direct the remote Shell to connect to the remote server using those credentials when it authenticates the session. The credentials can be different from your current user name and password. This is called *explicit authentication*. This procedure can be used even if there are no Exchange 2010 management tools installed.

1. Click **Start**, point to **All Programs**, point to **Windows PowerShell**, and then click **Windows PowerShell** or **Windows PowerShell ISE**.

   Note:
   Windows PowerShell Integrated Scripting Environment (ISE) is the new Windows PowerShell graphical console and can be used instead of the traditional text-based PowerShell console.

2. Enter your network credentials and store them in a variable by running the following command.

```
$UserCredential = Get-Credential
```

3. In the dialog box that opens, type the user name and password of the

administrator account that has access to administer the Exchange 2010 server you want to connect to, and then click **OK**.

4. Open the connection to Exchange 2010 by running the following command.

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -Connec
```

5. Import the server-side PowerShell session into your client-side session by running the following command.

```
Import-PSSession $Session
```

After you perform this procedure, you can run Exchange cmdlets in the remote Shell.

Other Tasks

After you connect to a remove Exchange 2010 server, you may also want to:

Disconnect Remote Exchange Management Shell from an Exchange Server

Troubleshooting the Exchange Management Shell

1.5.3.3.4 Disconnect Remote Exchange Management Shell from an Exchange Server

Disconnect Remote Exchange Management Shell from an Exchange Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

You can disconnect from a remote server running Microsoft Exchange Server 2010 using the remote Shell.

Looking for other management tasks related to the remote Shell? Check out Managing Exchange Management Shell Connections.

Caution:

If you close the Windows PowerShell window without following this procedure, the session will have to time out, and the quota for the maximum number of concurrent connections may prevent you from connecting back to the service on a timely basis.

Use the Shell to disconnect from an Exchange 2010 server

Note:

You can't use the EMC to disconnect from a remote Exchange 2010 server.

This example disconnects from the Exchange 2010 server.

```
Remove-PSSession $Session
```

1.5.4 Cmdlet Extension Agent

Cmdlet Extension Agent

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-11*

Understanding Cmdlet Extension Agents

Managing Cmdlet Extension Agents

Understanding the Scripting Agent

1.5.4.1 Understanding Cmdlet Extension Agents

Understanding Cmdlet Extension Agents

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-25*

Cmdlet extension agents are components in Microsoft Exchange Server 2010 called by Exchange 2010 cmdlets when the cmdlets run. As the name implies, cmdlet extension agents extend the capabilities of the cmdlets that call them by assisting in processing data or performing additional actions based on the requirements of the cmdlet. Cmdlet extension agents are available on any server role except the Edge Transport server role.

Agents can modify, replace, or extend functionality of Exchange Management Shell cmdlets. An agent can provide a value for a required parameter that isn't provided on a command, override a value provided by a user, perform other actions outside of the cmdlet workflow while a cmdlet runs, and more.

For example, the **New-Mailbox** cmdlet accepts the *Database* parameter that specifies the mailbox database in which to create a new mailbox. In Exchange Server 2007, if you don't specify the *Database* parameter when you run the **New-Mailbox** cmdlet, the command fails. With Exchange 2010, the **New-Mailbox** cmdlet calls the `Mailbox Resources Management` agent when the cmdlet runs. If the *Database* parameter isn't specified, the `Mailbox Resources Management` agent automatically determines a suitable mailbox database on which to create the new mailbox and inserts that value into the *Database* parameter.

Cmdlet extension agents can only be called by Exchange 2010 cmdlets. Exchange 2007 cmdlets and cmdlets provided by other Microsoft and third-party products can't call cmdlet extension agents. Scripts also can't call cmdlet extension agents directly. However, if scripts contain Exchange 2010 cmdlets, those cmdlets continue to call the cmdlet extension agents.

Looking for management tasks related to cmdlet extension agents? See Managing Cmdlet Extension Agents.

Agent Priority

The priority of an agent determines the order in which the agent is called while a cmdlet runs. An agent that has a higher priority, closer to 0, is called first. The priority of an agent becomes important when two or more agents attempt to set the value of the same property. The highest priority agent that attempts to set a property value succeeds, and all subsequent attempts to set the same property by lower priority agents are ignored. For example, if the **Name** property on an object is modified by an agent with a priority of 3 and another agent with a priority of 6 modifies the same object, the modification made by the agent with a priority of 6 is ignored.

If you want to use the `Scripting agent` to set the value of properties that might be set by other, higher priority agents, you have the following options:

- Disable the agent that currently sets the property.
- Set the `Scripting agent` to a priority higher than the existing agent you want to replace.
- Keep the priorities of the agents the same and make sure that the script that runs under the `Scripting agent` respects the value provided by the other agents.

Caution:

Changing the priority or replacing the functionality of a built-in agent is an advanced operation. Be sure that you completely understand the changes you're making.

For more information about changing the priority of an agent, see Change the Priority of a Cmdlet Extension Agent.

Built-in Agents

Exchange 2010 includes several agents that can be called when a cmdlet runs. The following table lists the agents, their order, and whether the agents are enabled by default. You can't add or remove agents to or from a server running Exchange 2010. You can, however, use the Scripting agent to run Microsoft Windows PowerShell scripts to extend the functionality of the cmdlets that use it. For more information about the Scripting agent, see Understanding the Scripting Agent.

You can enable or disable agents or change the priority of the agents if you want to replace the functionality of a particular agent with functionality you provide in a custom script that you call using the Scripting agent.

The configuration for agents is stored at the organization level. When you enable or disable an agent, or set its priority, you set that agent configuration across every server in the organization. The exception is adding scripts to the `Scripting agent`. You must update the scripts on each server individually. For more information about configuring scripts for use with the `Scripting agent`, see Understanding the Scripting Agent.

Caution:

Changing the priority of agents, or enabling or disabling agents, can cause unintended effects if you don't completely understand what each agent does and how they interact with Exchange cmdlets. Before you change the configuration of any agent, be sure you fully understand the changes and results you want and that you verify that your custom script will work as intended.

Exchange 2010 cmdlet extension agents

Agent name	Priority	Enabled by default
Admin Audit Log Agent	255	True
Scripting Agent	6	False

OAB Resources Management Agent	5	True
Provisioning Policy Agent	4	True
Mailbox Creation Time Agent	3	True
Mailbox Resources Management Agent	2	True
Rus Agent	1	True
Query Base DN Agent	0	True

1.5.4.1.1 Understanding the Scripting Agent

Understanding the Scripting Agent

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-20*

You can use the Scripting Agent cmdlet extension agent in Microsoft Exchange Server 2010 to insert your own scripting logic into the execution of Exchange cmdlets. Using the Scripting Agent, you can add conditions, override values, and set up reporting.

Caution:

When you enable the Scripting Agent cmdlet extension agent, the agent is called every time a cmdlet is run on a server running Exchange 2010. This includes not only cmdlets run directly by you in the Exchange Management Shell, but also cmdlets run by Exchange services, the Exchange Management Console (EMC), and the Exchange Control Panel (ECP). We strongly recommend that you test your scripts and any changes you make to the configuration file, before you copy your updated configuration file to your Exchange 2010 servers and enable the Scripting Agent cmdlet extension agent.

Every time an Exchange cmdlet is run, the cmdlet calls the Scripting Agent cmdlet extension agent. When this agent is called, the cmdlet checks whether any scripts are configured to be called by the cmdlet. If a script should be run for a cmdlet, the cmdlet tries to call any APIs defined in the script. The following APIs are available and are called in the following order:

1. **ProvisionDefaultProperties** This API can be used to set values of properties on objects when they're created. When you set a value, that value is returned to the cmdlet, and the cmdlet sets the value on the property. You can fill in values on properties if the user didn't specify a value, or you can override the value specified by the user. This API respects the values set by higher priority agents. The Scripting Agent cmdlet extension agent won't overwrite the values set by higher priority agents.
2. **UpdateAffectedIConfigurable** This API can be used to set values of properties on objects after all other processing has been completed, but the `Validate` API hasn't yet been called. This API respects the values set by higher priority agents. The Scripting Agent cmdlet extension agent won't overwrite the values set by higher priority agents.
3. **Validate** This API can be used to validate the values on an object's properties that are about to be set by the cmdlet. This API is called just before a cmdlet writes any data. You can configure validation checks that

allow a cmdlet to either succeed or fail. If a cmdlet passes the validation checks in this API, the cmdlet is allowed to write the data. If the cmdlet fails the validation checks, it returns any errors defined in this API.

4. **OnComplete** This API is used after all cmdlet processing is complete. It can be used to perform post-processing tasks, such as writing data to an external database.

Note:
The Scripting Agent cmdlet extension agent isn't called when cmdlets with the `Get` verb are run. Also, the agent doesn't run on Exchange servers running the Edge Transport server role because that server role doesn't support cmdlet extension agents.

The Scripting Agent is one of several cmdlet extension agents. For more information about cmdlet extension agents, see Understanding Cmdlet Extension Agents.

Contents

Scripting Agent Configuration File

The Scripting Agent configuration file contains all of the scripts that you want the Scripting Agent to run. Scripts in the configuration file are contained within XML tags that define the beginning and end of the script and various input parameters required to pass data to the script. Scripts are written using Windows PowerShell syntax. The configuration file is an XML file that uses the elements or attributes in the following table.

Element	Attribute	Description
`Configuration`	Not applicable	This element contains all of the scripts that the Scripting Agent cmdlet extension agent can run. The `Feature` tag is a child of this tag. There is only one `Configuration` tag in the configuration file.
`Feature`	Not applicable	This element contains a set of scripts that relate to a feature. Each script, defined in the `ApiCall` child tag, extends a specific part of the cmdlet execution pipeline. This tag contains the `Name` and `Cmdlets` attributes. There can be multiple `Feature` tags under the `Configuration` tag.
	`Name`	This attribute contains the name of the feature. Use this attribute to help identify which feature is extended by the scripts contained within the tag.
	`Cmdlets`	This attribute contains a list of the Exchange cmdlets that the set of scripts in this feature extension will be

		used by. You can specify multiple cmdlets by separating each cmdlet with a comma.
ApiCall	Not applicable	This element contains scripts that can extend a part of the cmdlet execution pipeline. Each script is defined by the API call name in the cmdlet execution pipeline it's extending. The following are the API names that can be extended: • ProvisionDefaultProperties • UpdateAffectedIConfigurable • Validate • OnComplete
	Name	This attribute includes the name of the API call that's extending the cmdlet execution pipeline.
Common	Not applicable	This element contains functions that can be used by any script in the configuration file.

Every Exchange 2010 server includes the file ScriptingAgentConfig.xml.sample in the *<installation path>*\V14\Bin\CmdletExtensionAgents folder. This file must be renamed to ScriptingAgentConfig.xml on every Exchange 2010 server if you enable the Scripting Agent cmdlet extension agent. The sample configuration file contains sample scripts that you can use to help you understand how to add scripts to the configuration file.

After you add a script to the configuration file, or if you make a change to the configuration file, you must update the file on every Exchange 2010 server in your organization. This must be done to make sure that each server contains an up-to-date version of the scripts that the Scripting Agent cmdlet extension agent runs.

Some characters typically used in scripts also have a special meaning in XML. To use these characters in your script, use escape sequences. For example, the following characters use an escape sequence:

- Instead of a greater than sign (>), use `>`
- Instead of a less than sign (<), use `$lt;`
- Instead of an ampersand (&), use `&`

Return to top

Enable the Scripting Agent

The Scripting Agent cmdlet extension agent is disabled by default. When you enable the Scripting Agent, the agent is enabled for the entire Exchange 2010 organization. Before you enable the Scripting Agent, verify that the Scripting Agent configuration file has been properly renamed and updated with your scripts on every Exchange 2010 server. You will receive an error message each time a cmdlet runs if you don't rename the configuration file correctly.

To enable the Scripting Agent, you must do the following:

1. Rename the ScriptingAgentConfig.xml.sample file in **<installation path>\V14\Bin\CmdletExtensionAgents** to ScriptingAgentConfig.xml on every

Exchange 2010 server in your organization.

Note:
You can copy the configuration file from one Exchange 2010 server to other Exchange 2010 servers. Be sure you update the configuration file you want to copy before you copy it.

2. Add your script to the renamed configuration file on every Exchange 2010 server in your organization.
3. Enable the Scripting Agent cmdlet extension agent. For more information about enabling cmdlet extension agents, see Enable a Cmdlet Extension Agent.

Return to top

Agent Priority

By default, the Scripting Agent cmdlet extension agent runs after every other agent, with the exception of the Admin Audit Log agent. If you want a script you created to replace an existing agent, you must either disable the other agent or change the priority of either agent so that the Scripting Agent cmdlet extension agent runs first. For more information about how to disable or change the priority of agents, see the following topics:

- Disable a Cmdlet Extension Agent
- Change the Priority of a Cmdlet Extension Agent

Return to top

1.5.4.2 Managing Cmdlet Extension Agents

Managing Cmdlet Extension Agents

Exchange Server 2010 > Exchange Management Shell > Cmdlet Extension Agent >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-02-23*

Change the Priority of a Cmdlet Extension Agent

View Existing Cmdlet Extension Agents

Enable a Cmdlet Extension Agent

Disable a Cmdlet Extension Agent

1.5.4.2.1 Change the Priority of a Cmdlet Extension Agent

Change the Priority of a Cmdlet Extension Agent

Exchange Management Shell > Cmdlet Extension Agent > Managing Cmdlet Extension Agents >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The ability to change the priority of a cmdlet extension agent in Microsoft Exchange Server

2010 is useful when you want a certain agent to be called by a cmdlet before another agent. This is especially useful if you create a custom script that's run in the `Scripting Agent`, and you want that script to take precedence over a built-in agent. For more information about the `Scripting Agent`, see Understanding the Scripting Agent.

Caution:
Changing the priority or replacing the functionality of a built-in agent is an advanced operation. Be sure that you completely understand the changes you're making.

Looking for other management tasks related to managing cmdlet extension agents? Check out Managing Cmdlet Extension Agents.

Use the Shell to change the priority of a cmdlet extension agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Cmdlet extension agents" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You can't use the EMC to change the priority of a cmdlet extension agent.

Agents are ordered from 0 to the maximum number of agents. The closer to zero the agent is, the higher the priority of the agent. Agents with a higher priority are called first. For more information about agent priorities, see Understanding Cmdlet Extension Agents.

This example changes the priority of a cmdlet extension agent by using the **Set-CmdletExtensionAgent** cmdlet. In this example, the priority of the `Scripting Agent` is changed to 3.

```
Set-CmdletExtensionAgent "Scripting Agent" -Priority 3
```

For detailed syntax and parameter information, see Set-CmdletExtensionAgent.

Other Tasks

After you change the priority of a cmdlet extension agent, you may also want to:

- Disable a Cmdlet Extension Agent
- Enable a Cmdlet Extension Agent
- View Existing Cmdlet Extension Agents

1.5.4.2.2 View Existing Cmdlet Extension Agents

View Existing Cmdlet Extension Agents

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Viewing cmdlet extension agents enables you to see which agents are run first, and

which agents are enabled in a Microsoft Exchange Server 2010 organization. For more information about pipelining and the **Format-Table** cmdlet, see the following topics:

- Pipelining
- Working with Command Output

Looking for other management tasks related to managing cmdlet extension agents? Check out Managing Cmdlet Extension Agents.

What Do You Want to Do?

- Use the Shell to view the details of a cmdlet extension agent
- Use the Shell to view multiple cmdlet extension agents

Use the Shell to view the details of a cmdlet extension agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Cmdlet extension agents" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You can't use the EMC to view existing cmdlet extension agents.

This example gets the details of a specific cmdlet extension agent by using the **Get-CmdletExtensionAgent** cmdlet. In this example, the details of the `Mailbox Permissions Agent` are returned.

```
Get-CmdletExtensionAgent "Mailbox Permissions Agent"
```

Use the Shell to view multiple cmdlet extension agents

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Cmdlet extension agents" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You cannot use the EMC to view existing cmdlet extension agents.

This example gets multiple cmdlet extension agents by using the **Get-CmdetExtensionAgent** cmdlet, and then pipes the output to the **Format-Table** cmdlet. This example displays a list of all of the cmdlet extension agents in the organization, and by using the **Format-Table** cmdlet, the **Name**, **Enabled**, and **Priority** properties of each agent are displayed in a table.

```
Get-CmdletExtensionAgent | Format-Table Name, Enabled, Priority
```

For detailed syntax and parameter information, see Get-CmdletExtensionAgent.

Other Tasks

After you view existing cmdlet extension agents, you may also want to:

- Change the Priority of a Cmdlet Extension Agent
- Disable a Cmdlet Extension Agent
- Enable a Cmdlet Extension Agent

1.5.4.2.3 Disable a Cmdlet Extension Agent

Disable a Cmdlet Extension Agent

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When you disable a cmdlet extension agent in Microsoft Exchange Server 2010, the agent is disabled on every server running Exchange 2010 in the organization. When an agent is disabled, it's not made available to cmdlets. Cmdlets can no longer use the agent to perform additional operations.

Caution:

Before you disable an agent, be sure that you're aware of how the agent works and what impact disabling the agent will have on your organization.

Looking for other management tasks related to managing cmdlet extension agents? Check out Managing Cmdlet Extension Agents.

Use the Shell to disable a cmdlet extension agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Cmdlet extension agents" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:

You can't use the EMC to disable a cmdlet extension agent.

To disable a cmdlet extension agent, use the **Disable-CmdletExtensionAgent** cmdlet. Specify the name of the agent you want to disable when you run the cmdlet. This example disables the `Scripting Agent`.

```
Disable-CmdletExtensionAgent "Scripting Agent"
```

For detailed syntax and parameter information, see Disable-CmdletExtensionAgent.

Other Tasks

After you disable a cmdlet extension agent, you may also want to:

- Change the Priority of a Cmdlet Extension Agent
- Enable a Cmdlet Extension Agent
- View Existing Cmdlet Extension Agents

1.5.4.2.4 Enable a Cmdlet Extension Agent

Enable a Cmdlet Extension Agent

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When you enable a cmdlet extension agent in Microsoft Exchange Server 2010, the agent is run on every server running Exchange 2010 in the organization. When an agent is enabled, it's made available to cmdlets, which can then use the agent to perform additional operations.

Caution:

Before you enable an agent, be sure that you're aware of how the agent works and what impact the agent will have on your organization.

Looking for other management tasks related to managing cmdlet extension agents? Check out Managing Cmdlet Extension Agents.

Prerequisites

Before you enable the `Scripting Agent`, you must verify that it's configured correctly. For more information about the `Scripting Agent`, see Understanding the Scripting Agent.

Use the Shell to enable a cmdlet extension agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Cmdlet extension agents" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:

You can't use the EMC to enable a cmdlet extension agent.

This example enables a cmdlet extension agent by using the **Enable-CmdletExtensionAgent** cmdlet. You must specify the name of the agent you want to enable when you run the cmdlet. Before you enable the `Scripting Agent`, you need to make sure that you've deployed the `ScriptingAgentConfig.xml` configuration file to all of the servers in your organization. If you don't deploy the configuration file first and you enable the `Scripting Agent`, all non-**Get** cmdlets fail when they're run. This example enables the `Scripting Agent`.

```
Enable-CmdletExtensionAgent "Scripting Agent"
```

For detailed syntax and parameter information, see Enable-CmdletExtensionAgent.

Other Tasks

After you enable a cmdlet extension agent, you may also want to:

- Change the Priority of a Cmdlet Extension Agent
- Disable a Cmdlet Extension Agent
- View Existing Cmdlet Extension Agents

1.5.5 Administrator Audit Logging

Administrator Audit Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-06-24*

In Microsoft Exchange Server 2010, administrator audit logging enables you to log each time a cmdlet is run in the Exchange Management Shell, the Exchange Management Console, or the Exchange Web management interface. For more information, see the following topics:

- Overview of Administrator Audit Logging
- Configure Administrator Audit Logging
- Search the Administrator Audit Log
- Disable Administrator Audit Logging
- Enable Administrator Audit Logging
- View Administrator Audit Logging Settings

1.5.5.1 Overview of Administrator Audit Logging

Overview of Administrator Audit Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-30*

You can use administrator audit logging in Microsoft Exchange Server 2010 to record actions taken by a user or administrator that make changes in your organization. By keeping a log of the changes, you can trace a change to the person who made it. You can also augment your change logs with detailed records of the change as it was implemented, use the records to comply with regulatory requirements and requests for discovery, and so on.

By default, audit logging is enabled in new installations of Microsoft Exchange Server 2010 Service Pack 1 (SP1).

What Gets Audited

Cmdlets that are run directly in the Exchange Management Shell are audited. In addition, operations that are performed by using the Exchange Management Console (EMC) and the Exchange Web management interface are also logged because those operations run cmdlets in the background.

Regardless of where it's run, a cmdlet is audited if it's on the cmdlet auditing list and if

one or more parameters on that cmdlet are on the parameter auditing list. **Get-** and **Search-** cmdlets aren't logged. Audit logging is intended to show what actions have been taken to modify objects in an Exchange organization rather than what objects have been viewed.

Important:

A cmdlet might not be logged if an error occurs before the cmdlet calls the Admin Audit Log cmdlet extension agent. If an error occurs after the Admin Audit Log agent is called, the cmdlet is logged together with the associated error. For more information, see the Admin Audit Log Agent section later in this topic.
Changes that are made by using Microsoft Exchange Server 2007 management tools aren't logged.
Changes to the audit log configuration are refreshed every 60 minutes on computers that have the Shell open at the time a configuration change is made. If you want to apply the changes immediately, close and then open the Shell again on each computer.

Audit Logging Configuration

By default, if audit logging is enabled, a log entry is created every time any cmdlet, other than a **Get-** or **Search-** cmdlet, is run. If you don't want to audit every cmdlet that's run, you can configure audit logging to audit only the cmdlets and parameters you're interested in. You configure audit logging with the **Set-AdminAuditLogConfig** cmdlet. The parameters referenced in the following sections are used with this cmdlet.

Important:

Changes to the administrator audit log configuration are always logged, regardless of whether the **Set-AdministratorAuditLog** cmdlet is included in the list of cmdlets being audited, or whether audit logging is enabled or disabled.

When a command is run, Exchange inspects the cmdlet that was used. If the cmdlet that was run matches any of the cmdlets provided with the *AdminAuditLogConfigCmdlets* parameter, Exchange then checks the parameters specified in the *AdminAuditLogConfigParameters* parameter. If at least one or more parameters from the parameters list are matched, Exchange logs the cmdlet that was run in the mailbox specified by using the *AdminAuditLogMailbox* parameter.

Note:

With Exchange 2010 release to manufacturing (RTM), you specify an administrator audit log mailbox. Administrator audit logging in Exchange 2010 SP1 uses a dedicated mailbox. This dedicated mailbox can't be changed or configured.

The following sections contain more information about each aspect of the audit logging configuration.

For more information about how to manage audit logging configuration, see Configure Administrator Audit Logging.

Cmdlets

You can control which cmdlets are audited by providing a list of cmdlets, and their parameters, that you want to log. When you configure audit logging, you can specify to audit every cmdlet, or you can specify the cmdlets you want to audit using the *AdminAuditLogConfigCmdlets* parameter. You can specify full cmdlet names, such as **New-Mailbox**, or you can specify partial cmdlet names and enclose those names in wildcard characters, such as an asterisk (*). For example, if you want to log when any cmdlet that contains the string `Transport` runs, you can specify a value of `*Transport*`. You can use a mix of full cmdlet names and partial cmdlet names at the same time to tailor the audit logging configuration to your needs.

Parameters

In addition to specifying which cmdlets you want to log, you can also indicate that cmdlets should only be logged if certain parameters on those cmdlets are used. Use the *AdminAuditLogConfigParameters* parameter to specify which parameters should be logged. As with cmdlets, you can specify full parameter names, such as `Database`, or partial parameter names enclosed in wildcard characters (*), such as `*Address*`, or a combination of both.

Audit Log Age Limit

By default, audit logging is configured to store audit log entries for 90 days. After 90 days, the audit log entry is deleted. You can change the audit log age limit using the *AdminAuditLogAgeLimit* parameter. You can specify the number of days, hours, minutes, and seconds that audit log entries should be kept. To specify a value, use the format `dd.hh:mm:ss` where the following applies:

- **dd** The number of days to keep the audit log entry.
- **hh** The number of hours to keep the audit log entry.
- **mm** The number of minutes to keep the audit log entry.
- **ss** The number of seconds to keep the audit log entry.

You must specify multiple years using the dd field. For example, 365 days equals one year; 730 days equals two years; 913 days equals two years and six months. For example, to set the audit log age limit to two years and six months, use the syntax `913.00:00:00`.

Caution:

You can set the audit log age limit to a value that's less than the current age limit. If you do this, any audit log entry whose age exceeds the new age limit is deleted.
If you set the age limit to 0, Exchange deletes all the entries in the audit log.
We recommend that you grant permissions to configure the audit log age limit only to highly trusted users.

Test Cmdlets

Cmdlets that begin with the verb **Test** aren't logged by default. You can indicate that **Test** cmdlets should be logged by setting the *TestCmdletLoggingEnabled* parameter to `$true`. Although you can enable logging of test cmdlets, we recommend that you do this only for short periods of time. This is because test cmdlets can produce a large amount of information.

Audit Logs

Each time that a cmdlet is logged, an audit log entry is created. Audit logs are stored in a hidden, dedicated arbitration mailbox that can be accessed only by using the Exchange Control Panel (ECP) **Auditing Reports** page or the **Search-AdminAuditLog** or **New-AdminAuditLogSearch** cmdlet. Audit logs can't be opened by using Microsoft Office Outlook Web App or Microsoft Outlook. The following sections provide information about the following:

- What's included in the logs
- Reports available on the ECP **Auditing Reports** page
- Audit log search cmdlets

Note:

With Exchange 2010 release to manufacturing (RTM), you specify an administrator audit log mailbox. Administrator audit logging in Exchange 2010 SP1 uses a dedicated mailbox. This dedicated mailbox can't be changed or configured.
The ECP **Auditing Reports** page, and the **Search-AdminAuditLog** and **New-AdminAuditLogSearch** cmdlets work only with Exchange 2010 SP1 administrator audit logs. To view the contents of an Exchange 2010 RTM audit log mailbox, you must open that mailbox using Outlook Web App or an e-mail client such as Outlook.

Audit Log Contents

Each audit log entry contains the information described in the following table. The audit log contains one or more audit log entries. The number of audit log entries is controlled by the audit log age limit that's specified by using the **Set-AdminAuditLog** cmdlet. Any audit log entry that exceeds the age limit is deleted.

Audit log entry fields

Field	Description
RunspaceId	This field is used internally by Exchange.
ObjectModified	This field contains the object that was modified by the cmdlet specified in the CmdletName field.
CmdletName	This field contains the name of the cmdlet that was run by the user in the Caller field.
CmdletParameters	This field contains the parameters that were specified when the cmdlet in the CmdletName field was run. Also stored in this field, but not visible in the default output, is the value specified with the parameter, if any. For more information about how to access the additional information in this field, see Search the Administrator Audit Log.
ModifiedProperties	This field contains the properties that were modified on the object in the ObjectModified field. Also stored in this field, but not visible in the default output, are the old value of the property and the new value that was stored. For more information about how to access the additional information in this field, see Search the Administrator Audit Log.
Caller	This field contains the user account of the user who ran the cmdlet in the CmdletName field.
Succeeded	This field specifies whether the cmdlet in the CmdletName field ran successfully. The value is either True or False.
Error	This field contains the error message generated if the cmdlet in the CmdletName field failed to complete successfully.
RunDate	This field contains the date and time when the cmdlet in the CmdletName field was run. The date and time are stored in Coordinated Universal Time (UTC) format.
Identity	This field is used internally by Exchange.
IsValid	This field is used internally by Exchange.

ECP Audit Reports

The **Auditing Reports** page in the ECP has several reports that provide information on

various types of compliance and administrative configuration changes. The following reports provide information on configuration changes in your organization:

- **Administrator Role Changes** This report enables you to search for changes to management role groups that you specify within a specified timeframe. The results that are returned include the role groups that have been changed, who changed them and when, and what changes were made. A maximum of 3,000 entries can be returned. If your search might return more than 3,000 entries, use the **Export Configuration Changes** report or the **Search-AdminAuditLog** cmdlet.
- **Export Configuration Changes** This report enables you to export the audit log entries recorded within a specified timeframe to a XML file and then email the file to a recipient you specify. For more information about the contents of the XML file, see Administrator Audit Log Structure.

For information about how to use these reports, see Search the Administrator Audit Log.

Reports for litigation hold, mailbox configuration changes, and non-owner mailbox access are also included on the **Auditing Reports** page. For more information about these reports, see:

- Understanding Litigation Hold
- Understanding Mailbox Audit Logging

Search-AdminAuditLog Cmdlet

When you run the **Search-AdminAuditLog** cmdlet, all the audit log entries that match the search criteria that you specify are returned. You can specify the following search criteria:

- **Cmdlets** Specifies the cmdlets you want to search for in the administrator audit log.
- **Parameters** Specifies the parameters you want to search for in the administrator audit log. You can only search for parameters if you specify a cmdlet to search for.
- **End date** Scopes the administrator audit log results to log entries that occurred on or before the specified date.
- **Start date** Scopes the administrator audit log results to log entries that occurred on or after the specified date.
- **Object IDs** Specifies that only administrator audit log entries that contain the specified changed objects should be returned
- **User IDs** Specifies that only the administrator audit log entries that contain the specified IDs of the user who ran the cmdlet should be returned.
- **Successful completion** Specifies whether only administrator audit log entries that indicated a success or failure should be returned.

Each audit log entry returned contains the information described in the table in Audit Log Contents. By default, only the first 1,000 log entries that match the criteria you specify are returned. However, you can override this default and return more or fewer entries using the *ResultSize* parameter. You can specify a value of `Unlimited` with the *ResultSize* parameter to return all log entries that match the specified criteria.

For information about how to use the **Search-AdminAuditLog** cmdlet, see Search the Administrator Audit Log.

New-AdminAuditLogSearch Cmdlet

The **New-AdminAuditLogSearch** cmdlet searches the audit log just like the **Search-AdminAuditLog** cmdlet. However, instead of displaying the results of the audit log search in the Shell, the **New-AdminAuditLogSearch** cmdlet performs the search and then sends the results of the search to a recipient you specify via e-mail. The results are included as an XML attachment to the e-mail message.

You can use the same search criteria with the **New-AdminAuditLogSearch** cmdlet that's used on the **Search-AdminAuditLog** cmdlet. For a list of the search criteria, see Search-AdminAuditLog Cmdlet.

After you run the **New-AdminAuditLogSearch** cmdlet, Exchange may take up to 15 minutes to deliver the report to the specified recipient. The XML file attached report can be a maximum of 10 megabytes (MB). The XML file contains the same information described in the table in Audit Log Contents. For more information about the structure of the XML file, see Administrator Audit Log Structure.

Note:

Outlook Web App doesn't allow you to open XML attachments by default. You can either configure Exchange to allow XML attachments to be viewed using Outlook Web App, or you can use another e-mail client, such as Microsoft Office Outlook, to view the attachment. For information about how to configure Outlook Web App to allow you to view an XML attachment, see View or Configure Outlook Web App Virtual Directories.

For information about how to use the **New-AdminAuditLogSearch** cmdlet, see Search the Administrator Audit Log.

Manual Audit Log Entries

In addition to logging Exchange cmdlets when they're run, Exchange 2010 SP1 enables you to manually write log entries to the audit log. Exchange 2010 SP1 supports this using the **Write-AdminAuditLog** cmdlet. Situations where you might want to add a manual log entry include the following:

- Custom script entry and exit
- Change control information
- Maintenance start and end times

With the **Write-AdminAuditLog** cmdlet, you specify a string of text to include in the audit log using the *Comment* parameter. The *Comment* parameter accepts an alphanumeric string up to 500 characters. Included in the manual audit log entry along with the comment string is all of the same information captured when an Exchange cmdlet is logged. For a description of each field included in the audit log, see the table in Audit Log Contents.

You can retrieve manual audit log entries the same way as any other log entry, using the ECP **Auditing Reports** page or using the **Search-AdminAuditLog** or **New-AdminAuditLogSearch** cmdlets.

To view the contents of the *Comment* parameter on the **Write-AdminAuditLog** cmdlet in a manual audit log entry, see Search the Administrator Audit Log.

Active Directory Replication

Administrator audit logging relies on Active Directory replication to replicate the configuration settings you specify to the domain controllers in your organization. Depending on your replication settings, the changes you make may not be immediately applied to all servers running Exchange 2010 in your organization.

Admin Audit Log Agent

The Admin Audit Log built-in cmdlet extension agent performs administrator audit logging of cmdlet operations in Exchange 2010. This agent reads the audit log configuration, and then performs an evaluation of each cmdlet run in your organization. If the criteria you've specified in the audit log configuration matches the cmdlet that's being run, the agent generates an audit log.

The Admin Audit Log agent is enabled by default, which is required for audit logging to function. It can't be disabled, and its priority can't be changed. For more information about cmdlet extension agents, see Understanding Cmdlet Extension Agents.

How Admin Audit Logs May Cause Rapid Database Growth

By default, the admin audit log is enabled in Exchange Server 2010. The log results are stored in the arbitration mailbox in the AdminAuditLogs folder. If cmdlets are executed in the Exchange Management Shell frequently, multiple log entries are generated, and may cause the size of the database to grow quickly. This behavior may occur even if no user mailboxes exist.

To determine the size of the AdminAuditLogs folder, run the following cmdlet in the Exchange Management Shell: **Get-MailboxFolderstatistics** *"Guid of arbitration mailbox"* **-FolderScope RecoverableItems –IncludeAnalysis**. Next, view the item count and size of the AdminAuditLogs folder.

If the item count and the size of the AdminAuditLogs folder are high, run the following cmdlet to delete the items from the folder: **Search-Mailbox** *Guid of arbitration mailbox* **-Dumpsteronly -deletecontent**.

A cmdlet that is being executed frequently may be causing the database growth. Typically, the cmdlet is in a script that is scheduled to run periodically. Identify the cmdlet that is causing the admin audit log to grow. After you confirm that the cmdlet can be excluded from the admin audit log, run the following cmdlet in the Exchange Management Shell: **Set-AdminAuditLogConfig AdminAuditLogExcludedCmdlets** *cmdlet name*. For example, run the following cmdlet: **Set-AdminAuditLogConfig AdminAuditLogExcludedCmdlets Add-DistributionGroupMember**. After you run the cmdlet, you must wait for replication to be completed.

1.5.5.1.1 Administrator Audit Log Structure

Administrator Audit Log Structure

Exchange Management Shell > Administrator Audit Logging > Overview of Administrator Audit Logging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-06-24*

Administrator audit logs contain a record of all the cmdlets and parameters that have been run in the Exchange Management Shell and by the Exchange Management Console (EMC) and Exchange Control Panel (ECP). They're created on-demand when you run the Export Configuration Changes report in the ECP, or when you run the **New-AdminAuditLogSearch** cmdlet in the Shell. For more information about audit logs, see Overview of Administrator Audit Logging.

The audit logs are XML files and can contain multiple audit log entries. The following table describes each XML tag and its associated attributes.

Audit log XML tags and attributes

Element	Attribute	Description

<?xml version="1.0" encoding="utf-8"?>	N/A	This is the XML document declaration tag. It's included in every audit log XML file and contains the XML version number and the character encoding value.
SearchResults	N/A	This tag contains all the audit log entries in the XML file. The Event tag is a child of this tag. There is only one SearchResults tag per XML file.
Event		This tag contains the audit log entry for an individual cmdlet. This tag contains the Caller, Cmdlet, ObjectModified, RunDate, Succeeded, and Error attributes. The CmdletParameters and ModifiedProperties tags are children of this tag. There is one Event tag per audit log entry.
	Caller	This attribute contains the user account of the user who ran the cmdlet in the Cmdlet attribute.
	Cmdlet	This attribute contains the name of the cmdlet that was run by the user in the Caller attribute.
	ObjectModified	This attribute contains the object that was modified by the cmdlet specified in the Cmdlet attribute. The ModifiedProperties tag shows which properties were modified on this object.
	RunDate	This attribute contains the date and time when the cmdlet in the Cmdlet attribute was run. The date and time are stored in Coordinated Universal Time (UTC) format.
	Succeeded	This attribute specifies whether the cmdlet in the Cmdlet attribute ran successfully. The value is

		either `True` or `False`.
	`Error`	This attribute contains the error message generated if the cmdlet in the `Cmdlet` attribute failed to complete successfully. If no error was encountered, the value is set to `None`.
`CmdletParameters`	`N/A`	This tag contains all of the parameters specified when the cmdlet was run. The `Parameter` tag is a child of this tag. There is one `CmdletParameters` tag per `Event` tag.
`Parameter`		This tag contains an individual parameter that was specified when the cmdlet was run. This tag contains the `Name` and `Value` attributes. There can be multiple `Parameter` tags per `CmdletParameters` tag.
	`Name`	This attribute contains the name of the parameter that was specified on the cmdlet that was run.
	`Value`	This attribute contains the value that was provided on the parameter specified in the `Name` attribute.
`ModifiedProperties`	`N/A`	This tag contains all of the properties that were modified by the cmdlet that was run. The `Property` tag is a child of this tag. There is one `ModifiedProperties` tag per `Event` tag.
`Property`		This tag contains an individual property that was specified when the cmdlet was run. This tag contains the `Name`, `OldValue`, and `NewValue` attributes. There can be multiple

		Property tags per ModifiedProperties tag.
	Name	This attribute contains the name of the property that was modified when the cmdlet was run.
	OldValue	This attribute contains the value that was contained in the property specified in the Name attribute before it was changed.
	NewValue	This attribute contains the value that the property in the Name attribute was changed to.

Example audit log entry

The following is an example of a typical audit log entry. Based on the information in log entry, we know the following occurred:

- On 3/5/2010 at 11:59 P.M. UTC, the user Administrator ran the cmdlet **Set-Mailbox**.
- The two following parameters were provided when the **Set-Mailbox** cmdlet was run:
  - *Identity* with a value of david
  - *ProhibitSendReceiveQuota* with a value of 1.727 GB
- The two following properties on the object david were modified:
  - *ProhibitSendReceiveQuota* with a new value of 1.727 GB, which replaced the old value of 523.4 MB
  - *ObjectState* with a new value of Changed, which replaced the old value of Unchanged
- The operation completed successfully without any errors.

```
<?xml version="1.0" encoding="utf-8"?>
<SearchResults>
  <Event Caller="Wally14.extest.microsoft.com/Users/Administrator" Cmdlet="Set-Ma
    <CmdletParameters>
      <Parameter Name="Identity" Value="david" />
      <Parameter Name="ProhibitSendReceiveQuota" Value="1.727 GB (1,854,030,822 b
    </CmdletParameters>
    <ModifiedProperties>
      <Property Name="ProhibitSendReceiveQuota" OldValue=" 523.4 MB (548,845,001
      <Property Name="ObjectState" OldValue="Unchanged" NewValue="Changed" />
    </ModifiedProperties>
  </Event>
</SearchResults>
```


1.5.5.2 Configure Administrator Audit Logging

Configure Administrator Audit Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Administrator audit logging in Microsoft Exchange Server 2010 enables you to create a log entry each time a specified cmdlet is run. Log entries detail what cmdlet was run, which parameters were used, who ran the cmdlet, and what objects were affected. For more information about administrator audit logging, see Overview of Administrator Audit Logging.

You must use the Shell to configure administrator audit logging.

Important:

Administrator audit logging relies on Active Directory replication to replicate the configuration settings you specify to the domain controllers in your organization. Depending on your replication settings, the changes you make may not be immediately applied to all Exchange 2010 servers in your organization.
Changes to the audit log configuration are refreshed every 60 minutes on computers that have the Shell open at the time a configuration change is made. If you want to apply the changes immediately, close and then open the Shell again on each computer.

Specify the cmdlets to be audited

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:

You can't use the EMC to specify the cmdlets to be audited.

By default, audit logging creates a log entry for every cmdlet that's run. If you're enabling audit logging for the first time and want this behavior, you don't have to change the cmdlet audit list. If you've previously specified cmdlets to audit and now want to audit all cmdlets, you can audit all cmdlets by specifying the asterisk (*) wildcard character with the *AdminAuditLogCmdlets* parameter on the **Set-AdminAuditLogConfig** cmdlet, as shown in the following command.

```
Set-AdminAuditLogConfig -AdminAuditLogCmdlets *
```

You can specify which cmdlets to audit by providing a list of cmdlets using the *AdminAuditLogCmdlets* parameter. When you provide the list of cmdlets to audit, you can provide single cmdlets, cmdlets with the asterisk (*) wildcard characters, or a mix of both. Each entry in the list is separated by commas. The following values are all valid:

- `New-Mailbox`
- `*TransportRule`
- `*Management*`
- `Set-Transport*`

This example audits the cmdlets specified in the preceding list.

```
Set-AdminAuditLogConfig -AdminAuditLogCmdlets New-Mailbox, *TransportRule, *Manag
```

For detailed syntax and parameter information, see Set-AdminAuditLogConfig.

Specify the parameters to be audited

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You can't use the EMC to specify the parameters to be audited.

By default, audit logging creates a log entry for every cmdlet that's run, regardless of the parameters specified. If you're enabling audit logging for the first time and want this behavior, you don't have to change the parameter audit list. If you've previously specified parameters to audit and now want to audit all parameters, you can do so by specifying the asterisk (*) wildcard character with the *AdminAuditLogParameters* parameter on the **Set-AdminAuditLogConfig** cmdlet, as shown in the following command.

```
Set-AdminAuditLogConfig -AdminAuditLogParameters *
```

You can specify which parameters you want to audit by using the *AdminAuditLogParameters* parameter. When you provide the list of parameters to audit, you can provide single parameters, parameters with the asterisk (*) wildcard characters, or a mix of both. Each entry in the list is separated by commas. The following values are all valid:

- `Database`
- `*Address*`
- `Custom*`
- `*Region`

Note:
For an audit log entry to be created when a command is run, the command must include at least one or more parameters that exist on at least one or more cmdlets specified with the *AdminAuditLogCmdlets* parameter.

This example audits the parameters specified in the preceding list.

```
Set-AdminAuditLogConfig -AdminAuditLogParameters Database, *Address*, Custom*, *R
```

For detailed syntax and parameter information, see Set-AdminAuditLogConfig.

Specify the audit log age limit

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You can't use the EMC to specify the audit log age limit.

The audit log age limit determines how long audit log entries will be retained. When a log entry exceeds the age limit, it's deleted. The default is one year.

You can specify the number of days, hours, minutes, and seconds that audit log entries should be kept. To specify a value, use the format dd.hh.mm:ss where the following applies:

- **dd** Number of days to keep the audit log entry
- **hh** Number of hours to keep the audit log entry
- **mm** Number of minutes to keep the audit log entry
- **ss** Number of seconds to keep the audit log entry

Caution:
You can set the audit log age limit to a value that's less than the current age limit. If you do this, any audit log entry whose age exceeds the new age limit will be deleted.
If you set the age limit to 0, Exchange deletes all the entries in the audit log.
We recommend that you grant permissions to configure the audit log age limit only to

highly trusted users.

This example specifies an age limit of two years and six months.

```
Set-AdminAuditLogConfig -AdminAuditLogAgeLimit 913.00:00:00
```

For detailed syntax and parameter information, see Set-AdminAuditLogConfig.

Enable or disable logging of Test cmdlets

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You can't use the EMC to enable or disable logging of **Test** cmdlets.

Cmdlets that start with the verb **Test** aren't logged by default. This is because **Test** cmdlets can generate a significant amount of data in a short time. Only enable the logging of **Test** cmdlets for short periods of time.

This command enables the logging of **Test** cmdlets.

```
Set-AdminAuditLogConfig -TestCmdletLoggingEnabled $True
```

This command disables the logging of **Test** cmdlets.

```
Set-AdminAuditLogConfig -TestCmdletLoggingEnabled $False
```

For detailed syntax and parameter information, see Set-AdminAuditLogConfig.

Other Tasks

After you configure administrator audit logging, you may also want to:

- Search the Administrator Audit Log
- View Administrator Audit Logging Settings
- Disable Administrator Audit Logging
- Configure Administrator Audit Logging

1.5.5.3 Search the Administrator Audit Log

Search the Administrator Audit Log

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can search the administrator audit logs to discover who made changes to organization, server, and recipient configuration. This can be helpful when trying to track the cause of unexpected behavior, to identify a malicious administrator, or to verify that compliance requirements are being met. For more information about administrator audit logging, see Overview of Administrator Audit Logging.

Note:
The Exchange Control Panel (ECP) Auditing Reports page, the **Search-AdminAuditLog** cmdlet, and the **New-AdminAuditLogSearch** cmdlet work only with Microsoft Exchange Server 2010 Service Pack 1 (SP1) administrator audit logs. To view the contents of an Exchange 2010 release to manufacturing (RTM) audit log mailbox, you must open that mailbox using Microsoft Office Outlook Web App or an e-mail client such as Microsoft Outlook.

If you want to search for changes to litigation hold changes, see Managing Discovery.

If you want to search the mailbox audit log, see Managing Mailbox Audit Logging.

Prerequisites

Administrator audit logging must be enabled for audit log entries to be stored in the audit log. For information about how to enable audit logging, see Configure Administrator Audit Logging.

Use the ECP to view management role group changes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "View-only administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

If you want to know what changes to management role group membership have been made to role groups in your organization, you can use the Administrator Role Changes report on the Auditing Reports page in the ECP. Using the Administrator Role Changes report, you can view a list of role groups that have changed during a specified date range. You can also select the specific role groups you want to view changes for.

1. Log on to Outlook Web App.
2. Click **Options**, and then click **See All Options**.
3. In the drop-down list box next to **Mail > Options**, click **My Organization** from the **Select what to manage** list.
4. Click **Reporting**, click **Auditing**, and then click **Administrator Role Changes**.
5. Select a date range using the **Start Date** and **End Date** fields.
6. Select the role groups you want to show changes for from the **Select Role Groups** field, or leave this field blank to search for changes in all role groups.
7. Click **Search**.

If any changes are found using the criteria you specified, a list of changes will be displayed in the **Search Results** pane. Clicking a role group displays the changes to the role group in the details pane.

Use the ECP to export the administrator audit log

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "View-only administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

If you want to create an XML file that contains changes made to your organization, you can use the Export Configuration Changes report on the Auditing Reports page in the ECP. Using the Export Configuration Changes report, you can specify a date range to search for audit log entries that contain changes made by users you specify. The XML file

is then sent to a recipient as an e-mail attachment. The maximum size of the XML file is 10 megabytes (MB).

Note:
Outlook Web App doesn't allow you to open XML attachments by default. You can either configure Exchange to allow XML attachments to be viewed using Outlook Web App, or you can use another e-mail client, such as Microsoft Office Outlook, to view the attachment. For information about how to configure Outlook Web App to allow you to view an XML attachment, see View or Configure Outlook Web App Virtual Directories.

1. Log on to Outlook Web App.
2. Click **Options**, and then click **See All Options**.
3. In the drop-down list box next to **Mail > Options**, click **My Organization** from the **Select what to manage** list.
4. Click **Reporting**, click **Auditing**, and then click **Export Configuration Changes**.
5. Select a date range using the **Start Date** and **End Date** fields.
6. Select the recipient who should receive the XML file using the **Select users to email the audit log to** field.
7. Click **Export**.

If any log entries are found using the criteria you specified, an XML file will be created and sent as an e-mail attachment to the recipient you specified.

Use the Shell to search for audit log entries

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "View-only administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You can't use the EMC to search for audit log entries.

You can use the Shell to search for audit log entries that meet the criteria you specify. For a list of search criteria, see Overview of Administrator Audit Logging. This procedure uses the **Search-AdminAuditLog** cmdlet and displays search results in the Shell. It can be used when you need to return a set of results that exceeds the limits defined on the **New-AdminAuditLogSearch** cmdlet or in the ECP Audit Reporting reports.

If you want to send audit log search results in an e-mail attachment to a recipient, see Use the Shell to search for audit log entries and send results to a recipient later in this topic.

To search the audit log for criteria you specify, use the following syntax.

```
Search-AdminAuditLog - Cmdlets <cmdlet 1, cmdlet 2, ...> -Parameters <parameter 1
```

Note:
The **Search-AdminAuditLog** cmdlet returns a maximum of 1,000 log entries by default. Use the *ResultSize* parameter to specify up to 250,000 log entries.

This example performs a search for all audit log entries with the following criteria:

- **Start date** 02/04/2010
- **End date** 04/03/2010
- **User IDs** davids, chrisd, kima
- **Cmdlets** **Set-Mailbox**
- **Parameters** *ProhibitSendQuota*, *ProhibitSendReceiveQuota*, *IssueWarningQuota*, *MaxSendsize*, *MaxReceiveSize*

```
Search-AdminAuditLog -Cmdlets Set-Mailbox -Parameters ProhibitSendQuota, Prohibit
```

This example searches for changes made to a specific mailbox. This is useful if you're troubleshooting or you need to provide information for an investigation. The following criteria are used:

- **Start date** 01/01/2010
- **End date** 08/03/2010
- **Object ID** contoso.com/Users/DavidS

```
Search-AdminAuditLog -StartDate 01/01/2010 -EndDate 08/03/2010 -ObjectID contoso.
```

If your searches return many log entries, we recommend that you use the procedure provided in Use the Shell to search for audit log entries and send results to a recipient later in this topic. The procedure in that section sends an XML file as an e-mail attachment to the recipients you specify, enabling you to more easily extract the data you're interested in.

For detailed syntax and parameter information, see Search-AdminAuditLog.

View details of audit log entries

The **Search-AdminAuditLog** cmdlet returns the fields described in the "Audit log contents" section of Overview of Administrator Audit Logging. Of the fields returned by the cmdlet, two fields, **CmdletParameters** and **ModifiedProperties**, contain additional information that isn't viewable by default.

To view the contents of the **CmdletParameters** and **ModifiedProperties** fields, use the following steps. Or, you can use the procedure in Use the Shell to search for audit log entries and send results to a recipient later in this topic to create an XML file.

This procedure uses the following concepts:

- Arrays
- User-Defined Variables

1. Decide the criteria you want to search for, run the **Search-AdminAuditLog** cmdlet, and store the results in a variable using the following command.

   ```
   $Results = Search-AdminAuditLog <search criteria>
   ```

2. Each audit log entry is stored as an array element in the variable `$Results`. You can select an array element by specifying its array element index. Array element indexes start at 0 for the first array element. For example, to retrieve the 5th array element, which has an index of 4, use the following command.

   ```
   $Results[4]
   ```

3. The previous command returns the log entry stored in array element 4. To see the contents of the **CmdletParameters** and **ModifiedProperties** fields for this log entry, use the following commands.

   ```
   $Results[4].CmdletParameters
   $Results[4].ModifiedProperties
   ```

4. To view the contents of the **CmdletParameters** or **ModifiedParameters** fields in another log entry, change the array element index.

Use the Shell to search for audit log entries and send results to a recipient

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "View-only administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You can't use the EMC to search for audit log entries and send results to a recipient.

You can use the Shell to search for audit log entries that meet the criteria you specify, and then send those results to a recipient you specify as an XML file attachment. The results are sent to the recipient within 15 minutes. For a list of search criteria, see Overview of Administrator Audit Logging.

Note:
Outlook Web App doesn't allow you to open XML attachments by default. You can either configure Exchange to allow XML attachments to be viewed using Outlook Web App, or you can use another e-mail client, such as Microsoft Office Outlook, to view the attachment. For information about how to configure Outlook Web App to allow you to view an XML attachment, see View or Configure Outlook Web App Virtual Directories.

To search the audit log for criteria you specify, use the following syntax.

```
New-AdminAuditLogSearch -Cmdlets <cmdlet 1, cmdlet 2, ...> -Parameters <parameter
```

This example performs a search for all audit log entries with the following criteria:

- **Start date** 02/04/2010
- **End date** 04/03/2010
- **User IDs** davids, chrisd, kima
- **Cmdlets** **Set-Mailbox**
- **Parameters** *ProhibitSendQuota*, *ProhibitSendReceiveQuota*, *IssueWarningQuota*, *MaxSendsize*, *MaxReceiveSize*

The command sends the results to the davids mailbox with "Mailbox limit changes" included in the subject line of the message.

```
New-AdminAuditLogSearch -Cmdlets Set-Mailbox -Parameters ProhibitSendQuota, Prohi
```

Note:
The report that the **New-AdminAuditLogSearch** cmdlet generates can be a maximum of 10 MB in size. If the search you perform returns a report larger than 10 MB, change the search criteria you specified. For example, reduce the size of the date range and run multiple reports, each with a portion of the original date range.

For more information about the format of the XML file, see Administrator Audit Log Structure.

For detailed syntax and parameter information, see New-AdminAuditLogSearch.

1.5.5.4 Disable Administrator Audit Logging

Disable Administrator Audit Logging

Exchange Server 2010 > Exchange Management Shell > Administrator Audit Logging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use this topic to disable administrator audit logging if it's enabled. Administrator audit logging in Microsoft Exchange Server 2010 enables you to create a log entry each time a specified cmdlet is run. For more information about administrator audit logging, see Overview of Administrator Audit Logging.

Important:
Administrator audit logging relies on Active Directory replication to replicate the configuration settings you specify to the domain controllers in your organization. Depending on your replication settings, the changes you make may not be immediately applied to all Exchange 2010 servers in your organization.
Changes to the audit log configuration are refreshed every 60 minutes on computers that have the Shell open at the time a configuration change is made. If you want to apply the changes immediately, close and then open the Shell again on each computer.

Use the Shell to disable administrator audit logging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

To disable administrator audit logging, use the following command:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $False
```

Other Tasks

After you disable administrator audit logging, you may also want to:

- View Administrator Audit Logging Settings
- Configure Administrator Audit Logging

1.5.5.5 Enable Administrator Audit Logging

Enable Administrator Audit Logging

Exchange Server 2010 > Exchange Management Shell > Administrator Audit Logging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use this topic to enable administrator audit logging if it's disabled. Administrator audit logging in Microsoft Exchange Server 2010 enables you to create a log entry each time a specified cmdlet is run. For more information about administrator audit logging, see Overview of Administrator Audit Logging.

Important:
Administrator audit logging relies on Active Directory replication to replicate the configuration settings you specify to the domain controllers in your organization. Depending on your replication settings, the changes you make may not be immediately applied to all Exchange 2010 servers in your organization.
Changes to the audit log configuration are refreshed every 60 minutes on computers that have the Shell open at the time a configuration change is made. If you want to apply the changes immediately, close and then open the Shell again on each computer.

Prerequisites

You must specify the cmdlets and parameters you want to audit, and you must also specify the destination audit logging mailbox before you enable administrator audit logging. For more information about how to configure administrator audit logging, see Configure Administrator Audit Logging.

Use the Shell to enable administrator audit logging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

To enable administrator audit logging, use the following command:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
```

Other Tasks

After you enable administrator audit logging, you may also want to:

- View Administrator Audit Logging Settings
- Configure Administrator Audit Logging

1.5.5.6 View Administrator Audit Logging Settings

View Administrator Audit Logging Settings

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use this topic to view the administrator audit logging settings that you've configured for your organization. Administrator audit logging in Microsoft Exchange Server 2010 enables you to create a log entry each time a specified cmdlet is run. For more information about administrator audit logging, see Overview of Administrator Audit Logging.

Use the Shell to view administrator audit logging settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Administrator audit logging" entry in the Exchange and Shell Infrastructure Permissions topic.

To view the administrator audit logging settings that you've configured for your organization, use the following command:

```
Get-AdminAuditLogConfig
```

1.5.6 Troubleshooting the Exchange Management Shell

Troubleshooting the Exchange Management Shell

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

While using the remote Exchange Management Shell with Microsoft Exchange Server 2010, you may encounter problems. You can use the information in this topic to diagnose and resolve client and connection issues.

This topic addresses problems with the Shell that administrators of on-premises installations of Exchange 2010 might encounter. If you're troubleshooting problems with the remote Shell for your Microsoft Office Outlook Web App organization, see Windows PowerShell: FAQ for Administrators.

Client Issues

The following sections describe techniques for resolving client issues that you may encounter.

Script Execution Error Caused by Windows PowerShell Execution Policy

You might get the following error message when you attempt to open the Shell using the instructions in the topic Open the Shell. The error is caused by setting the script execution policy in Windows PowerShell to `Restricted` or `AllSigned`. To resolve this issue, you need to set the script execution policy to `RemoteSigned`. For more information, see Install Windows Management Framework.

```
File D:\Program Files\Microsoft\Exchange Server\V14\bin\RemoteExchange.ps1 cann
ot be loaded because the execution of scripts is disabled on this system. Pleas
e see "get-help about_signing" for more details.
At line:1 char:2
+ . <<<<  'D:\Program Files\Microsoft\Exchange Server\V14\bin\RemoteExchange.ps
1'; Connect-ExchangeServer -auto
    + CategoryInfo          : NotSpecified: (:) [], PSSecurityException
    + FullyQualifiedErrorId : RuntimeException
The term 'Connect-ExchangeServer' is not recognized as the name of a cmdlet, fu
nction, script file, or operable program. Check the spelling of the name, or if
 a path was included, verify that the path is correct and try again.
At line:1 char:98
+ . 'D:\Program Files\Microsoft\Exchange Server\V14\bin\RemoteExchange.ps1'; Co
nnect-ExchangeServer <<<<  -auto
    + CategoryInfo          : ObjectNotFound: (Connect-ExchangeServer:String)
   [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

Import-PSSession Error Caused by Windows PowerShell Execution Policy

You might get the following error message when you attempt to use the remote Shell to connect to a remote Exchange 2010 server using the instructions in the topic Connect Remote Exchange Management Shell to an Exchange Server. The error is caused by setting the script execution policy in Windows PowerShell to `Restricted` or `AllSigned`. To resolve this issue, you need to set the script execution policy to `RemoteSigned`. For more information, see Install Windows Management Framework.

```
Import-Module : There were errors in loading the format data file:
Microsoft.PowerShell, , D:\Users\Administrator\AppData\Local\Temp\1\tmp_88ee1dec-
vh\tmp_88ee1dec-ed9c-4b0c-bc3d-68ca394f6d0f_4ilp43pe.xvh.format.ps1xml : File ski
on exception: File D:\Users\Administrator\AppData\Local\Temp\1\tmp_88ee1dec-ed9c-
```

```
p_88ee1dec-ed9c-4b0c-bc3d-68ca394f6d0f_4ilp43pe.xvh.format.ps1xml cannot be loade
disabled on this system. Please see "get-help about_signing" for more details..
At line:3 char:30
+                 Import-Module <<<<  -Name $name -Alias * -Function * -Prefix $p
eChecking -PassThru -ArgumentList @($session)
    + CategoryInfo          : InvalidOperation: (:) [Import-Module], RuntimeExcep
    + FullyQualifiedErrorId : FormatXmlUpateException,Microsoft.PowerShell.Comman
```

Error When the ForEach Cmdlet Is Used in a Pipeline and Cmdlets Are Used in its Script Block

You might get the following error message when you use the **ForEach** cmdlet in a pipeline and the following circumstances are true:

- The **ForEach** cmdlet accepts data from a cmdlet earlier in the pipeline.
- The script block on the **ForEach** cmdlet contains a cmdlet.

This error is caused because the Windows PowerShell remoting feature doesn't support more than one pipeline running at the same time. To resolve this issue, store the output of the cmdlet earlier in the pipeline in a variable, and then pipe the data stored in the variable to the **ForEach** cmdlet. This example results in a concurrent pipeline error.

```
Get-Mailbox | ForEach { Set-Mailbox -ProhibitSendReceiveQuota 3GB }
```

The following error message is generated.

```
Pipeline not executed because a pipeline is already executing. Pipelines cannot b
    + CategoryInfo          : OperationStopped: (Microsoft.Power...tHelperRunspac
   PSInvalidOperationException
    + FullyQualifiedErrorId : RemotePipelineExecutionFailed
```

To resolve the error, store the output of the **Get-Mailbox** cmdlet in a variable, and then pipe the variable to the **ForEach** cmdlet, as shown in this example.

```
$Mailboxes = Get-Mailbox
$Mailboxes | ForEach { Set-Mailbox -ProhibitSendReceiveQuota 3GB }
```

Incorrect Version of Windows PowerShell Installed

You might get the following error messages if you don't have the correct version of Windows PowerShell installed. You must have Windows PowerShell 2.0, available in Windows Management Framework, to connect to a remote Exchange 2010 server. For more information, see Install Windows Management Framework.

You might receive the following error message if you have Windows PowerShell 1.0 installed.

```
The term 'New-PSSession' is not recognized as a cmdlet, function, operable progra
 try again.
At line:1 char:25
+ $Session = New-PSSession  <<<< -ConfigurationName Microsoft.Exchange -Connectio
/PowerShell/ -Authentication Kerberos
```

You might receive the following error messages if you have a pre-release version of Windows PowerShell 2.0 installed.

```
New-PSSession : Cannot bind parameter 'Authentication'. Cannot convert value "Ker
mation.Runspaces.AuthenticationMechanism" due to invalid enumeration values. Spec
alues and try again. The possible enumeration values are "Default, Basic, Negotia
redssp".
At line:1 char:125
+ $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri h
ication <<<<  Kerberos
    + CategoryInfo          : InvalidArgument: (:) [New-PSSession], ParameterBind
    + FullyQualifiedErrorId : CannotConvertArgumentNoMessage,Microsoft.PowerShell
```

Or

```
The term 'New-PSSessionOption' is not recognized as a cmdlet, function, operable
rm and try again.
At D:\Program Files\Microsoft\Exchange Server\V14\bin\ConnectFunctions.ps1:220 ch
+     $so = New-PSSessionOption <<<<  -OperationTimeout $sessionOptionsTimeout -I
nTimeout $sessionOptionsTimeout;
    + CategoryInfo          : ObjectNotFound: (New-PSSessionOption:String) [], Co
    + FullyQualifiedErrorId : CommandNotFoundException
New-PSSession : [4367r10-b36.dvktun-dom.extest.microsoft.com] Processing data fro
ing error message: The Windows Remote Shell cannot process the request; the selec
AF1CF7F3 specified in the request was not found.
At D:\Program Files\Microsoft\Exchange Server\V14\bin\ConnectFunctions.ps1:229 ch
+             $session = new-pssession <<<<  -connectionURI "http://$fqdn/powersh
ationName Microsoft.Exchange -SessionOption $so #-erroraction silentlycontinue
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   gTransportException
    + FullyQualifiedErrorId : RemoteRunspaceOpenFailed
```

Connection Issues

The following sections describe techniques for resolving connection issues that you may encounter.

Incorrect User Name or Password

You can receive the following error message if you specify an incorrect user name or password. Verify that the user name and password you're using are correct.

```
New-PSSession : [ExchServer] Connecting to remote server failed with the followin
At line:1 char:19
+ $Session = New-PSSession <<<<  -ConfigurationName Microsoft.Exchange -Connectio
$c -SessionOption $SkipCertificate
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   gTransportException
    + FullyQualifiedErrorId : RemoteRunspaceOpenFailed
```

User Isn't Enabled for Remote Shell

You can receive the following error message if a user tries to connect to a remote Exchange 2010 server and the remote Shell isn't enabled. For more information about how to enable users for the remote Shell, see Enable Remote Exchange Management Shell for a User.

```
[ExchServer] Connecting to remote server failed with the following error message
request. It cannot determine the content type of the HTTP response from the desti
bsent or invalid. For more information, see the about_Remote_Troubleshooting Help
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```

Server Name Provided Doesn't Exist

You can receive the following error message if the server name you specified in the remote Shell URL doesn't exist. To resolve this issue, verify the server name. For more information, see Connect Remote Exchange Management Shell to an Exchange Server.

```
[exchserver01] Connecting to remote server failed with the following error messag
The following error occured while using Kerberos authentication: The network path
 Possible causes are:
  -The user name or password specified are invalid.
  -Kerberos is used when no authentication method and no user name are specified.
  -Kerberos accepts domain user names, but not local user names.
  -The Service Principal Name (SPN) for the remote computer name and port does no
  -The client and remote computers are in different domains and there is no trust
 After checking for the above issues, try the following:
  -Check the Event Viewer for events related to authentication.
  -Change the authentication method; add the destination computer to the WinRM Tr
e HTTPS transport.
 Note that computers in the TrustedHosts list might not be authenticated.
   -For more information about WinRM configuration, run the following command: wi
 see the about_Remote_Troubleshooting Help topic.
```

```
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```

Incorrect Virtual Directory Name

You can receive the following error message if you specify the wrong virtual directory when connecting to a remote Exchange 2010 server. To resolve this issue, verify the virtual directory name. For more information, see Connect Remote Exchange Management Shell to an Exchange Server.

```
[ExchServer] Connecting to remote server failed with the following error message
atus code of 403 from the remote WS-Management service. For more information, see
 topic.
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```

Warning When the Import-PSSession Cmdlet Is Run

When you connect to a remote Exchange 2010 server using the procedure provided in the Connect Remote Exchange Management Shell to an Exchange Server topic, it's normal to see the following warning after you import the Exchange 2010 cmdlets into your local client.

```
WARNING: Some imported command names include unapproved verbs which might make th
 parameter for more detail or type Get-Verb to see the list of approved verbs.
```

HTTPS Used When Connecting to a Remote Server

You might receive an error message when connecting to a remote Exchange 2010 server if you use the HTTPS protocol. This error occurs because your computer doesn't trust the certification authority (CA) used to sign the Secure Sockets Layer (SSL) certificate used by the remote server. To connect to a remote Exchange 2010 server, you must use the HTTP protocol and the Kerberos authentication method. For more information, see Connect Remote Exchange Management Shell to an Exchange Server.

```
[ExchServer] Connecting to remote server failed with the following error message
ation computer (ExchServer:443) has the following errors:
The SSL certificate is signed by an unknown certificate authority. For more infor
ooting Help topic.
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```

Incorrect Connection Name When Connecting to a Remote Server

You might receive the following error message if you specify an incorrect value for the *ConnectionName* parameter when connecting to a remote Exchange 2010 server. You must use the value `Microsoft.Exchange` with the *ConnectionName* parameter. For more information, see Connect Remote Exchange Management Shell to an Exchange Server.

```
[ExchServer] Connecting to remote server failed with the following error message
cess the request. The resource URI (http://schemas.microsoft.com/powershell/MS.Ex
 catalog. The catalog contains the metadata that describes resources, or logical
he about_Remote_Troubleshooting Help topic.
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```

Incorrect Authentication Used When Connecting to a Remote Server

You might receive one of the following error messages when connecting to a remote Exchange 2010 server if you specify an authentication method other than Kerberos. To connect to a remote Exchange 2010 server, you must use Kerberos authentication and the HTTP protocol. For more information, see Connect Remote Exchange Management Shell to an Exchange Server.

```
[ExchServer] Connecting to remote server failed with the following error message
request. CredSSP authentication is currently disabled in the client configuration
```

```
try the request again. CredSSP authentication must also be enabled in the server
 be edited to allow credential delegation to the target computer. Use gpedit.msc
uter Configuration -> Administrative Templates -> System -> Credentials Delegatio
s.  Verify that it is enabled and configured with an SPN appropriate for the targ
 computer name "myserver.domain.com", the SPN can be one of the following: WSMAN/
com For more information, see the about_Remote_Troubleshooting Help topic.
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```

Or

```
[ExchServer] Connecting to remote server failed with the following error message
request. Default credentials can be used only with Kerberos authentication or Neg
he Allow implicit credentials for Negotiate is specified. Explicit credentials mu
tion scheme is specified. For more information, see the about_Remote_Troubleshoot
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```

Or

```
[ExchServer] Connecting to remote server failed with the following error message
request. If the authentication scheme is different from Kerberos, or if the clien
then HTTPS transport must be used or the destination machine must be added to the
se winrm.cmd to configure TrustedHosts. Note that computers in the TrustedHosts l
n get more information about that by running the following command: winrm help co
out_Remote_Troubleshooting Help topic.
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```

Or

```
[ExchServer] Connecting to remote server failed with the following error message
request. Unencrypted traffic is currently disabled in the client configuration. C
 the request again. For more information, see the about_Remote_Troubleshooting He
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```

Or

```
[ExchServer] Connecting to remote server failed with the following error message
request. Unencrypted traffic is currently disabled in the client configuration. C
 the request again. For more information, see the about_Remote_Troubleshooting He
    + CategoryInfo          : OpenError: (System.Manageme....RemoteRunspace:Remot
   eption
    + FullyQualifiedErrorId : PSSessionOpenFailed
```


1.6 Client Access

Client Access

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-05-03*

In Microsoft Exchange Server 2010, the Client Access server role supports the Outlook Web App and Microsoft Exchange ActiveSync client applications, and the Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4rev1 (IMAP4)

protocols. The Client Access server role also provides access to free/busy data by using the Availability service and enables certain clients to download automatic configuration settings from the Autodiscover service. You must install the Client Access server role in every Exchange organization and every Active Directory site that has the Mailbox server role installed.

The following topics are gateways to information about the Client Access servers in Exchange 2010.

Understanding Client Access

This topic provides feature information about the Client Access server role.

Managing Client Access Servers

This topic is a collection of links that provide information about managing Client Access features in your organization.

Securing Client Access Servers

This topic provides information about the security features of your Client Access server.

Upgrade from Exchange 2003 Client Access

This topic provides overview information about upgrading your organization's Client Access infrastructure from Exchange 2003 to Exchange 2010.

Upgrade from Exchange 2007 Client Access

This topic provides overview information about upgrading your organization's Client Access infrastructure from Exchange 2007 to Exchange 2010.

1.6.1 Understanding Client Access

Understanding Client Access

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-09*

The Client Access server role is one of five distinct server roles for Microsoft Exchange Server 2010. It supports the Outlook Web App and Microsoft Exchange ActiveSync client applications, and the Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4rev1 (IMAP4) protocols. The Client Access server role also provides access to free/busy data by using the Availability service and enables certain clients to download automatic configuration settings from the Autodiscover service.

The Client Access server role accepts connections to your Exchange 2010 server from different clients. Software clients such as Microsoft Outlook Express and Eudora use POP3 or IMAP4 connections to communicate with the Exchange server. Hardware clients, such as mobile phones, use ActiveSync, POP3, or IMAP4 to communicate with the Exchange server. You must install the Client Access server role in every Exchange organization and every Active Directory site that has the Mailbox server role installed.

Looking for management tasks related to Client Access? See Managing Client Access Servers.

Contents

Client Access Server Network Architecture

In addition to needing a Client Access server in every Active Directory site that contains a Mailbox server, it's important to avoid restrict traffic among Exchange servers. Otherwise, Exchange functionality can be negatively affected. Make sure that all defined ports used by Exchange are open in both directions between all source and destination servers. Installing a firewall between Exchange servers or between an Exchange Server 2010 Mailbox server or Exchange Server 2010 Client Access server and Active Directory isn't supported. However, you can install a network device as long as traffic isn't restricted and all available ports are open between the various Exchange servers and Active Directory. For a complete list of Exchange Server 2010 ports, see Exchange Network Port Reference.

Outlook Web App

Outlook Web App lets you access your e-mail from any Web browser. Outlook Web App (known as Outlook Web Access in earlier versions of Microsoft Exchange) has been redesigned in Exchange 2010. Features such as Chat, Text Messaging, mobile phone integration, and Conversation View provide an enhanced user experience from any computer that has a Web browser. In Exchange Server 2010, these features can be accessed from an expanded set of Web browsers including versions of Internet Explorer later than 6.0, Firefox, Safari, and Google's Chrome.

For more information about Outlook Web App, see the following topics:

- Managing Outlook Web App
- Understanding Outlook Web App

Exchange ActiveSync

Exchange ActiveSync lets you synchronize data between your mobile phone and Exchange 2010. You can synchronize e-mail, contacts, calendar information, and tasks.

If you use a phone that has Windows Mobile 5.0 with the Messaging Security and Feature Pack (MSFP) installed or a later version, your mobile phone will support Direct Push. Direct Push technology is built into Exchange ActiveSync and keeps a mobile phone continuously synchronized with an Exchange mailbox.

Note:

Mobile phones and devices that are running versions of Windows Mobile earlier than Windows Mobile 5.0 with MSFP can still send and receive messages on a set schedule, but can't use Direct Push to synchronize items as they arrive. All versions of Windows Mobile and Pocket PC operating systems can synchronize items with Exchange 2010 by using a cable connection to a desktop or portable computer.

For more information about Exchange ActiveSync, see the following topics:

- Understanding Exchange ActiveSync

- Managing Exchange ActiveSync

POP3 and IMAP

In addition to supporting MAPI and HTTP clients, Exchange 2010 also supports POP3 and IMAP4 clients. By default, POP3 and IMAP4 are installed, but the services are disabled when you install the Client Access server role.

For more information about POP3 and IMAP4, see the following topics:

- Understanding POP3 and IMAP4
- Managing POP3 and IMAP4

The Availability Service

The Exchange 2010 Availability service provides secure, consistent, and up-to-date free/busy data to computers that are running Microsoft Office Outlook 2007 and later versions of Outlook. These versions of Outlook use the Autodiscover service to obtain the URL of the Availability service. Essentially, the Autodiscover service helps capable Outlook clients locate different Web services, such as the Microsoft Exchange Unified Messaging service, the Offline Address Book, and Availability services.

For more information about the Availability service, see the following topics:

- Understanding the Availability Service
- Managing the Availability Service

The Autodiscover Service

The Autodiscover service enables Outlook clients and some mobile phones to receive their necessary profile settings directly from the Exchange server by using the client's domain credentials. These settings automatically update the client with the information that's needed to create the user's profile.

For more information about the Autodiscover service, see the following topics:

- Understanding the Autodiscover Service
- Understanding Exchange ActiveSync Autodiscover

1.6.1.1 Understanding Client Access Server Namespaces

Understanding Client Access Server Namespaces

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-08*

When you plan your Microsoft Exchange Server 2010 organization, one of the most important decisions that you must make is how to arrange your organization's external namespace. A namespace is a logical structure that's usually represented by a domain

name in DNS. When you define your namespace, you must consider the different locations of your clients and the servers that house their mailboxes. In addition to the physical locations of clients, you must evaluate how they connect to Exchange 2010. The answers to these questions will determine how many namespaces you must have. Your namespaces will typically align with your DNS configuration. We recommend that each Active Directory site in a region that has one or more Internet-facing Client Access servers have a unique namespace. This is usually represented in DNS by an A record, for example, mail.contoso.com or mail.europe.contoso.com.

Before you create an Exchange 2010 organization, you must decide how your organization will be configured and how your external namespaces will be defined. The decisions that you make about your namespaces will affect the following:

- How you configure DNS.
- The certificates you must have to encrypt communications between your computers running Exchange 2010 and your client computers and devices.
- How your clients access their mailboxes when they use Outlook Anywhere, Outlook Web App, and POP3 and IMAP4 clients.

Making these decisions involves examining your physical and logical network structure and choosing an organizational topology. This topic discusses the different topologies and provides information about how each topology affects your Exchange organization.

Note:

This topic doesn't discuss internal namespace planning, which may be required if you deploy load balancing within an Active Directory site. For details about the impact of deploying load balancing internally, see Understanding Proxying and Redirection.

Exchange 2010 Organizational Models

This topic examines the following types of topology:

- **Consolidated Datacenter Model** This model consists of a single physical site. All servers are located within the site, and there's a single namespace, for example, mail.contoso.com.
- **Single Namespace with Proxy Sites** This model consists of multiple physical sites. Only one site contains an Internet-facing Client Access server. The other sites aren't exposed to the Internet. There's only one namespace for the sites in this model, for example, mail.contoso.com.
- **Single Namespace and Multiple Sites** This model consists of multiple physical sites. Each site can have an Internet-facing Client Access server. Or, there may be only a single site that contains Internet-facing Client Access servers. There's only one namespace for the sites in this model, for example, mail.contoso.com.
- **Regional Namespaces** This model consists of multiple physical sites and multiple namespaces. For example, a site that's located in New York City would have the namespace mail.usa.contoso.com, a site that's located in Toronto would have the namespace mail.canada.contoso.com, and a site that's located in London would have the namespace mail.europe.contoso.com.
- **Multiple Forests** This model consists of multiple forests that have multiple namespaces. An organization that uses this model could be made up of two partner companies, for example, Contoso and ContosoOnline. Namespaces might include mail.usa.contoso.com, mail.europe.contoso.com, mail.asia.contosoonline.com, and mail.europe.contosoonline.com.

Consolidated Datacenter Model

The consolidated datacenter model is the simplest model considered in this topic. It consists of a single physical site.

The advantages of the consolidated datacenter model are as follows:

- There are fewer DNS records to manage than with multiple namespace models.
- There are fewer certificates to manage. Communications between the Exchange Client Access server and clients can be encrypted in several ways. The recommended method for encryption is to use a single certificate that supports Subject Alternative Names.

Note:
A Subject Alternative Name is an attribute of a digital certificate that allows the site administrator to configure a single certificate that lists all the namespaces that require a server certificate.

Note:
Alternative methods for managing certificates for a consolidated datacenter model include a wildcard certificate, multiple certificates, and configuring SRV records appropriately.

- End users don't have to determine which namespace to use. All end users use the same namespace and URL to access Microsoft Exchange.

Disadvantages to the consolidated datacenter model include:

- This model doesn't support multiple datacenters.
- If regional Internet links are slow because of low bandwidth, high latency, or high use, end users in those regions will experience poor performance.

Single Namespace with Proxy Sites

This model consists of multiple physical sites that use a single namespace. Behind an ISA Server computer or another firewall, one of the sites has one or more Internet-facing Client Access servers. The other sites don't contain Internet-facing Client Access servers.

Important:
Installing a Client Access server in a perimeter network isn't supported.

Caution:
This model isn't recommended if all sites have Internet connectivity. If your topology uses multiple Active Directory sites that have Internet connectivity and aren't near to each other, consider a regional namespace model.

This model offers the following advantages:

- There are fewer DNS records to manage than with multiple namespace topologies. This reduces operational complexity.
- There are fewer certificates to manage. Communications between the Client Access server and clients can be encrypted by using a single certificate that supports Subject Alternative Names.
- End users don't have to determine which namespace to use. All end users use the same namespace and URL to access Microsoft Exchange.

Disadvantages to deploying a single namespace with proxy sites include:

- Some users will access their Mailbox server through proxying. If a user connects to a Client Access server that isn't in the same physical site as their Mailbox server, they will be proxied to a Client Access server that's in the same physical site as their Mailbox server. Because of the added proxying, WAN link costs will increase and performance won't be optimal. The effect on performance depends on the distance between the two physical datacenters and the numbers of proxied connections.

Important:
It may be necessary to configure the target virtual directories on each Client Access server in the site being proxied to for Integrated Windows authentication. For more information, see Understanding Proxying and

Redirection.

Single Namespace with Multiple Sites

This model consists of multiple physical sites that use a single namespace. There are two deployment options for this model. You can use an ISA Server computer in front of one or more sites or use a Client Access server proxy site. There can be one or more Internet-accessible servers behind each site. This model also requires a load balancing solution that splits the incoming traffic equally between the Internet-facing sites.

Important:

Installing a Client Access server in a perimeter network isn't supported.

Deployment with an ISA Server computer

In this configuration, ISA Server performs pre-authentication of the connection to determine the client's group membership. Traffic is then forwarded to the correct site based on the configured publishing rules.

The advantages of this model are as follows:

- There are fewer DNS records to manage than with multiple namespace models. This reduces operational complexity.
- There are fewer certificates to manage. Communications between the Client Access server and clients can be encrypted by using a single certificate that supports Subject Alternative Names. The ISA Server computer could be configured to use an external, trusted certificate from a recognized provider. The traffic between the ISA Server computer and the Client Access servers could be secured using an internally generated certificate.
- End users don't have to determine which namespace to use. All users use the same namespace and URL to access Microsoft Exchange.
- Mailboxes can be moved between sites without external namespace changes. This provides flexibility for administrators who want to load balance traffic between sites without changing client configuration.
- If required, a regional namespace can be added at a later stage. This same model can be repeated in another location using a different external URL.
- ISA Server 2006 forms-based authentication can be customized to suit an organization's specific requirements.

The disadvantages to deploying this model include the following:

- Wide Area Network (WAN) use will likely increase. The increased use depends on the physical location of the ISA Server computer.
- ISA Server must be deployed and configured correctly.
- Group memberships must be managed to ensure traffic is forwarded to the correct site. By default, Recipient Administrators can't create security groups, so Active Directory delegation must be configured so that dedicated Exchange Administrators can create and update group membership. Using groups creates an additional operational overhead that must be considered when new mailboxes are created or moved. Placing a global catalog server close to the ISA Server computer is the recommended way to avoid unnecessary authentication request travel on the WAN.

Deployment with a Client Access Server Proxy Site

In this model, all client connections that originate externally go to an Active Directory site that contains no user mailboxes. The connections are then proxied by a Client Access server in that site to the site that contains the user's mailbox.

The advantages of this model are as follows:

- There are fewer DNS records to manage than with multiple namespace models. This reduces operational complexity.

- There are fewer certificates to manage. Communications between the Client Access server and clients can be encrypted by using a single certificate that supports Subject Alternative Names. ISA Server can be configured to use an external, trusted certificate from a recognized provider. And traffic between the ISA Server and Client Access servers can be secured using a certificate that's internally generated.
- End users don't have to determine which namespace to use. All end users use the same namespace and URLs to access Microsoft Exchange. If split DNS is configured, this model could also be used to unify an internal namespace. If split DNS isn't configured, all internal client requests will reach the firewall and be forwarded appropriately.
- Mailboxes can be moved between sites without the namespace being changed from an external user's perspective. This provides flexibility for administrators who want to load balance between sites. It is also useful when a disaster occurs and the entire service must be moved between sites, because the client configuration doesn't have to be changed.
- A regional namespace can be added at a later stage, if required. This same model can be repeated in another location, using a different external URL.

The disadvantages of this model are as follows:

- WAN use will likely increase and depends on the physical location of the Client Access servers in the Internet-facing site.
- Additional Client Access servers must be deployed and configured correctly.
- All users will access their mailbox through proxying. When a user connects to a Client Access server in the proxy site, it isn't in the same Active Directory site as their Mailbox server. They will be proxied to a Client Access server that's in the same Active Directory site as their Mailbox server. Performance won't be optimal because of the additional proxying. The effect on performance depends on the distance between the two physical sites.
- Access to Windows SharePoint Services libraries and Windows file shares isn't possible when users connect to a Client Access server that isn't within the same site as their Mailbox server. This is because access to Windows SharePoint Services libraries and Windows file shares requires the user's user name and password. In a proxying scenario, communication to Windows SharePoint Services libraries and Windows file shares is performed through the Exchange system account. This account isn't aware of the user's user name and password.

Important:

The **ExternalURL** property on each virtual directory in a site that contains user mailboxes must be set to $null.

Important:

Client Access servers don't support multiple levels of proxying. Each site that contains user mailboxes must be accessed by the Client Access servers in the dedicated proxy site.

Note:

Additional network configuration might be required if multiple locations are used. This can include configuring hardware load balancers, multiple DNS records, and route redundancy. The physical deployment will vary based on your organization's network topology.

Regional Namespaces

The multiple site model that uses a different namespace for each site is known as a regional namespace model. The advantages of this model are as follows:

- Proxying is reduced because a larger percentage of users will be able to connect to a Client Access server in the same Active Directory site as their Mailbox server. This will improve the end-user experience and performance. Users who have mailboxes in a site that doesn't have an Internet-facing Client

Access server will still be proxied.

The disadvantages to this model are as follows:

- Multiple DNS records must be managed.
- Multiple certificates must be obtained, configured, and managed.
- Managing security is more complex because each Internet-facing site requires an ISA Server computer or other firewall.
- Each user must connect to their own regional namespace. This may result in additional helpdesk calls and training.

Important:

The regional namespace model is generally recommended for any topology that involves multiple Active Directory sites that have their own Internet connectivity.

Multiple Forests

This model consists of multiple forests with multiple namespaces. An organization that uses this model could be made up of two partner companies, Contoso and ContosoOnline. Namespaces might include mail.usa.contoso.com, mail.europe.contoso.com, mail.asia.contosoonline.com, and mail.europe.contosoonline.com.

Consider implementing a regional namespace model for each forest to provide the highest level of performance for end users. Multiple certificates must be managed for each forest.

1.6.1.2 Understanding Proxying and Redirection

Understanding Proxying and Redirection

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-12-26*

In a Microsoft Exchange Server 2010 organization, a Client Access server can act as a proxy for other Client Access servers within the organization. This is useful when multiple Client Access servers exist in different Active Directory sites in an organization, and at least one of those sites isn't exposed to the Internet.

A Client Access server can also perform redirection for Microsoft Office Outlook Web App URLs and for Exchange ActiveSync devices. Redirection is useful when users connect to a Client Access server that isn't in their local Active Directory site, or if a mailbox has moved between Active Directory sites. It's also useful if users should actually be using a more effective URL. For example, users should be using a URL that's closer to the Active Directory site in which their mailbox resides.

The Client Access server's response can vary by protocol. Typically, however, a Client Access server takes the following action if it receives a request for a user whose mailbox is in an Active Directory site other than the one to which the Client Access server belongs: In this case, the server looks for the presence of an **ExternalURL** property on the relevant virtual directory on a Client Access server that's in the same Active Directory site as the user's mailbox. If the **ExternalURL** property exists, and the client type supports redirection (for example, Outlook Web App or Exchange ActiveSync), the Client Access server issues a redirect to that client. If no **ExternalURL** property exists, or if the client type doesn't support redirection (for example, POP3 or IMAP4), the Client Access server

will try to proxy the connection to the target Active Directory site.

This topic explains proxying and redirection, the circumstances under which each is used, and how to configure your Client Access servers for each scenario.

Note:
If you don't have multiple Active Directory sites in your organization, you don't have to configure Exchange 2010 for proxying or redirection. However, you might want to configure load balancing of URLs as described later in this topic.

Note:
Client Access servers that aren't exposed to the Internet don't have to have separate Secure Sockets Layer (SSL) certificates to allow proxied traffic from another Client Access server. By default, they can use the self-signed certificate installed with Exchange 2010. However, these certificates aren't usually trusted by internal clients such as Outlook Web App or Outlook, and their use will usually result in certificate warnings. If there are internal clients in the same Active Directory sites as Client Access servers with self-signed certificates, you should replace the self-signed certificates with certificates issued by a certification authority that's trusted by the clients.

Contents

Overview of Proxying

In Microsoft Exchange Server 2003, the front-end server communicates with the back-end server over HTTP. In Exchange Server 2007 and Exchange 2010, the Client Access server communicates with an Exchange Mailbox server over RPC. You must have an Exchange 2010 Client Access server in every Active Directory site that contains an Exchange 2010 Mailbox server. Proxying occurs when one Client Access server sends traffic to another Client Access server. An Exchange 2010 Client Access server can proxy requests in the following situations:

- **Between Exchange 2010 Client Access servers** Proxying requests between two Exchange 2010 Client Access servers enables organizations that have multiple Active Directory sites to designate one Client Access server as an Internet-facing server and have that server proxy requests to Client Access servers in sites that have no Internet presence. The Internet-facing Client Access server then proxies the request to the Client Access server closest to the user's mailbox.
- **Between an Exchange 2010 Client Access server and Exchange 2007 Client Access servers** Proxying requests between an Exchange 2010 Client Access server and an Exchange 2007 Client Access server within one Active Directory site or between Active Directory sites enables Exchange 2010 and Exchange 2007 to coexist in the same organization. For more information about how to upgrade and coexistence, see Upgrade from Exchange 2003 Client Access and Upgrade from Exchange 2007 Client Access.

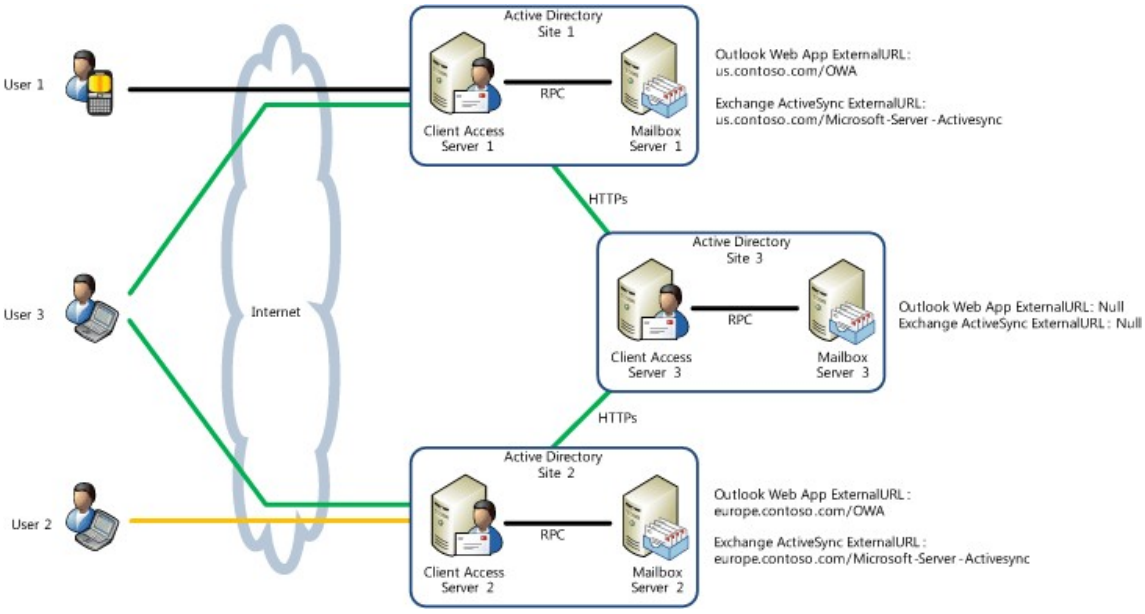
Proxying is supported for clients that use Outlook Web App, Exchange ActiveSync, the Exchange Control Panel (ECP), POP3, IMAP4, and Exchange Web Services. Proxying is supported from one Client Access server to another Client Access server when the destination Client Access server is running the same version of Microsoft Exchange as, or an earlier version of Microsoft Exchange than, the source Client Access server.

Warning:

When an IMAP4 client using NTLM authentication tries to connect to a Client Access server in an Active Directory site that doesn't contain the target mailbox, the connection will fail. If you want an IMAP4 client to be proxied from one Active Directory site to another, you have to choose an alternate authentication method.

Note:

In each Exchange organization that wants to allow access from Internet-based clients, at least one Active Directory site must be Internet facing. All non-Internet-facing Active Directory sites rely on the Internet-facing Client Access server or servers to proxy all pertinent requests from external clients.



In the previous figure, the mailbox of User 1 is located on Mailbox server 1. The mailbox of User 2 is located on Mailbox server 2, and the mailbox of User 3 is located on Mailbox server 3. Each Mailbox server is in a different Active Directory site. User 1 can access their mailbox through Client Access server 1 without using proxying, and User 2 can access their mailbox through Client Access server 2. If User 3 tries to access their mailbox through Client Access server 1 or 2, either server will proxy their request to Client Access server 3. Client Access server 3 isn't Internet facing but can receive requests from other servers inside the firewall. Proxying isn't visible to the user.

Note:

Communications between Client Access servers in different sites occur over Secure HTTP (HTTPS), but Client Access servers don't check the status of the certificate that's used by default. The certificate is used only for encryption, not authentication, and so name mismatches, expiration dates, and trust status are ignored.

Return to top

Overview of Redirection

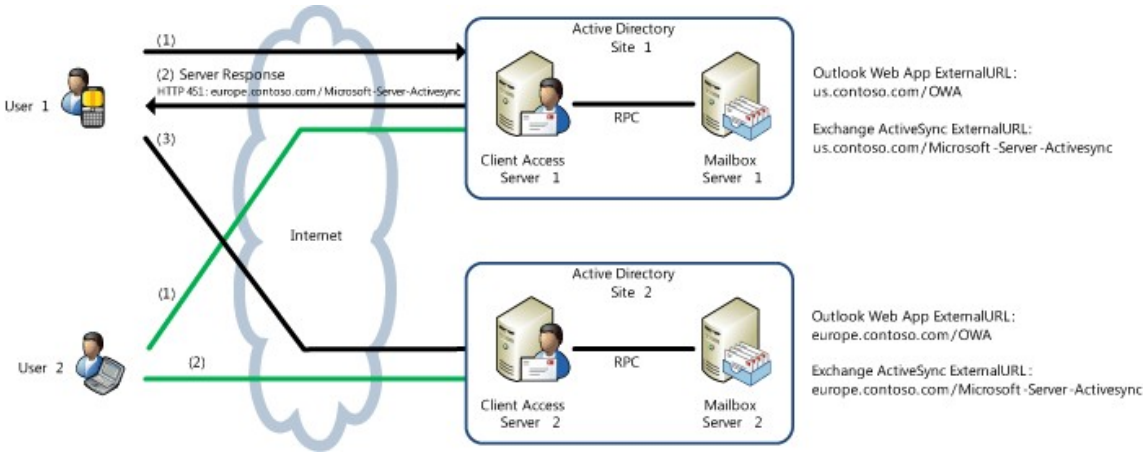
Outlook Web App users who access an Internet-facing Client Access server in a different Active Directory site than the site that contains their mailbox can be redirected to the Client Access server in the same site as their Mailbox server if that Client Access server is Internet facing. When an Outlook Web App user tries to connect to a Client Access server outside the Active Directory site that contains their Mailbox server, they'll see a Web page that contains a link to the correct Client Access server for their mailbox. This is known as manual redirection. In Exchange 2010 SP2, administrators can configure cross-site silent redirection to enable this redirection process to happen without the user's knowledge. For more information, see Cross-Site Silent Redirection later in this topic.

Note:

You cannot use cross-site silent redirection in a hybrid environment that uses an on-premises Exchange Server together with Office 365.

Exchange ActiveSync users who access an Internet-facing Client Access server in a different Active Directory site than the site that contains their mailbox can be redirected to the Client Access server in the same site as their Mailbox server if that Client Access server is Internet facing and if the client mobile phone or device has correctly implemented the redirection logic built in to the protocol that's used when communicating with Exchange 2007 and Exchange 2010. The redirection for Exchange ActiveSync users is achieved by sending the device an HTTP 451 error code that contains the URL the device should be using. The device then reconfigures itself to use the new URL.

The following figure shows how redirection works in an organization that has multiple Client Access servers in multiple Active Directory sites.



In the previous figure, User 1 usually accesses their mailbox in Active Directory site 1 using their mobile phone. The administrator then moves their mailbox to Mailbox server 2 in Active Directory site 2. The next time the device tries to synchronize, the server responds with an HTTP 451 status error. This contains the URL the device should now use for that user. In step 3 of the sequence, the device reconfigures itself and connects to the specified URL. User 2, whose mailbox is in Active Directory site 2, tries to open their mailbox using Outlook Web App by connecting to Client Access server 1 over the Internet. With manual redirection, as soon as the user authenticates, Client Access server 1 presents a page to the user, with a link to the Outlook Web App URL for the Client Access server in Active Directory site 2. The user clicks the link, is taken to Active Directory site 2, and signs in again to access their mailbox.With silent redirection, when the user authenticates, they're silently redirected to the Outlook Web App URL for the Client Access server in Active Directory site 2.

Cross-Site Silent Redirection

Note:
You cannot use cross-site silent redirection in a hybrid environment that uses an on-premises Exchange Server together with Office 365.

Exchange 2010 SP2 lets administrators configure cross-site silent redirection. Cross-site silent redirection performs silent redirection for client requests that are destined for a CAS that is located in a different Active Directory site in the same Exchange organization. For example, a user with a mailbox in Active Directory SiteA who accesses the Outlook Web App URL in Active Directory SiteB will be silently redirected to the Outlook Web App URL for Active Directory in SiteA.

To configure cross-site silent redirection, the administrator must use the new ***CrossSiteRedirectType*** parameter that's been added to the **Set-OWAVirtualDirectory** cmdlet. The parameter has two possible settings. The default setting is `Manual`.

- **Silent** When this setting is configured, a user's web browser is automatically redirected whenever a Client Access server must redirect an Outlook Web App request to Client Access server or server array located in another Active Directory site. When forms-based authentication is configured on the source and target CAS OWA virtual directories (SSL is required), then the silent redirection is also a single sign-on event. For redirection to occur, the target Client Access server Outlook Web App virtual directory must have an `ExternalURL` value configured.
- **Manual** When this setting is configured, users will receive a notification that they're accessing the wrong URL and that they must click a link to access the correct Outlook Web App URL for their mailbox. This notification only occurs when a Client Access server determines that it must redirect an Outlook Web App request to Client Access server or server array located in another Active Directory site. For redirection to occur, the target Client Access server Outlook Web App virtual directory must have an `ExternalURL` value configured.

For example:

```
Set-OWAVirtualDirectory -Identity "Contoso\owa (Default Web site)" -
CrossSiteRedirectType Silent
```

For more information about the **Set-OwaVirtualDirectory** cmdlet, see: Set-OwaVirtualDirectory

Proxying and Redirection for Exchange ActiveSync

The following series of steps shows how incoming requests are handled for a user who connects to an Exchange 2010 Client Access server named CAS-01 using a mobile phone.

1. The Client Access server queries Active Directory to determine the location of the user's mailbox and the version of Microsoft Exchange installed on the Mailbox server.
2. If the user's mailbox is on an Exchange 2003 server, the incoming request is proxied directly to the Exchange 2003 server that hosts the user's mailbox and the Exchange ActiveSync virtual directory. By default, in Exchange 2003, the Exchange ActiveSync virtual directory was installed on all mailbox servers. The Active Directory site of the user's mailbox isn't applicable in this case because Exchange 2003 doesn't use Active Directory sites to determine location. The connection is always made directly from the Exchange 2010 Client Access server to the Exchange 2003 mailbox server.

   Note:
   Users who have mailboxes on an Exchange 2003 server who try to use Exchange ActiveSync through an Exchange 2010 Client Access server will receive an error and be unable to synchronize unless Integrated Windows

authentication is enabled on the Microsoft-Server-ActiveSync virtual directory on the Exchange 2003 server. Integrated Windows authentication enables the Exchange 2010 Client Access server and the Exchange 2003 back-end server to communicate.

3. If the user's mailbox is on an Exchange 2007 Mailbox server, CAS-01 locates an Exchange 2007 Client Access server in the same Active Directory site as the user's Mailbox server. This may be the same Active Directory site as CAS-01. CAS-01 determines whether the Exchange 2007 Client Access server has the **ExternalURL** property configured on the Exchange ActiveSync virtual directory. If so, CAS-01 issues the client an HTTP error code 451 that contains the ExternalURL value and instructs the client to redirect to the location specified in the **ExternalURL** property. If no ExternalURL value is set, the connection will be proxied to the Client Access server using the FQDN specified by the **InternalURL** property, specifically to the /Proxy virtual directory, This virtual directory is located beneath the Exchange ActiveSync virtual directory in IIS and, by default, has Integrated Windows authentication enabled on it.
4. If the user's mailbox is on an Exchange 2010 Mailbox server in the same Active Directory site as CAS-01, CAS-01 provides access to the mailbox. If the user's mailbox is on an Exchange 2010 Mailbox server in a different Active Directory site, CAS-01 locates a Client Access server in the same Active Directory site as the user's Mailbox server. CAS-01 determines whether any Exchange 2010 Client Access server in that Active Directory site has the **ExternalURL** property configured on the Exchange ActiveSync virtual directory. If so, CAS-01 issues the client an HTTP error code 451 that contains the ExternalURL value and instructs the client to redirect to that location. If no ExternalURL value is set, the connection will be proxied to the Client Access server using the FQDN specified by the **InternalURL** property, specifically to the /Proxy virtual directory. This virtual directory is located beneath the Exchange ActiveSync virtual directory in IIS and, by default, has Integrated Windows authentication enabled on it.

Important:

Proxying isn't possible between virtual directories that use Basic authentication. For client communications to be proxied between Exchange ActiveSync virtual directories on different servers, the /Proxy virtual directory must use Integrated Windows authentication.

Return to top

Proxying and Redirection for Outlook Web App

The following series of steps shows how incoming requests are handled for a user who connects to an Exchange 2010 Client Access server named CAS-01 using Outlook Web App.

1. The Client Access server queries Active Directory to determine the location of the user's mailbox and the version of Microsoft Exchange installed on the Mailbox server.
2. If the user's mailbox is on an Exchange 2003 server and the user tries to access Outlook Web App using https://domain name/owa, they'll receive an error because an Exchange 2010 Client Access server can't directly provide Outlook Web App access to an Exchange 2003 mailbox. However, if the administrator configured redirection from Exchange 2010 to Exchange 2003, which would be usual during a migration from Exchange 2003 to Exchange 2010, the **Exchange2003URL** property of the Outlook Web App virtual directory was set to the value of an Exchange 2003 server facing the Internet.
3. If the user's mailbox is on an Exchange 2007 mailbox server, CAS-01 locates a Client Access server in the same Active Directory site as the user's mailbox server. If the Exchange 2007 Mailbox server is in the same Active Directory site as CAS-01, one of four possible actions will result.

- CAS-01 will look for an Exchange 2007 **ExternalURL** property that has an *ExternalAuthenticationMethods* setting that's identical to the *InternalAuthenticationMethods* setting on the Exchange 2010 Client Access server. If the settings match, CAS-01 will redirect to this external URL. If source and target CAS have Forms Based Authentication (FBA) enabled, the source CAS issues a hidden form back to the browser that contains the user's credentials and FBA settings, along with the redirect URL. This is transparent to the user.
- If a matching *ExternalURL* setting isn't found, CAS-01 will look for an Exchange 2007 Client Access server that has the **ExternalURL** property configured, regardless of matching. If one is found, CAS-01 will redirect to this external URL. This will result in the user being prompted for authentication.
- If no matching *ExternalURL* setting is found, CAS-01 will look for an Exchange 2007 Client Access server with an **InternalURL** property that has an *InternalAuthenticationMethods* setting identical to the InternalAuthenticationMethods setting on the Exchange 2010 Client Access server. If one is found, CAS-01 will redirect to this InternalURL. If forms-based authentication is enabled, this will result in a single sign-on redirection.
- If no matching InternalURL is found, CAS-01 will look for an Exchange 2007 Client Access server with an InternalURL configured, regardless of matching. If one is found, CAS-01 will redirect to this InternalURL. This will result in the user being prompted for authentication.

If the Exchange 2007 Mailbox server is in a different Active Directory site, CAS-01 determines whether the ExternalURL property is set in that Active Directory site. If it is, and cross-site silent redirection is not enabled, the CrossSiteRedirectType value is set to Manual, and a manual redirect is issued. In this scenario, the user is provided with a clickable link that redirects them to the specified URL.
If cross-site silent redirection has been enabled, the CrossSiteRedirectType value is set to Silent and the user is automatically redirected to the specified URL. If the ExternalURL property is not present, and the authentication method on the /OWA virtual directory is set to Integrated Windows authentication, CAS-01 will proxy the user's request to the Client Access server that's specified by the InternalURL property.

Important:
To allow an Exchange 2010 Client Access server to proxy Outlook Web App requests to an Exchange 2007 Client Access server in another Active Directory site, you must copy the highest-versioned folder from an Exchange 2007 Client Access server in the destination Active Directory site from the %installpath%\ClientAccess\OWA\ folder to the same path on the Exchange 2010 Client Access server that's making the proxy request.

Important:
An Exchange 2010 Client Access server will never proxy Outlook Web App requests to an Exchange 2007 Client Access server in the same Active Directory site. All requests within the same Active Directory site are redirected to an Exchange 2007 Client Access server, using either the **InternalURL** or **ExternalURL** properties for Client Access server, depending on which properties are configured.

4. If the user's mailbox is on an Exchange 2010 Mailbox server in the same Active Directory site as CAS-01, CAS-01 provides access to the mailbox. If the user's mailbox is on an Exchange 2010 Mailbox server in a different Active Directory site, CAS-01 locates a Client Access server in the same Active Directory site as the user's Mailbox server. When one is found, Exchange 2010 determines whether the Client Access server has the **ExternalURL** property set in that Active Directory site. If it is, and cross-site silent redirection hasn't been enabled, the user is provided with a clickable link that

redirects them to the specified URL. If cross-site silent redirection has been enabled, the user will be automatically redirected to the specified URL. If the **ExternalURL** isn't set and the authentication method on the virtual directory is set to Integrated Windows authentication, CAS-01 will proxy the user's request to the Client Access server that's specified by the **InternalURL** property.

Proxying for the Exchange Control Panel

Exchange 2010 provides a Web-based interface for both users and organization administrators to configure settings for their mailbox or for the organization. The Exchange Control Panel (ECP) is accessed either through the Options menu in Outlook Web App or, in Outlook 2010, by choosing the Voice Mail options, requesting message tracking information, or configuring mobile notifications. Selecting any of these options within Outlook launches a Web browser session.

The destination of the session depends on the current connection state of the Outlook client. If the Outlook client is connected using RPC over TCP, the client connects to the InternalURL value of the ECP virtual directory. If the client is connected using Outlook Anywhere, the Outlook client will launch a browser session. The browser session will try to connect to the ExternalURL value of the ECP virtual directory. The URLs are provided to the Outlook client via the Autodiscover service.

When an internal client is connected through TCP, the ECP session will always connect to a Client Access server in the same Active Directory site as the user's mailbox. Proxying isn't used in this scenario. When a client outside the corporate network uses Outlook Anywhere to connect, the client opens a browser session to the external URL of the ECP virtual directory or to the external URL of an Internet-facing Active Directory site if the user's mailbox is located in a non-Internet-facing site.

The proxying logic for the ECP is the same as for Outlook Web App. If the user's mailbox is on an Exchange 2010 Mailbox server in the same Active Directory site as the Client Access server receiving the request, that Client Access server provides access to the mailbox. If the user's mailbox is on an Exchange 2010 Mailbox server in a different Active Directory site, the Client Access server locates a Client Access server in the same Active Directory site as the user's Mailbox server. The original Client Access server will proxy the user's request to that Client Access server.

The ECP does perform redirection, but unless the user explicitly enters the URL to access the ECP, it's rarely performed. If a user accesses the ECP from Outlook Web App, Outlook Web App is responsible for making sure the user is using the correct URL. If the user is using Outlook 2010, Outlook and the Autodiscover service are responsible for making sure the user uses the correct URL for the ECP.

Return to top

Proxying for Exchange Web Services

Exchange Web Services provides an XML messaging interface that enables you to manage Exchange store items and access Exchange server functionality from client applications. From a proxy, redirection, and client perspective this functionality is usually used in the context of one of the following:

- Availability service requests
- Autodiscover requests
- Setting and checking Automatic Replies (OOF) status

An application written using Exchange Web Services can use proxying behavior for such tasks as setting an automatic-reply (Out of Office) message, which will be proxied between Active Directory sites, if required.

The following steps show how incoming requests are handled for a user who makes an Availability service request to an Exchange 2010 Client Access server named CAS-01. The

user is using Outlook Web App to check the availability of another user in the same Exchange organization.

1. CAS-01 queries Active Directory to determine the location of the user's mailbox and the version of Microsoft Exchange installed on the Mailbox server.
2. If the user's mailbox is on an Exchange 2003 server, Outlook Web App makes an HTTP connection to the /Public virtual directory of the Exchange 2003 server and retrieves the requested information from the Free/Busy system folder.
3. If the user's mailbox is on an Exchange 2007 Mailbox server, an error is returned to the user. In any Exchange organization that contains mailboxes on an Exchange 2007 Mailbox server, there must be an externally accessible Exchange 2007 Client Access server. The Autodiscover service is responsible for returning the correct Exchange Web Services URL to the client. This URL must match the version of the Mailbox server that the user's mailbox is on.
4. If the user's mailbox is on an Exchange 2010 Mailbox server in the same Active Directory site as CAS-01, CAS-01 accesses the mailbox itself to retrieve the requested information. If the user's mailbox is on an Exchange 2010 Mailbox server in a different Active Directory site, CAS-01 proxies to a Client Access server in that Active Directory site by using the FQDN specified by the **InternalURL** property of the /EWS virtual directory.

Important:

An Exchange Client Access server will proxy Availability service requests from one server to another whether the **ExternalURL** property is set or not.

Important:

Some Exchange Web Services applications use Web methods such as **GetEvents** and **Unsubscribe**, which have very strong Client Access server affinity. When one Client Access server must proxy one of these requests to another Active Directory site, it can use the **InternalNLBBypassURL** property of the Client Access server, which should always be set to the FQDN of the host server itself. This ensures the Client Access server making the request can maintain affinity with a specific Client Access server in the target Active Directory site.

Exchange Web Services itself doesn't provide redirection functionality, because the Autodiscover service, which is used to provide URLs to an application, provides the URLs required to access a specific mailbox. For example, when a mailbox is moved between Active Directory sites, Outlook receives the updated Active Directory site-specific URLs from the Autodiscover service when it next issues a query. This can sometimes result in a client making Availability service requests to a Client Access server in an Active Directory site other than the one that their mailbox is in. But, because the Availability service will still process the requests and proxy them as necessary, there's no impact on the user.

Important:

In any Exchange organization that contains mailboxes on an Exchange 2007 Mailbox server, there must be an externally accessible Exchange 2007 Client Access server. When the Autodiscover service returns the correct Exchange Web Services URL to a requesting client, this URL matches the version of server that the user's mailbox is on. For any Exchange organization that contains mailboxes on both Exchange 2007 Mailbox servers and Exchange 2010 Mailbox servers, two external URL's must be configured for Exchange Web Services, one for each installed version of Exchange.

Proxying for POP3 and IMAP4

Exchange 2010 can proxy POP3 and IMAP4 sessions between Client Access servers and Active Directory sites.

The following steps show how incoming requests are handled for a user who makes a request to an Exchange 2010 Client Access server named CAS-01 using a POP3 client.

1. CAS-01 queries Active Directory to determine the location of the user's mailbox and the version of Microsoft Exchange installed on the Mailbox server.
2. If the user's mailbox is on an Exchange 2003 server, CAS-01 proxies the connection to the POP3 service running on the Exchange 2003 server that's hosting the user's mailbox.
3. If the user's mailbox is on an Exchange 2007 Mailbox server, CAS-01 locates an Exchange 2007 Client Access server in the same Active Directory site as the user's Mailbox server, which may be in the same Active Directory site as CAS-01. CAS-01 proxies the request to the Client Access server.
4. If the user's mailbox is on an Exchange 2010 Mailbox server in the same Active Directory site as CAS-01, CAS-01 accesses the mailbox itself. If the user's mailbox is on an Exchange 2010 Mailbox server in a different Active Directory site, CAS-01 proxies to a Client Access server using the FQDN specified by the **InternalConnectionSettings** property of the POP configuration for that server.

Important:

There are no InternalURL or ExternalURL settings for the POP3 or IMAP4 services and an Exchange 2010 Client Access server will proxy POP3 and IMAP4 service requests from one server to another when it's needed.

Important:

Client Access servers trying to proxy to another Active Directory site don't check whether the POP3 or IMAP4 service is actually running on the remote Client Access server. It's important, therefore, to not only ensure that the services are running on every Client Access server in the remote Active Directory site, but to consider using a load balancer for the service. Load balances will be discussed later in this topic.

Return to top

Proxying Configuration

If your Client Access server is Internet facing, set the **ExternalURL** property on the /Microsoft-Server-ActiveSync, /OWA, /ECP, and /EWS virtual directories using the Exchange Management Console (EMC) or the Exchange Management Shell (Shell). The EWS virtual directory can only be configured using the Shell. The **InternalURL** property is configured automatically during the initial setup of Exchange 2010 and should only be changed if you want to use a load balancing solution. The **ExternalURL** property should contain the FQDN that's registered for your Exchange organization in DNS.

The following table contains the appropriate values for the **ExternalURL** and **InternalURL** properties for an Internet-facing Client Access server for an Exchange organization that accesses Outlook Web App by using the URL https://mail.contoso.com. The second table contains the appropriate **ExternalURL** and **InternalURL** property values for a non-Internet-facing Client Access server in a second Active Directory site for the same organization. You must ensure that the authentication method for all these virtual directories is set to Integrated Windows authentication. Proxying isn't supported for virtual directories that use other authentication methods except for POP3 and IMAP4, which use SSL/TLS and proxy the user's Basic authentication credentials.

Note:

If new Outlook Web App virtual directories are created using the Shell, you must manually configure the **InternalURL** property on those virtual directories.

InternalURL and ExternalURL settings for an Internet-facing Client Access server

Exchange 2010 service	InternalURL setting	ExternalURL setting
Outlook Web App	https://	https://mail.contoso.com/

	fullyqualifiedcomputername/OWA	OWA
Exchange ActiveSync	https://fullyqualifiedcomputername/Microsoft-Server-ActiveSync	https://mail.contoso.com/Microsoft-Server-ActiveSync
Exchange Web Services	https://*fullyqualifiedcomputername*/EWS/Exchange.asmx	https://mail.contoso.com/EWS/Exchange.asmx
Exchange Control Panel	https://*fullyqualifiedcomputername*/ECP	https://mail.contoso.com/ECP

InternalURL and ExternalURL settings for a non-Internet-facing Client Access server

Exchange 2010 service	InternalURL setting	ExternalURL setting
Outlook Web App	https://*fullyqualifiedcomputername*/OWA	$Null
Exchange ActiveSync	https://*fullyqualifiedcomputername*/Microsoft-Server-ActiveSync	$Null
Exchange Web Services	https://*fullyqualifiedcomputername*/EWS/Exchange.asmx	$Null
Exchange Control Panel	https://*fullyqualifiedcomputername*/ECP	$Null

Configuring Redirection

If more than one of your Active Directory sites are Internet facing, set the **ExternalURL** property on the /OWA and /Microsoft-Server-ActiveSync virtual directories using the EMC or the Shell to allow redirection between them. The **InternalURL** property is configured automatically during the initial setup of Exchange 2010 and should only be changed if you want to use a load balancing solution. The following two tables list the ExternalURL and InternalURL settings for Client Access servers in two Active Directory sites for a company named Contoso. The two sites are usa.contoso.com and europe.contoso.com.

Note:

If new Outlook Web App virtual directories are created using the Shell, you must manually configure the **InternalURL** property on those virtual directories.

InternalURL and ExternalURL property settings for an Internet-facing Client Access server in the usa.contoso.com site

Exchange 2010 service	InternalURL setting	ExternalURL setting
Outlook Web App	https://fullyqualified*computername*/OWA	https://usa.contoso.com/OWA
Exchange Control Panel	https://fullyqualified*computername*/ECP	https://usa.contoso.com/ECP

Exchange ActiveSync	https://fullyqualified*computername* / Microsoft-Server-ActiveSync	https://usa.contoso.com/Microsoft-Server-ActiveSync
Exchange Web Services	https://fullyqualified*computername* / EWS/Exchange.asmx	https://usa.contoso.com/EWS/Exchange.asmx

InternalURL and ExternalURL property settings for an Internet-facing Client Access server in the europe.contoso.com site

Exchange 2010 service	InternalURL setting	ExternalURL setting
Outlook Web App	https://fullyqualified*computername*/OWA	https://europe.contoso.com/OWA
Exchange Control Panel	https://fullyqualified*computername*/ECP	https://europe.contoso.com/ECP
Exchange ActiveSync	https://fullyqualified*computername* / Microsoft-Server-ActiveSync	https://europe.contoso.com/Microsoft-Server-ActiveSync
Exchange Web Services	https://fullyqualified*computername* / EWS/Exchange.asmx	https://europe.contoso.com/EWS/Exchange.asmx

Note:

If the **ExternalURL** property isn't set on the Exchange ActiveSync virtual directory in at least one Active Directory site, the Autodiscover service will fail when it configures mobile phones because the value set on the **ExternalURL** property is passed to the mobile phones during the Autodiscover process.

Return to top

Proxying with Network Load Balancing

In an organization that has multiple Active Directory sites and multiple Client Access servers in each site, you can use Network Load Balancing (NLB) to load balance traffic proxied between the Client Access servers in each site and for users directly accessing those servers. Just deploying a load balancer isn't enough to ensure traffic is balanced effectively. You must also perform some additional configuration of the **InternalURL** and **ExternalURL** properties. We recommend that you include only Client Access servers within the same Active Directory site in a load-balancing array. You can deploy NLB in an Internet-facing Active Directory site and in a non-Internet-facing Active Directory site.

The following table lists the settings you should configure for the virtual directories on the Client Access servers in both Internet-facing and non-Internet-facing sites. The FQDN of the NLB should be configured in DNS to resolve to the load balancing device or service. The load balancing solution will then be responsible for forwarding the traffic to the appropriate Client Access servers.

Virtual directory settings for Client Access servers in an organization that uses NLB

Virtual directory / service	InternalURL	ExternalURL (Internet-facing	ExternalURL (non-Internet-facing

		Active Directory site)	Active Directory site)
/OWA	NLB FQDN (see the following guidelines)	NLB FQDN	$null
/ECP	NLB FQDN (see the following guidelines)	NLB FQDN	$null
/Microsoft-Server-ActiveSync	NLB FQDN	NLB FQDN	$null
/OAB	NLB FQDN	NLB FQDN	$null
/EWS	NLB FQDN	NLB FQDN	$null
POP/IMAP	(InternalConnections Settings) NLB FQDN	Not applicable	Not applicable

We recommend that you use the following guidelines to set the InternalURL property:

- The InternalURL property for the /OWA and /ECP virtual directories on all Client Access servers in an Active Directory site can be set to the NLB FQDN of the servers in that site if there are internal Outlook 2010 users.
- If a Client Access server in an Active Directory site is the target of an Outlook Web App or ECP proxy request from a Client Access server in any other Active Directory site, make sure that you configure your load balancer to ensure affinity is maintained. This is because the Client Access server in the Internet-facing site cannot select a server for each individual request and maintain its own affinity

The following table lists the various authentication settings that are needed on virtual directories in an organization that uses network load balancing (NLB). In an organization that uses NLB, the NLB URL is used in place of a specific Client Access server URL for client connectivity.

Virtual directory authentication settings for Client Access servers in an organization that uses NLB URLs for fault tolerance and load balancing

Virtual directory /service	Internet-facing Active Directory site	Non-Internet-facing Active Directory site
/OWA	If Microsoft Forefront Threat Management Gateway 2010 (Forefront TMG) or Microsoft Forefront Unified Access Gateway 2010 (Forefront UAG) are being used, and forms-based authentication is enabled, use Basic or Integrated Windows authentication, depending on firewall rule delegation settings. If traffic from the Internet passes to the Client Access server with no pre-authentication, then use forms-based authentication.	Integrated Windows authentication

	The same authentication method should be enabled on the /OWA and /ECP virtual directories.	
/ECP	If Forefront TMG or Forefront UAFG are being used, and forms-based authentication is enabled, use Basic or Integrated Windows authentication, depending on firewall rule delegation settings. If traffic from the Internet passes to the Client Access server with no pre-authentication, then use forms-based authentication. The same authentication method should be enabled on the /OWA and /ECP virtual directories.	Integrated Windows authentication
/Microsoft-Server-ActiveSync	Basic authentication.	Basic authentication (Proxying is performed using the /Proxy sub virtual directory.)
/OAB	Basic or Integrated Windows authentication, depending on firewall rule delegation settings.	Basic or Integrated Windows authentication, depending on firewall rule delegation settings (OAB requests are never proxied between Active Directory sites. This virtual directory is only used by Outlook clients.)
/EWS	Basic (optional - depending on firewall rule delegation settings). Integrated Windows authentication required.	Integrated Windows authentication
POP/IMAP	As required by client connection method.	As required by client connection method

Return to top

Load Balancing Logic Used by Client Access Servers When Proxying Between Active Directory Sites

When multiple Client Access servers exist in the site that will be the target of a proxy attempt, and the server on which the user's mailbox is located is a combined Client Access server and Mailbox server, the Client Access server in the source Active Directory site will always choose that combined Client Access server and Mailbox server as the target of the proxy attempt.

Outlook Web App, the ECP, and Exchange Web Services handle load balancing differently than the Availability service and Exchange ActiveSync do. Outlook Web App, the ECP, and Exchange Web Services implement their own load balancing when they're deployed on multiple Client Access servers within the same Active Directory site. If a user tries to access Outlook Web App through https://mail.contoso.com/owa and is proxied to CAS-01, the next time that user tries to access Outlook Web App, they'll again be proxied to CAS-01, This will happen even if CAS-02 has fewer concurrent connections. This is done to ensure long-running transactions can be completed without reauthentication or requesting data again. This is known as Affinity. If CAS-01 is unavailable, the user will be proxied to CAS-02 and the user may be required to reauthenticate.

Exchange Web Services can maintain affinity when proxied between Active Directory sites despite the **InternalURL** property of the target server being configured with an NLB URL. This is because the Client Access server making the proxy request for an application that requires affinity uses the **InternalNLBBypassURL** property on the target server. The **InternalNLBBypassURL** property is configured with the FQDN of the target server and uses Windows authentication by default.

Note:

For Outlook Web App, the ECP, and Exchange Web Services, your firewall should be configured for cookie-based or IP-based affinity. This ensures that a particular client application connects to the same server every time. This is required so that the SSL negotiation isn't performed repeatedly for each request. It's important to maintain affinity from the client application through to the final Client Access server involved in the transaction.

Note:

You shouldn't change the value of the**InternalNLBBypassURL** property on a Client Access server. If you change it, you'll break proxied Exchange Web Services requests.

The process is different for Exchange ActiveSync. When an Internet-facing Client Access server proxies a request to a non-Internet-facing Client Access server, the requesting Client Access server looks for a Client Access server in the target site and tries to connect to it using the value configured in the **InternalURL** property. If the server doesn't respond, the request will fail and an error will be returned to the client. We recommend implementing round-robin load balancing within an NLB array and setting the **InternalURL** property to a load-balanced value.

We also recommend load balancing for the Availability service. Availability service requests don't have to maintain their connection state. In other words, two consecutive Availability service requests from the same client can be proxied to different Client Access servers in the destination Active Directory site without performance being affected, and there are no authentication issues if the **InternalURL** property is set to be a load balanced value. In addition, setting the **InternalURL** property to a load-balanced value benefits any Outlook 2007 and Outlook 2010 clients internally, because the Autodiscover service provides those clients with the load-balanced value set in the **InternalURL** property to allow them to complete their Availability service requests.

For more information about network load balancing, see Understanding Load Balancing in Exchange 2010.

Note:

In many deployments, the Client Access server role and the Hub Transport server role are installed on the same computer. In this topology, you can configure NLB for the Client Access server role separately from the Hub Transport server role. Currently NLB isn't supported on the Hub Transport server role. However, it's supported for the Client Access server role. To configure NLB for the Client Access server role and not the Hub Transport server role, configure ports 80 and 443 for client access. The Hub Transport server role implements its own high availability within the software.

Return to top

Summary of Client Access Methods

The following table summarizes the protocols used to access Exchange 2010 and how they're used for proxying and redirection.

Client Access protocols for redirection and proxying

Protocol/Application	Redirection supported between Client Access servers	Proxying supported between Client Access servers	Comments
Outlook Web App	Yes	Yes	Must have a Client Access server in each Active Directory site to use Outlook Web App.
Exchange Control Panel	Yes	Yes	Must have a Client Access server in each Active Directory site to use the ECP.
Exchange ActiveSync	Yes	Yes	Must have a Client Access server in each Active Directory site to use Exchange ActiveSync.
Exchange Web Services	No (The Autodiscover service provides the application with the correct ExternalURL value)	Yes	Must have a Client Access server in each Active Directory site to use Exchange Web Services.
Availability service	No (The Autodiscover service provides the application with the correct ExternalURL value)	Yes	Must have a Client Access server in each Active Directory site to use the Availability service.
POP3 and IMAP4	No	Yes	Must have a Client Access server in each Active Directory site to use POP3 and IMAP4.

Proxying Performance and Scalability

In an Exchange 2010 proxying environment, poor performance often results when the Client Access servers receive lots of concurrent requests. This problem is frequently caused by the exhaustion of threads and available connections because of Web service requests from ASP.NET. This can cause the Client Access servers to deny requests or exhibit high latency when the requests are being processed.

To resolve these issues, you can configure several ASP.NET parameters by editing the Machine.config file on the Client Access servers. For more information about how to

configure these parameters, see Microsoft Knowledge Base article 821268, Contention, poor performance, and deadlocks when you make Web service requests from ASP.NET applications.

Two of the parameters explained in Knowledge Base article 821268 must be set differently in an Exchange 2010 proxying environment. We recommend that you allow for 36 threads per processor, and that you set the *maxconnections* value to 2,000.

For more information about server performance, see Managing the .NET Framework on Windows Server 2003.

1.6.1.3 Understanding Client Throttling Policies

Understanding Client Throttling Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-30*

Microsoft Exchange Server 2010 uses client throttling policies to manage the performance of your Exchange organization. To do this, Exchange tracks the resources that each user consumes, and enforces connection bandwidth limits, as necessary.

Among other things, client throttling helps you make sure that:

- Users aren't intentionally taxing the system.
- Users aren't unintentionally taxing the system.
- Users of various connectivity methods are sharing resources proportionally.

In Exchange Server 2010 SP1, all client throttling policies are turned on by default. If you are experiencing problems that may be caused by these policies, you can turn off client throttling. To turn off client throttling, you can set all policy parameters to `$Null`.

Contents

Default and Non-Default Policies

When an Exchange organization is created, a default throttling policy is automatically created that implicitly governs all users within that organization. Although the default client throttling policy is generally sufficient to manage the load placed on your Exchange system, you can customize the default policy or add additional policies based on the needs of your organization.

If you're hosting multiple tenants in your Exchange organization, you can define an acceptable load for each user of a tenant. Similarly, if you're an on-premise organization, you can define an acceptable load on a user-by-user basis. Through policies, Exchange evaluates how each user uses the system and ensures that the resulting per-user load falls within acceptable boundaries as defined by the user's policy. The client throttling system tracks system usage on a per-user basis and uses the throttling policy associated with that user to determine if throttling should occur.

In Exchange 2010 Enterprise installations, there's a single default throttling policy called First Organization. In multi-tenant deployments, each tenant has its own default throttling policy.

Fallback Policy

The throttling framework is designed to protect Exchange resources. Therefore, if the non-default policy is corrupted or missing, the throttling policy will first fall back to the default throttling policy for the organization. However, if the default policy is corrupted or missing, the throttling policy falls back to the *fallback policy*. Because the fallback policy is embedded in Exchange, it's less likely to fail.

The fallback policy is also applied to authenticated accounts, such as computer accounts, cross-forest contacts, and Active Directory accounts that do not have mailboxes. These accounts will have the fallback policy values assigned. Because these accounts use the fallback policy, the policy values cannot be modified.

The fallback policy uses the following values:

Access Type	MaxConcurrency	PercentTimeInAD	PercentTimeInCAS	PercentTimeInRPC	Other
Anonymous	1	$null	$null	$null	
EAS	10	$null	$null	$null	10 (maxDevices) $null ($MaxDeviceDeletesPerMonth
EWS	10	50	90	60	5000 (maxSubscription) 60 (fastSearchTimeout)1000 (findCountLimit)
IMAP	$null	$null	$null	$null	
OWA	5	30	150	150	
POP	20	$null	$null	$null	
PowerShell	18				$null (maxTenantConcurrency) $null (maxCmdletsTime$null

					(MaxCmdlets) Period) $null (ExchangeMax Cmdlets) $null (maxCmdletQu eueDepth) $null (maxDestructi veCmdlets) $null (maxDestructi veCMdletsTim ePeriod)
RCA	2000	5	205	200	
CPA	20		205	200	
General					$null (MessageRate Limit) $null (RecipientRate Limit) $null (ForwardeeLi mit) $null (cpuStartPerce nt)

Return to top

Understanding Policy Parameters

You manage throttling policy settings through the Exchange Management Shell using the **Get-ThrottlingPolicy**, **Set-ThrottlingPolicy**, **New-ThrottlingPolicy**, and **Remove-ThrottlingPolicy** cmdlets.

The acceptable load of a throttling policy is defined by the cmdlet parameter values on that throttling policy. The component types covered by throttling policies are as follows:

- Microsoft Exchange ActiveSync
- Exchange Web Services
- IMAP
- Outlook Web App
- POP
- Windows PowerShell

All these component types have policy parameters that work similarly, except for the Windows PowerShell component type.

The common component types are governed by four policy parameters: *<Component Acronym>MaxConcurrency*, *<Component Acronym>PercentTimeInAD*, *<Component Acronym>PercentTimeInCAS*, and -*<Component Acronym>PercentTimeInMailboxRPC*. The parameter names are prefixed by the component type acronym. The following table lists the component type acronyms that are used for the parameters in the throttling policy

cmdlets.

Component type acronyms that are used in throttling policy cmdlets

Component Acronym	Description	Example
EAS	Exchange ActiveSync	In the parameter *EASPercentTimeInCAS*, the component acronym EAS represents the Exchange ActiveSync component.
EWS	Exchange Web Services	In the parameter *EWSPercentTimeInCAS*, the component acronym EWS represents the Exchange Web Services component.
OWA	Outlook Web App	In the parameter *OWAPercentTimeInCAS*, the component acronym OWA represents the Outlook Web App component.
IMAP	IMAP4	In the parameter *IMAPPercentTimeInCAS*, the component acronym IMAP represents the IMAP4 component.
POP	POP3	In the parameter *POPPercentTimeInCAS*, the component acronym POP represents the POP3 component.

Note:

Unified Messaging users are considered Exchange Web Services users and their connections to the Exchange server are throttled by Exchange Web Services parameters such as *EWSMaxConcurrency*, *EWSPercentTimeInAD*, *EWSPercentTimeInCAS*, and *EWSPercentTimeInMailboxRPC*.

Return to top

MaxConcurrency

The value for a *MaxConcurrency* policy parameter indicates how many concurrent connections a specified user can have against an Exchange server at one time. A connection is held from the moment a request is received until a response is sent in its entirety to the requestor. If users try to make more concurrent requests than their policy allows, the new connection attempt fails. However, the existing connections remain valid. *<Component Acronym>MaxConcurrency* has a valid range from 0 through 2147483647 inclusive. To indicate that *<Component Acronym>MaxConcurrency* should be unthrottled (no limit), this value should be set to `$null`.

Important:

Don't set throttling policy parameters to `$null` unless you have a business need to do so. Unthrottled users aren't limited in their ability to intentionally or inadvertently place a high load on the server.

PercentTimeInCAS, PercentTimeInAD, and PercentTimeInMailboxRPC

The value for a *PercentTimeInCAS*, *PercentTimeInAD*, or *PercentTimeInMailboxRPC* policy parameter indicates what percentage of a minute can be spent:

- Running Client Access server code (*<Component Acronym>PercentTimeInCAS*)
- Running LDAP requests (*<Component Acronym>PercentTimeInAD*)
- Running mailbox RPC requests (*<Component Acronym>PercentTimeInMailboxRPC*)

A value of 100 indicates that for every one-minute window, the process can spend 60 seconds of that time consuming the resource in question. Although, it appears that a process would never encounter throttling with a value set to 100, you have to consider the effect of concurrent requests. If a process makes two concurrent requests that spend 60 seconds each running code on the Client Access server, the process has effectively used 120 seconds in a 60 second window, thus representing a *<Component Acronym>PercentTimeInCAS* value of 200 percent.

To indicate that *PercentTimeInCAS*, *PercentTimeInAD*, and *PercentTimeInMailboxRPC* should be unthrottled (no limit), this value should be set to `$null`.

Important:
Don't set throttling policy parameters to `$null` unless you have a business need to do so. Users aren't limited in their ability to intentionally or inadvertently place a high load on the server.

It's important to note that *<Component Acronym>PercentTimeInCAS* is an overlapping superset of *<Component Acronym>PercentTimeInAD* and *<Component Acronym>PercentTimeInMailboxRPC*. This means that the expenditure in Client Access server processing time will always be larger than the expenditures in *<Component Acronym>PercentTimeInAD* and *<Component Acronym>PercentTimeInMailboxRPC*. This is because for the Exchange component to make an Active Directory or RPC call, it must already be running Client Access server code. In addition, the expenditure in processing time for *<Component Acronym>PercentTimeInCAS* doesn't stop while LDAP or RPC calls are being made. Even though the request might be synchronously waiting for a response from Active Directory or the Exchange store, the process is still consuming a thread on the server and therefore should continue being charged for that usage. As a result, the *<Component Acronym>PercentTimeInCAS* value must be set to a value larger than the *<Component Acronym>PercentTimeInAD* value and the *<Component Acronym>PercentTimeInMailboxRPC* value.

Return to top

Exchange Management Shell Commands and Parameters

This section discusses the following Windows PowerShell parameters:

- *PowerShellMaxConcurrency*
- *PowerShellMaxCmdlets*
- *PowerShellMaxCmdletsTimePeriod*
- *PowerShellMaxCmdletQueueDepth*

PowerShellMaxConcurrency

In the context of remote Shell, the *PowerShellMaxConcurrency* parameter defines the maximum number of remote Shell sessions that a remote Shell user can have open at the same time. In the context of Web services, the *PowerShellMaxConcurrency* parameter defines the number of concurrent cmdlets that a user can have running at the same time. This value doesn't necessarily match the number of browsers opened by the user.

PowerShellMaxCmdlets

The *PowerShellMaxCmdlets* parameter defines the number of cmdlets that can be run per time period without being throttled. This parameter directly depends on the value defined by the *PowerShellMaxCmdletsTimePeriod* parameter. Both values should be set at the same time.

PowerShellMaxCmdletsTimePeriod

The *PowerShellMaxCmdletsTimePeriod* parameter defines the time period, in seconds, that a user can run the number of cmdlets defined by the *PowerShellMaxCmdlets* parameter.

PowerShellMaxCmdletQueueDepth

The *PowerShellMaxCmdletQueueDepth* parameter defines the number of operations that a user can run at the same time. This value directly affects the behavior of the *PowerShellMaxCmdlets* and *PowerShellMaxConcurrency* parameters. For example, the *PowerShellMaxConcurrency* parameter will use up at least two of the operations defined by the *PowerShellMaxCmdletQueueDepth* parameter, but additional operations will also be counted against the throttling limit each time the cmdlet is run. The number of operations that count toward the throttling limit depends on the cmdlets that are run. We recommend that the value for the *PowerShellMaxCmdletQueueDepth* parameter be at least three times larger than the value of the *PowerShellMaxConcurrency* parameter. This parameter won't affect operations that are run using the Exchange Control Panel or operations that are run through Exchange Web Services.

Return to top

Managing Client Throttling Policies

The Exchange Management Shell enables you to modify and view the client throttling policy settings using the cmdlets described in the following table.

Cmdlets for managing client throttling policies on a Client Access server

Cmdlet name	Description
New-ThrottlingPolicy	This cmdlet creates a new throttling policy.
Remove-ThrottlingPolicy	This cmdlet removes a throttling policy.
Get-ThrottlingPolicy	This cmdlet lets you view the settings of a throttling policy.
Set-ThrottlingPolicy	This cmdlet modifies all available settings for a throttling policy.

To view the syntax and parameters for these cmdlets, see New-ThrottlingPolicy, Remove-ThrottlingPolicy, Get-ThrottlingPolicy, and Set-ThrottlingPolicy.

You can associate a throttling policy with a specific object. The object can be a user with a mailbox, a user without a mailbox, a contact, or a computer account. For the syntax and parameters for these cmdlets, see Get-ThrottlingPolicyAssociation and Set-ThrottlingPolicyAssociation.

Note:
To associate a throttling policy with a single user or a group of users, use the *ThrottlingPolicy* parameter with the New-Mailbox and Set-Mailbox cmdlets.

Managing Client Throttling Policy Settings on a Per-User Basis

You can use the *ThrottlingPolicy* parameter of the **Set-Mailbox** and **New-Mailbox** cmdlets in the Exchange Management Shell to associate client throttling policies with a user or a group of users by modifying properties on their mailbox. For more information, see Set-Mailbox and New-Mailbox.

Return to top

Common Throttling Policy Management Tasks

The following are some ways you can manage client throttling policies.

Retrieving the Default Throttling Policy

By default, client throttling policies have the *IsDefault* parameter set to true. You can retrieve the default throttling policy using the `where-object` filter. The following example shows how to retrieve the default throttling policy.

```
Get-ThrottlingPolicy | where-object {$_.IsDefault -eq $true}
```

Retrieving the Throttling Policy That Governs a User

You can set throttling policies on a per-user basis. Therefore, you may want to retrieve the policy governing a specific user. You can obtain the `ThrottlingPolicy` parameter from the mailbox of the user you're interested in and pass it to the **Get-ThrottlingPolicy** cmdlet. In the following example, the mailbox of a user named Tony Smith is used.

```
$policy = $null;
$policyLink = (Get-Mailbox tonysmith).ThrottlingPolicy;
if ($policyLink -eq $null)
{
    $policy = Get-ThrottlingPolicy | ? {$_.IsDefault};
}
else
{
    $policy = $policyLink | Get-ThrottlingPolicy;
}
```

Return to top

Creating a New, Non-Default Throttling Policy

To create a new, non-default throttling policy, run the **New-ThrottlingPolicy** cmdlet and set the parameters you want. Any parameters that you omit will inherit the values from the default throttling policy. The following example creates a new throttling policy, `ClientThrottlingPolicy2`. The new policy has nearly the same settings as the default throttling policy. The difference is that the new non-default throttling policy, `ClientThrottlingPolicy2`, sets `EWSPercentTimeInCAS` to 80 and turns off `EWSPercentTimeInAD` throttling.

```
New-ThrottlingPolicy -Name ClientThrottlingPolicy2 -EWSPercentTimeInCAS 80 -EWSPe
```

Assigning a Non-Default Throttling Policy to a User

To assign a non-default throttling policy to a user, use the **Set-Mailbox** cmdlet, as follows.

```
$b = Get-ThrottlingPolicy ClientThrottlingPolicy2;
Set-Mailbox -Identity tonysmith -ThrottlingPolicy $b;
```

If a user is governed by a non-default throttling policy and you want the user to use the default policy, you might think you can make this change by setting the *ThrottlingPolicy* parameter to `$null`. Unfortunately, setting the *ThrottlingPolicy* parameter to `$null` doesn't modify the Mailbox object. To make the default throttling policy apply to the user, you must explicitly set the default throttling policy for that user by using the following command.

```
$policy = Get-ThrottlingPolicy | where-object {$_.IsDefault -eq $true};
Set-Mailbox -Identity tonysmith -ThrottlingPolicy $policy;
```

Return to top

Finding All Users Governed by a Specific Throttling Policy

If you want to learn which users are governed by a specific throttling policy, run the **Get-Mailbox** cmdlet and filter the throttling policy identity as shown in the following example. In this example, `$policy` is the policy for which you are filtering.

```
Get-Mailbox | where-object {$_.ThrottlingPolicy -eq $policy.Identity}
```

Removing Throttling Policies

You can only remove throttling policies that are non-default policies and aren't associated with any mailboxes. To do this, run the **Remove-ThrottlingPolicy** cmdlet and pass the identity of the throttling policy, using the following command.

```
Remove-ThrottlingPolicy ClientThrottlingPolicy2
```

If you have a throttling policy associated with users, you must first reassign those users to another policy, and then you can remove the policy you want to remove. The following example shows how to do this.

```
$policy = Get-ThrottlingPolicy ClientThrottlingPolicy2;
$mailboxes = Get-Mailbox | where-object {$_.ThrottlingPolicy -eq $policy.Identity
$defaultPolicy = Get-ThrottlingPolicy | where-object {$_.IsDefault -eq $true};
foreach ($mailbox in $mailboxes)
{
Set-Mailbox -Identity $mailbox.Identity -ThrottlingPolicy $defaultPolicy;
}
Remove-ThrottlingPolicy ClientThrottlingPolicy2;
```

Return to top

Modifying Throttling Policies

You modify an existing throttling policy (including the default) by running the **Set-ThrottlingPolicy** cmdlet and specifying which parameters to change. For example, to change the *EWSMaxConcurrency* parameter value for the default throttling policy to 4, you could use the following command.

```
$a = Get-ThrottlingPolicy | where-object {$_.IsDefault -eq $true}
$a | Set-ThrottlingPolicy -EWSMaxConcurrency 4
```

Throttling Performance Counters

Because throttling helps govern the overall usage of Exchange components on an Exchange server, it's often useful to examine how throttling is affecting the system. Exchange offers a set of throttling performance counters per process. An Exchange process such as Outlook Web App will have its own set of counters, for example, and Exchange Web Services will have its own set. In the Windows Performance tool, these counters are called instances.

Enable throttling logging in the RPC Client Access log

By default, throttling logging is disabled for the RPC client access service. Therefore, you will not see throttling information in the RPC Client Access logs. To enable throttling logging, follow these steps:

1. Open the following file in a text editor, such as Notepad: **C:\Program Files\Microsoft\Exchange Server\V14\Bin\Microsoft.Exchange.RpcClientAccess.Service.exe.config**
2. In the file, locate the **<add key="LoggingTag" value="ConnectDisconnect, Logon, Failures, ApplicationData, Warnings" />** section.

3. Type **Throttling** in the comma-separated string. For example, type **Throttling** in the string that resembles the following: **<add key="LoggingTag" value="ConnectDisconnect, Logon, Failures, ApplicationData, Warnings, Throttling" />**.
   Save and then close the file.
4. Restart the RPC Client Access service.

Return to top

1.6.1.4 Understanding Exchange ActiveSync

Understanding Exchange ActiveSync

Exchange Server 2010 > Client Access > Understanding Client Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-09*

By default, when you install the Client Access server role on a computer that's running Microsoft Exchange Server 2010, you enable Microsoft Exchange ActiveSync. Exchange ActiveSync lets you synchronize a mobile phone with your Exchange 2010 mailbox.

Overview of Exchange ActiveSync

Exchange ActiveSync is a Microsoft Exchange synchronization protocol that's optimized to work together with high-latency and low-bandwidth networks. The protocol, based on HTTP and XML, lets mobile phones access an organization's information on a server that's running Microsoft Exchange. Exchange ActiveSync enables mobile phone users to access their e-mail, calendar, contacts, and tasks and to continue to be able to access this information while they're working offline.

Note:
Exchange ActiveSync can synchronize e-mail messages, calendar items, contacts, tasks, and notes.

Important:
Windows Phone 7 mobile phones only support a subset of all Exchange ActiveSync mailbox policy settings. For a complete list, see Windows Phone 7 Synchronization.

Features in Exchange ActiveSync

Exchange ActiveSync provides the following:

- Support for HTML messages
- Support for follow-up flags
- Conversation grouping of e-mail messages
- Ability to synchronize or not synchronize an entire conversation
- Synchronization of SMS messages with a user's Exchange mailbox
- Support for viewing of message reply status
- Support for fast message retrieval
- Meeting attendee information
- Enhanced Exchange Search
- PIN reset
- Enhanced device security through password policies
- Autodiscover for over-the-air provisioning
- Support for setting auto-replies when users are away, on vacation, or out of the office

- Support for tasks synchronization
- Direct Push
- Support for availability information for contacts

Managing Exchange ActiveSync

By default, Exchange ActiveSync is enabled. All users who have an Exchange mailbox can synchronize their mobile phone with the Microsoft Exchange server.

You can perform the following Exchange ActiveSync tasks:

- Enable and disable Exchange ActiveSync for users
- Set policies such as minimum password length, device locking, and maximum failed password attempts
- Initiate a remote wipe to clear all data from a lost or stolen mobile phone
- Run a variety of reports for viewing or exporting into a reporting solution

Security in Exchange ActiveSync

You can configure Exchange ActiveSync to use Secure Sockets Layer (SSL) encryption for communications between the Exchange server and the mobile phone client. Certificate-based authentication works with a self-signed certificate, a certificate from an existing public key infrastructure, or a third-party commercial certificate. You can use certificate-based authentication together with other security features, such as local device wipe and a device password, to turn the mobile phone into a smartcard. The private key and certificate for client authentication are stored in memory on the mobile phone. If an unauthorized user tries to bypass the mobile phone password, all user data is purged. This includes the certificate and private key. For more security, you can deploy RSA SecurID two-factor authentication on the Exchange server.

Device Security Features in Exchange ActiveSync

In addition to the ability to configure security options for communications between the Exchange server and your mobile phones, Exchange ActiveSync offers the following features to enhance the security of mobile phones:

- **Remote wipe** If a mobile phone is lost, stolen, or otherwise compromised, you can issue a remote wipe command from the Exchange Server computer or from any Web browser by using Outlook Web App. This command erases all data from the mobile phone.
- **Device password policies** Exchange ActiveSync lets you configure several options for device passwords. These options include the following:
  - **Minimum password length (characters)** This option specifies the length of the password for the mobile phone. The default length is 4 characters, but as many as 18 can be included.
  - **Minimum number of character sets** Use this text box to specify the complexity of the alphanumeric password and force users to use a number of different sets of characters from among the following: lowercase letters, uppercase letters, symbols and numbers.
  - **Require alphanumeric password** This option determines password strength. You can enforce the usage of a character or symbol in the password in addition to numbers.
  - **Inactivity time (seconds)** This option determines how long the mobile phone must be inactive before the user is prompted for a password to unlock the mobile phone.
  - **Enforce password history** Select this check box to force the mobile phone to prevent the user from reusing their previous passwords. The number that you set determines the number of past passwords that the user won't be allowed to reuse.
  - **Enable password recovery** Select this check box to enable password recovery for the mobile phone. Users can use Outlook Web App to look up their recovery password and unlock their mobile phone. Administrators can use the EMC to look up a user's recovery password.

- **Wipe device after failed (attempts)** This option lets you specify whether you want the phone's memory to be wiped after multiple failed password attempts.

- **Device Encryption Policies** There are a number of mobile phone or device encryption policies that you can enforce for a group of users. These policies include the following:
  - **Require encryption on device** Select this check box to require encryption on the mobile phone. This increases security by encrypting all information on the mobile phone.
  - **Require encryption on storage cards** Select this check box to require encryption on the mobile phone's removable storage card. This increases security by encrypting all information on the storage cards for the mobile phone.

Windows Phone 7 Synchronization

If you have Windows Phone 7 mobile phones in your organization, these phones will experience synchronization problems if certain Exchange ActiveSync mailbox policy properties are configured. To allow Windows Phone 7 mobile phones to synchronize with an Exchange mailbox, either set the **AllowNonProvisionableDevices** property to true or only configure the following Exchange ActiveSync mailbox policy properties:

- PasswordRequired
- MinPasswordLength
- IdleTimeoutFrequencyValue
- DeviceWipeThreshold
- AllowSimplePassword
- PasswordExpiration
- PasswordHistory
- DisableRemovableStorage
- DisableIrDA
- DisableDesktopSync
- BlockRemoteDesktop
- BlockInternetSharing

1.6.1.4.1 Understanding Direct Push

Understanding Direct Push

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-03-18*

Direct Push is a feature that's built into Microsoft Exchange Server 2010. Direct Push keeps a mobile phone current over a cellular network connection. It provides notification to the mobile phone when new content is ready to be synchronized to the mobile phone.

Overview

For Direct Push to work, the mobile phone or other mobile device must be Direct Push capable. These devices include the following:

- Mobile phones that have Windows Mobile 5.0 with the Messaging and Security Feature Pack (MSFP) or a later version of Windows Mobile.

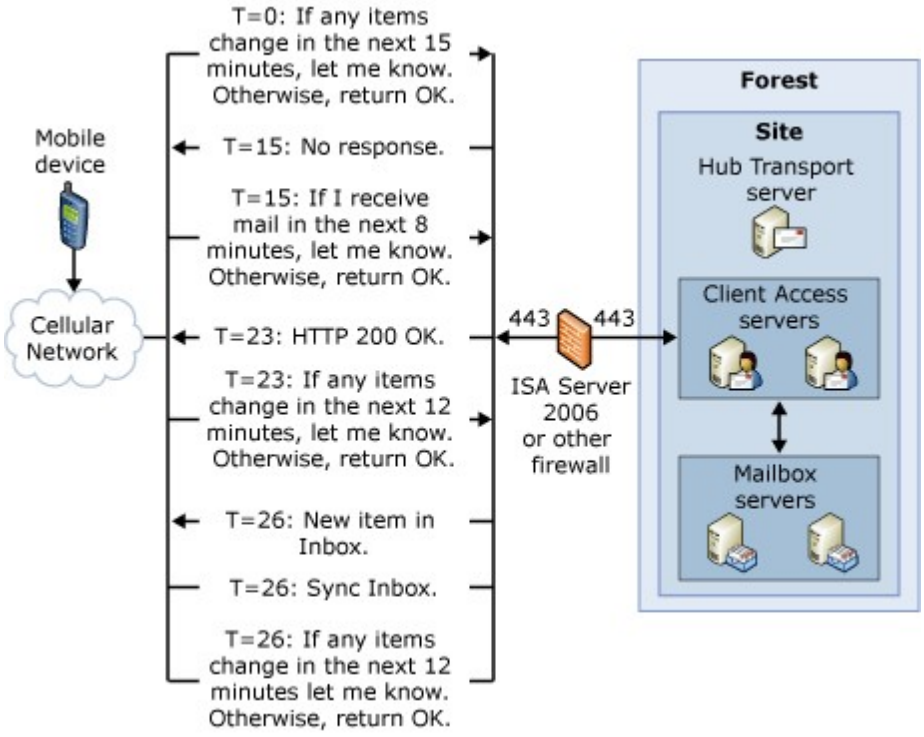
- Mobile phones that are produced by Microsoft Exchange ActiveSync licensees and are designed specifically to be Direct Push compatible.

By default, Direct Push is enabled in Exchange 2010. Mobile phones that support Direct Push issue a long-lived HTTPS request to the server running Microsoft Exchange. The Exchange server monitors activity on the user's mailbox and sends a response to the device if there are any changes, such as new or changed e-mail messages or calendar or contact items. If changes occur within the lifespan of the HTTPS request, the Exchange server issues a response to the device that states that changes have occurred and the device should initiate synchronization with the Exchange server. The device then issues this request to the server. When synchronization is complete, a new long-lived HTTPS request is generated to start the process again. This guarantees that e-mail, calendar, contact, and task items are delivered quickly to the mobile phone, and the device is always synchronized with the Exchange server.

Direct Push Topology

The following figure shows a typical Exchange 2010 topology that's configured for Direct Push. This figure assumes you have the Client Access and Mailbox server roles installed on two separate Exchange computers. You can also install both server roles on the same physical Exchange 2010 computer.

Direct Push network design



Direct Push operates in the following way:

1. A mobile phone that's configured to synchronize with an Exchange 2010 server issues an HTTPS request to the server. This request is known as a PING. The request tells the server to notify the device if any items change in any folder that's configured to synchronize in the next 15 minutes. Otherwise, the server should return an HTTP 200 OK message. The mobile phone then stands by. The 15-minute time span is known as a heartbeat interval.
2. If no items change in 15 minutes, the server returns a response of HTTP 200 OK. The mobile phone receives this response, resumes activity (known as

waking up), and issues its request again. This restarts the process.

3. If any items change or new items are received within the 15-minute heartbeat interval, the server sends a response that informs the mobile phone that there's a new or changed item and provides the name of the folder in which the new or changed item resides. After the mobile phone receives this response, it issues a synchronization request for the folder that has the new or changed items. When synchronization is complete, the mobile phone issues a new PING request and the whole process starts over.

Direct Push depends on network conditions that support a long-standing HTTPS request. If the carrier network for the mobile phone or the firewall doesn't support long-standing HTTPS requests, the HTTPS request is stopped. The following steps describe how Direct Push operates when a mobile phone's carrier network has a time-out value of 13 minutes:

1. A mobile phone issues an HTTPS request to the server. The request tells the server to notify the device if any items change in any folder that is configured to synchronize in the next 15 minutes. Otherwise, the server should return an HTTP 200 OK message. The mobile phone then stands by.
2. If the server does not respond after 15 minutes, the mobile phone wakes up and concludes that the connection to the server was timed out by the network. The device reissues the HTTPS request, but this time it uses a heartbeat interval of 8 minutes.
3. After 8 minutes, the server sends an HTTP 200 OK message. The device then tries to gain a longer connection by issuing a new HTTPS request to the server that has a heartbeat interval of 12 minutes.
4. After 4 minutes, a new e-mail message is received and the server responds by sending an HTTPS request that tells the device to synchronize. The device synchronizes and reissues the HTTPS request that has a heartbeat of 12 minutes.
5. After 12 minutes, if there are no new or changed items, the server responds by sending an HTTP 200 OK message. The device wakes up and concludes that network conditions support a heartbeat interval of 12 minutes. The device then tries to gain a longer connection by reissuing an HTTPS request that has a heartbeat interval of 16 minutes.
6. After 16 minutes, no response is received from the server. The device wakes up and concludes that network conditions cannot support a heartbeat interval of 16 minutes. Because this failure occurred directly after the device tried to increase the heartbeat interval, it concludes that the heartbeat interval has reached its maximum limit. The device then issues an HTTPS request that has a heartbeat interval of 12 minutes because this was the last successful heartbeat interval.

The mobile phone tries to use the longest heartbeat interval the network supports. This extends battery life on the device and reduces how much data is transferred over the network. Mobile carriers can specify a maximum, minimum, and initial heartbeat value in the registry settings for the mobile phone.

Configuring Direct Push to Work Through Your Firewall

For Direct Push to work through your firewall, you must open TCP port 443. This port is required for Secure Sockets Layer (SSL) and must be opened between the Internet and the Client Access server.

In addition to opening ports on your firewall, for optimal Direct Push performance, you should increase the time-out value on your firewall from the default of 15 minutes to 30 minutes. The maximum length of the HTTPS request is determined by the following settings:

- The maximum time-out value that's set on the firewalls that control the traffic from the Internet to the Client Access server
- The Firewall time-out values that are set by the mobile service provider

A short time-out value causes the device to initiate a new HTTPS request more frequently. This can shorten battery life on the device. For more information about how to configure your firewall, see the ISA Server Product Documentation.

1.6.1.4.2 Understanding Exchange ActiveSync Mailbox Policies

Understanding Exchange ActiveSync Mailbox Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-02*

This topic discusses Microsoft Exchange ActiveSync mailbox policies and how they can be used in your Microsoft Exchange Server 2010 environment.

Overview

Exchange ActiveSync mailbox policies let you apply a common set of policy or security settings to a user or group of users. The following table summarizes the settings you can specify by using Exchange ActiveSync mailbox policies.

Important:
Windows Phone 7 mobile phones only support a subset of all Exchange ActiveSync mailbox policy settings. For a complete list, see Windows Phone 7 Synchronization later in this topic.

Exchange ActiveSync mailbox policy settings

Setting	Description
Allow Bluetooth	This setting specifies whether a mobile phone allows Bluetooth connections. The available options are Disable, HandsFree Only, and Allow. This policy setting requires an Enterprise Client Access License.
Allow Browser	This setting specifies whether Pocket Internet Explorer is allowed on the mobile phone. This setting doesn't affect third-party browsers installed on the phone. This policy setting requires an Exchange Enterprise Client Access License.
Allow Camera	This setting specifies whether the mobile phone camera can be used. This policy setting requires an Exchange Enterprise Client Access License.
Allow Consumer Mail	This setting specifies whether the mobile phone user can configure a personal e-mail account (either POP3 or IMAP4) on the mobile phone. This policy setting requires an Exchange Enterprise Client Access License.
Allow Desktop Sync	This setting specifies whether the mobile phone can synchronize with a computer

	through a cable, Bluetooth, or IrDA connection. This policy setting requires an Exchange Enterprise Client Access License.
Allow HTML E-mail	This setting specifies whether e-mail synchronized to the mobile phone can be in HTML format. If this setting is set to `$false`, all e-mail is converted to plain text.
Allow Internet Sharing	This setting specifies whether the mobile phone can be used as a modem for a desktop or a portable computer. This policy setting requires an Exchange Enterprise Client Access License.
AllowIrDA	This setting specifies whether infrared connections are allowed to and from the mobile phone. This policy setting requires an Exchange Enterprise Client Access License.
Allow non-provisionable devices	This setting specifies whether older phones that may not support application of all policy settings are allowed to connect to Exchange 2010 by using Exchange ActiveSync.
Allow POPIMAPEmail	This setting specifies whether the user can configure a POP3 or an IMAP4 e-mail account on the mobile phone.
Allow Remote Desktop	This setting specifies whether the mobile phone can initiate a remote desktop connection. This policy setting requires an Exchange Enterprise Client Access License.
Allow simple password	This setting enables or disables the ability to use a simple password such as 1234. The default value is `$true`.
Allow S/MIME software certificates	This setting specifies whether S/MIME software certificates are allowed on the mobile phone.
Allow storage card	This setting specifies whether the mobile phone can access information that's stored on a storage card.
Allow text messaging	This setting specifies whether text messaging is allowed from the mobile phone. This policy setting requires an Exchange Enterprise Client Access License.
Allow unsigned applications	This setting specifies whether unsigned applications can be installed on the mobile phone. This policy setting requires an Exchange Enterprise Client Access License.
Allow unsigned installation packages	This setting specifies whether an unsigned installation package can be run on the mobile phone. This policy setting requires an Exchange Enterprise Client Access License.
Allow Wi-Fi	This setting specifies whether wireless

	Internet access is allowed on the mobile phone. This policy setting requires an Exchange Enterprise Client Access License.
Alphanumeric password required	This setting requires that a password contains numeric and non-numeric characters.
Approved Application List	This setting stores a list of approved applications that can be run on the mobile phone. This policy setting requires an Exchange Enterprise Client Access License.
Attachments enabled	This setting enables attachments to be downloaded to the mobile phone.
Device encryption enabled	This setting enables encryption on the mobile phone. Not all mobile phones can enforce encryption. For more information, see the phone and mobile operating system documentation.
Password enabled	This setting enables the mobile phone password.
Password expiration	This setting enables the administrator to configure a length of time after which a mobile phone password must be changed.
Password history	This setting specifies the number of past passwords that can be stored in a user's mailbox. A user can't reuse a stored password.
Policy refresh interval	This setting defines how frequently the mobile phone updates the Exchange ActiveSync policy from the server.
Maximum attachment size	This setting specifies the maximum size of attachments that are automatically downloaded to the mobile phone.
Maximum calendar age filter	This setting specifies the maximum range of calendar days that can be synchronized to the mobile phone. The value is specified in days.
Maximum failed password attempts	This setting specifies how many times an incorrect password can be entered before the mobile phone performs a wipe of all data.
Maximum inactivity time lock	This setting specifies the length of time that a mobile phone can go without user input before it locks.
Minimum password length	This setting specifies the minimum password length.
Maximum e-mail age filter	This setting specifies the maximum number of days' worth of e-mail items to synchronize to the mobile phone. The value is specified

	in days.
Maximum HTML e-mail body truncation size	This setting specifies the size beyond which HTML-formatted e-mail messages are truncated when they are synchronized to the mobile phone. The value is specified in kilobytes (KB).
Minimum device password complex characters	This setting specifies the minimum number of complex characters required in a mobile phone password. A complex character is any character that is not a letter.
Maximum e-mail body truncation size	This setting specifies the size beyond which e-mail messages are truncated when they are synchronized to the mobile phone. The value is specified in kilobytes (KB).
Password recovery	When this setting is enabled, the mobile phone generates a recovery password that's sent to the server. If the user forgets their mobile phone password, the recovery password can be used to unlock the mobile phone and enable the user to create a new mobile phone password.
Require Device Encryption	This setting specifies whether device encryption is required. If set to `$true`, the mobile phone must be able to support and implement encryption to synchronize with the server.
Require encrypted S/MIME messages	This setting specifies whether S/MIME messages must be encrypted.
Require manual synchronization while roaming	This setting specifies whether the mobile phone must synchronize manually while roaming. Allowing automatic synchronization while roaming will frequently lead to larger-than-expected data costs for the mobile phone plan.
Require storage card encryption	This setting specifies whether the storage card must be encrypted. Not all mobile phone operating systems support storage card encryption. For more information, see your mobile phone and mobile operating system for more information.
Unapproved InROM application list	This setting specifies a list of applications that cannot be run in ROM. This policy setting requires an Exchange Enterprise Client Access License.

Return to top

The following mailbox policies require an Exchange Enterprise Client Access License:

- Disable desktop ActiveSync
- Disable removable storage
- Disable camera
- Disable SMS text messaging

- Disable Wi-Fi
- Disable Bluetooth
- Disable IrDA
- Allow Internet sharing from device
- Allow desktop sharing from device
- Disable POP3/IMAP4 email
- Allow consumer email
- Allow web browser
- Allow unsigned applications
- Allow unsigned CABs
- Application allow list
- Application block list
- Unapproved InROM application list

For example, you can create a policy that you apply to all users in your Exchange organization. The following table lists possible settings for this policy.

Sample Exchange ActiveSync mailbox policy settings for all users

Setting	Value
Allow non-provisionable devices	False
Allow POPIMAPEmail	True
Allow Remote Desktop	True
Allow simple password	True
Allow S/MIME software certificates	True
Allow storage card	False
Allow text messaging	True
Allow unsigned applications	False
Allow unsigned installation packages	True
Allow Wi-Fi	False
Alphanumeric password required	True
Approved Application List	Null
Attachments enabled	True
Device encryption enabled	True
Maximum calendar age filter	15
Maximum attachment size	500 kilobytes (KB)
Maximum failed password attempts	4
Minimum password length	4
Maximum e-mail age filter	10
Maximum e-mail body truncation size	3 KB
Minimum device password complex characters	2
Maximum HTML e-mail body truncation size	7 KB

Password enabled	True
Password expiration	10 days
Password history	8 passwords stored
Require manual synchronization while roaming	True
UNC file access	Disabled
WSS file access	Disabled

Note:
You don't have to specify all policy settings when you create a new Exchange ActiveSync mailbox policy. Any policy setting you don't explicitly set will keep its default value.

Exchange ActiveSync mailbox policies can be created in the Exchange Management Console or the Exchange Management Shell. If you create a policy in the EMC, you can configure only a subset of the available settings. You can configure the rest of the settings using the Shell.

When you install Exchange 2010, a default Exchange ActiveSync mailbox policy is created. The default policy is automatically applied when a new user is created through the EMC or the Shell.

Return to top

You don't have to assign a user to an Exchange ActiveSync mailbox policy. The following table summarizes the policy settings used if you don't assign a user to a policy.

Default Exchange ActiveSync settings

Setting	Value
Allow Bluetooth	Allow
Allow Browser	True
Allow Camera	True
Allow Consumer Email	True
Allow Desktop Sync	True
Allow HTML E-mail	True
Allow Internet Sharing	True
AllowIrDA	True
Allow non-provisionable devices	True
Allow simple password	False
Allow POPIMAPEmail	True
Allow Remote Desktop	True
Alphanumeric password required	False
Allow S/MIME software certificates	True

Allow storage card	True
Allow text messaging	True
Allow unsigned applications	True
Allow unsigned installation packages	True
Allow Wi-Fi	True
Attachments enabled	True
Device encryption enabled	False
Maximum calendar age filter	7
Password enabled	False
Password expiration	Unlimited
Password history	0
Policy refresh interval	Unlimited
Document browsing enabled	True
Maximum attachment size	Unlimited
Maximum failed password attempts	4
Maximum inactivity time lock	15 minutes
Minimum password length	4
Maximum e-mail age filter	3
Maximum e-mail body truncation size	3 KB
Minimum device password complex characters	0
Maximum HTML e-mail body truncation size	3 KB
Require Device Encryption	False
Require encrypted S/MIME messages	False
Require manual synchronization while roaming	False
Require storage card encryption	False
Unapproved InROM application list	Null
Password recovery	Disabled
UNC file access	Enabled
WSS file access	Enabled

Windows Phone 7 Synchronization

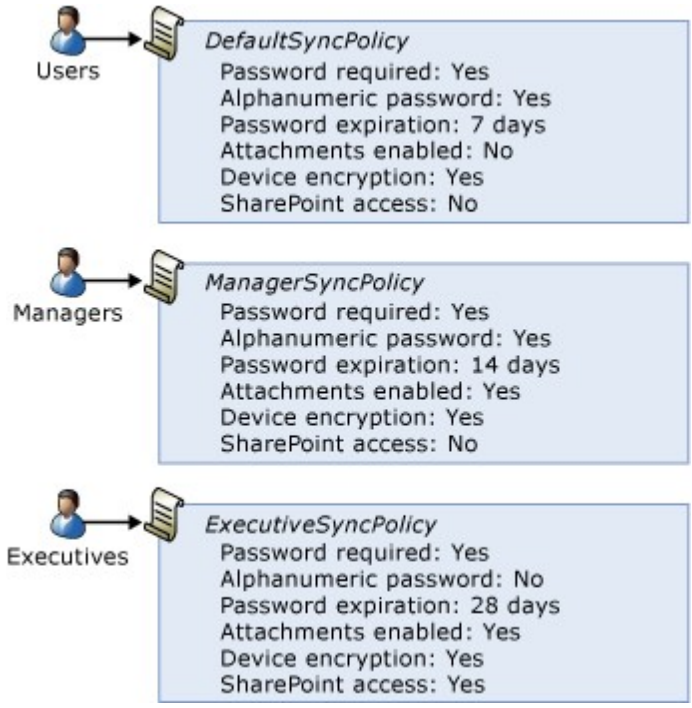
If you have Windows Phone 7 mobile phones in your organization, these phones will experience synchronization problems if certain Exchange ActiveSync mailbox policy

properties are configured. To allow Windows Phone 7 mobile phones to synchronize with an Exchange mailbox, either set the **AllowNonProvisionableDevices** property to true or only configure the following Exchange ActiveSync mailbox policy properties:

- PasswordRequired
- MinPasswordLength
- IdleTimeoutFrequencyValue
- DeviceWipeThreshold
- AllowSimplePassword
- PasswordExpiration
- PasswordHistory
- DisableRemovableStorage
- DisableIrDA
- DisableDesktopSync
- BlockRemoteDesktop
- BlockInternetSharing

Exchange ActiveSync Mailbox Policy Examples

The following figure shows how Exchange ActiveSync mailbox policies can be created to control different settings for three groups of users.



Return to top

Understanding Remote Device Wipe

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-24*

Mobile phones can store sensitive corporate data and provide access to many corporate resources. If a device is lost or stolen, that data can be compromised. Through Microsoft Exchange ActiveSync policies, you can add a password requirement to your mobile phones. This requires users to enter a password to access their mobile phones. We recommend that, in addition to requiring a device password, you configure your mobile phones to automatically prompt for a password after a period of inactivity. The combination of a device password and inactivity locking provides more security for your corporate data.

In addition to these features, Microsoft Exchange Server 2010 provides a remote device wipe feature. You can issue a remote device wipe command from the Exchange Management Shell. Users can issue their own remote device wipe commands from the Microsoft Office Outlook Web App user interface.

The remote device wipe feature also includes a confirmation function that writes a time stamp in the sync state data of the user's mailbox. This time stamp is displayed in Outlook Web App and in the user's mobile phone properties dialog box in the Exchange Management Console.

Important:

In addition to resetting the mobile phone to factory default condition, a remote device wipe also deletes any data on any storage card that's inserted in the mobile phone. If you're performing a remote device wipe on a mobile phone in your possession and want to keep the data on the storage card, remove the storage card before you initiate the remote device wipe.

Caution:

After a remote device wipe has occurred, data recovery is very difficult. However, no data removal process leaves a device as free from residual data as when it's new. Recovery of data from a device may still be possible using sophisticated tools.

Remote Device Wipe vs. Local Device Wipe

Local device wipe is the mechanism by which a mobile phone wipes itself without the request coming from the server. If your organization has implemented Exchange ActiveSync policies that specify a maximum number of password attempts and that maximum is exceeded, the mobile phone performs a local device wipe. The result of a local device wipe is the same as that of a remote device wipe. The device is returned to its factory default condition. When a mobile phone performs a local device wipe, no confirmation is sent to the Exchange server.

Understanding Exchange ActiveSync Autodiscover

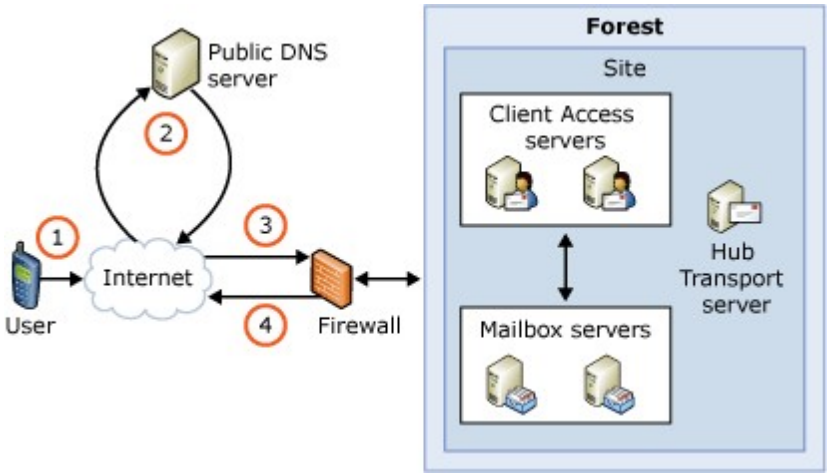
Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-09*

Microsoft Exchange Server 2010 includes the Autodiscover service, which simplifies the provisioning of your mobile phone by returning the required system settings after a user enters their e-mail address and password. The Autodiscover service is enabled by default in Exchange 2010. Looking for more information about managing the Autodiscover service? See Managing the Autodiscover Service.

Overview of Autodiscover with Exchange ActiveSync

If your mobile phone supports Autodiscover, you can configure your mobile phone to synchronize with Exchange 2010. The following figure shows this synchronization process.



1. The user enters their e-mail address and password on the mobile phone.
2. The mobile phone connects to a root DNS server to retrieve the URL for the Autodiscover service and the IP address for the user's domain.
3. The mobile phone uses a Secure Sockets Layer (SSL) connection to connect through the firewall to the Autodiscover service virtual directory. The Autodiscover service assembles the XML response based on the server synchronization settings.
4. The Autodiscover service sends the XML response through the firewall over SSL. This XML response is interpreted by the mobile phone, and synchronization settings are configured automatically on the mobile phone.

Note:

The ability to use Autodiscover depends on the operating system of the mobile phone you're using. Not all mobile phone operating systems that support synchronization with Exchange 2010 support Autodiscover. For more information about operating systems that support Autodiscover, contact the manufacturer of your mobile phone.

Note:

Windows Mobile 5.0 doesn't support Autodiscover.

1.6.1.4.5 Understanding Mobile Phone Connectivity

Understanding Mobile Phone Connectivity

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-03*

Many different mobile phones can synchronize with Microsoft Exchange Server 2010. These mobile phones can run operating systems such as Windows Mobile, Symbian, Palm, and Nokia. For an overview of the different mobile phones that are enabled for Microsoft Exchange ActiveSync, see Understanding Mobile Phones.

Regardless of the type of mobile phone you choose, you have two primary options to connect to Exchange 2010: by using cellular connectivity, and by using wireless connectivity. This topic provides an overview of these connectivity options.

Cellular Connectivity

All mobile phones that are enabled for Exchange ActiveSync can use cellular connectivity to synchronize with Exchange 2010. There are several types of cellular data networks. Regardless of the type of cellular data network that your mobile phone uses, the method of synchronization is the same. If you have a Windows Mobile phone, or another phone that supports Direct Push, synchronization is done through Direct Push. If your mobile phone has another operating system, manual synchronization is used. When a mobile phone uses Direct Push to synchronize with Exchange 2010, it establishes a long-standing HTTPS connection with the server running Exchange. When the connection is first established, the mobile phone sets what is called a heartbeat interval. The default heartbeat interval is 15 minutes. If any new messages are added to monitored folders on the Exchange server within this heartbeat interval, the server informs the mobile phone and the mobile phone initiates synchronization. When synchronization is complete, a new HTTPS request is initiated and the process is repeated. For more information about Direct Push, see Understanding Direct Push.

Cellular data plans can charge by the minute, by the megabyte, or offer unlimited data transfer. When you use a cellular data connection with Exchange 2010 Direct Push, we recommend purchasing an unlimited data plan.

Wireless Connectivity

Many mobile phones and other mobile devices that are enabled for Exchange ActiveSync can connect to a wireless LAN. A wireless LAN connection can provide faster network speeds and better coverage in areas where cellular coverage is unreliable. In addition, wireless access is sometimes offered at commercial locations such as coffee shops and book stores.

Understanding Mobile Phones

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-17*

Mobile phones that are enabled for Microsoft Exchange ActiveSync let users access most of their Microsoft Exchange mailbox data any time, anywhere. There are many different devices enabled for Exchange ActiveSync. These include Windows Mobile phones, Nokia mobile phones, and Palm mobile phones. This topic provides an overview of these mobile phones.

Although there are several non-phone devices that support Exchange ActiveSync, in most Exchange ActiveSync documentation, these devices are referred to as *mobile phones*. Unless the feature or features we're discussing require a cellular telephone signal, such as SMS message notification, the term mobile phone means both mobile phone and mobile device.

Exchange ActiveSync

Exchange ActiveSync is a communications protocol that enables mobile access, over the air, to e-mail messages, scheduling data, contacts, and tasks. Exchange ActiveSync is available on Windows Mobile phones and third-party phones that are enabled for Exchange ActiveSync.

Exchange ActiveSync offers Direct Push technology. Direct Push uses an encrypted HTTPS connection that's established and maintained between the phone and the server to push new e-mail messages and other Exchange data to the phone.

To use Direct Push with Microsoft Exchange Server 2010, your users must have a Windows Mobile phone or a phone with another mobile operating system that's designed to support Direct Push.

Exchange ActiveSync Features

Exchange ActiveSync provides access to many different features. These features enable you to enforce security policies on mobile phones. By using Exchange 2010, you can configure multiple Exchange ActiveSync policies and control which phones can synchronize with your Exchange server. Exchange ActiveSync enables you to send a remote device wipe command that wipes all data from a mobile phone in case that phone is lost or stolen. Users can also initiate a remote device wipe from Outlook Web App.

Exchange ActiveSync allows users to generate a recovery password. This recovery password is saved on the mobile phone and is used when a user forgets their password. The user generates the recovery password at the same time that they generate the device password or PIN. This recovery password can be used to unlock the phone. Immediately after this recovery password is used, the user will be required to create a new PIN.

Mobile Phones Enabled for Exchange ActiveSync

Users can take advantage of the features offered by Exchange ActiveSync by selecting mobile phones that are compatible with Exchange ActiveSync. These phones are available from many manufacturers. For more information, see the documentation for the phone

you're considering.

Mobile phones that are compatible with Microsoft Exchange include the following:

- **Apple** The Apple iPhone offers Exchange ActiveSync functionality. Users can configure an Exchange ActiveSync account on their Apple iPhone and synchronize e-mail, calendar, and contact data. When a user uses the Apple iPhone to synchronize e-mail messages, all e-mail messages in their inbox are synchronized to the iPhone. Users can't limit the synchronization to only 3 days of e-mail messages as they can with other phones. The iPhone is compatible with Exchange ActiveSync version 2.5 and doesn't support all the features included with Exchange ActiveSync for Exchange 2010. Specifically, the Apple iPhone supports only the following policies:
  - Remote wipe
  - Enforce password on device
  - Minimum password length
  - Require alphanumeric password
  - Require complex password
  - Inactivity time lockout
- **Nokia** Nokia offers Mail for Exchange on their Eseries mobile phones. E-mail, calendar, and contact data can be synchronized over a cellular network or a wireless LAN.
- **Sony Ericsson** Sony Ericsson offers Exchange ActiveSync support on several of their newer smartphones. They also support Direct Push through a third-party program.
- **Palm** Palm offers several Windows Mobile phones.
- **Motorola** Motorola has its own synchronization framework that enables over-the-air synchronization through Exchange ActiveSync on many its devices.
- **Symbian** Symbian Limited licenses Exchange ActiveSync for use in the Symbian operating system. This operating system is an open standard operating system for mobile telephones.

Windows Mobile Software Feature Matrix

Mobile phones that have a version of Windows Mobile software as their operating system offer the greatest functionality when synchronizing with Exchange 2010. The following table shows some features that are available with the different versions of Windows Mobile software.

Windows Mobile software feature matrix

Operating system	Productivity enhancements	Security enhancements	Administration enhancements
Windows Mobile 6 and later versions	• Direct Push • HTML e-mail support • Message flags • Quick message retrieval • Enhanced calendar views • Meeting attendee information • Ability to send auto-replies when you're away, on	• Enforcement of Exchange ActiveSync mailbox policies • Remote device wipe • Certificate-based authentication • S/MIME support • Device storage card encryption • Rights management	• Detailed device monitoring • Error reporting

	vacation, or out of the office • Exchange search • Windows SharePoint Services and Windows file share (UNC) document access	support	

For more information about how to manage Windows Mobile phones, visit the Windows Mobile Center Web site..

Windows Phone 7 synchronization

If you're configuring a Windows Phone 7 mobile phone to synchronize with an Exchange mailbox using Exchange ActiveSync, synchronization will fail under the following two simultaneous conditions:

- If the **AllowNonProvisionableDevices** property of the Exchange ActiveSync mailbox policy is set to False.
- If any policy properties that aren't included in the following list are configured for the Exchange ActiveSync mailbox policy:
  - PasswordRequired
  - MinPasswordLength
  - IdleTimeoutFrequencyValue
  - DeviceWipeThreshold
  - AllowSimplePassword
  - PasswordExpiration
  - PasswordHistory
  - DisableRemovableStorage
  - DisableIrDA
  - DisableDesktopSync
  - BlockRemoteDesktop
  - BlockInternetSharing

If you have Windows Phone 7 mobile phones in your organization, you can set **AllowNonProvisionalDevices** property to true or you can create a separate Exchange ActiveSync mailbox policy for users with Windows Phone 7 mobile phones. This new Exchange ActiveSync mailbox policy should either have the **AllowNonProvisionalDevices** property set to true or only have the preceding list of policy properties configured. For more information about Exchange ActiveSync Mailbox Policy properties and Windows Phone 7, see Understanding Exchange ActiveSync Mailbox Policies.

1.6.1.4.7 Understanding Exchange ActiveSync Reporting Services

Understanding Exchange ActiveSync Reporting Services

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-30*

Microsoft Exchange Server 2010 and Exchange ActiveSync offer many different features for both users and administrators. As an administrator, it's important that you know the

volume and usage patterns of your deployment. This information can help you effectively manage your Exchange ActiveSync deployment, better understand user productivity, and plan for future needs. Reporting in Exchange ActiveSync for Exchange 2010 is a Windows PowerShell task that compiles a set of Internet Information Services (IIS) logs and processes to create a series of output files. Each file is a separate report that can help you understand your Exchange ActiveSync deployment. This topic provides an overview of the cmdlet you can use to generate these reports, and information about the content of these reports.

Contents

Generating Exchange ActiveSync Reports

You can generate Exchange ActiveSync reports using the **Export-ActiveSyncLog** cmdlet. This cmdlet lets you specify many input parameters. These parameters include the location of the IIS log files, the start dates and the end dates for the reports, and the output path for the reports. To run this cmdlet, you must be delegated the permissions associated with the Exchange Server Administrator or Exchange Organization Administrator role. You must also have read access to the directory where the IIS logs are located. For more information about the syntax of the **Export-ActiveSyncLog** cmdlet, see Export-ActiveSyncLog.

Available Exchange ActiveSync Reports

The different Exchange ActiveSync reports available include the following:

- **Exchange ActiveSync Usage Report** This report includes several monitored parameters. These include the total bytes that were sent and received in addition to a count of each type of item sent and received. Item types are e-mail messages, calendar items, contact items, and task items.
- **Hits Report** This report lets you see the total number of synchronization requests processed per hour, in addition to the total number of unique devices that are initiating synchronization requests.
- **HTTP Status Report** This report provides a general overview of the performance of the Client Access server. It includes a summary of the different error response codes and the percentage of the time each code was encountered.
- **Policy Compliance Report** This report provides information about the number of fully compliant, partially compliant, and noncompliant devices. A fully compliant device is one that has accepted the Exchange ActiveSync policy and can implement all aspects of the policy. A partially compliant device is one that has accepted the policy, but has a mobile device operating system that's unable to enforce all aspects of the policy. A noncompliant device is either unable to accept the policy or has rejected the policy.
- **User Agent List** This report returns the total number of unique users, organized by mobile phone operating system.

Interpreting the Internet Information Services Log Files

The following table lists the different elements of the Exchange ActiveSync IIS logs. In the log file, each element is separated by an underscore character.

Elements of the Exchange ActiveSync protocol logs

<table>
<tr><th>Letter identifier</th><th>Element name</th><th>Definition</th><th>Possible values</th></tr>
<tr><td>V</td><td>Protocol version</td><td>The protocol version the device is using to synchronize with the Exchange server.</td><td><table><tr><th>Value</th><th>Meaning</th></tr><tr><td>120</td><td>Version 12</td></tr><tr><td>25</td><td>Version 2.5</td></tr><tr><td>21</td><td>Version 2.1</td></tr><tr><td>20</td><td>Version 2.0</td></tr><tr><td>10</td><td>Version 1.0</td></tr></table></td></tr>
<tr><td>Ty</td><td>Type</td><td>The type of folder that's being synchronized.</td><td><table><tr><th>Value</th><th>Meaning</th></tr><tr><td>Em</td><td>E-mail</td></tr><tr><td>Co</td><td>Contacts</td></tr><tr><td>Ca</td><td>Calendar</td></tr><tr><td>Ta</td><td>Tasks</td></tr></table></td></tr>
<tr><td>Fid</td><td>Folder ID</td><td>The ID of the folder that's being synchronized.</td><td>Positive Integer</td></tr>
<tr><td>Fc</td><td>Folder count</td><td>The number of folders that are being synchronized.</td><td>Positive Integer</td></tr>
<tr><td>Filt</td><td>Filter type</td><td>The data that the user requested.</td><td><table><tr><th>Value</th><th>Meaning</th><th>E-mail?</th><th>Calendar?</th><th>Tasks?</th></tr><tr><td>0</td><td>No filter</td><td>Yes</td><td>Yes</td><td>Yes</td></tr><tr><td>1</td><td>1 day back</td><td>Yes</td><td>No</td><td>No</td></tr><tr><td>2</td><td>3 days back</td><td>Yes</td><td>No</td><td>No</td></tr><tr><td>3</td><td>1 week back</td><td>Yes</td><td>No</td><td>No</td></tr><tr><td>4</td><td>2 weeks back</td><td>Yes</td><td>Yes</td><td>No</td></tr><tr><td>5</td><td>1 month</td><td>Yes</td><td>Yes</td><td>No</td></tr></table></td></tr>
</table>

			<table><tr><td></td><td>back</td><td></td><td></td><td></td></tr><tr><td>6</td><td>3 months back</td><td>No</td><td>Yes</td><td>No</td></tr><tr><td>7</td><td>6 months back</td><td>No</td><td>Yes</td><td>No</td></tr><tr><td>8</td><td>Incomplete</td><td>No</td><td>No</td><td>Yes</td></tr></table>
St	Sync type	The type of synchronization that's being performed.	<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>F</td><td>First sync</td></tr><tr><td>S</td><td>Subsequent sync</td></tr><tr><td>R</td><td>Recovery sync</td></tr><tr><td>I</td><td>Invalid sync</td></tr></table>
Sk	Sync key	The actual sync key that's used between the mobile phone and the Exchange server.	Positive integer
Cli:	Client statistics	Stores the count of each type of activity from the Client. Output is in the form `Cli:0A0C3D1F0E`.	<table><tr><th>Identifier value</th><th>Meaning</th></tr><tr><td>A</td><td>Adds</td></tr><tr><td>C</td><td>Changes</td></tr><tr><td>D</td><td>Deletes</td></tr><tr><td>F</td><td>Fetches</td></tr><tr><td>E</td><td>Errors</td></tr></table>
Srv:	Server statistics	Stores the count of each type of activity from the server. Output is in the form `Srv:2A0C2D1F1E`.	<table><tr><th>Identifier value</th><th>Meaning</th></tr><tr><td>A</td><td>Adds</td></tr><tr><td>C</td><td>Changes</td></tr><tr><td>D</td><td>Deletes</td></tr><tr><td>F</td><td>Fetches</td></tr><tr><td>E</td><td>Errors</td></tr></table>
E	Number of errors	The number of errors encountered	Positive integer

		in a request.	
Io	Items opened	The number of items that were opened. This feature hasn't yet been implemented.	Positive integer
Hb	Heartbeat interval	The Heartbeat interval that's used for the PING command.	Positive integer
Ssp	SharePoint documents	The number of files that were accessed from Windows SharePoint Services.	Positive integer
Sspb	SharePoint bytes	The number of bytes that were accessed from Windows SharePoint Services.	Positive integer
Unc	UNC files	The number of files that were accessed through Windows file shares.	Positive integer
Uncb	UNC bytes	The number of bytes that were accessed through Windows file shares.	Positive integer
Att	Attachments	The number of attachments that were retrieved.	Positive integer
Attb	Attachment bytes	The number of bytes that were retrieved for attachments.	Positive integer
Pk	Policy key received	The element that's used by the client and server to correlate acknowledgements to a particular policy setting.	Not applicable
Pa	Policy acknowledge status	The element that indicates success if all the policy settings were applied correctly.	**Value** / **Meaning** 1 / Policy was successfully applied 2 / Policy was partially applied 3 / Policy was not applied

Oof	OOf action	The action that is performed on the Out of Office status stored on the Exchange server.	**Value** / **Meaning** Get / Retrieves the OOF status and message Set / Sets the OOF status and message
UserInfo	User information action	The parameter that specifies retrieval of the user information data.	Get
DevModel	Device model	The device information that is supplied by the device manufacturer.	Possible values include manufacturer name, model name, and model number.
DevIMEI	IMEI	The International Mobile Equipment Identity (IMEI). It is a 15-digit code that's assigned to each device.	String
DevName	Device friendly name	This element stores the user's description of their device.	String
DevOS	Device OS	The operating system that is running on the device.	String
DevLang	Device OS language	The localized language of the device operating system.	String
Error	Error	The error section of the request.	String
S	Status	This element returns the status of the device.	String
R	Not Relevant	This element returns a count of items that have changed but aren't relevant to the mobile phone or device.	Positive integer

The following is a sample log for mobile device synchronization:

&Log=V123_Ty:Em_Fid:37_Fc1_Filt2_St:S_SK:1805_Srv:1a0c0d0s0e0r_Pk2260121383_S1

1.6.1.4.8 Understanding Mobile Device Management

Understanding Mobile Device Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-03*

Microsoft Exchange Server 2010 Service Pack 1 (SP1) and Microsoft Exchange ActiveSync offer many different features for both users and administrators. As an administrator, you can create allow lists, block lists, and quarantine lists specifying which mobile devices are allowed to access your Exchange mailboxes. A quarantine list lets you allow only a user's assigned device to connect to the Exchange server.

Note:

Throughout this topic, the term mobile device refers to mobile devices with and without cellular telephone service. All mobile phones and devices are assumed to have some form of Internet connectivity, either with a cellular data plan or with wireless Internet access.

Contents

Determining a Mobile Device's Access State

Exchange 2010 SP1 servers follow a simple, logical sequence to determine the access state of each mobile device. Every device can be either allowed, blocked, or quarantined. You can define the access state of each device through an organizational rule or through an *exemption*. An exemption is a rule that's applied to a single user or single device. This occurs each time an Exchange ActiveSync request is received from a mobile device that's trying to synchronize data from a mailbox stored on an Exchange 2010 server. The sequence of challenges includes the following steps:

1. **Is the mobile device authenticated?** If not, challenge the mobile device for the correct credentials. Otherwise, go on to the next step.
2. **Is Exchange ActiveSync enabled for the current user?** If not, return an "access restricted" error to the device. Otherwise, go on to the next step.
3. **Are the mobile policy enforcement criteria met by the current mobile device?** If not, block access. Otherwise, go on to the next step.
4. **Is this mobile device blocked by a personal exemption for the user?** If so, block access. Otherwise, go on to the next step.
5. **Is this mobile device allowed by a personal exemption for the user?** If so, grant full access. Otherwise, go on to the next step.
6. **Is this mobile device blocked by a device access rule?** If so, block access. Otherwise, go on to the next step.

7. **Is this mobile device quarantined by a device access rule?** If so, quarantine the device. Otherwise, go on to the next step.
8. **Is this mobile device allowed by a device access rule?** If so, grant full access. Otherwise, go on to the next step.
9. **Apply the default access state per the Exchange ActiveSync organizational settings.** This grants access, blocks access, or quarantines the current device, depending on the organizational settings.

Return to top

Understanding Device Access States

A *device access state* is the status of a particular device. The access state of a device can be one of the following: allowed, blocked, or quarantined. You can control device access states in several ways. A mobile device will behave differently in each access state.

The Allow Access State

In the allow access state, a mobile device can synchronize through Exchange ActiveSync and connect to the Exchange server to retrieve e-mail and manipulate calendar information, contacts, tasks, and notes. This will continue as long as the device complies with the Exchange ActiveSync mailbox policies that you've configured.

For more information, see View or Configure Exchange ActiveSync Mailbox Policy Properties.

The Block Access State

A mobile device that's blocked because of a device access setting you configured won't be allowed to connect to the Exchange server and will receive HTTP 403 Forbidden errors. The user will receive an e-mail message from the Exchange server telling them that the mobile device was blocked from accessing their mailbox. You can add customized text to this message to provide instructions for users whose devices are blocked.

A mobile device may also be blocked because it fails to apply the Exchange ActiveSync mailbox policies. If this is the case, the user won't receive an e-mail message that tells them that the mobile device was blocked from accessing their mailbox. However, the mobile device information displayed in Outlook Web App will show that it's blocked due to the failure by the device to apply the Exchange ActiveSync mailbox policies.

The Quarantine Access State

When a mobile device is quarantined, the mobile device is allowed to connect to the Exchange server. However, it is given only limited access to data. The user can add content to their own Calendar, Contacts, Tasks, and Notes folders but the server won't allow the device to retrieve any content from the user's mailbox. The user will receive a single e-mail message that tells them that the mobile device is quarantined. This message will be received by the device and will also be available in the user's mailbox. You can add customized text to this message to provide instructions for users whose devices are quarantined.

When you configure the Exchange ActiveSync organizational settings, you can specify one or more administrators who will receive an e-mail message the first time a quarantined device tries to connect to the Exchange server. The administrators can then decide whether to release the mobile device from quarantine by creating a personal exemption, block the device completely, or create a rule that will take action on the mobile device and other similar mobile devices.

Note A default *Upgrade Grace Period* allows quarantined devices to continue to sync with mailboxes that have been moved from previous versions of Exchange to Exchange Server 2010. The default Upgrade Grace Period is seven (7) days, beginning when the device synchronization state is upgraded. The device access state is upgraded only when a

device contacts the Exchange server. Therefore, if the device does not contact a server, its access state is not upgraded.

Also, if a synchronization state is not detected for the device before the upgrade when it is running on the previous version of Exchange, the device does not receive an Upgrade Grace Period.

The Device Discovery Access State

When a mobile device first connects to Exchange ActiveSync, the device is momentarily in the device-discovery access state. In this state, the device is quarantined until it's recognized by the server. This state can last from 1 to 14 minutes. No email message is sent to administrators or to the user when a mobile device is in this state.

The Mailbox Upgrade Access State

When a mobile device is in the mailbox upgrade access state, it's granted full access to the user's mailbox. The mailbox upgrade access state is the same as the allowed state, except that it lasts no more than seven days from the first time the device connects to an Exchange 2010 server after a mailbox move from an earlier version of Microsoft Exchange. This state is necessary to give mobile devices time to correctly upgrade their information and communication protocols to the latest Exchange ActiveSync version and be recognized by the device access management system. As soon as a mobile device is recognized, Exchange applies the appropriate access based on the Exchange 2010 configuration.

Return to top

Controlling Device Access

You can control device access by configuring the following:

- Personal exemptions for users.
- Organization-wide rules for mobile device families or specific models.
- A default access state for all devices that don't belong in another category.

Creating Personal Exemptions

You can assign a particular mobile device to a particular user. This assignment allows you to explicitly grant access for a particular device or explicitly block a particular device regardless of the rules and other device access settings. If a mobile device is not explicitly granted or blocked for the particular user, then the device's access will be determined according to the numbered steps discussed previously.

Note:

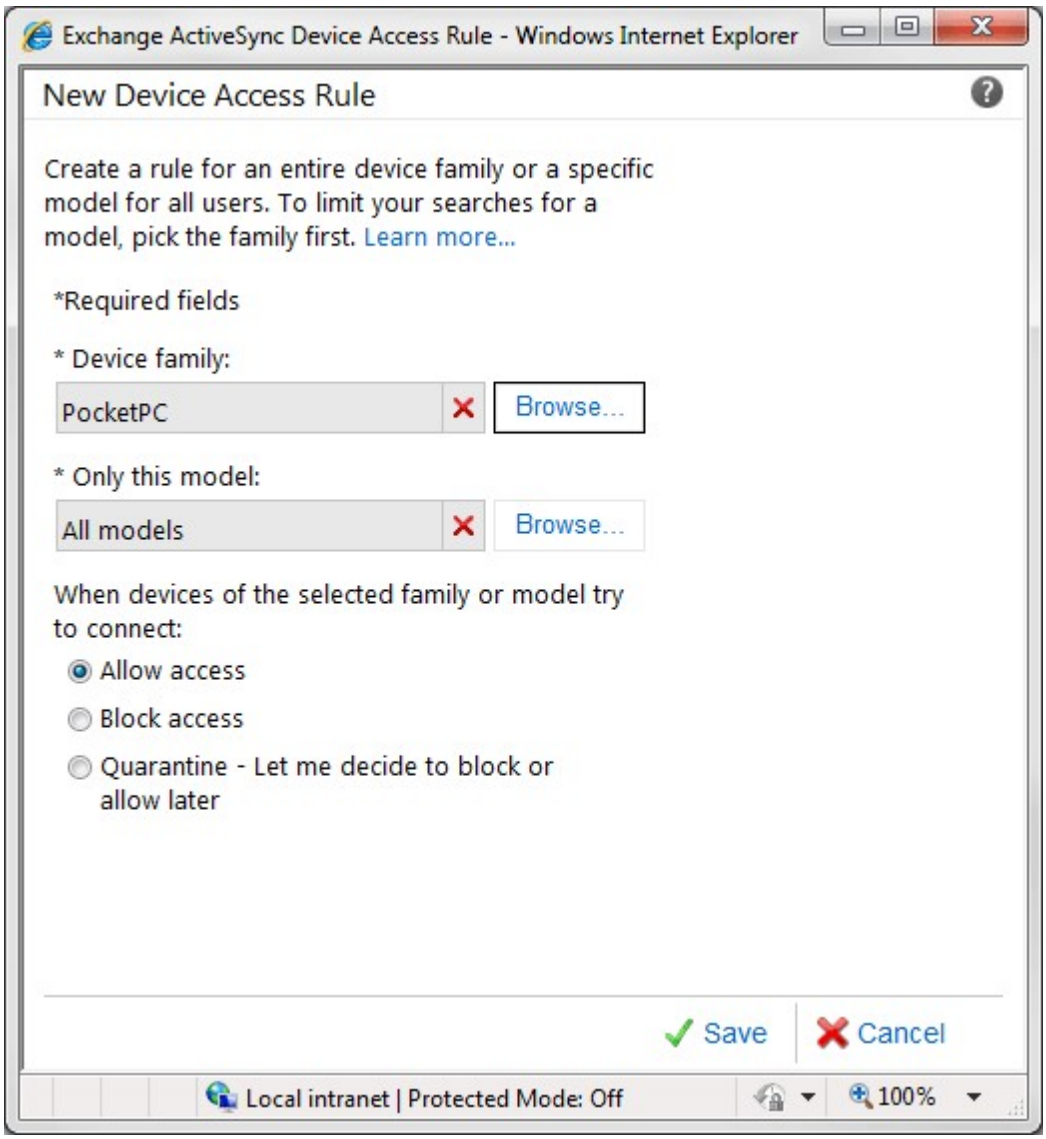
Unlike Microsoft Exchange Server 2007, explicitly granting access for a specific device for a user doesn't implicitly deny access for other devices. If a user tries to connect a different device, that device's access state will be determined by the organization's device access settings.

Personal exemptions can be created by using the **Set-CASMailbox** cmdlet or the Exchange Control Panel (ECP).

Creating Organization Access Rules

Organizational access rules let you set the type of access available to a particular group of devices based on some properties of the device, such as model. To create these rules, you need to know the device model and family information. This information can be obtained after a mobile device has successfully synchronized with the Exchange server.

Organizational access rules can be created by using the **Set-CASMailbox** cmdlet or through the ECP, as shown in the following figure.



When you set up a rule for a device, it's important to understand the difference between the device "family" and the specific device. This information is communicated as part of the EAS protocol, and it's reported by the device itself. For example, a device rule applies only to a specific device type. A device family represents a range of similar devices, such as a Pocket PC. This distinction is important because many device manufacturers release the same device by using different names on different carriers. When you create a rule, you select the device family or the specific model, but not both.

On the **New Device Access Rule** page, click **Browse**, to display a list of all the devices or device families that have recently connected to your Exchange server. Then, select the action to take. You can select any of the following actions:

Allow access

Block access

Quarantine

Quarantine notifications

Quarantine notifications let you specify who receives an email alert when a device is placed in quarantine. You can add one or more administrators, users, or distribution groups to the list. Anyone who is on this list receives an email notification that provides information about the device, the person who tried to connect the device, and the time that the attempt was made.

Setting the Default Organizational Access State

The default organizational access state for Exchange ActiveSync determines the access level that's granted to mobile devices that aren't managed by organizational rules or personal exemptions. The default organizational access state can be set by using the **Set-CASMailbox** cmdlet or the ECP.

Return to top

Configuring Common Access Management Strategies

Before you specify the level of access for mobile devices, you might want to get a list of all mobile phones and devices within your organization. You can get this list by using the **Get-CASMailbox** cmdlet with the **Get-ActiveSyncDeviceStatistics** cmdlet. For more information, see Get-ActiveSyncDeviceStatistics.

Creating an Allow List

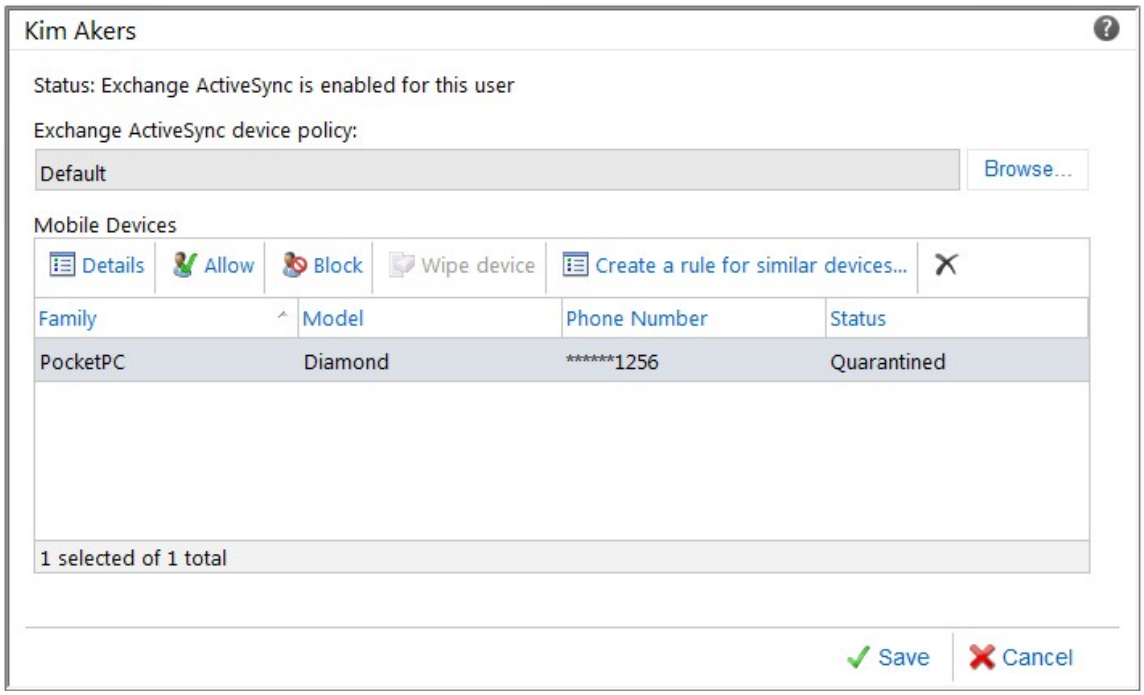
You can use an allow list to grant access to a list of known devices and restrict access for everything else. To do this, you must create rules so that the specific devices you want are allowed to access users' mailboxes. As soon as you create such a rule, you must set the organization’s default access state to block all other devices. To add a new device to the allow list, create a new rule.

Creating a Block List

You can use a block list to grant access to all devices by default, but to block access for a set of devices that you don't want to access your organization. You create a block list by creating block rules for the devices that you don't want to synchronize with the organization’s mailboxes. The organizational settings should be set to allow everything by granting access to all devices that aren't explicitly blocked by the existing rules. To add a new device or set of devices to the block list, create a new rule.

Mixed Allow and Block List Environments

In addition to creating allow and block lists, you can quarantine new mobile devices as they're introduced into the organization while you evaluate them. For example, if you have a block list for mobile devices that aren't allowed within your organization, and an allow list for mobile devices that are allowed within the organization, you can set the default organizational access setting to quarantine. All other devices will automatically be quarantined, which lets you discover new devices as they're introduced to the organization and decide whether to add them to the allow list or the block list. The following figure shows a mobile device that's been quarantined for a specific user.



Live Auditing

You can use live auditing to discover all the devices that are currently synchronizing with the Exchange server in your organization. You set up live auditing by setting the default organizational access setting to quarantine.

A list of quarantined devices will be generated within a few minutes of time the default organizational access setting is switched to quarantine. You can use that list to create your allow and block lists. All users will be prevented from synchronizing with the Exchange server until the allow and block lists have been created.

Return to top

1.6.1.5 Understanding POP3 and IMAP4

Understanding POP3 and IMAP4

Exchange Server 2010 > Client Access > Understanding Client Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-06*

By default, POP3 and IMAP4 are disabled in Microsoft Exchange Server 2010. To support clients that still rely on these protocols, you must first start the POP3 and IMAP4 services on the Exchange 2010 Client Access server. You must also configure SMTP for your POP3 and IMAP4 clients to send e-mail.

For detailed steps for enabling the POP3 and IMAP4 services, see Enable POP3 in Exchange 2010 and Enable IMAP4 in Exchange 2010.

By default, users who have mailboxes on computers that are running Exchange 2010 can access their mailboxes by using Microsoft Outlook or Outlook Web App, Microsoft Exchange ActiveSync, or Outlook Voice Access. Outlook, Outlook Web App, and Outlook

Voice Access enable your e-mail users to use the comprehensive set of features that are available to clients that have mailboxes on Exchange 2010 servers.

Contents

Overview of POP3 and IMAP4 Functionality

This section describes the POP3 and IMAP4 functionality for Exchange 2010.

These two protocols have the following benefits and limitations:

- **POP3** POP3 was designed to support offline mail processing. With POP3, e-mail messages are removed from the server and stored on the local POP3 client, unless the client has been set to leave mail on the server. This puts the data management and security responsibility in the hands of the user. POP3 doesn't offer advanced collaboration features such as calendaring, contacts, and tasks.
- **IMAP4** IMAP4 offers offline and online access, but like POP3, IMAP4 doesn't offer advanced collaboration features such as calendaring, contacts, and tasks.

POP3 and IMAP4 can't be used to send messages from a client application to the e-mail server. E-mail applications that use POP3 and IMAP4 to send messages rely on the SMTP protocol to send messages. The connector for receiving e-mail submissions from client applications that use POP3 or IMAP4 is created automatically on every Hub Transport server. For more information about connectors, see Understanding Receive Connectors.

POP3 and IMAP4 Cross-Site Connectivity

In earlier versions of Exchange, you had to perform a manual configuration step to allow your POP3 and IMAP4 clients to connect to their mail from one site in your organization when their mailbox was located in a different site in your organization. By default, Exchange 2010 automatically proxies from a Client Access server in one site to the correct server.

Managing POP3 and IMAP4 with Exchange 2003

When you deploy Client Access servers to support clients that use POP3 and IMAP4, and their mailboxes are located on Exchange Server 2003 back-end servers, you must use Basic authentication. Also, you won't be able to use Secure Sockets Layer (SSL) encryption. Instead, you must use Internet Protocol security (IPsec) to help secure the communication between these servers.

Using Non-Standard Accounts with POP3 and IMAP4

You can't use an Anonymous account or Guest account to sign in to an Exchange 2010 mailbox through POP3 or IMAP4. This kind of access is blocked because of security vulnerabilities when you use non-standard accounts for POP3 and IMAP4 access. Additionally, you can't connect to the Administrator mailbox through POP3 or IMAP4. This limitation was included intentionally in Exchange 2010 to enhance security for the Administrator mailbox. To access the Administrator mailbox, you must use Microsoft Office Outlook or Outlook Web App.

Understanding Differences Between POP3 and IMAP4

POP3 is a frequently used e-mail Internet protocol. By default, when POP3 e-mail applications download e-mail messages to a client computer, the downloaded messages are removed from the server. When a copy of your user's e-mail isn't kept on the e-mail server, the user can't access the same e-mail messages from multiple computers. However, some POP3 e-mail applications can be configured to keep copies of the messages on the server so that the same e-mail messages can be accessed from another computer. POP3 client applications can only be used to download messages from the e-mail server to a single folder (usually the Inbox) on the client computer. The POP3 protocol can't synchronize multiple folders on the e-mail server with multiple folders on the client computer. POP3 also doesn't support public folder access.

E-mail client applications that use IMAP4 are more flexible and generally offer more features than e-mail client applications that use POP3. By default, when IMAP4 e-mail applications download e-mail messages to a client computer, a copy of downloaded messages remains on the e-mail server. Because a copy of the user’s e-mail message is kept on the e-mail server, the user can access the same e-mail message from multiple computers. With IMAP4 e-mail, the user can access and create multiple e-mail folders on the e-mail server. Users can then access any of their messages on the server from computers in multiple locations. For example, most IMAP4 applications can be configured to keep a copy of a user's sent items on the server so that they can view their sent items from any other computer. IMAP4 supports additional features that are supported by most IMAP4 applications. For example, some IMAP4 applications include a feature that lets the user view only the headers of their e-mail messages on the server—who the message is from and the subject—and then download only the messages that they want to read. IMAP4 doesn’t support public folder access.

Note:

IMAP4 and POP3 clients have limited access to calendar information for Exchange. For more information, see Configure Calendar Options for IMAP4 and Configure Calendar Options for POP3.

Send Receive Options for POP3 and IMAP4 E-Mail Applications

POP3 and IMAP4 e-mail applications let users choose when they want to connect to the

server to send and receive e-mail. This section discusses some of the most common connectivity options and also provides some factors your users should consider when they select connection options available in their POP3 and IMAP4 e-mail applications.

Common Configuration Settings

Three of the most common connection settings that can be set on the POP3 or IMAP4 client application are:

- To send and receive messages every time the e-mail application is started. When this option is used, mail is only sent and received upon starting the e-mail application.
- To send and receive messages manually. When this option is used, messages are only sent and received when the user clicks a "send and receive" option in the client user interface.
- To send and receive messages every set number of minutes. When this option is used, the client application connects to the server every set number of minutes to send messages and download any new messages.

For information about how to configure these settings for the e-mail application that you use, see the Help documentation that's provided with the respective e-mail application.

Considerations When Selecting Send Receive Options

If the device or computer that's running the POP3 or IMAP4 e-mail application is always connected to the Internet, users may want to configure their e-mail application to send and receive messages every set number of minutes. Connecting to the server at frequent intervals lets the user keep their e-mail application up-to-date with the most current information on the server. However, if the device or computer that's running the POP3 or IMAP4 e-mail application isn't always connected to the Internet (for example, if the user connects to the Internet by using a dial-up connection), the user may want to configure the e-mail application to send and receive messages manually. In a dial-up connectivity scenario, sending and receiving messages manually can potentially reduce the time that a user is connected to the Internet.

Note:

If the user is using an IMAP4-compliant e-mail application that supports the IMAP4 IDLE command, the user may be able to send e-mail to and receive e-mail from their Exchange mailbox in near real time. For this connection method to work, both the e-mail server application and the client application must support the IMAP4 IDLE command. In most cases, users don't have to configure any settings in their IMAP4 application to use this connection method.

POP3 and IMAP4 Applications

Because Exchange 2010 supports POP3 and IMAP4, users can use any applications that support POP3 and IMAP4 client applications to connect to Exchange 2010. These applications include Outlook, Windows Mail, Microsoft Outlook Express, Entourage, and many third-party applications such as Mozilla Thunderbird and Eudora. The features supported by each e-mail client applications vary. For information about the specific features offered by specific POP3 and IMAP4 client applications, see the documentation that's included with each application.

User Settings to Configure POP3 or IMAP4 Access to Their Exchange 2010 Mailboxes

After you enable POP3 and IMAP4 client access on your Client Access servers, you have to give users the information they need to connect their e-mail programs to their Exchange 2010 mailbox. They'll need the following information:

To connect from inside the corporate network, users will need the following information:

- Internal POP3 or IMAP4 server name
- Internal POP3 or IMAP4 port number
- Internal POP3 or IMAP4 encryption method
- Internal SMTP (outgoing server) name
- Internal SMTP (outgoing server) port number
- Internal SMTP (outgoing server) encryption method

To connect from the Internet, they'll need the following information:

- External POP3 or IMAP4 server name
- External POP3 or IMAP4 port number
- External POP3 or IMAP4 encryption method
- External SMTP (outgoing server) name
- External SMTP (outgoing server) port number
- External SMTP (outgoing server) encryption method

You can make these settings available to your users through e-mail or other manual communication methods. You can also configure Exchange so that your users can use Outlook Web App to look up their own settings.

Configuring Exchange So Users Can Look Up Their Internal POP3, IMAP4, and SMTP Server Settings

By default, your users can look up their internal POP3 and IMAP4 server settings through Outlook Web App. However, to allow your users to access internal SMTP (outgoing) server settings, you must run the **Set-ReceiveConnector** cmdlet with the *AdvertiseClientSettings* parameter. After you run this command, your users can access their internal POP, IMAP, and SMTP server settings through Outlook Web App by clicking the drop-down arrow next to the Help question mark, and then clicking **About**.

For detailed information about how to configure this setting, see Allow POP3, IMAP4, and SMTP Server Settings to be Viewed By End Users in Outlook Web App.

Configuring Exchange So Users Can Look Up Their External POP3, IMAP4, and SMTP Server Settings

By default, external POP3, IMAP4, and SMTP server settings aren't available to your users through Outlook Web App. You can change the default setting as follows:

- To allow your users to look up their own external POP3 settings, you must run the **Set-POPSettings** cmdlet with the *ExternalConnectionSettings* parameter.
- To allow your users to look up their own external IMAP4 settings, you must run the **Set-IMAPSettings** cmdlet with the *ExternalConnectionSettings* parameter.
- To allow your users to access external SMTP server settings, you must run the **Set-ReceiveConnector** cmdlet with the *AdvertiseClientSettings* parameter.

After you change your default settings by running the **Set-POPSettings**, **Set-IMAPSettings**, and **Set-ReceiveConnector** cmdlets, your users can look up their external POP, IMAP, and SMTP server settings in Outlook Web App as follows:

- If you're running Exchange Server 2010 SP1, your users can look up their settings in Outlook Web App by clicking **Options** > **All Options** > **Account** > **My Account** > **Settings for POP, IMAP, and SMTP access**.
- If you're running the RTM version of Exchange 2010, your users can look up their settings in Outlook Web App by clicking the drop-down arrow next to the Help question mark, and then clicking **About**.

For detailed information about how to configure this setting, see Allow POP3, IMAP4, and SMTP Server Settings to be Viewed By End Users in Outlook Web App.

Leaving a Copy of Messages on the Server

The default setting on some e-mail programs isn't to keep a copy of messages on the server after they're retrieved. Be sure to recommend that your users set up their e-mail program to keep a copy of all messages the client retrieves on the server. By keeping a copy of messages on the server, your users can access their messages from a different e-mail program.

1.6.1.5.1 Understanding POP3 and IMAP4 Settings

Understanding POP3 and IMAP4 Settings

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

If you administer POP3 and IMAP4, you'll perform all your administrative tasks in the Exchange Management Shell or the Exchange Management Console.

Managing POP3 and IMAP4 Using the Shell

You can use the Shell to manage the POP3 and IMAP4 services on a per-server basis or on a per-user basis in Microsoft Exchange Server 2010.

Managing POP3 and IMAP4 on Per-Server Basis

You can view and configure POP3 and IMAP4 settings on the Exchange 2010 Client Access server by using the cmdlets included in the following table.

Cmdlets for managing POP3 and IMAP4

Cmdlet name	Description
Set-PopSettings	This cmdlet can be used to configure all available settings for POP3 on a Client Access server.
Set-ImapSettings	This cmdlet can be used to configure all available settings for IMAP4 on a Client Access server.

For more information about how to use the **Set-PopSettings** and **Set-ImapSettings** cmdlets to manage POP3 and IMAP4 settings for a user, see Set-PopSettings and Set-ImapSettings.

Managing POP3 and IMAP4 Settings on a Per-User Basis

You can use the **Set-CASMailbox** cmdlet in the Shell to manage POP3 and IMAP4 settings for individual users by modifying properties on their mailboxes. The following table describes the parameters that you can use with the **Set-CASMailbox** cmdlet.

Parameters to use with the Set-CASMailbox cmdlet to manage POP3 and IMAP4

Parameter name	Description
`ImapEnabled`	This parameter specifies whether the IMAP4 protocol is enabled for this mailbox.

ImapMessagesRetrievalMimeFormat	This parameter specifies the format of messages retrieved from the server.
ImapUseProtocolDefaults	This parameter specifies whether to use the default protocol settings specified on the Client Access server for the IMAP4 protocol.
PopEnabled	This parameter specifies whether the POP3 protocol is enabled for a mailbox.
PopMessagesRetrievalMimeFormat	This parameter specifies the format of messages retrieved from the server.
PopUseProtocolDefaults	This parameter specifies whether to use the default protocol settings specified on the Client Access server for the POP3 protocol.

For more information about how to use the **Set-CASMailbox** cmdlet to manage POP3 and IMAP4 settings for a user, see Set-CASMailbox.

Managing POP3 and IMAP4 Using the EMC

1. In the console tree, navigate to **Server Configuration**> **Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab
3. Select either POP3 or IMAP4 and then, in the action pane, under **IMAP4** or **POP**, click **Properties**.
4. Click any of the available tabs to view and configure POP3 or IMAP4 settings.

1.6.1.5.2 Understanding Protocol Logging for POP3 and IMAP4

Understanding Protocol Logging for POP3 and IMAP4

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can use protocol logging to review the POP3 and IMAP4 connections in your Exchange environment. This can be useful if you're troubleshooting issues related to POP3 or IMAP4 performance.

Enabling POP3 and IMAP4 Protocol Logging

You can enable or disable protocol logging using the Exchange Management Shell. If you enable protocol logging using the Shell, the default protocol logging settings will be used. These default settings are generally recommended.

Alternatively, you can enable, disable, and modify protocol logging options by editing the Microsoft.Exchange.Pop3.exe.config and Microsoft.Exchange.Imap4.exe.config configuration files located on your Microsoft Exchange Server 2010 Client Access server.

For more information about how to manage POP3 and IMAP4 protocol settings, see Configure Protocol Logging for POP3 and IMAP4.

Reviewing the Protocol Log

The information included on each line of the POP3 and IMAP4 protocol logs is organized by fields that are separated by commas. The following table explains the fields that are used to classify each protocol event.

Fields used to classify each protocol event

Field name	Description
date-time	The date and time of the protocol event. The value is formatted as *yyyy-mm-ddhh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu. Zulu is another way to indicate Coordinated Universal Time (UTC).
connector-id	This field is not used for POP3 and IMAP4 protocol logging.
session-id	A GUID that is unique for each SMTP session but is the same for each event that is associated with that SMTP session.
sequence-number	A counter that starts at 0 and is incremented for each event in the same session.
local-endpoint	The local endpoint of a POP3 or IMAP4 session. This consists of an IP address and TCP port number that is formatted as *<IP address>:<port>*.
remote-endpoint	The remote endpoint of a POP3 or IMAP4 session. This consists of an IP address and TCP port number that is formatted as *<IP address>:<port>*.
event	A single character that represents the protocol event. The possible values for the event are as follows: • + Connect • - Disconnect • > Send • < Receive • * Information
data	Text information that is associated with the POP3 or IMAP4 event.
context	This field is not used for POP3 and IMAP4 protocol logging.

1.6.1.6 Understanding Outlook Web App

Understanding Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-06-13*

By default, when you install the Client Access server role on a computer that's running Microsoft Exchange Server 2010, you enable Outlook Web App. Microsoft Office Outlook Web App lets you access your Exchange mailbox from almost any Web browser.

Note:
Outlook Web App was called Outlook Web Access in previous versions of Microsoft Exchange.

Looking for management tasks related to Outlook Web App? See Managing Outlook Web App.

Contents

New Features in Outlook Web App

Outlook Web App has been redesigned for Exchange 2010 to create a new look, add new features, and improve usability.

New features in Outlook Web App include:

- **Outlook Web App mailbox policies** In previous versions of Outlook Web App, you controlled users' access to features by configuring the Outlook Web App virtual directories or by configuring individual mailboxes. In Exchange 2010, you can use Outlook Web App mailbox policies to control users' access to features in Outlook Web App. For more information, see Understanding Outlook Web App Mailbox Policies.
- **More Web browsers supported** In Exchange 2010, users have access to the standard version of Outlook Web App through Safari and Firefox, in addition to Internet Explorer. For more information, see Outlook Web App Supported Browsers.
- **Conversation view** Conversation view lets users see all messages in a thread, including messages not in the current folder.
- **Chat** Outlook Web App can be configured to work with Microsoft Office Communications Server 2007 or with Microsoft Lync Server 2010 to allow users to chat without having to install Office Communicator 2007 or Lync 2010. For more information, see Understanding Outlook Web App and Instant Messaging Integration.
- **Filters** Users have access to a set of predefined filters to quickly search the contents of folders.
- **Right-click** More actions have been added to the right-click menus in Outlook Web App.
- **Attach messages to messages** Users can attach a message from their

mailbox to a new message. In previous versions of Outlook Web App, users could attach files to messages, but couldn't attach a message to a message.

For more information about new features for users in Outlook Web App, see What's New in Outlook Web App.

Managing Outlook Web App

When you install the Client Access server role, a default virtual directory named owa is created. For more information about Outlook Web App virtual directories, see Managing Outlook Web App Virtual Directories.

In Exchange 2010, the most common Outlook Web App management tasks can be accomplished in the Exchange Management Console. All these tasks, and many other tasks, can be accomplished by using the Exchange Management Shell. You'll still use tools such as Internet Information Services (IIS) Manager for some tasks, for example, configuring Secure Sockets Layer (SSL) or setting up simple URLs for users.

For more information about how to manage Outlook Web App, see the following topics:

- Managing Outlook Web App
- Managing Outlook Web App Security

Tools for Managing Outlook Web App

The following table lists the tools that you can use to configure and manage Outlook Web App in Exchange 2010.

Tools for managing Outlook Web App

Tool	Description
Exchange Management Console	This graphical user interface is used to manage an Exchange 2010 organization. The EMC can be used to manage the most common settings for Outlook Web App.
Exchange Management Shell	This command-line interface for Exchange Server and the associated command-line plug-ins automate administrative tasks and management for many features that aren't included in the EMC.
Internet Information Services (IIS) Manager	IIS Manager is used to manage user access to the Outlook Web App virtual directories, for example, for simplifying the URL and forcing users to use an HTTPS address.
Web.config	Some Outlook Web App settings, such as the `ConnectionCacheSize` and `MaxRequestLength` values, must be configured by modifying Web.config because these settings are specific to ASP .NET. Web.config should be modified only by using tools such as Notepad. If you modify Web.config by using IIS, the file will become corrupted.
Registry Editor	Some Outlook Web App configuration settings, such as the `PublicClientTimeout`, `TrustedClientTimeout`, and `SSLOffloaded` values, must be configured by using Registry

	Editor. **Caution:** Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Return to top

Administrative Tasks for Managing Outlook Web App

The following table lists the configuration and management tasks that you can perform for Outlook Web App.

Configuration and management tasks for Outlook Web App

Task	Description	Link
Configure the virtual directories that are created for Web access to Exchange content	When you install the Client Access server role on your Exchange server, four virtual directories are created in the default IIS Web site on the Exchange 2010 server.	Managing Outlook Web App Virtual Directories
Simplify the Outlook Web App URL	By using IIS Manager, you can simplify the Outlook Web App URL that users use to access Outlook Web App.	Simplify the Outlook Web App URL
Modify attachment handling settings	You can configure the types of attachments that can be accessed in Outlook Web App and how those attachments are displayed.	Managing File and Data Access for Outlook Web App
Configure authentication methods	You can configure authentication methods, such as standard and forms-based authentication, for Outlook Web App.	Managing Outlook Web App Security
Modify language and character handling settings	You can configure the default language and character settings for an Outlook Web App virtual directory.	Configure Language Settings for Outlook Web App
Configure Gzip compression settings	Gzip enables data compression. By using Gzip, you can improve performance for users who are using Outlook Web App over slow network connections.	Configure Gzip Compression Settings

Disable Web beacons	Outlook Web App prevents senders from using Web beacons in junk e-mail messages to retrieve e-mail addresses.	Configure Web Beacon and HTML Form Filtering for Outlook Web App
Configure segmentation settings	You can enable or disable specific Outlook Web App features according to the needs of your organization.	Configure Segmentation in Outlook Web App
Configure Outlook Web App mailbox policies	Outlook Web App mailbox policies can be used to manage users' access to features through Outlook Web App at the organization level.	Understanding Outlook Web App Mailbox Policies

Return to top

1.6.1.6.1 Understanding Outlook Web App Virtual Directories

Understanding Outlook Web App Virtual Directories

Client Access > Understanding Client Access > Understanding Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-01*

When you install the Client Access server role on your Exchange server, one Microsoft Office Outlook Web App virtual directory is created in the default Internet Information Services (IIS) Web site on the Exchange server. You can manage the virtual directory by using the Exchange Management Shell, the Exchange Management Console, and IIS Manager.

Looking for management tasks related to Outlook Web App virtual directories? See Managing Outlook Web App Virtual Directories.

Configuring Outlook Web App Virtual Directories

Exchange 2010 supports access to mailboxes on Exchange 2010 servers through Exchange 2010 Client Access servers.

Most organizations find that the default Outlook Web App virtual directory that's created during installation of the Exchange 2010 Client Access server role is sufficient. You may not need to create new Outlook Web App virtual directories. Generally, new Outlook Web App virtual directories are created by businesses that provide hosting or for troubleshooting issues, such as the deletion and re-creation of Outlook Web App virtual directories.

Note:

You can’t create more than one Outlook Web App virtual directory in a site. To create multiple Outlook Web App virtual directories, you must create additional sites in IIS Manager.

Perform the following tasks on Outlook Web App virtual directories, depending on the needs of your organization.

- **Create a new Outlook Web App virtual directory** You can use the Exchange Management Shell to create a new Outlook Web App virtual directory. For more information, see Create an Outlook Web App Virtual Directory.

  Note:
  When the Client Access server role is installed, the Outlook Web App virtual directory is installed under the default Web site. All new virtual directories are installed under the default Web site unless a different Web site is specified when the virtual directory is created.

- **View or configure properties of an Outlook Web App virtual directory** You can use the Shell and the EMC to view or configure the properties of an Outlook Web App virtual directory. For more information, see View or Configure Outlook Web App Virtual Directories.
- **Manage properties on an Outlook Web App virtual directory** If you're running only the Client Access server role on a computer, you manage the properties of the virtual directories from the **Outlook Web App** tab in the EMC. You can access the **Outlook Web App** tab by clicking **Server Configuration** and then clicking **Client Access**.

1.6.1.6.2 Understanding Outlook Web App URLs

Understanding Outlook Web App URLs

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

Microsoft Office Outlook Web App in Microsoft Exchange Server 2010 enables users to read and manage the contents of Exchange 2010 mailboxes from most Internet browsers. You can use Internet Information Services (IIS) Manager to manage the default URLs to make connecting to Outlook Web App more secure and easier for users.

Looking for management tasks related to Outlook Web App URLs? See Managing Outlook Web App URLs.

Default Outlook Web App URL

When you install the Client Access server role on an Exchange 2010 server, one virtual directory is created for Outlook Web App. This virtual directory is named owa. For more information about virtual directories, see Managing Outlook Web App Virtual Directories.

The default URL for Outlook Web App for mailboxes on an Exchange 2010 server is http://*<server name>*/owa.

Understanding File and Data Access for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-07*

You can manage the different ways users access information in Microsoft Office Outlook Web App by using the Exchange Management Console.

Looking for management tasks related to file and data access for Outlook Web App? See Managing File and Data Access for Outlook Web App.

Contents

WebReady Document Viewing

Microsoft Exchange Server 2010 includes a feature named WebReady Document Viewing. WebReady Document Viewing lets users view common file types in the Outlook Web App Web browser without having the applications associated with those file types installed on the computer they're using. Users can view the following kinds of files using WebReady Document Viewing:

- .doc
- .docx
- .pdf
- .ppt
- .pptx
- .xls
- .xlsx

Additionally, the following MIME types are supported:

- application/pdf
- application/vnd.ms-excel
- application/vnd.ms-powerpoint
- application/word
- application/x-mspowerpoint
- application/x-msexcel

For more information about how to manage WebReady Document Viewing for users, see Configure WebReady Document Viewing.

Public and Private Computer File Access

You can configure how users interact with files by using the Allow, Block, or Force Save options for direct file access in the Exchange Management Console. This means that you can specify the types of files that users can access. More important, you can directly specify which types of files are prohibited. For more information about how to manage public and private computer file access, see Configure Public and Private Computer File Access.

Understanding Outlook Web App Advanced Features

Client Access > Understanding Client Access > Understanding Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-06*

You can manage advanced features in Outlook Web App in Microsoft Exchange Server 2010 by using the Exchange Management Console and the Exchange Management Shell. In Exchange 2010, you can enable and disable Outlook Web App features for your whole organization or for individual users by using segmentation. To increase protection against spammers, you can disable Web beacons in Outlook Web App. If the default language and character settings for Outlook Web App at initial sign-in aren't appropriate for your users, you can change them using the language and character settings. If users will be using Outlook Web App over a slow network connection, you can enable Gzip compression to improve the performance of Outlook Web App on the client computer.

Looking for management tasks related to Outlook Web App advanced features? Check out Managing Outlook Web App Advanced Features.

Contents

Segmentation of Features in Outlook Web App

Segmentation lets you enable and disable features that are available to users in Outlook Web App. By default, any mail-enabled user in your Exchange 2010 organization can access their mailbox by using Outlook Web App. Depending on the needs of your organization, you can use segmentation to configure the following restrictions for user access:

- Restrict access to Outlook Web App for specific users.
- Control access to certain Outlook Web App features for specific users.
- Disable an Outlook Web App feature completely.

Many features can be set for an Outlook Web App virtual directory by using the EMC. You can use the Set-OwaVirtualDirectory cmdlet in the Shell to enable or disable the same features that you can enable and disable by using the EMC, in addition to many other Outlook Web App features for an Outlook Web App virtual directory. For example, you can use the `RemindersandNotificationsEnabled` parameter to disable the **Reminders** feature in Outlook Web App. The **Reminders** feature enables users to receive new mail notifications. You can also modify other Outlook Web App features, such as Tasks and

Contacts.

For more information about the parameters that you can use to configure segmentation for all users, see Set-OwaVirtualDirectory.

For more information about the features that can be configured using the EMC, see Configure Segmentation in Outlook Web App.

For more information about how to enable and disable features for specific users, see Set-CASMailbox.

Return to top

Segmentation Features in Exchange 2003 vs. Exchange 2010 and Exchange 2007

The following table lists the differences between Outlook Web App segmentation in Exchange Server 2003 vs. Exchange 2010 and Exchange Server 2007.

Outlook Web App segmentation in Exchange 2003 vs. Exchange 2010 and Exchange 2007

Type	Exchange 2003	Exchange 2010 and Exchange 2007
Segmentation basis	Segmentation can be performed for individual users and for individual servers. The segmentation setting for each Outlook Web App feature is stored as a DWORD value in the registry. If the DWORD value is 1, the Outlook Web App feature is enabled. If the DWORD value is 0, the Outlook Web App feature is disabled. By default, all features are enabled.	Segmentation can be performed for individual users and for individual virtual directories. You can administer the user and virtual directory segmentation settings for each Outlook Web App feature by using the Shell. Unlike Exchange 2003, segmentation settings in Exchange 2010 and Exchange 2007 aren't configured by editing the registry.
Storing segmentation values	The DWORD values that are set for users and for servers are the same. However, they're stored in different locations. • The server DWORD value is stored in a registry key. • The user DWORD value is stored in the **msExchMailboxFolderSet** Active Directory attribute on the user object. By default, the **msExchMailboxFolderSet** attribute exists, but the value isn't configured.	• The segmentation value that's set for an Outlook Web App virtual directory is stored on the virtual directory object. • The segmentation value that's set for a user is stored in the **msExchMailboxFolderSet** Active Directory attribute on the user object. By default, the **msExchMailboxFolderSet** attribute exists for each user, but the value isn't configured. Use the Set-

		CASMailbox cmdlet to configure values for individual users.
Features in Outlook Web App in Exchange 2010 or Exchange 2007 that can be segmented	• Not applicable	• You can segment the following Outlook Web App features: • Unified Messaging integration • Windows SharePoint Services and Windows file shares integration • Exchange ActiveSync integration from **Mobile Settings** on the **Options** page

Return to top

Understanding Web Beacons

A Web beacon is a file object, such as a transparent graphic or an image, which is put on a Web site or in an e-mail message. Web beacons are typically used together with HTML cookies to monitor user behavior on a Web site or to validate a recipient's e-mail address when an e-mail that contains a Web beacon is opened. Web beacon configuration is set on a per virtual directory basis for each Outlook Web App virtual directory in your organization.

Web beacons frequently come in the form of images that are downloaded onto a user's computer when the user opens a junk e-mail message. After the images are downloaded, a Web beacon notification is sent to the sender of the junk e-mail that informs the sender that the recipient e-mail address is valid. After a user opens a message that sends a Web beacon notification back to the junk e-mail sender, the user may receive junk e-mail more frequently because the junk e-mail sender has verified that the user's e-mail address is valid. Web beacons can also contain harmful code and be used to circumvent e-mail filters to deliver a spammer's message.

Note:

By default, Outlook Web App disables all potential Web beacon content in e-mail messages.

In Outlook Web App, an incoming e-mail message that has any content that can be used as a Web beacon, regardless of whether the message actually contains a Web beacon, prompts Outlook Web App to display a warning message to the user to inform the user that the content has been blocked. If a user knows that a message is legitimate, they can enable the blocked content. If a user doesn't recognize the sender or the message, they can open the message without unblocking the content and then delete the message without triggering beacons. If your organization doesn't want to use this feature, you can disable the blocking option for Outlook Web App.

Return to top

Configuring Web Beacons

The configuration settings for filtering Web beacons are stored in Active Directory. You can configure how Web beacons are filtered by using the Set-OwaVirtualDirectory cmdlet in the Shell. For more information about syntax and parameters, see Set-OwaVirtualDirectory.

The following list describes the parameters in the **FilterWebBeacons** property for Web beacon filtering in Outlook Web App:

- `UserFilterChoice` You can let users decide whether they want to enable or continue to disable blocked Web beacon content by using the `UserFilterChoice` parameter. Outlook Web App blocks all potential Web beacon content in an e-mail message and displays a message in the information bar when a user receives an e-mail message that contains potential Web beacon content warning them that content is blocked. To view the blocked Web beacon content, the user can click **Click Here** in the infobar message.

  Note:
  By default, the `UserFilterChoice` parameter is enabled on Outlook Web App.

- `ForceFilter` You can block all potential Web beacon content by using the `ForceFilter` parameter. Users can't override the `ForceFilter` parameter to view the blocked Web beacon content.
- `DisableFilter` You can enable all Web beacon content on Outlook Web App by using the `DisableFilter` parameter setting.

For more information about how to disable Web beacons, see Configure Web Beacon and HTML Form Filtering for Outlook Web App.

Return to top

Language Settings

You can configure the following language parameter settings on an Outlook Web App virtual directory by using the Set-OwaVirtualDirectory cmdlet in the Shell:

- `DefaultClientLanguage` The `DefaultClientLanguage` parameter, a Regional property setting, specifies the Outlook Web App language that's used when a user who hasn't selected a specific language on the **Options** page signs in to Outlook Web App. This prevents the user from being able to view the initial page to set the time zone and language, but doesn't prevent the user from changing these settings using **Options** in Outlook Web App after they've signed in. This parameter doesn't apply to Microsoft Exchange 2000 Server or Exchange 2003 virtual directories.
- `LogonAndErrorLanguage` The `LogonAndErrorLanguage` parameter specifies which language Outlook Web App uses for forms-based authentication and for error messages that occur when a user's current language setting can't be read. This parameter applies to Exchange 2003 virtual directories.

The user can configure the language that's used by Outlook Web App by using the **Regional Settings** option in the **Options** menu after he or she is successfully authenticated for an Outlook Web App session. The `LogonAndErrorLanguage` parameter can be configured only by an administrator. The administrator must configure the `LogonAndErrorLanguage` parameter before the user authenticates into Outlook Web App.

Note:
To make all Arabic, Asian, Hebrew, and Urdu text display correctly in Outlook Web App, support for languages that are read from right-to-left and script languages must be installed on the client computer. Other languages may also require that the appropriate language pack be installed on the client computer.

For detailed syntax and parameter information, see Set-OwaVirtualDirectory.

For more information about how to configure the language settings for an Outlook Web App virtual directory, see Configure Language Settings for Outlook Web App.

Return to top

Character Settings

The Charset parameter specifies how the Web browser decodes data and appends the character set, for example, ISO-8859-15, of the content-type header in the Response object of the Web page. You can use the Response object to send output to the client.

You can configure the character settings on an Outlook Web App virtual directory by using the **Set-OwaVirtualDirectory** cmdlet in the Shell. You can configure the following character settings on an Outlook Web App virtual directory:

- OutboundCharset The OutboundCharset parameter specifies the character set that's used on messages that are sent by users on a specific Outlook Web App virtual directory. It accepts three settings: autodetect, alwaysUTF8, and UserLanguageChoice. Autodetect causes Exchange to examine the first 2 kilobytes (KB) of text and deduce the character set to use. This is the preferred method. AlwaysUTF8 causes Exchange to always use UTF-8 encoded UNICODE characters on outgoing messages. UserLanguageChoice causes Exchange to use the language that's used in the Outlook Web App user interface to encode messages. This can be a problem if the preferred language and the language that's used on an individual message aren't the same.
- UseGB18030 The UseGB18030 parameter, a Regional property setting, specifies when the character set GB18030 is used. This parameter is a character-handling key in Active Directory that works in coordination with the OutboundCharset registry key. If USEGB18030 is on and OutboundCharset is set to Autodetect, Outlook Web App will use GB18030 whenever GB18032 is detected.
- UseISO8859-15 The UseISO8859-15 parameter, a Regional property setting, specifies when the character set ISO8859-15 is used. This parameter is a character-handling key in Active Directory that works in coordination with the OutboundCharset registry key. If USEISO8859-15 is on and OutboundCharset is set to Autodetect, Outlook Web App will use ISO8859-15 whenever ISO8859-1 is detected

For detailed syntax and parameter information, see Set-OwaVirtualDirectory.

For more information about how to configure the character settings for Outlook Web App, see Configure Character Settings for Outlook Web App.

Return to top

Gzip Compression Settings

Gzip compression enables data compression. Data compression helps optimize response time over slow network connections. Depending on the type of compression setting that you select, Outlook Web App compresses static Web pages, dynamic Web pages, or both static Web pages and dynamic Web pages. Gzip compression is performed by the Client Access server.

You can configure Gzip compression settings on an Outlook Web App virtual directory by using the Set-OwaVirtualDirectory cmdlet in the Shell. You can use the Get-OwaVirtualDirectory cmdlet to retrieve information about the current settings on an

Outlook Web App virtual directory. For more information about syntax and parameters, see Set-OwaVirtualDirectory.

The following table describes the three levels of data compression settings for Outlook Web App.

Data compression settings for Outlook Web App

Data compression setting	Description
High	This setting compresses static and dynamic pages.
Low	This setting compresses only static pages. By default, Gzip compression is set to *low*.
Off	No compression is used.

For more information about how to configure Gzip settings, see Configure Gzip Compression Settings.

Return to top

Customizing the Forms-Based Authentication Sign-In Page

You can customize the appearance of the forms-based authentication page by writing a new version of the sign-in page that sends the same HTML form to Outlook Web App as the original forms-based authentication sign-in page.

The forms-based authentication page is enabled for anonymous access. Therefore, you must use caution when you decide what content to display on the Outlook Web App sign-in page. Don't reveal any sensitive data that may pose a security risk for your organization on the Outlook Web App sign-in page.

If you customize the sign-in page, your changes may be overwritten when you install hot fixes and service packs on the Client Access server that provides the sign-in page. For more information about how to customize the forms-based authentication sign-in page, see Customize the Outlook Web App Sign-In and Sign-Out Pages.

Return to top

Creating a Custom Theme for Outlook Web App

You can create a custom theme for Outlook Web App by copying an existing theme and modifying the files that define the icons, logos, and colors. For more information, see Create a Theme for Outlook Web App.

Understanding Outlook Web App Mailbox Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-16*

Use Microsoft Office Outlook Web App mailbox policies to create organization-level policies to manage access to features in Outlook Web App. Outlook Web App mailbox policies allow you to create multiple policies at the organization level and apply them to individual mailboxes.

Looking for management tasks related to Outlook Web App mailbox policies? See Managing Outlook Web App Mailbox Policies.

Contents

Outlook Web App Mailbox Policies

In Exchange 2010, you can create multiple Outlook Web App mailbox policies and apply them to individual mailboxes. When an Outlook Web App mailbox policy is applied to a mailbox, it will override the settings of the virtual directory.

In previous versions of Exchange, Outlook Web App features were managed by configuring the Outlook Web App virtual directories. Exceptions for individual mailboxes were accommodated by enabling or disabling features on individual mailboxes.

Configuring Outlook Web App Mailbox Policies

A default Outlook Web App mailbox policy is created automatically when the Client Access server role is installed. By default, all options are enabled on the default Outlook Web App mailbox policy. You can create as many Outlook Web App mailbox policies as necessary to meet the needs of your organization.

Note:
The default Outlook Web App mailbox policy is not automatically applied to any mailboxes.

For example, you may want to create a policy that forces users to use WebReady Document Viewing to view attachments or a policy that limits users to the Light version of Outlook Web App.

You can use the Exchange Management Console or the Exchange Management Shell to create and configure Outlook Web App mailbox policies.

Applying Outlook Web App Mailbox

Policies

Only one Outlook Web App mailbox policy can be applied to a mailbox.

If there's no Outlook Web App mailbox policy applied to a mailbox, the settings defined on the virtual directory will be applied.

An Outlook Web App mailbox policy can be applied to a mailbox as part of the new mailbox wizard, by using the EMC to modify an existing mailbox, or by using the Shell and the Set-CASMailbox cmdlet to apply a mailbox policy.

1.6.1.6.6 Understanding Outlook Web App and Instant Messaging Integration

Understanding Outlook Web App and Instant Messaging Integration

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-01*

Microsoft Office Outlook Web App in Microsoft Exchange Server 2010 supports the integration of Outlook Web App and Microsoft Office Communications Server 2007 or Microsoft Lync Server 2010. When integration with either instant messaging server is configured and instant messaging is enabled in Outlook Web App, users will see their instant messaging contacts and groups in the Navigation Pane of Outlook Web App.

Users can respond to or initiate IM sessions in Outlook Web App and can manage their instant messaging contacts and groups from Outlook Web App.

Looking for management tasks related to Outlook Web App and Communications Server 2007 or Lync Server 2010 integration? See Managing Outlook Web App and Instant Messaging Integration.

1.6.1.6.7 Understanding the Mini Version of Outlook Web App

Understanding the Mini Version of Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-08*

The mini version of Outlook Web App is a lightweight browser-based client, similar to the Outlook Mobile Access client in Exchange 2003. It provides access from simple HTML-compatible browsers that support cookies and it’s designed to be used on a mobile operating system.

Functionality in the mini version of Outlook Web App

The mini version of Outlook Web App provides functionality that lets users:

- Access e-mail, calendar, contacts, tasks, and the global address list.
- Access e-mail subfolders.
- Compose, reply, and forward e-mail messages.
- Create calendar, contact, and task items.
- Handle meeting requests.
- Set the time zone and automatic-reply messages for when they're out of the office, away, or not available to respond to e-mail.

The mini version of Outlook Web App is based on Outlook Web App architecture. Because it's an application within Outlook Web App, it uses all the segmentation flags that exist in Outlook Web App.

Authentication and Security Concerns

In order to be compatible with the widest array of mobile phone browsers, the mini version of Outlook Web App is designed to use Basic authentication. Basic authentication allows the credentials to be exchanged within the header of the HTTP request. The request should always be sent using a secure socket layer (SSL) encrypted channel.

Different browsers handle passing credential information differently. Some request that the user type the information for each new session. Others only request the information if it has changed.

Warning:
If a user's mobile phone is lost or stolen, the user's password should be changed immediately.

The mini version of Outlook Web App uses the same public session time-out value used by Outlook Web App. Users who don't complete operations such as the creation of a new e-mail or calendar item might see blank items created in their drafts folder, Calendar folder, or Contacts folder.

There is no logoff functionality in the mini version of Outlook Web App because there is no guarantee that the mobile device browser will forget the stored password after the default time-out value.

Accessing the mini version of Outlook Web App

The mini version of Outlook Web App is implemented as a virtual directory named OMA, which is created below the Outlook Web App virtual directory. You can access the mini version of Outlook Web App by appending /oma to your Outlook Web App URL. For example, if your Outlook Web App URL is https://mail.contoso.com, the URL for the mini version of Outlook Web App would be something like https://mail.contoso.com/owa/oma. There is no client detection logic or configurable redirection on the virtual directory for the mini version of Outlook Web App. The user must specify the full URL to access it.

When you use the mini version of Outlook Web App, the same segmentation flags that are used for Outlook Web App are leveraged. For example, if access to the user's calendars is disabled, the mini version of Outlook Web App won't provide access to the user's calendars. For more information about segmentation flags, see Understanding Segmentation for Outlook Web App.

1.6.1.7 Understanding Outlook Anywhere

Understanding Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-03*

In Microsoft Exchange Server 2010, the Outlook Anywhere feature, formerly known as RPC over HTTP, lets clients that use Microsoft Office Outlook 2010, Outlook 2007, or Outlook 2003 connect to their Exchange servers from outside the corporate network or over the Internet using the RPC over HTTP Windows networking component. This topic describes the Outlook Anywhere feature, provides information about deploying Outlook Anywhere, discusses coexistence with older versions of Exchange, and lists the benefits of using Outlook Anywhere.

Looking for management tasks related to Outlook Anywhere? See Managing Outlook Anywhere.

Contents

Outlook Anywhere and Exchange 2010

The Windows RPC over HTTP Proxy component, which Outlook Anywhere clients use to connect, wraps remote procedure calls (RPCs) with an HTTP layer. This allows traffic to traverse network firewalls without requiring RPC ports to be opened. In Exchange 2010, as in Exchange 2007, it's easy to deploy and manage this feature. To deploy Outlook Anywhere in your Exchange 2010 messaging environment, you need to enable Outlook Anywhere on at least one Client Access server using the Enable Outlook Anywhere wizard in the Exchange Management Console.

Note:

Outlook Anywhere should be enabled only on Client Access servers that are exposed to the Internet. Do not enable Outlook Anywhere on internal Client Access servers.

Benefits of Using Outlook Anywhere

Outlook Anywhere offers the following benefits to clients that use Outlook 2010, Outlook 2007, or Outlook 2003 to access your Exchange messaging infrastructure:

- Users have remote access to Exchange servers from the Internet.
- You can use the same URL and namespace that you use for Outlook Web App and Microsoft Exchange ActiveSync.
- You can use the same Secure Sockets Layer (SSL) server certificate that you use for both Outlook Web App and Exchange ActiveSync.
- Unauthenticated requests from Outlook can't access Exchange servers.
- You don't have to use a virtual private network (VPN) to access Exchange servers across the Internet.

- You don't have to configure anything in Exchange 2010 when you're using SSL session ID load balancing on the Client Access server with Outlook Anywhere.
- If you already use Outlook Web App with SSL or Exchange ActiveSync with SSL, you don't have to open any additional ports from the Internet.
- You can test end-to-end client connectivity for Outlook Anywhere and TCP-based connections by using the **Test-OutlookConnectivity** cmdlet.

Return to top

Deploying Outlook Anywhere

Deploying Outlook Anywhere for your organization is straightforward. The following recommendations should be followed to successfully deploy Outlook Anywhere:

- **Use at least one Client Access server per site** In Exchange 2010, a site is a network location with high-bandwidth connectivity between all computers. We recommend that you install at least one Client Access server in each site to provide client access to the Mailbox server. However, you can have multiple Client Access servers in each site for increased performance and reliability.
- **Enable Outlook Anywhere on an Internet-exposed Client Access server** Outlook Anywhere should be enabled on Internet-exposed Client Access servers only. This lets clients that use Outlook 2010 or Outlook 2007 connect to a user's mailbox through the Client Access server in the site. Users will connect by using HTTPS to the Client Access server that's in the site where the user's mailbox is located.

For more information, see Enable Outlook Anywhere.

Managing Outlook Anywhere

You can manage Outlook Anywhere by using the Exchange Management Console or the Exchange Management Shell. By default, when you enable Outlook Anywhere on a Client Access server, all users who have mailboxes on Exchange 2010 Mailbox servers are enabled for Outlook Anywhere. For more information, see Managing Outlook Anywhere.

Return to top

Coexistence

For mailboxes on Exchange 2010 Mailbox servers, clients must connect through Exchange 2010 Client Access servers. Outlook Anywhere can be used in environments where Microsoft Exchange Server 2007 and Exchange Server 2003 servers are still being used. If you have users with mailboxes on Exchange 2003 servers, and these users are using Outlook 2007 or Outlook 2003 to connect, you must configure these clients manually. To configure Outlook Anywhere with Exchange 2007 or Exchange 2003, see Configure Outlook Anywhere in an Environment with Earlier Versions of Exchange.

Return to top

Outlook Anywhere in Multiple Active Directory Sites

If you have multiple Active Directory sites that are separated by low-bandwidth network connectivity, you can enable a Client Access server in each site. The Autodiscover service will then automatically detect which Client Access server is closest to the user's mailbox

that resides either on an Exchange 2003 back-end server enabled for RPC over HTTP or on a later Exchange version running the Mailbox server role. After the user has connected across the Internet using RPC over HTTP, the Client Access server will then use RPC requests. This ensures that RPC requests stay within the site's intranet. For more information about how to provide an external host name for Outlook Anywhere, see Configure an External Host Name for Outlook Anywhere.

Users

Users with mailboxes on Exchange Server 2003 servers with SP1 or a later version or Exchange 2003 servers enabled for RPC over HTTP will also be able to access their Exchange information from the Internet. For these users, you can use the Shell to manage the Outlook Anywhere feature on the Exchange 2010 Client Access server in the site.

Return to top

Testing Outlook Anywhere Connectivity

After you enable Outlook Anywhere in your Microsoft Exchange Server 2010 organization, you can test for end-to-end client Outlook connectivity. You can test end-to-end Outlook connectivity by doing either of the following:

- Running the **Test-OutlookConnectivity** cmdlet. The cmdlet tests for Outlook Anywhere (RPC over HTTP) and TCP/IP connections. If the cmdlet test fails, the output notes the step that failed.
- Running the Outlook Anywhere connectivity test using the Exchange Remote Connectivity Analyzer (ExRCA). When you run this test, you get a detailed summary showing where the test failed and what steps you can take to fix issues.

Both tests try to log on through Outlook Anywhere after obtaining server settings from the Autodiscover service. End-to-end verification includes the following:

- Testing for Autodiscover connectivity
- Validating DNS
- Validating certificates (whether the certificate name matches the Web site, whether the certificate has expired, and whether it's trusted)
- Checking that the firewall is set up correctly (ExRCA checks overall firewall setup. The cmdlet tests for Windows firewall configuration.)
- Verifying client connectivity by logging on to the user's mailbox

For more information, see Test Outlook Anywhere Connectivity.

Return to top

1.6.1.7.1 Understanding SSL for Outlook Anyw here

Understanding SSL for Outlook Anywhere

Client Access > Understanding Client Access > Understanding Outlook Anywhere >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-11*

Outlook Anywhere client connectivity is encrypted using Secure Sockets Layer (SSL) on the Microsoft Exchange Server 2010 Client Access server. This topic explains SSL

certificates, SSL offloading, and using SSL to manage security for Outlook Anywhere.

Looking for management tasks related to Outlook Anywhere? See Managing Outlook Anywhere.

Contents

Valid SSL Certificate

The default self-signed certificate that's available in Exchange 2010 Setup works with Outlook Web App and Exchange ActiveSync, but it doesn't work with Outlook 2007 or Outlook 2010 and Outlook 2003 clients that are using Outlook Anywhere. Instead, you must use a valid SSL certificate that's created by a certification authority (CA) that's trusted by the client computer's operating system. For more information about how to install a valid SSL certificate from a CA that the client trusts, see Obtain a Server Certificate from a Certification Authority.

After you obtain a valid SSL certificate to use with the Client Access server on the default Web site or on the Web site where you host your /rpc virtual directory, you can configure the Web site to require SSL. You can enable SSL for all Web sites that are hosted by the Client Access server or enable SSL only for the /rpc virtual directory.

SSL Offloading

If you plan to close the SSL connection from the client computer running Outlook 2007, Outlook 2010, or Outlook 2003 to the firewall, you can use SSL offloading. With SSL offloading, the traffic from the firewall to the Client Access server won't be encrypted by using SSL. For SSL offloading to work, you must have a certificate on the firewall that the client trusts. We recommend that you encrypt all traffic from the client to the Client Access server. For more information, see Configure SSL Offloading for Outlook Anywhere.

Return to top

Managing Security for Outlook Anywhere

When you install Exchange Server 2010, a default virtual directory named /rpc is created on the default Internet Information Services (IIS) Web site on the Exchange Server 2010 Client Access server. You can configure the /rpc virtual directory to use SSL to manage security for Outlook Anywhere and external client access. For more information, see Configure SSL for Outlook Anywhere. Configuring the /rpc virtual directory to use SSL is only one step in managing security. For more information, see Securing Client Access Servers and Managing Outlook Anywhere Security.

Return to top

1.6.1.7.2 Understanding Redirection for Outlook Anywhere with a Single SSL Certificate

Understanding Redirection for Outlook Anywhere with a Single SSL Certificate

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-04*

When Microsoft Office Outlook 2007 or Outlook 2010 clients aren't joined to your domain or don't have direct access to Active Directory in your Exchange forest, you can redirect them. When the Outlook clients are redirected, they can access Exchange Web services, such as the Autodiscover service, the offline address book, and Unified Messaging, in your Exchange 2010 organization.

You can set up your Outlook Anywhere deployment to use a single Secure Sockets Layer (SSL) certificate with redirection. For information about how to do this, see Configure Outlook Anywhere to Use an SSL Certificate with Redirection.

Looking for other management tasks related to Outlook Anywhere? See Managing Outlook Anywhere.

Using a Single SSL Certificate with Redirection

After you configure Exchange to use an SSL certificate with redirection, clients that aren't domain-joined and clients that don't have direct connectivity to Active Directory receive a redirect from the Autodiscover site to the site that's dedicated to handling e-mail. When this occurs, a warning message is displayed in Outlook 2007 and Outlook 2010 that says **Allow this website to configure server settings?** Both Outlook 2007 and Outlook 2010 give users the opportunity to prevent this warning message appearing in the future. We recommend that you inform your users that they can turn off the warning message on their Outlook 2010 or Outlook 2007 client.

Using a Single SSL Certificate with Redirection for Hosting Scenarios

You can use a single SSL certificate with redirection if you're hosting multiple Simple Mail Transfer Protocol (SMTP) domains and you don't want to obtain a separate SSL certificate for each domain. In this hosting scenario, after you've configured the Autodiscover redirect site, you would need to create a DNS entry in each of the domains to have the Autodiscover service point to this non-SSL redirect site. This redirect site would redirect all clients that are connecting to your SMTP domains to a single URL, such as https://mail.contoso.com/autodiscover/autodiscover.xml. For more information, see Configure Outlook Anywhere to Use an SSL Certificate with Redirection.

1.6.1.8 Understanding the Autodiscover Service

Understanding the Autodiscover Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-28*

Microsoft Exchange Server 2010 includes a service named the Autodiscover service. This topic gives an overview of the service, explains how it works, how it configures Outlook clients, and what options there are for deploying the Autodiscover service in your messaging environment.

The Autodiscover service does the following:

- Automatically configures user profile settings for clients running Microsoft Office Outlook 2007 or Outlook 2010, as well as supported mobile phones. Phones running Windows Mobile 6.1 or a later version are supported. If your phone isn't a Windows Mobile phone, check your mobile phone documentation to see if it's supported.
- Provides access to Exchange features for Outlook 2007 or Outlook 2010 clients that are connected to your Exchange messaging environment.
- Uses a user's e-mail address and password to provide profile settings to Outlook 2007 or Outlook 2010 clients and supported mobile phones. If the Outlook client is joined to a domain, the user's domain account is used.

Looking for management tasks related to the Autodiscover service? See Managing the Autodiscover Service.

Contents

Overview of the Autodiscover Service

The Autodiscover service makes it easier to configure Outlook 2007 or Outlook 2010 and some mobile phones. You can't use the Autodiscover service with earlier versions of Outlook, including Outlook 2003. In earlier versions of Microsoft Exchange (Exchange 2003 SP2 or earlier) and Outlook (Outlook 2003 or earlier), you had to configure all user profiles manually to access Exchange. Extra work was required to manage these profiles if changes occurred to the messaging environment. Otherwise, the Outlook clients would stop functioning correctly.

The Autodiscover service uses a user's e-mail address and password to automatically configure a user's profile. Using the e-mail address, the Autodiscover service provides the following information to the client:

- The user’s display name
- Separate connection settings for internal and external connectivity
- The location of the user’s Mailbox server
- The URLs for various Outlook features that govern functionality such as free/busy information, Unified Messaging, and the offline address book
- Outlook Anywhere server settings

When a user's Exchange information is changed, Outlook automatically reconfigures the user's profile using the Autodiscover service. For example, if a user's mailbox is moved or the client can't connect to the user's mailbox or to available Exchange features, Outlook will contact the Autodiscover service and automatically update the user's profile to include the information that's required to connect to the mailbox and Exchange features.

Return to top

How the Autodiscover Service Works

When you install the Client Access server role on a computer running Exchange 2010, a default virtual directory named Autodiscover is created under the default Web site in Internet Information Services (IIS). This virtual directory handles Autodiscover service requests from Outlook 2007 or Outlook 2010 clients and supported mobile phones under the following circumstances:

- When a new user account is configured or updated
- When an Outlook client periodically checks for changes to the Exchange Web Services URLs
- When underlying network connection changes occur in your Exchange messaging environment

Additionally, a new Active Directory object named the service connection point (SCP) is created on the server where you install the Client Access server role.

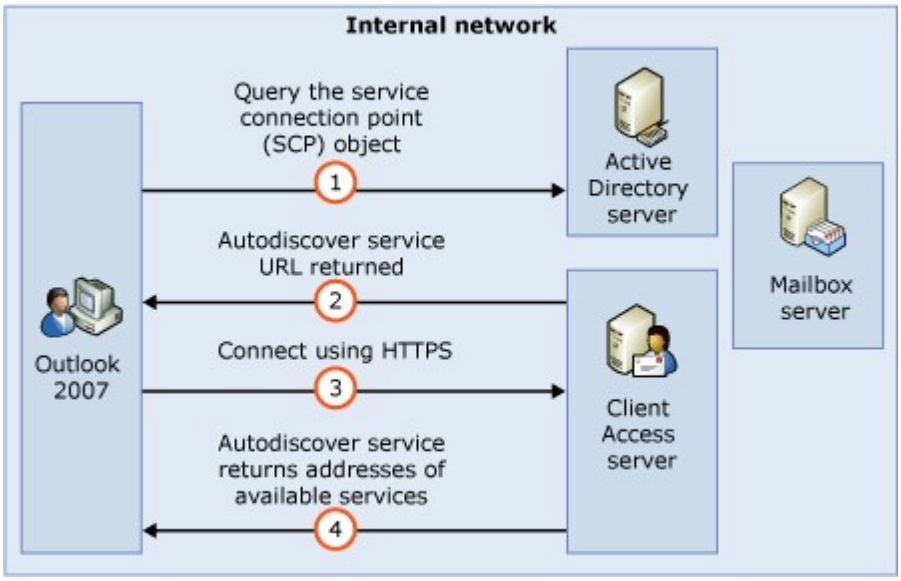
The SCP object contains the authoritative list of Autodiscover service URLs for the forest. You can use the **Set-ClientAccessServer** cmdlet to update the SCP object. For more information, see Set-ClientAccessServer.

Important:

Before you run the **Set-ClientAccessServer** cmdlet, make sure the Authenticated Users account on the Client Access server has Read permissions for the SCP object. If users don't have the correct permissions, they can't search for and read items.

For more information about SCP objects, see Publishing with Service Connection Points.

The following figure shows how a client connects to a Client Access server the first time from inside the internal network.



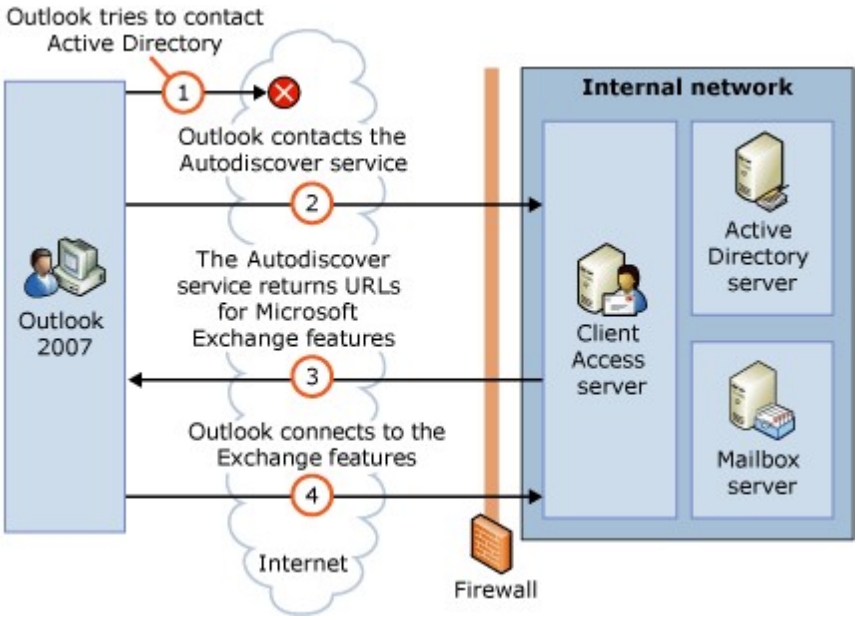
For external access, or using DNS, the client locates the Autodiscover service on the Internet by using the primary SMTP domain address from the user's e-mail address.

Note:

You must provide a host record for the Autodiscover service for external DNS. For more

information, see your Windows documentation for how to configure DNS, and also see the White Paper: Exchange 2007 Autodiscover Service.

Depending on whether you've configured the Autodiscover service on a separate site, the Autodiscover service URL will be either https://*<smtp-address-domain>*/autodiscover/autodiscover.xml or https://autodiscover.*<smtp-address-domain>*/autodiscover/autodiscover.xml, where ://*<smtp-address-domain>* is the primary SMTP domain address. For example, if the user's e-mail address is tony@contoso.com, the primary SMTP domain address is contoso.com. The following figure shows a simple topology with a client connecting from the Internet.



When the client connects to Active Directory, the client looks for the SCP object created during Setup. In deployments that include multiple Client Access servers, an Autodiscover SCP object is created for each Client Access server. The SCP object contains the *ServiceBindingInfo* attribute with the fully qualified domain name (FQDN) of the Client Access server in the form https://CAS01/autodiscover/autodiscover.xml, where CAS01 is the FQDN for the Client Access server. Using the user credentials, the Outlook 2007 or Outlook 2010 client authenticates to Active Directory and searches for the Autodiscover SCP objects. After the client obtains and enumerates the instances of the Autodiscover service, the client connects to the first Client Access server in the enumerated list and obtains the profile information in the form of XML data that's needed to connect to the user's mailbox and available Exchange features.

Return to top

Deployment Options for the Autodiscover Service

The Autodiscover service must be deployed and configured correctly for Outlook 2007 and Outlook 2010 clients to automatically connect to Exchange features such as the offline address book, the Availability service, and Unified Messaging (UM). Deploying the Autodiscover service is only one step in making sure your Microsoft Exchange services, such as the Availability service, can be accessed by Outlook 2007 or Outlook 2010 clients. For more information, see Configure Exchange Services for the Autodiscover Service.

Configuring Autodiscover for Cross-Forest Moves

The Autodiscover service can provide user profile information to connecting Outlook clients for mailboxes that have been moved from one Microsoft Exchange forest to another. For this to happen, you must configure a mail-enabled user in both the original forest where the user's mailbox resided and in the target forest using the **New-MailUser** cmdlet. In the source forest, you should use the *ExternalEmailAddress* parameter in the cmdlet to specify the new e-mail address of the mailbox in the target forest. For more information, see New-MailUser.

When you configure a mail-enabled user, the Autodiscover service in the original forest will redirect the authenticating user to the new e-mail address in the target forest. The connecting Outlook client will then be redirected to the Client Access server in the target forest where the mailbox has been moved. For more information, see Understanding Move Requests.

Return to top

1.6.1.9 Understanding the Availability Service

Understanding the Availability Service

Exchange Server 2010 > Client Access > Understanding Client Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-24*

The Microsoft Exchange Server 2010 Availability service makes free/busy information available to Microsoft Office Outlook 2007 and Outlook Web App clients. The Availability service improves information workers' calendaring and meeting scheduling experience by providing secure, consistent, and up-to-date free/busy information. By default, this service is installed with Exchange 2010.

Outlook 2007 and Outlook Web App use the Availability service to perform the following tasks:

- Retrieve current free/busy information for Exchange 2010 mailboxes
- Retrieve current free/busy information from other Exchange 2010 organizations
- Retrieve published free/busy information from public folders for mailboxes on servers that have versions of Exchange earlier than Exchange 2010
- View attendee working hours
- Show meeting time suggestions

Contents

Distribution Group Handling

Availability Service API

Availability Service Network Load Balancing

Methods Used to Retrieve Free/Busy Information

Overview of the Availability Service

The Availability service retrieves free/busy information directly from the target mailbox for users on Exchange 2010 and Exchange 2007 and can be configured to retrieve free/busy information for users on earlier versions of Exchange. For topologies that have Exchange 2007 or Exchange 2010 mailboxes in which all clients are running Outlook 2007, the Availability service is used to retrieve free/busy information.

Note:

If you have Outlook 2007 clients running on Exchange Server 2003 mailboxes, Outlook 2007 will use public folders to retrieve free/busy information.

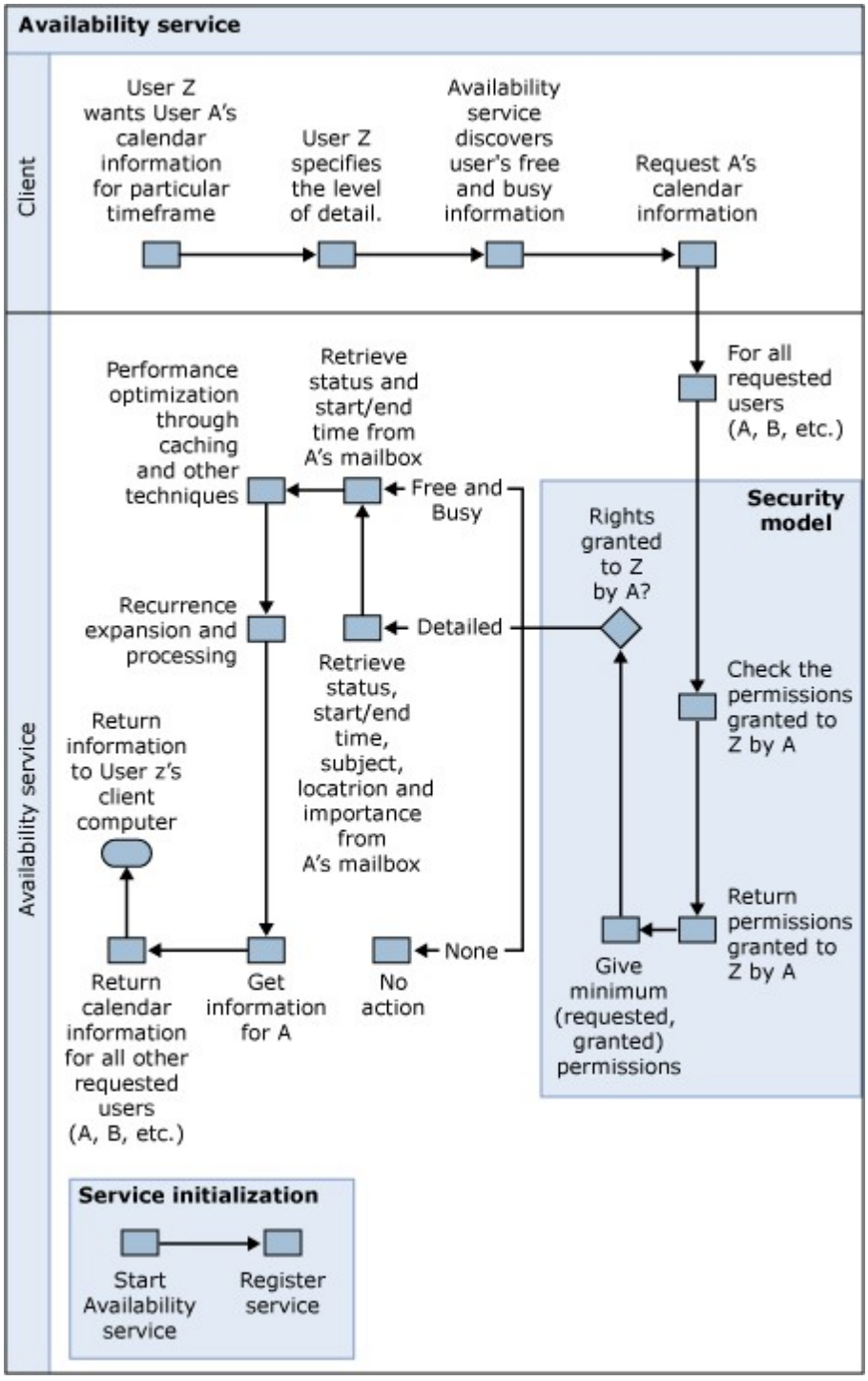
Outlook 2007 uses the Exchange Server 2010 Autodiscover service to obtain the URL of the Availability service. For more information about the Autodiscover service, see Managing the Autodiscover Service.

The Availability service is part of the Exchange 2010 programming interface. It is available as a public Web service to allow developers to write third-party tools for integration purposes.

You can use the Exchange Management Shell to configure the Availability service. You can't use the Exchange Management Console to configure the Availability service.

Availability Service Process Flow

The following figure illustrates the process flow for the Availability service.



Return to top

Improvements Over Exchange 2003 Free/Busy

The following table lists the improvements to free/busy functionality that Exchange 2010

and Exchange 2007 provide over Exchange 2003.

Free/busy improvements

Free/busy component	Outlook 2003 running on Exchange 2003	Outlook 2007 running on Exchange 2010 or Exchange 2007
Up-to-date information	There was no guarantee that free/busy information was up-to-date. There were multiple factors that caused free/busy information to be outdated: • By default, Outlook only updated free/busy information every 45 minutes. Also, because of bandwidth and scalability issues, you could not decrease this interval. • There were latencies that resulted from public folder replication. • In cross-forest scenarios, there were delays when you used the Microsoft Exchange Inter-Organization Replication tool to replicate free/busy information across forests.	Free/busy information is guaranteed to be up to date within a small time period (60 seconds) on all the data retrieved.
Granularity	The four meeting states (**Free**, **Tentative**, **Busy**, and **Out-Of-Office**) were available in one stream. To retrieve appointment details, additional MAPI calls were required.	By default, free/busy information displays the start and end times for individual appointments. Additional calendar properties (such as **Subject** and **Location**) will be available through the Availability service.
Security	For any authenticated user, all free/busy data was available in a public folder. This meant that any authenticated user could delete, modify, or publish another user's free/busy information.	Free/busy information provides increased security, similar to general calendar sharing. In compliance with your company's policy, you can specify how much free/busy information to share with a specific user. Because the Availability service reads directly from a user's mailbox, a user cannot modify or publish another user's free/busy information.
Publishing frequency	Outlook 2003 has a 45-minute default publishing interval.	No publishing is required in an Exchange 2010 and Outlook 2007 organization.

Return to top

Information About Away Status

The Availability service also provides access to automatic-reply messages that users send when they are out of the office or away for an extended period of time.

Information workers use the Automatic Replies feature (formerly known as Out of Office) in Outlook and Outlook Web App to alert others when they're unavailable to respond to e-mail messages. This functionality makes it easier to set and manage automatic-reply messages for both information workers and administrators.

For more information, see Managing Automatic Replies.

Performance

You can use the performance counters listed under **MSExchange Availability Service** in the Performance Monitor tool to automatically collect performance data about the Availability service from local or remote computers that are running Exchange 2010.

Return to top

Distribution Group Handling

In Exchange 2010, distribution group expansion is processed on the Exchange 2010 server instead of on the Outlook client. In Exchange 2007, distribution group expansion is processed on the Exchange 2007 server. The primary benefit of moving distribution group expansion to Exchange 2010 is to provide consistent behavior for any Availability service consumer. In Exchange 2003 and earlier versions of Exchange, if the number of users in a distribution group was too large, the free/busy data for the distribution group members would not display when the group was expanded.

In Exchange 2010, the following improvements have been made to the handling of distribution groups:

- The Availability service expands a distribution group up to only two-levels deep, regardless of the total number of distribution group members.
- A distribution group's free/busy data can expand up to a maximum of one hundred members.

Availability Service API

The Availability service is part of the Exchange 2010 programming interface. It's available as a Web service to let developers write third-party tools for integration purposes.

Availability Service Network Load Balancing

Using Network Load Balancing (NLB) on your Client Access servers that are running the Availability service can improve performance and reliability for your users who rely on free/busy information. Outlook 2007 discovers the Availability service URL using the Autodiscover service. To use network load balancing with the Availability service, you must make changes to your configuration.

The internal URL is used from the intranet, and the external URL is used from the Internet. If you want to use the same URL for both internal and external traffic, make sure that DNS is correctly configured to route internal traffic directly to the internal URL. Also, make sure that the URL can be accessed both internally and externally. For the Autodiscover and Availability services to work, DNS must be configured so that mail.<*domain name*>.com and autodiscover.mail.<*domain name*>.com point to the Network Load Balancing (NLB) array of Client Access servers, where <*domain name*> is the name of your domain.

Note:

For more information, see Network Load Balancing Technical Reference and Network Load Balancing Clusters. You can also search for third-party load-balancing software Web sites.

For information, see Configure the Availability Service for Network Load Balanced Computers.

Return to top

Methods Used to Retrieve Free/Busy Information

The following table lists the different methods used to retrieve free/busy information in different single-forest topologies.

Client	Mailbox retrieving free/busy information is running	Target mailbox is running	Free/busy retrieval method
Outlook 2007	Exchange 2010 or Exchange 2007	Exchange 2010 or Exchange 2007	The Availability service reads free/busy information from the target mailbox.
Outlook 2007	Exchange 2010 or Exchange 2007	Exchange 2003	The Availability service makes HTTP connections to the /public virtual directory of the Exchange 2003 mailbox.
Outlook 2003	Exchange 2010 or Exchange 2007	Exchange 2010 or Exchange 2007	Free/busy information is published in local public folders.
Outlook 2003	Exchange 2010 or Exchange 2007	Exchange 2003	Free/busy information is published in local public folders.
Outlook Web App	Exchange 2010 or Exchange 2007	Exchange 2010 or Exchange 2007	Outlook Web App in Exchange 2010 or Outlook Web Access in Exchange 2007 calls the Availability service API, which reads the free/busy information from the target mailbox.

Outlook Web App	Exchange 2010 or Exchange 2007	Exchange 2003	Outlook Web App in Exchange 2010 or Outlook Web Access in Exchange 2007 calls the Availability service API, which makes an HTTP connection to the /public virtual directory of the Exchange 2003 mailbox.
Any	Exchange 2003	Exchange 2010 or Exchange 2007	Free/busy information is published in local public folders.

Return to top

1.6.1.10 Understanding Client Access Server Publishing

Understanding Client Access Server Publishing

Exchange Server 2010 > Client Access > Understanding Client Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-20*

When you publish Microsoft Exchange for access from the Internet, Microsoft offers two software-based options: Microsoft Forefront Threat Management Gateway 2010 and Microsoft Forefront Unified Access Gateway 2010. Both options offer publishing wizards and security features to provide secure access to Exchange when it's accessed from outside the safety of the corporate network. For more information about Forefront Unified Access Gateway 2010 and Forefront Threat Management Gateway 2010, see Publishing Exchange Server 2010 with Forefront Unified Access Gateway 2010 and Forefront Threat Management Gateway 2010.

1.6.1.11 Understanding Client Access Security

Understanding Client Access Security

Exchange Server 2010 > Client Access > Understanding Client Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-20*

Security is an important aspect of any Microsoft Exchange Server 2010 installation. By default, all Exchange 2010 protocols, including Microsoft Office Outlook Web App, Microsoft Exchange ActiveSync, and the Autodiscover service are automatically configured for Secure Sockets Layer (SSL) connectivity. For more information about Exchange Client Access and SSL see Understanding Digital Certificates and SSL.

Installing a Client Access Server in a

Perimeter Network

It is not supported to locate an Exchange 2010 Client Access server in a perimeter network. Exchange 2010 Client Access servers have direct access to Exchange 2010 Mailbox servers.

Client Access Protocols and Security

Each of the various Exchange 2010 Client Access protocols has a variety of security settings you can configure for your organization. For more information, see the following topics.

- Understanding Security for Exchange ActiveSync
- Understanding Security for Outlook Anywhere
- Understanding Security for POP3 and IMAP4
- Understanding Security for Outlook Web App

1.6.1.11.1 Understanding Digital Certificates and SSL

Understanding Digital Certificates and SSL

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-04*

Secure Sockets Layer (SSL) is a method for securing communications between a client and a server. For a Microsoft Exchange Server 2010 Client Access server, SSL is used to help secure communications between the server and clients. Clients include mobile devices, computers inside an organization's network, and computers outside an organization's network. These include clients with and without virtual private network (VPN) connections.

By default, when you install Exchange 2010, client communications are encrypted using SSL when you use Microsoft Office Outlook Web App, Exchange ActiveSync, and Outlook Anywhere. By default, Post Office Protocol version 3 (POP3) and Internet Message Access Protocol Version 4 rev1 (IMAP4) aren't configured to communicate over SSL.

SSL requires that you use digital certificates. This topic summarizes the different types of digital certificates, and information about how to configure the Client Access server to use these types of digital certificates.

Note:

Cryptography Next Generation (CNG) certificates are not supported in Microsoft Exchange Server 2010.

Contents

Client Limitations

Overview of Digital Certificates

Digital certificates are electronic files that work like an online password to verify the identity of a user or a computer. They're used to create the SSL encrypted channel that's used for client communications. A certificate is a digital statement that's issued by a certification authority (CA) that vouches for the identity of the certificate holder and enables the parties to communicate in a secure manner using encryption.

Digital certificates do the following:

- They authenticate that their holders—people, Web sites, and even network resources such as routers—are truly who or what they claim to be.
- They protect data that's exchanged online from theft or tampering.

Digital certificates can be issued by a trusted third-party CA or a Microsoft Windows public key infrastructure (PKI) using Certificate Services, or they can be self-signed. Each type of certificate has advantages and disadvantages. Each type of digital certificate is tamper-proof and can't be forged.

Certificates can be issued for several uses. These uses include Web user authentication, Web server authentication, Secure/Multipurpose Internet Mail Extensions (S/MIME), Internet Protocol security (IPsec), Transport Layer Security (TLS), and code signing.

A certificate contains a public key and attaches that public key to the identity of a person, computer, or service that holds the corresponding private key. The public and private keys are used by the client and the server to encrypt the data before it's transmitted. For Windows-based users, computers, and services, trust in a CA is established when there's a copy of the root certificate in the trusted root certificate store and the certificate contains a valid certification path. For the certificate to be valid, the certificate must not have been revoked and the validity period must not have expired.

Types of Certificates

There are three primary types of digital certificates: self-signed certificates, Windows PKI-generated certificates, and third-party certificates.

Self-Signed Certificates

When you install Exchange 2010, a self-signed certificate is automatically configured. A self-signed certificate is signed by the application that created it. The subject and the name of the certificate match. The issuer and the subject are defined on the certificate. A self-signed certificate will allow some client protocols to use SSL for their communications. Exchange ActiveSync and Outlook Web App can establish an SSL connection by using a self-signed certificate. Outlook Anywhere won't work with a self-signed certificate. Self-signed certificates must be manually copied to the trusted root certificate store on the client computer or mobile device. When a client connects to a server over SSL and the server presents a self-signed certificate, the client will be prompted to verify that the certificate was issued by a trusted authority. The client must explicitly trust the issuing authority. If the client confirms the trust, then, SSL communications can continue.

Frequently, small organizations decide not to use a third-party certificate or not to install their own PKI to issue their own certificates. They might make this decision because those solutions are too expensive, because their administrators lack the experience and knowledge to create their own certificate hierarchy, or for both reasons. The cost is minimal and the setup is simple when you use self-signed certificates. However, it's much more difficult to establish an infrastructure for certificate life-cycle management, renewal, trust management, and revocation when you use self-signed certificates.

Windows Public Key Infrastructure Certificates

The second type of certificate is a Windows PKI-generated certificate. A PKI is a system of digital certificates, certification authorities, and registration authorities (RAs) that verify and authenticate the validity of each party that's involved in an electronic transaction by using public key cryptography. When you implement a PKI in an organization that uses Active Directory, you provide an infrastructure for certificate life-cycle management, renewal, trust management, and revocation. However, there is some additional cost involved in deploying servers and infrastructure to create and manage Windows PKI-generated certificates.

Certificate Services are required to deploy a Windows PKI and can be installed through **Add Or Remove Programs** in Control Panel. You can install Certificate Services on any server in the domain.

If you obtain certificates from a domain-joined Windows CA, you can use the CA to request or sign certificates to issue to your own servers or computers on your network. This enables you to use a PKI that resembles a third-party certificate vendor, but is less expensive. These PKI certificates can't be deployed publicly, as other types of certificates can be. However, when a PKI CA signs the requestor's certificate by using the private key, the requestor is verified. The public key of this CA is part of the certificate. A server that has this certificate in the trusted root certificate store can use that public key to decrypt the requestor's certificate and authenticate the requestor.

The steps for deploying a PKI-generated certificate resemble those required for deploying a self-signed certificate. You must still install a copy of the trusted root certificate from the PKI to the trusted root certificate store of the computers or mobile devices that you want to be able to establish an SSL connection to Microsoft Exchange.

A Windows PKI enables organizations to publish their own certificates. Clients can request and receive certificates from a Windows PKI on the internal network. The Windows PKI can renew or revoke certificates.

Trusted Third-Party Certificates

Third-party or commercial certificates are certificates that are generated by a third-party or commercial CA and then purchased for you to use on your network servers. One problem with self-signed and PKI-based certificates is that, because the certificate is not automatically trusted by the client computer or mobile device, you must make sure that you import the certificate into the trusted root certificate store on client computers and devices. Third-party or commercial certificates do not have this problem. Most commercial CA certificates are already trusted because the certificate already resides in the trusted root certificate store. Because the issuer is trusted, the certificate is also trusted. Using third-party certificates greatly simplifies deployment.

For larger organizations or organizations that must publicly deploy certificates, the best solution is to use a third-party or commercial certificate, even though there is a cost associated with the certificate. Commercial certificates may not be the best solution for small and medium-size organizations, and you might decide to use one of the other certificate options that are available.

Return to top

Choosing a Certificate Type

When you choose the type of certificate to install, there are several things to consider. A certificate must be signed to be valid. It can be self-signed or signed by a CA. A self-signed certificate has limitations. For example, not all mobile devices let a user install a digital certificate in the trusted root certificate store. The ability to install certificates on a mobile device depends on the mobile device manufacturer and the mobile service provider. Some manufacturers and mobile service providers disable access to the trusted root certificate store. In this case, neither a self-signed certificate nor a certificate from a Windows PKI CA can be installed on the mobile device.

Most mobile devices have several trusted third-party commercial certificates preinstalled. For the optimal user experience, implement certificate-based authentication for Exchange ActiveSync by using devices that are running Windows Mobile 6.0 or a later version and use a digital certificate from a trusted third-party CA.

Default Exchange Certificates

By default, Exchange installs a default self-signed certificate so that all network communication is encrypted. Encrypting all network communication requires that every Exchange server have an X.509 certificate that it can use. You should replace this self-signed certificate with one that is automatically trusted by your clients.

"Self-signed" means that a certificate was created and signed only by the Exchange server itself. Because it wasn't created and signed by a generally trusted CA, the default self-signed certificate won't be trusted by any software except other Exchange servers in the same organization. The default certificate is enabled for all Exchange services. It has a Subject Alternative Name (SAN) that corresponds to the server name of the Exchange server that it's installed on. It also has a list of SANs that include both the server name and the fully qualified domain name (FQDN) of the server.

Although other Exchange servers in your Exchange organization trust this certificate automatically, clients like Web browsers, Outlook clients, mobile phones, and other e-mail clients in addition to external e-mail servers won't automatically trust it. Therefore, consider replacing this certificate with a trusted third-party certificate on your Exchange servers that have the Client Access server role installed and also on any external-facing Hub Transport servers. If you have your own internal PKI, and all your clients trust that entity, you can also use certificates that you issue yourself.

Certificate Requirements by Service

Certificates are used for several things in Exchange. Most customers also use certificates on more than one Exchange server. In general, the fewer certificates you have, the easier certificate management becomes.

IIS

All the following Exchange services use the same certificate on a given Exchange server:

- Outlook Web App
- Exchange Control Panel
- Exchange Web Services
- Exchange ActiveSync
- Outlook Anywhere
- Autodiscover
- Outlook Address Book distribution

Because only a single certificate can be associated with a Web site, and because all these services are offered under a single Web site by default, all the names that clients of these services use must be in the certificate (or fall under a wildcard name in the certificate).

POP/IMAP

Certificates that are used for POP or IMAP can be specified separately from the certificate that's used for IIS. However, to simplify administration, we recommend that you include the POP or IMAP service name in your IIS certificate and use a single certificate for all these services.

SMTP

A separate certificate can be used for each receive connector that you configure on your Hub Transport servers or Edge Transport servers. The certificate must include the name that SMTP clients (or other SMTP servers) use to reach that connector. To simplify certificate management, consider including all names for which you have to support TLS traffic in a single certificate.

Live Federation

The certificate that's used for federating with Windows Live for Exchange sharing scenarios can include any name. During the federation process, you identify the certificate that you want your Exchange server to use. This certificate must be issued by a third-party certification authority that's trusted by Windows Live. If you get your Exchange certificate for other services from a third-party certification authority that's trusted by Windows Live, you can use a single certificate for those services and also for federation with Windows Live.

Unified Messaging

When you connect Exchange Unified Messaging servers to Microsoft Office Communications Server 2007 R2 servers or to third-party SIP gateways or Private Branch eXchange (PBX) telephony equipment, you can use self-signed or trusted third-party certificates in order to establish secured sessions. You can use a single certificate on all the Unified Messaging servers as long as the certificate has the FQDNs of all the Unified Messaging servers in its SAN list. Or, you will have to generate a different certificate for each Unified Messaging server, wherein the FQDN of the Unified Messaging server is present in the subject common name (CN) or SAN lists. Exchange Unified Messaging doesn't support wildcard certificates with Communications Server 2007 and Communications Server 2007 R2.

Outlook Web App Instant Messaging with Office Communications Server 2007 R2

Outlook Web App in Exchange 2010 includes a programming interface that allows instant messaging providers to write add-ins to control presence and instant messaging functionality. An add-in exists for Communications Server 2007 R2. When you use this add-in, you must use a certificate to secure the connection between the Communications Server 2007 R2 server and the Exchange 2010 Client Access server. The certificate must be installed on the Exchange Client Access servers. You can use multiple certificates or a single certificate on all Exchange 2010 Client Access servers, as long as one of the host names in the certificate CN or SAN is present in the Host Authorization List on the Communications Server. This value can be any host name which is available in the certificate, for example mail.contoso.com. Wildcard certificates aren't supported for establishing secure connections to Communications Server 2007 or 2007 R2.

Legacy Exchange Servers

If you follow the best practices for transitioning from Microsoft Exchange Server 2003 or Exchange Server 2007 to Exchange 2010, you'll be introducing a new host name - legacy.contoso.com for use during the coexistence period when you have mailboxes both on legacy versions of Exchange and on Exchange 2010. This legacy host name should also be included in the certificate that you use. For more information about how to upgrade from Exchange Server 2003 and Exchange 2007 to Exchange 2010, see Upgrade from Exchange 2003 Client Access and Upgrade from Exchange 2007 Client Access.

Return to top

Digital Certificates and Proxying

Proxying is the method by which one Client Access server sends client connections to another Client Access server. There are two scenarios where one Client Access server will proxy traffic to another Client Access server.

1. Client Access servers in an Internet-facing Active Directory site will proxy traffic to Client Access servers in a non-Internet-facing site. This ensures that all processing of client requests is handled as close to the client's Mailbox server as possible.
2. Client Access servers for Exchange 2010 will proxy connections from clients that have mailboxes on Exchange 2003 or Exchange 2007. These client connections will be proxied to Exchange 2007 Client Access servers. This happens because, for many Exchange services, the Client Access server can't

process requests for Mailbox servers that are running an older version of Exchange.

When Client Access servers proxy requests, SSL is used for encryption but not for authentication. In most cases, a self-signed certificate can be used for Client Access server proxying. If your organization requires extraordinary security rules, there's a configuration key you can set to require trusted certificates for Client Access server proxying. You can configure the following key by setting it to false for this scenario:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeOWA
\AllowInternalUntrustedCerts

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

For more information about proxying, see Understanding Proxying and Redirection.

Reverse Proxies and Certificates

Most Exchange deployments use reverse proxies to publish Exchange services on the Internet. Examples of popular Reverse Proxy products are Microsoft Internet Security and Acceleration (ISA) Server and Checkpoint. These reverse proxies can be configured to terminate SSL encryption, examine the traffic in the clear on the server, and then open a new SSL encryption channel from the reverse proxy server to the Exchange servers behind them. This is known as SSL bridging. Another way to configure the reverse proxy servers is to let the SSL connections pass straight through to the Exchange servers behind the reverse proxy servers. With either deployment model, the clients on the Internet connect to the reverse proxy server using a host name for Exchange access, such as mail.contoso.com. Then the reverse proxy server connects to Exchange using a different host name, such as the machine name of the Exchange Client Access server. You don't have to include the machine name of the Exchange Client Access server on your certificate because most common reverse proxy servers are able to match the original host name that's used by the client to the internal host name of the Exchange Client Access server.

Load Balancing and Certificates

If you have more than one Client Access server, consider configuring a Client Access server array. This array will allow all clients to connect to your Exchange Client Access servers through a single host name. You can add as many Client Access server computers as you want to one Client Access server array provided that all the Client Access servers are located within the same Active Directory site. For more information about load balancing and Client Access server arrays, see Understanding Proxying and Redirection and Managing Client Access Servers.

SSL and Split DNS

Split DNS is a technology that allows you to configure different IP addresses for the same host name, depending on where the originating DNS request came from. This is also known as split-horizon DNS, split-view DNS, or split-brain DNS. Split DNS can help you reduce the number of host names that you must manage for Exchange by allowing your clients to connect to Exchange through the same host name whether they're connecting from the Internet or from the Intranet. Split DNS allows requests that originate from the Intranet to receive a different IP address than requests that originate from the Internet.

Split DNS is usually unnecessary in a small Exchange deployment because users can access the same DNS endpoint whether they're coming from the Intranet or the Internet. However, with larger deployments, this configuration will result in too high of a load on your outgoing Internet proxy server and your reverse proxy server. For larger deployments, configure split DNS so that external users access mail.contoso.com and internal users access internal.contoso.com. Using split DNS for this configuration ensures that your users won't have to remember to use different host names depending on where

they're located.

Remote PowerShell

Kerberos authentication and Kerberos encryption are used for Remote PowerShell access, both from the Exchange Management Console and the Exchange Management Shell. Therefore, you won't have to configure your SSL certificates for use with Remote PowerShell.

Return to top

Digital Certificates Best Practices

Although the configuration of your organization's digital certificates will vary based on its specific needs, information about best practices has been included to help you choose the digital certificate configuration that's right for you.

Best Practice: Use a Trusted Third-Party Certificate

To prevent clients from receiving errors regarding untrusted certificates, the certificate that's used by your Exchange server must be issued by someone that the client trusts. Although most clients can be configured to trust any certificate or certificate issuer, it's simpler to use a trusted third-party certificate on your Exchange server. This is because most clients already trust their root certificates. There are several third-party certificate issuers that offer certificates configured specifically for Exchange. You can use the Exchange Management Console to generate certificate requests that work with most certificate issuers.

How to Select a Certification Authority

A certification authority is a company that issues and ensures the validity of certificates. Client software (for example, browsers such as Microsoft Internet Explorer, or operating systems such as Windows or Mac OS) have a built-in list of CAs they trust. This list can usually be configured to add and remove CAs, but that configuration is often cumbersome. Use the following criteria when you select a CA to buy your certificates from:

- Ensure the CA is trusted by the client software (operating systems, browsers, and mobile phones) that will connect to your Exchange servers.
- Choose a CA that says it supports "Unified Communications certificates" for use with Exchange server.
- Make sure that the CA supports the kinds of certificates that you'll use. Consider using Subject Alternative Name (SAN) certificates. Not all CAs support SAN certificates, and other CAs don't support as many host names as you might need.
- Make sure that the license you buy for the certificates allows you to put the certificate on the number of servers that you intend to use. Some CAs only allow you to put a certificate on one server.
- Compare certificate prices between CAs.

Best Practice: Use SAN Certificates

Depending on how you configure the service names in your Exchange deployment, your Exchange server may require a certificate that can represent multiple domain names. Although a wildcard certificate, such as one for *.contoso.com, can resolve this problem, many customers are uncomfortable with the security implications of maintaining a certificate that can be used for any sub-domain. A more secure alternative is to list each of the required domains as SANs in the certificate. By default, this approach is used when certificate requests are generated by Exchange.

Best Practice: Use the Exchange Certificate Wizard to Request Certificates

There are many services in Exchange that use certificates. A common error when

requesting certificates is to make the request without including the correct set of service names. The certificate request wizard in the Exchange Management Console will help you include the correct list of names in the certificate request. The wizard lets you specify which services the certificate has to work with and, based on the services selected, includes the names that you must have in the certificate so that it can be used with those services. Run the certificate wizard when you've deployed your initial set of Exchange 2010 servers and determined which host names to use for the different services for your deployment. Ideally you'll only have to run the certificate wizard one time for each Active Directory site where you deploy Exchange.

Instead of worrying about forgetting a host name in the SAN list of the certificate that you purchase, you can use a certification authority that offers, at no charge, a grace period during which you can return a certificate and request the same new certificate with a few additional host names.

Best Practice: Use As Few Host Names as Possible

In addition to using as few certificates as possible, you should also use as few host names as possible. This practice can save money. Many certificate providers charge a fee based on the number of host names you add to your certificate.

The most important step you can take to reduce the number of host names that you must have and, therefore, the complexity of your certificate management, is not to include individual server host names in your certificate's subject alternative names.

The host names you must include in your Exchange certificates are the host names used by client applications to connect to Exchange. The following is a list of typical host names that would be required for a company named Contoso:

- **Mail.contoso.com** This host name covers most connections to Exchange, including Microsoft Office Outlook, Outlook Web App, Outlook Anywhere, the Offline Address Book, Exchange Web Services, POP3, IMAP4, SMTP, Exchange Control Panel, and ActiveSync.
- **Autodiscover.contoso.com** This host name is used by clients that support Autodiscover, including Microsoft Office Outlook 2007 and later versions, Exchange ActiveSync, and Exchange Web Services clients.
- **Legacy.contoso.com** This host name is required in a coexistence scenario with Exchange Server 2003 or Exchange 2007. If you'll have clients with mailboxes on both a legacy version of Exchange and Exchange 2010, configuring a legacy host name prevents your users from having to learn a second URL during the upgrade process. For more information about upgrade and coexistence, see Upgrade from Exchange 2003 Client Access and Upgrade from Exchange 2007 Client Access.

Understanding Wildcard Certificates

A wildcard certificate is designed to support a domain and multiple subdomains. For example, configuring a wildcard certificate for *.contoso.com results in a certificate that will work for mail.contoso.com, web.contoso.com, and autodiscover.contoso.com.

Return to top

Client Limitations

Several Exchange clients limit the certificates they support. These clients and their limitations are summarized as follows:

- **Outlook on Windows XP or earlier operating systems** The Windows RPC over HTTP component used for Outlook Anywhere requires that the SAN or common name of the certificate must match the Certificate Principal Name configured for Outlook Anywhere. Outlook 2007 and later versions use Autodiscover to obtain this Certificate Principal Name. To configure this value on your Exchange 2010 Client Access server, use the **Set-OutlookProvider**

command with the *-CertPrincipalName* parameter. Set this parameter to the external host name that Outlook clients use to connect to Outlook Anywhere.

- **Versions of Outlook earlier than Outlook 2010 don't support SAN certificates for POP3 and IMAP4 access** A hotfix is available for SAN support in Outlook 2007 Service Pack 2. That hotfix can be found here.
- **Mobile devices** Some mobile devices, including those running Windows Mobile 5.0 and some Palm devices, don't support wildcard certificates.

1.6.1.11.2 Understanding Security for Exchange ActiveSync

Understanding Security for Exchange ActiveSync

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-25*

When you allow mobile phones or other mobile devices to synchronize with your Exchange 2010 server, you allow sensitive corporate information to be stored on small, portable devices that can be easily lost or stolen. Before you deploy Exchange ActiveSync, we recommend that you familiarize yourself with the various security settings you can configure to keep your corporate information safe. You can configure an authentication method for Exchange ActiveSync, deploy Exchange ActiveSync mailbox policies, and use remote device wipe to remove personal and corporate data from a lost or stolen mobile phone.

Exchange ActiveSync Server Security

There are several security-related tasks you can perform on a server that's running Exchange ActiveSync. One of the most important tasks is to configure an authentication method. Exchange ActiveSync runs on a computer running Exchange 2010 that has the Client Access server role installed. This server role is installed with a default self-signed digital certificate. Although the self-signed certificate is supported for Exchange ActiveSync, it isn't the most secure method of authentication. For additional security, consider deploying a trusted certificate from a third-party commercial certification authority (CA) or a trusted Windows public key infrastructure (PKI) certification authority. For more information about how to configure a trusted digital certificate, see Configure SSL for Exchange ActiveSync.

Selecting an Authentication Method for Exchange ActiveSync

In addition to deploying a trusted digital certificate, you should consider the different authentication methods that are available for Exchange ActiveSync. By default, when the Client Access server role is installed, Exchange ActiveSync is configured to use Basic authentication with Secure Sockets Layer (SSL). To provide increased security, consider changing your authentication method to Digest authentication or Integrated Windows authentication.

Device Security

In addition to enhancing the security of the Exchange ActiveSync server, you should also consider enhancing the security of your users' mobile phones. There are several methods that you can use to enhance the security of mobile phones.

Exchange ActiveSync Mailbox Policies

Exchange ActiveSync for Exchange 2010 enables you to create Exchange ActiveSync mailbox policies to apply a common set of security settings to a collection of users. These settings include the following:

- Requiring a password
- Specifying the minimum password length
- Requiring numbers or special characters in the password
- Designating how long a mobile phone can be inactive before the user is required to re-enter the password
- Specifying that the mobile phone or mobile device be wiped if an incorrect password is entered more than a specific number of times

For more information about Exchange ActiveSync mailbox policies, see Managing Exchange ActiveSync with Policies.

Remote Device Wipe

Mobile phones can store sensitive data that belongs to your organization and provide access to many of your organization's resources. If a mobile phone is lost or stolen, that data can be compromised. Remote device wipe is a feature that enables the Exchange server to set a mobile phone to delete all data the next time that the mobile phone connects to the Exchange server. A remote device wipe effectively removes all synchronized information and personal settings from a mobile phone. This can be useful when a mobile phone is lost, stolen, or otherwise compromised.

Warning:

After a remote device wipe has occurred, data recovery is very difficult. However, no data removal process leaves a mobile phone or other mobile device as free from residual data as it is when it's new. Recovery of data from a mobile phone or other mobile device may still be possible using sophisticated tools.

For more information about remote device wipe, see Understanding Remote Device Wipe.

1.6.1.11.2.1 Configuring Authentication for Exchange ActiveSync

Configuring Authentication for Exchange ActiveSync

Understanding Client Access > Understanding Client Access Security > Understanding Security for Exchange ActiveSync >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-01*

Authentication is the process by which a client and a server verify their identities for transmitting data. In Microsoft Exchange Server 2010, authentication is used to determine whether a user or client that wants to communicate with the Exchange server is who or what it says it is. You can use authentication to verify that a device belongs to a particular individual or that a particular individual is trying to sign in to Microsoft Office Outlook Web App.

When you install Exchange 2010 and the Client Access server role, virtual directories are configured for several services. These include Outlook Web App, the Availability service, Unified Messaging, and Microsoft Exchange ActiveSync. By default, each virtual directory is configured to use an authentication method. For Exchange ActiveSync, the virtual directory is configured to use Basic authentication and Secure Sockets Layer (SSL). You can change the authentication method for your Exchange ActiveSync server by changing the authentication method on the Exchange ActiveSync virtual directory.

This topic summarizes the authentication methods available for your Exchange ActiveSync server. For Exchange ActiveSync, the client is the physical device used to synchronize with the Exchange 2010 server.

Looking for management tasks related to Exchange ActiveSync? See Managing Exchange ActiveSync.

Contents

Choosing an Authentication Method

There are three primary types of authentication you can choose for Exchange ActiveSync: Basic authentication, certificate-based authentication, and token-based authentication. When you install the Client Access server role on a computer that's running Exchange 2010, Exchange ActiveSync is configured to use Basic authentication with SSL. To establish the SSL connection, certificate-based authentication requires a mobile device to have a valid client certificate installed that was created for user authentication. In addition, the mobile device must have a copy of the trusted root certificate from the server. If you choose token-based authentication, you'll have to work with the token vendor for configuration.

Basic Authentication

Basic authentication is the simplest method of authentication. With Basic authentication, the server requests that the client submit a user name and a password. That user name and password are sent in clear text over the Internet to the server. The server verifies that the supplied user name and password are valid and grants access to the client. By default, this kind of authentication is enabled for Exchange ActiveSync. However, we recommend that you disable Basic authentication unless you're also deploying SSL. When you're using Basic authentication over SSL, the user name and password are still sent in plain text, but the communication channel is encrypted.

Certificate-Based Authentication

Certificate-based authentication uses a digital certificate to verify an identity. Other credentials are provided, in addition to the user name and password. These prove the identity of the user who's trying to access the mailbox resources that are stored on the Exchange 2010 server. A digital certificate consists of two components: the private key that's stored on the device and the public key that's installed on the server. If you configure Exchange 2010 to require certificate-based authentication for Exchange ActiveSync, only devices that meet the following criteria can synchronize with Exchange 2010:

- The device has a valid client certificate installed that was created for user authentication.
- The device has a trusted root certificate for the server to which the user is connecting to establish the SSL connection.

Deploying certificate-based authentication prevents users who have only a user name and password from synchronizing with Exchange 2010. As an additional level of security, the client certificate for authentication can be installed only when the device is connected to a domain-joined computer through either Desktop ActiveSync 4.5 or a later version in Windows XP or the Windows Mobile Device Center in Windows Vista or Windows 7.

Token-Based Authentication Systems

A token-based authentication system is a two-factor authentication system. Two-factor authentication is based on a piece of information the user knows, such as their password, and an external device that usually takes the form of a credit card or a key fob a user can carry with them. Each device has a unique serial number. In addition to hardware tokens, some vendors offer software-based tokens that can run on mobile devices.

Tokens work by displaying a unique number, typically six digits long, that changes every 60 seconds. When a token is issued to a user, it's synchronized with the server software. To authenticate, the user enters their user name, password, and the number that's currently displayed on the token. Some token-based authentication systems also require the user to enter a PIN.

Token-based authentication is a strong form of authentication. The disadvantage of token-based authentication is that you must install authentication server software and deploy the authentication software on every user's computer or mobile device. There's also the risk that the user can lose the external device. This can be financially costly because you'll need to replace lost external devices. However, the device is useless to a third party without the original user's authentication information.

Several companies issue token-based authentication systems. One company is RSA. Their product, SecurID, comes in many different forms, including a key fob and a credit card. A one-time authentication code is issued through the token. Each authentication code is valid for 60 seconds. Most tokens also have an expiration indicator on the device, for example, a series of dots that disappear as the length of time that the code has left decreases. This helps prevent a user from entering the correct code only to have it expire before the authentication process is complete. After authentication has finished, the user doesn't have to authenticate with a new code unless they're signed out, either by choice or because the device times out because of inactivity. For more information about how to configure a token-based authentication system, see the documentation for the particular system.

1.6.1.11.2.2 Configuring SSL and Exchange ActiveSync

Configuring SSL and Exchange ActiveSync

Understanding Client Access > Understanding Client Access Security > Understanding Security for Exchange ActiveSync >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-19*

By default, when you install the Client Access server role on a computer that's running Microsoft Exchange Server 2010, a Microsoft Exchange ActiveSync virtual directory is created on the default Internet Information Services (IIS) Web site on the Exchange server.

After you obtain a Secure Sockets Layer (SSL) certificate to use together with the Client

Access server on the default Web site or on the Web site where you host your Exchange ActiveSync virtual directory, you can configure the Web site to require SSL. You can enable SSL for all Web sites hosted by the Client Access server or enable SSL only for Exchange ActiveSync.

Configuring an Exchange ActiveSync virtual directory to use SSL is just one step in managing security for Exchange ActiveSync. For more information about how to manage security for Exchange ActiveSync, see Managing Exchange ActiveSync Security.

1.6.1.11.2.3 Configuring Exchange ActiveSync Policies

Configuring Exchange ActiveSync Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-06*

In Microsoft Exchange Server 2010, you can create Microsoft Exchange ActiveSync mailbox policies to apply a common set of policies or security settings to a collection of users. After you deploy Exchange ActiveSync in your Exchange 2010 organization, you can create new Exchange ActiveSync mailbox policies or modify existing policies. This topic discusses Exchange ActiveSync mailbox policies and how they can be managed in your Exchange 2010 organization.

Looking for management tasks related to Exchange ActiveSync policies? See Managing Exchange ActiveSync with Policies.

Important:

Windows Phone 7 mobile phones only support a subset of all Exchange ActiveSync mailbox policy settings. For a complete list, see Windows Phone 7 Synchronization.

Overview of Exchange ActiveSync Mailbox Policies

You can use Exchange ActiveSync mailbox policies to manage many different settings. These include the following:

- Require a password
- Specify the minimum password length
- Require a number or special character in the password
- Designate how long a device can be inactive before requiring the user to re-enter a password
- Wipe a device after a specific number of failed password attempts

For more information about all the settings you can configure, see Set-ActiveSyncMailboxPolicy.

Managing Exchange ActiveSync Mailbox Policies

After you install the Client Access server role on an Exchange 2010 computer, you can

create, configure, and manage Exchange ActiveSync mailbox policies. After you create an Exchange ActiveSync mailbox policy, you can add users individually or add a filtered list of users to the policy using the Exchange Management Shell.

You can use the Exchange Management Console to manage some Exchange ActiveSync mailbox policy settings and the Shell to manage all the Exchange ActiveSync mailbox policy settings.

Windows Phone 7 Synchronization

If you have Windows Phone 7 mobile phones in your organization, these phones will experience synchronization problems if certain Exchange ActiveSync mailbox policy properties are configured. To allow Windows Phone 7 mobile phones to synchronize with an Exchange mailbox, either set the **AllowNonProvisionableDevices** property to True or only configure the following Exchange ActiveSync mailbox policy properties:

- PasswordRequired
- MinPasswordLength
- IdleTimeoutFrequencyValue
- DeviceWipeThreshold
- AllowSimplePassword
- PasswordExpiration
- PasswordHistory
- DisableRemovableStorage
- DisableIrDA
- DisableDesktopSync
- BlockRemoteDesktop
- BlockInternetSharing

1.6.1.11.3 Understanding Security for Outlook Anywhere

Understanding Security for Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-13*

There are several methods available to help secure Outlook Anywhere (formerly known as RPC over HTTP). In a Microsoft Exchange Server 2010 messaging environment enabled for Outlook Anywhere, users can access Exchange from the Internet. When a user accesses their mailbox over the Internet using Outlook Anywhere, each time they create or update their Outlook profile, the Autodiscover service automatically detects their Outlook profile information and provides the user access to Exchange Web services including the Offline Address Book, the Availability service, and Unified Messaging. Because traffic on the Internet is vulnerable to interception and attack, consider a security strategy that involves as many security options as possible.

Looking for management tasks related to Outlook Anywhere? See Managing Outlook Anywhere.

Contents

Using an Advanced Firewall Server for Outlook Anywhere

Using an advanced firewall server such as Microsoft Internet Security and Acceleration (ISA) Server 2006 improves security for your Outlook Anywhere deployment. ISA Server 2006 provides a setup wizard that lets you configure ISA Server 2006 for Exchange 2010 to work with Outlook Anywhere. For more information, see Using ISA Server with Outlook Anywhere.

Using SSL with Outlook Anywhere

When you use Outlook Anywhere to access Exchange information from the Internet, you must install a valid Secure Sockets Layer (SSL) certificate issued by a certification authority (CA) that's trusted by the client computer's operating system. For more information about how to use SSL certificates for client access, see Understanding Digital Certificates and SSL. For more information about how to use SSL with Outlook Anywhere, see Configure SSL for Outlook Anywhere.

For Outlook 2007 and Outlook 2010 clients that are located outside the organization, Outlook Anywhere provides connectivity to the Exchange organization. In this situation, Outlook 2007 or Outlook 2010 uses Domain Name System (DNS) to locate information about how to connect to the Autodiscover service. Because DNS is open to several kinds of malicious attacks, Outlook 2007 and Outlook 2010 request Autodiscover service information from only two URL combinations secured by SSL.

For an organization named www.contoso.com that has e-mail addresses that are derived from the main site name, for example, kwekua@contoso.com, the two URL combinations would be formed as follows:

1. Outlook will first try the URL https://contoso.com/autodiscover/autodiscover.xml.
2. If the previous URL cannot locate the Autodiscover service, Outlook will then try https://autodiscover.contoso.com/autodiscover/autodiscover.xml.

Return to top

Choosing an SSL Deployment Option for Outlook Anywhere

There are several ways to use Secure Sockets Layer (SSL) to help secure communication between Outlook 2007 and Outlook 2010 clients and the Autodiscover service. With Outlook Anywhere, Outlook clients query DNS for the Autodiscover service connection point. We recommend that you use the Subject Alternative Name field on your SSL certificate to help secure communication between clients and the Client Access server

that's hosting the Autodiscover service. For more information about how to configure the Subject Alternative Name for an SSL certificate, see Configure SSL Certificates to Use Multiple Client Access Server Host Names.

Alternatively, you can use multiple SSL certificates. For more information, see Configure Outlook Anywhere to Use Multiple SSL Certificates.

Another option is to use an SSL certificate together with redirection. For more information, see Configure Outlook Anywhere to Use an SSL Certificate with Redirection.

Using SSL Offloading for Outlook Anywhere

If you have a hardware solution for offloading the SSL encryption for traffic that's destined for your Client Access server, you must configure SSL offloading for Outlook Anywhere. For more information, see Configure SSL Offloading for Outlook Anywhere.

Return to top

Configuring Authentication for Outlook Anywhere

When you use the Enable Outlook Anywhere wizard to configure your Client Access server to provide Outlook Anywhere access, you must select an authentication method for your Outlook clients to use. After you select an authentication method, you can change this method by using the **Set-OutlookAnywhere** cmdlet in the Exchange Management Shell.

Understanding Authentication for Outlook Anywhere and the RPC Virtual Directory

The authentication method you select for Outlook Anywhere is the authentication method that will be used by the Outlook 2007 or Outlook 2010 client. This authentication method is automatically provided to the client by the Autodiscover service. You choose the authentication type for the RPC virtual directory when you enable Outlook Anywhere. You can choose to allow Basic authentication, NTLM authentication, or both Basic authentication and NTLM authentication. You may want to enable both Basic and NTLM authentication if you're using the IIS virtual directory with multiple applications that require different authentication methods.

Note:

When you configure this setting using the IIS interface, you can enable as many authentication methods as you want.

The authentication method on the RPC virtual directory can be modified by using the **Set-OutlookAnywhere** cmdlet. For more information, see Configure Authentication for Outlook Anywhere.

Return to top

Basic Authentication and Outlook Anywhere

You can use Basic authentication with Outlook Anywhere. Basic authentication requires a user name and password, and then sends the user name and password over the Internet in plain text. As long as you use Secure Sockets Layer (SSL) to help secure the

connection between the Microsoft Office Outlook Web App client and the Exchange messaging infrastructure, using Basic authentication with Outlook Anywhere is supported. For more information, see Configure Authentication for Outlook Anywhere.

Integrated Windows Authentication and Outlook Anywhere

ISA Server 2006 supports using Integrated Windows authentication for Outlook Anywhere. However, if you're using a firewall that doesn't handle Integrated Windows authentication, you must use Basic authentication with SSL. For more information, see Configure Authentication for Outlook Anywhere.

Return to top

1.6.1.11.4 Understanding Security for POP3 and IMAP4

Understanding Security for POP3 and IMAP4

Client Access > Understanding Client Access > Understanding Client Access Security >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

This topic explains security settings that you can use on the Microsoft Exchange Server 2010 Client Access server that has the POP3 and IMAP4 services installed.

Looking for management tasks related to POP3 and IMAP4? See Managing POP3 and IMAP4.

Configuring SSL and TLS for POP3 and IMAP4 Clients

To help secure communications between POP3 and IMAP4 clients and the Exchange 2010 Client Access server, we strongly recommend that you use Secure Sockets Layer (SSL) or Transport Layer Security (TLS). By default, Exchange Setup provides a self-signed certificate for test environments. However, we recommend that you install a certificate from a certification authority (CA) that's trusted by the client's operating system. For more information, see Managing SSL for a Client Access Server.

You can use the Exchange Management Console or the Exchange Management Shell to configure SSL or TLS for POP3 and IMAP4 on an Exchange 2010 server.

For more information about how to use the EMC or the Shell to configure SSL or TLS for POP3 and IMAP4, see the following topics:

- Configure POP3 to Use TLS or SSL
- Configure IMAP4 to Use TLS or SSL

Configuring Authentication for POP3 and IMAP4

When you use POP3 and IMAP4 clients, you can set authentication options such as the ability to use SSL or TLS encryption and the ability to configure ports to communicate with clients. When you use SSL or TLS for POP3 and IMAP4 access, the Exchange server uses the ports listed in the following table to communicate with clients.

Ports for POP3 and IMAP4 access when using SSL

Protocol	Default port
IMAP4 with SSL	993 (TCP)
IMAP4 with or without TLS	143 (TCP)
POP3 with SSL	995 (TCP)
POP3 with or without TLS	110 (TCP)

By default, the values in the previous table are used for communicating with clients. You can specify other ports to use with POP3 and IMAP4 clients if you want to disable communication through the default ports.

For more information about how to configure authentication for POP3, see the following topics:

- Configure Authentication for POP3
- Configure Ports for POP3 Authentication

For more information about how to configure authentication for IMAP4, see the following topics:

- Configure Authentication for IMAP4
- Configure Ports for IMAP4 Authentication

1.6.1.11.5 Understanding Security for Outlook Web App

Understanding Security for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-06-30*

Outlook Web App for Microsoft Exchange Server 2010 offers a variety of security features that you can configure to suit your organization's security requirements. Because Outlook Web App may be used to provide users access to their mailboxes from workstations that are not secure, security is a priority. By default, when you install the Client Access server role on an Exchange 2010 server, Outlook Web App is configured to use Secure Sockets Layer (SSL) and forms-based authentication.

Looking for management tasks related to securing Outlook Web App? See Managing Outlook Web App Security.

Contents

Authentication

You can configure the following types of authentication methods on the Exchange 2010 Client Access server:

- Standard authentication methods such as the following:
  - Basic authentication
  - Integrated Windows authentication
  - Digest authentication
- Forms-based authentication

For more information about authentication methods for Outlook Web App, see Understanding Authentication for Outlook Web App.

Segmentation

Segmentation lets you enable and disable features that are available to users in Exchange 2010 Outlook Web App. By default, any mail-enabled user in your Exchange 2010 organization can access their mailbox by using Outlook Web App. Depending on the needs of your organization, you can use segmentation to configure the following for user access:

- Restrict access to Outlook Web App for specific users.
- Control access to certain Outlook Web App features for specific users.
- Disable an Outlook Web App feature completely.

For more information about segmentation in Outlook Web App, see Understanding Segmentation for Outlook Web App.

Web Beacons

A Web beacon is a file object, such as a transparent graphic or an image, which is put on a Web site or in an e-mail message. Web beacons are typically used together with HTML cookies to monitor user behavior on a Web site or to validate a recipient's e-mail address when an e-mail that contains a Web beacon is opened.

Note:

By default, Outlook Web App disables all potential Web beacon content in e-mail messages.

For more information about how to deal with Web beacons in Outlook Web App, see Understanding Web Beacon and HTML Form Filtering in Outlook Web App.

File and Data Access

There are a variety of features that enable users to access files and data in Outlook Web App. Each of these features includes options for controlling access to files and data from Outlook Web App.

WebReady Document Viewing

Exchange 2010 includes a feature named WebReady Document Viewing. WebReady Document Viewing lets users view common file types in the Outlook Web App Web browser without having the applications that are associated with those file types installed on the computer they are using. Allowing files that are accessed through Outlook Web App to be viewed only by using WebReady Document Viewing protects against the potential security risk that is caused when files that are opened from within Outlook Web

App are cached on the client computer. For more information about how to configure file and data access for Outlook Web App, see Understanding Security for File and Data Access for Outlook Web App.

Return to top

Direct File Access

Direct file access enables users to open attached files directly from inside Outlook Web App. You can also configure how users interact with files by using the Allow, Block, or Force Save options for direct file access in the Exchange Management Console. This means that you can specify the types of files that users can access. More important, you can specify which types of files are prohibited.

For more information about how to configure file and data access for Outlook Web App, see Understanding Security for File and Data Access for Outlook Web App.

Windows File Share Integration

By using Outlook Web App, users can access remote files that are stored on Microsoft Windows file share (also known as UNC) servers. You can configure how users interact with files on these servers by using the Allow and Block options in the Exchange Management Console. This means that you can specify which servers your users can access. You can also specify the behavior for Windows file share servers that have not been specifically allowed or blocked when users try to access them by using Outlook Web App.

For more information about how to configure file and data access for Outlook Web App, see Understanding Security for File and Data Access for Outlook Web App.

Secure Sockets Layer

SSL is a method for securing communications between a client and a server. For a computer that is running Exchange 2010 that has the Client Access server role installed, SSL is used to help secure communications between the server and the clients. Clients include mobile phones, computers inside an organization's network, and computers outside an organization's network. These include clients that have and do not have virtual private network (VPN) connections.

For more information about SSL, see the following topics:

- Understanding Digital Certificates and SSL
- Understanding SSL for Outlook Web App

1.6.1.11.5.1 Understanding Segmentation for Outlook Web App

Understanding Segmentation for Outlook Web App

Understanding Client Access > Understanding Client Access Security > Understanding Security for Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

Segmentation lets you enable and disable features that are available to users in the version of Microsoft Office Outlook Web App released with Microsoft Exchange Server 2010. By default, any mail-enabled user in your Exchange 2010 organization can access

their mailbox using Outlook Web App. Depending on the needs of your organization, you can use segmentation to do the following:

- Restrict access to Outlook Web App for specific users.
- Control access to certain Outlook Web App features for specific users.
- Disable an Outlook Web App feature completely.

Looking for management tasks related to Outlook Web App features? See Managing Outlook Web App.

Configuring Segmentation

Many features can be set for an Outlook Web App virtual directory using the Exchange Management Console. You can also use the **Set-OwaVirtualDirectory** cmdlet in the Exchange Management Shell to enable or disable the same features that you can enable and disable using the EMC, plus some features that you can't configure using the EMC.

For more information about the parameters you can use to configure segmentation for all users, see Set-OwaVirtualDirectory.

For more information about the features that you can configure using the EMC and how to configure them, see Configure Segmentation in Outlook Web App.

For more information about how to enable and disable features for specific users, see Set-CASMailbox and Understanding Outlook Web App Mailbox Policies.

1.6.1.11.5.2 Understanding Security for File and Data Access for Outlook Web App

Understanding Security for File and Data Access for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-30*

There are two methods for accessing files and data from inside Outlook Web App. These data access methods include WebReady Document Viewing and direct file access. You can allow or block these features as needed to meet the requirements of your organization.

Looking for management tasks related to file and data access for Outlook Web App? See Configure WebReady Document Viewing, Configure Public and Private Computer File Access, and Set-OwaVirtualDirectory.

WebReady Document Viewing

Microsoft Exchange Server 2010 includes a feature named WebReady Document Viewing. WebReady Document Viewing lets users view common file types in the Outlook Web App Web browser without having the applications associated with those file types installed on the computer they're using. Users can view the following kinds of files using WebReady Document Viewing:

- .doc
- .pdf
- .ppt
- .xls

- .docx
- .xslx
- .pptx

Additionally, the supported MIME types are as follows:

- application/pdf
- application/vnd.ms-excel
- application/vnd.ms-powerpoint
- application/word
- application/x-mspowerpoint
- application/x-msexcel

Direct File Access

You can control direct file access through Outlook Web App by specifying the types of files that users can access and how the files can be accessed. You do this using the Allow, Block, and Force Save options for direct file access in the Exchange Management Console, or by using the file access parameters available in the **Set-OWAVirtualDirectory** cmdlet in the Exchange Management Shell. In addition to being able to specify Allow, Block, or Force Save for different file types, you can configure the file access options depending on whether the user clicks **This is a public computer** or **This is a private computer** when they sign in to Outlook Web App. For more information about how to manage file access, see Configure Public and Private Computer File Access and Set-OwaVirtualDirectory.

1.6.1.11.5.3 Understanding Web Beacon and HTML Form Filtering in Outlook Web App

Understanding Web Beacon and HTML Form Filtering in Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Web beacons frequently come in the form of images that are downloaded onto a user's computer when the user opens a junk e-mail message. After the images are downloaded, a Web beacon notification is sent to the sender of the junk e-mail message that informs the sender that the recipient e-mail address is valid. After a user opens a message that sends a Web beacon notification back to the junk e-mail sender, the user may receive junk e-mail more frequently because the junk e-mail sender has verified that the user's e-mail address is valid. Web beacons can also contain harmful code and can be used to circumvent e-mail filters to deliver an e-mail message from someone who is sending unsolicited commercial e-mail.

Note:

By default, Outlook Web App enables users to choose to allow or disable potential Web beacon content in individual e-mail messages.

Controlling Web Beacon and HTML Form Filtering

In Outlook Web App, an incoming e-mail message that contains content that can be used as a Web beacon prompts Outlook Web App to display a warning message to the user to inform the user that the content has been blocked. This occurs regardless of whether the

message actually contains a Web beacon. If a user knows that a message is legitimate, they can enable the blocked content. If a user does not recognize the sender of the message, they can open the message without unblocking the content, and then delete the message without triggering beacons. If your organization does not want to use this feature, you can disable the blocking option for Outlook Web App.

The settings for filtering Web beacons are stored in Active Directory. You can configure how potential Web beacon content is filtered by using the **Set-OwaVirtualDirectory** cmdlet in the Exchange Management Shell. For more information about syntax and parameters, see Set-OwaVirtualDirectory.

The following list describes the parameters in the *FilterWebBeacons* property for Web beacon filtering in Outlook Web App:

- **UserFilterChoice** By using the *UserFilterChoice* parameter, you can let users decide whether they want to enable or continue to disable the blocked Web beacon content. Outlook Web App blocks all potential Web beacon content in an e-mail message and displays the following message in the information bar when a user receives an e-mail message that contains potential Web beacon content: "To help protect your privacy, Outlook Web App has blocked some images, sounds, or forms that can communicate your information to other Web sites. If you are sure that this message is from a trusted sender and you want to re-enable the blocked features, Click Here." To view the blocked content, the user can click the **Click Here** option.

  Note:
  By default, the *UserFilterChoice* parameter is enabled in Outlook Web App.

- **ForceFilter** By using the *ForceFilter* parameter, you can block all potential Web beacon content. Outlook Web App blocks all potential Web beacon content in an e-mail message and displays the following message in the information bar when a user receives an e-mail message that contains potential Web beacon content: "To help protect your privacy, Outlook Web App has blocked some images, sounds, or forms that can communicate your information to other Web sites." Users cannot override the *ForceFilter* parameter to view the blocked Web beacon content.
- **DisableFilter** By using the *DisableFilter* parameter setting, you can enable all potential Web beacon content in Outlook Web App.

1.6.1.11.5.4 Understanding Authentication for Outlook Web App

Understanding Authentication for Outlook Web App

Understanding Client Access > Understanding Client Access Security > Understanding Security for Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-19*

This topic explains the types of authentication that are available for Outlook Web App in Microsoft Exchange Server 2010. The authentication method that's best for your organization depends on your organization's security needs. By default, Outlook Web App uses forms-based authentication and is configured to use Secure Sockets Layer (SSL) encryption.

Forms-Based Authentication

Forms-based authentication enables a sign-in page for Outlook Web App that uses a cookie to store a user's encrypted sign-in credentials in the Internet browser. Tracking the use of this cookie enables the Exchange server to monitor the activity of Outlook Web App sessions on public and private computers. If a session is inactive for too long, the server blocks access until the user re-authenticates.

The first time that the user name and password are sent to the Client Access server to authenticate an Outlook Web App session, an encrypted cookie is created that's used to track user activity. When the user closes the Internet browser or clicks **Sign Out** to sign out from their Outlook Web App session, the cookie is cleared. The user name and password are sent to the Client Access server only for the initial user sign-in. After the initial sign-in is complete, only the cookie is used for authentication between the client computer and the Client Access server.

For more information about forms-based authentication and how to configure it, see:

- Setting Up Forms-Based Authentication for Outlook Web App
- Configure Forms-Based Authentication for Outlook Web App

Single Sign On for Outlook Web App and Exchange Control Panel

To support single sign on between Outlook Web App and Exchange Control Panel, a new service, the Exchange FBA Authentication service, is available in Exchange 2010. To use this new feature, ensure that the authentication mode for both Outlook Web App and Exchange Control Panel virtual directories is set to forms-based authentication.

Setting the Value for Cookie Time-Out

The cookie time-out is set based on the user's choice of either the **This is a public or shared computer** option or the **This is a private computer** option on the Outlook Web App sign-in page. By default, the cookie on the computer expires automatically and the user is signed out after they haven't used Outlook Web App for between 15 and 22.5 minutes if they've selected the public computer option, and after they haven't used Outlook Web App for between eight and twelve hours if they've selected the private computer option.

Automatic time-out is valuable because it helps protect users' accounts from unauthorized access. To match the security requirements of your organization, you can configure the inactivity time-out values on the Exchange Client Access server.

Although automatic time-out greatly reduces the risk of unauthorized access, it doesn't completely eliminate the possibility that an unauthorized user might access an Exchange mailbox if a session is left running on a public computer. Therefore, make sure that you warn users to take precautions to avoid risks, such as by telling them to sign out from Outlook Web App and close the Web browser after they've finished using Outlook Web App.

For more information about how to configure the cookie time-out values for public and private computers, see:

- Set the Forms-Based Authentication Public Computer Cookie Time-Out Value
- Set the Forms-Based Authentication Private Computer Cookie Time-Out Value

Return to top

Standard Authentication Methods

In Exchange 2010, Client Access servers support Integrated Windows authentication and HTTP 1.1 Digest authentication for Exchange 2010 virtual directories.

For more information about standard authentication methods, see Setting Up Standard Authentication Methods for Outlook Web App.

Basic Authentication

Basic authentication is a simple authentication mechanism that's defined by the HTTP specification that encodes a user's sign-in name and password before the user's credentials are sent to the server.

Basic authentication doesn't support single sign-on. Windows Server 2008 and Windows Server 2003 authentication enable single sign-on to all network resources. With single sign-on, a user can sign in to the domain one time by using a single password or smart card and authenticate to any computer in the domain.

Basic authentication is supported by all Web browsers, but is not secure unless you require SSL encryption.

For more information about how to configure Basic authentication on an Outlook Web App virtual directory, see Configure Basic Authentication.

Digest Authentication

Digest authentication transmits passwords over the network as a hash value for additional security. Digest authentication can be used only in Windows Server 2008, Windows Server 2003, and Microsoft Windows 2000 Server domains for users who have an account that's stored in Active Directory. For more information about Digest authentication, see the Windows Server 2003 and Internet Information Services (IIS) Manager documentation.

Digest authentication is available only on Exchange 2010 virtual directories.

Important:

If you're using Digest or Basic authentication, when a user uses a kiosk, caching credentials can pose a security risk if the user doesn't close the browser and end the browser process between sessions. This risk occurs because a user's credentials remain in the cache when the next user accesses the kiosk. To enable Outlook Web App on a kiosk, make sure that the user can close the browser between sessions and end the browser processes. Otherwise, consider using a third-party product that incorporates two-factor authentication, in which the user must present a physical token together with a password to use Outlook Web App on a kiosk.

For more information about how to configure Digest authentication on an Outlook Web App virtual directory, see Configure Digest Authentication.

Return to top

Integrated Windows Authentication

Integrated Windows authentication requires that users have a valid Windows Server 2008, Windows Server 2003, or Windows 2000 Server user account name and password to access information. Users signed in to the local network aren't prompted for their user names and passwords. Instead, the server negotiates with the Windows security packages that are installed on the client computer. This method enables the server to authenticate users without prompting them for sign-in information. The authentication credentials are protected, but all other communication will be sent in clear text unless SSL is used.

Microsoft Internet Explorer allows single sign-on for Web applications that include Outlook Web App Web Parts if the server that's being accessed has Integrated Windows authentication enabled. Users must enter credentials only one time for each browser session. However, their credentials are cached in the browser process.

On an Exchange 2010 server on which only the Client Access server role is installed, Integrated Windows authentication can be used only with Exchange 2010 virtual directories. On a server that has both the Client Access and Mailbox roles installed, Integrated Windows authentication can be used with any virtual directory. For more information about Integrated Windows authentication, see the Windows Server 2003 documentation.

Note:

Integrated Windows authentication is supported only on computers that are running a Windows operating system and Internet Explorer. Integrated Windows authentication may work with other Web browsers if they've been configured to pass the user's sign-in credentials to the server that's requesting authentication.

For more information about how to configure Integrated Windows authentication on an Outlook Web App virtual directory, see Configure Integrated Windows Authentication.

1.6.1.11.5.5 Understanding SSL for Outlook Web App

Understanding SSL for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

Secure Sockets Layer (SSL) encryption is used in Outlook Web App to help secure the connection between the Exchange Server 2010 Client Access server and the client. By default, Outlook Web App uses forms-based authentication and requires SSL encryption.

Looking for management tasks related to using SSL in Outlook Web App? See Managing Outlook Web App Security.

SSL Encryption and Outlook Web App

When you install the Client Access server role, four Outlook Web App virtual directories are created in the default Internet Information Services (IIS) Web site on the Exchange server. The four virtual directories are named \owa, \exchange, \public, and \exchweb. By default, these virtual directories and the default Web site are configured to require SSL.

If you want to use SSL to help secure additional Outlook Web App virtual directories or Web sites that you have created, you must do so manually. To configure a site to use SSL, you must obtain a certificate and configure the Web site or virtual directory to require SSL by using that certificate.

1.6.1.12 Understanding RPC Client Access

Understanding RPC Client Access

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-09-21*

In Microsoft Exchange Server 2007, the Client Access server role was introduced to handle incoming client connections to Exchange mailboxes. Although the majority of types of client connections were made to the Client Access server, Microsoft Office Outlook still connected directly to the Mailbox server when it was running internally with the MAPI protocol.

A new service was introduced with Exchange Server 2010 to allow these MAPI connections to be handled by the Client Access server. The RPC Client Access service provides data access through a single, common path of the Client Access server, with the exception of public folder requests, which are still made directly to the Mailbox server. This change applies business logic to clients more consistently, and provides a better client experience when failover occurs.

Contents

RPC Client Access Service and the Address Book Service

In addition to moving processing of incoming Outlook Mailbox connections to the Client Access server, in Exchange 2010, directory access is also handled by the Client Access server. For more information about directory access, see Understanding the Address Book Service.

Microsoft Outlook still connects directly to the Mailbox server to access Public Folder databases. If a client tries to connect to a Mailbox server for public folder access, the RPC Client Access service (MsExchangeRpc) answers the RPC endpoint. If the endpoint is on a server that has the Mailbox server role installed, the RPC Client Access service will only allow public folder logons and will provide a referral to a Client Access server or a Client Access server array. If the endpoint is on a Client Access server or Client Access server array, it will allow only Private folder logons and will provide a referral to a Mailbox server for public folder access.

Advantages of the RPC Client Access Service

There are a number of advantages to the RPC Client Access service. Clients encounter less downtime during a mailbox failover, because all connections are made through the Client Access servers. When failover occurred in Exchange 2007, Outlook clients would be disconnected from the Mailbox server for a period of time that depended on their network configuration. In Exchange 2010, if a single Client Access server in a Client Access server array fails, the client will immediately be redirected to another Client Access server in the array. If a Mailbox server that is part of a Database Availability Group (DAG) fails, the client is disconnected for only the amount of time it takes for a failover database to be mounted.

A load-balanced array of Client Access servers lets you spread the traffic load over all Client Access servers in the array equally.

Other problems resolved by this new architecture include the following:

- Some issues with messages displaying differently on different clients.
- Problems uploading certificates to the global address list.
- The inability to create profiles for hidden users.
- Inconsistent application of business logic to clients.
- Public folders connecting to the RPC Client Access service on the Mailbox server, rather than the Client Access server.

Additionally, the DSProxy service has been removed and the new Address Book service is responsible for updating certificates and distribution list membership and maintaining delegate information for Outlook clients.

MAPI Client Connections

In Exchange 2007, Outlook and other MAPI clients communicated with the Client Access server for HTTPS connections such as Exchange Web Services (including the Availability service and Out of Office settings), and Offline Address Book downloads, but communicated directly with the MAPI RPC component on the Mailbox server and the NSPI endpoint on Global Catalog servers for Directory Service inquiries.

In Exchange 2010, these connections are made to the MAPI RPC connection point on the Client Access server or the Client Access server array.

The Address Book Service

In previous versions of Exchange, DSProxy, a referral service that told Outlook clients where to find the Name Service Provider Interface (NSPI) endpoint, was responsible for directing Outlook to a global catalog server. DSProxy was located on the Mailbox server. DSProxy has been eliminated in Exchange 2010 and replaced with the Address Book service.

Currently, when an Outlook client makes a request of the Client Access server, it results in one of two possible actions.

- If the user's mailbox is on an Exchange 2010 Mailbox server, then either the request is handled by a Client Access server in the current Active Directory site, or if the user’s mailbox is in a different Active Directory site, the request is proxied to the destination Active Directory site.
- If the user's mailbox is on a legacy Exchange Mailbox server, the directory request is referred to the user's Mailbox server. Legacy Mailbox servers can't communicate directly with Exchange 2010 Client Access servers for directory information.

The Address Book service also provides information about writable domain controllers as well as global address list access. For more information about the Address Book service, see Understanding the Address Book Service.

The Client Access Server Array

In addition to the RPC Client Access service, Exchange 2010 introduced a new logical structure to the Exchange organization: the Client Access server array. When a Client Access server array is defined in an Active Directory site, it serves as a single contact point for all client connections within that Active Directory site. A Client Access server array can include one or many Client Access servers.

Each Active Directory site can have a single Client Access server array. A Client Access server array doesn’t provide load balancing. A separate load balancing solution is still needed. For more information about load balancing, see Understanding Load Balancing in Exchange 2010.

We recommend that you create a Client Access server array even if you only have a single

Client Access server within your organization. When a Client Access server array is created, clients connect through the virtual name of the Client Access server array rather than directly to the fully-qualified domain name (FQDN) of your single Client Access server. If a single Client Access server needs to be replaced within an Active Directory site or a second Client Access server is added, no profile updates are necessary on the clients.

After a Client Access server array is defined within an Active Directory site, all Client Access servers within that Active Directory site are automatically part of the Client Access server array.

Configuring the RPC Client Access Service and the Address Book Service

To configure the RPC Client Access service and the Address Book service, you must perform the following steps.

1. Create a Client Access array
2. Configure load balancing
3. Configure IP ports
4. Configure RPC encryption settings
5. Configure your Mailbox databases
6. Ensure low latency and sufficient network speed

Create a Client Access Array

You can create a Client Access array within your Active Directory site by using the following command.

```
New-ClientAccessArray -Name name -Site site_name -FQDN internal_only_CAS_Array_FQ
```

Note:

After the Client Access array has been created, you'll also need to create the address in DNS and associate it with the virtual IP address used for the Client Access array.

It's important that the (FQDN) specified in the command be only resolvable internally. If the name is also resolvable externally, these external clients will attempt to connect to the array via a TCP connection instead of HTTPS.

Configure Load Balancing

Load balancing is recommended for high availability, failover, and for spreading the traffic load over multiple servers to help performance. When you choose a load balancing solution, consider the following:

- Windows Network Load Balancing isn't supported on Windows failover cluster servers.
- You can't use a Client Access array across multiple Active Directory sites. Instead, create two Client Access arrays and load balance separately within the sites.
- Hardware load balancers typically monitor return traffic, port availability, or service availability to ensure that servers that can't answer client requests aren't given network connections.
- Some load balancing solutions, such as ISA 2006 or TMG 2010, can't do RPC load balancing or monitor RPC services. These solutions aren't recommended unless all clients are connecting via Outlook Anywhere and all traffic is encapsulated inside HTTP.

For more information about load balancing, see Understanding Load Balancing in Exchange 2010.

Configure IP Ports

An IP port is an opening through which information can pass from the originating computer to the destination computer. By default, the dynamic port range for outgoing connections on Windows Server 2008 R2 is 49152 to 65535. Exchange 2010 Client Access changes this range to 6005 through 65535. The range was expanded to provide sufficient scaling for large deployments. This is a large range of ports to balance through your firewall between the client and the Client Access servers or Client Access array.

By fixing the MAPI and directory endpoints, you can greatly reduce the number of ports that need to be load balanced. The MAPI endpoint can be statically configured in the registry and the directory endpoint can be fixed in a configuration file.

To fix the MAPI endpoint, use the following setting in the registry.

HKLM\SYSTEM\CurrentControlSet\ Services\MSExchangeRPC\ParametersSystem \TCP/IP Port [DWORD] is the value for the IP port to use.

To fix the directory services endpoint, edit the RpcTcpPort value in the configuration file Microsoft.Exchange.AddressBook.Service.Exe.config.

Note:

We don't recommend that you change the default value of the Outlook Anywhere ports.

Configure RPC Encryption Settings

In the RTM version of Exchange 2010, the RPC endpoint is encrypted by default. However, Outlook 2003 doesn't enforce encrypted MAPI connections. When you upgrade your organization to the RTM version of Exchange 2010, your clients running Outlook 2007 or later versions will automatically be compatible with the change to RPC Client Access, since they support RPC encryption by default. Outlook 2003 doesn't use RPC encryption, however, and RPC Client Access requires it by default. If you haven't turned off RPC encryption, which we don't recommend, your users will need to configure Outlook 2003 for RPC encryption or you'll need to use a Group Policy to force Outlook 2003 to use RPC encryption.

Symptoms of this problem include the following error messages:

- Cannot start Microsoft Office Outlook. Unable to open the Office window. The set of folders could not be opened.
- Unable to open your default e-mail folders. The information store could not be opened.

If your users are using Cached Exchange Mode, Office won't display an error, but will start in disconnected mode.

By default, Exchange 2010 Service Pack 1 (SP1) doesn't encrypt the RPC endpoint. If you've completed the installation of Exchange 2010 SP1 in your organization, Outlook 2003 clients will be able to connect to the Exchange server without further configuration.

For more information about this issue, including workarounds, see Outlook Connection Issues with Exchange 2010 Mailboxes.

Configure Outlook 2003 to Use RPC Encryption

To configure Outlook 2003 to use RPC encryption, use the following steps.

1. Click **Tools** > **E-Mail Accounts** > **View or Change an Existing Account**.
2. Select the account and click **More Settings**.
3. Select the **Security** tab.
4. Select **Encrypt data between Microsoft Office Outlook and Microsoft Exchange Server**.
5. Click **OK**.

Configure Your Mailbox Database

Each Mailbox database contains an **RPCClientAccessServer** value. This value is established when the database is created and it determines the Client Access server or

Client Access array that the clients with mailboxes on that Mailbox server will use. This value also determines the location of the RPC end point. For Outlook 2007 and Outlook 2010 clients, this value is obtained from the Autodiscover service.

The default value of the **RPCClientAccessServer** is determined by the following rules:

- If you have configured a Client Access Server array within your Active Directory site, the address of that array will be used.
- If an array does not exist within the Active Directory site and if you have both the Client Access server role and the Mailbox server role on the same physical server, the value of **RPCClientAccessServer** property for a particular Mailbox server will be the same as the Mailbox server.
- Otherwise, the value of the **RPCClientAccessServer** property for a particular Mailbox server will be set to a random Client Access server within the Active Directory site.

Note:
We don't recommend that you install all the server roles on a single computer that's also a domain controller. Although this configuration is supported, it's not recommended.

- If you created a Mailbox database before the creation of a Client Access array or the installed a Client Access server within the Active Directory site, you'll need to reconfigure the value of the **RPCClientAccessServer** property. If no Client Access server exists in the Active Directory site when the Mailbox database is created, the value of the **RPCClientAccessServer** property will be set to the FQDN of the Mailbox server. To configure the value of the **RPCClientAccessServer** property, use the following command.

```
Set-MailboxDatabase <name> -RPCClientAccessServer <internal_only_CAS_Ar
```

Latency and Bandwidth Requirements

For users running Outlook without Cached Exchange Mode, high latency times between the client and the server directly affect how frequently Outlook is unresponsive. In general, a latency of greater than 200 milliseconds (ms) to the home Mailbox server will result in poor client performance.

Because latency between the Client Access server and the mailbox should be less than 10 ms, we recommend that the value of the **RPCClientAccessServer** property always be configured to a Client Access array in the active Mailbox database site.

Note:
Changing the value of the **RPCClientAccessServer** property will force all clients to reconnect.

Configuring the Address Book Service

The Address Book service is configured through the Microsoft.Exchange.AddressBook.Service.config file. This file allows you to configure the following:

- The number of concurrent connections per user (the default limit is 50).
- Disable or enable logging.
- The location, size, and retention period for the log files.

To enable logging, use the following value:

```
< add key="ProtocolLoggingEnabled" value="true" />
```

1.6.1.13 Understanding the Address Book Service

Understanding the Address Book Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-12*

In versions of Microsoft Exchange earlier than Exchange Server 2010, Exchange provided a referral service that told clients such as Outlook where they could find a server running the NSPI service. This referral usually pointed Outlook to a global catalog server. But some Outlook Anywhere connections would point Outlook back to the local server, and the NSPI calls would be proxied to a global catalog server.

Outlook expects to find this referral service on the same server that's used for mailbox access. In Exchange 2010, both mailbox access and directory access are handled by the Client Access server.

Directory Access on a Client Access Server

When Outlook contacts the Client Access server, two possible actions occur. If the user's mailbox is on an Exchange Server 2007 Mailbox server or an Exchange Server 2003 server, the directory request is referred to the user's mailbox server. If the user's mailbox is on an Exchange 2010 Mailbox server, then one of two actions happens.

If the user's mailbox is in the same site as the Client Access server, the request is referred to the Client Access server. If the user's mailbox is in a different site, the request is referred to a Client Access server in the remote site.

For Exchange 2010, the Client Access server hosts both the referral service and the NSPI endpoint. These two components are necessary for directory access to flow through the Client Access server.

Note:

If your Client Access server is installed on a domain controller, Outlook will communicate directly with the domain controller and will bypass the Client Access server.

Exchange 2007 Users

If a user who has a mailbox on a Microsoft Exchange Server 2007 Mailbox server queries the referral service, the Exchange 2010 Client Access server will refer the user to the Exchange 2007 Mailbox server. This is the same behavior that was experienced in a pure Exchange 2007 environment.

1.6.1.14 Client Access Availability and Scalability

Client Access Availability and Scalability

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-03*

When you plan the deployment of your Exchange Server 2010 organization, performance and scalability are two important considerations. It's very important to estimate your Exchange 2010 Client Access server capacity needs. The Client Access server is the entry

point for all users. In addition, the Client Access server hosts important services that are used by the other Exchange server roles. For information about the relative CPU weights of different protocols on the Client Access server, see White Paper: Understanding Granular and Relative Costs of Client Access Server Workloads In Exchange Server.

1.6.1.15 Sizing Client Access Servers

Sizing Client Access Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-18*

It's very important that you estimate your Microsoft Exchange Server 2010 Client Access server capacity needs when you plan the deployment of your Exchange 2010 organization. The Client Access server is the entry point for all users. In addition, the Client Access server hosts important services that are used by the other Exchange server roles.

For information about the relative CPU weights of different protocols on the Client Access server, see White Paper: Understanding the Relative Costs of Client Access Server Workloads In Exchange Server 2010.

1.6.1.16 Understanding Exchange Web Services Virtual Directories

Understanding Exchange Web Services Virtual Directories

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-03-18*

When you install the Client Access server role on your Exchange server, one Exchange Web Services virtual directory is created in the default Internet Information Services (IIS) Web site on the Exchange server. You can manage the virtual directory by using the Exchange Management Shell, IIS Manager, and through a configuration file located in the directory to which you installed Microsoft Exchange Server 2010.

Exchange Web Services virtual directories support the calendar sharing and other functionality offered by Exchange Web Services. The Exchange Web services included in Exchange 2010 provide an XML messaging interface that enables you to manage Exchange store items and access Exchange server functionality from client applications. For an overview of Exchange Web Services, see Introduction to Web Services.

Looking for management tasks related to Exchange Web Services virtual directories? Check out the Exchange Web Services virtual directory cmdlets referenced in the Client Access Cmdlets topic.

Contents

Configuring Exchange Web Services Virtual Directories

Most organizations find that the default Exchange Web Services virtual directory that's created during installation of the Exchange 2010 Client Access server role is sufficient. However, you can remove, create, and modify the settings of an Exchange Web Services virtual directory.

Managing Exchange Web Services Information in Your Infrastructure

For the functionality provided by Exchange Web Services to work, you must keep the information in the following locations in sync:

- Internet Information Services (IIS)
- Active Directory
- The Exchange Web Services web.config file

If there's a discrepancy between what you've configured in IIS for the Exchange Web Services virtual directory, what's configured in the web.config file, and what's is stored in Active Directory, Exchange Web Services won't initialize and calendaring sharing and other functionality won't work.

When Exchange Web Services doesn't initialize, an event is logged with the following error code: `ServiceActivationException`. If you get this error, it's a best practice to remove and then re-create the Exchange Web Services virtual directory. For more information about the cmdlets and parameters you need to use to perform these actions, see Remove-WebServicesVirtualDirectory and New-WebServicesVirtualDirectory.

Configuring Exchange Web Services to Manage SSL Offloading

SSL is enabled by default on Exchange Web Services virtual directories. If you want to enable SSL offloading, you must disable SSL on each Client Access server in your organization.

If you don't have an SSL offloading device and you want to maintain secure communication between client and server, SSL must be enabled on each Client Access server in your organization.

Important:

You can't disable or enable SSL using the Shell. If you disable or enable SSL on an Exchange Web Services virtual directory, you must make the configuration change in both IIS Manager and the Exchange Web Services web.config file.

For more information about how to manage SSL on Exchange Web Services virtual directories, see Enable or Disable SSL on Exchange Web Services Virtual Directories.

1.6.1.17 Understanding External Access to Exchange 2010

Understanding External Access to Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-20*

This topic describes how to configure firewalls for use with a Microsoft Exchange Server 2010 Client Access server. You can use software and hardware solutions as a firewall to help secure your messaging environment. We recommend that you use an advanced firewall server such as Microsoft Internet Acceleration and Security (ISA) Server 2006 with Exchange 2010 because these two products are designed to work together to help secure and enhance the client access experience.

Forefront Unified Access Gateway 2010 and Forefront Threat Management Gateway 2010

When you publish Exchange for access from the Internet, Microsoft offers two software-based options: Microsoft Forefront Threat Management Gateway 2010 and Microsoft Forefront Unified Access Gateway 2010. Both options offer publishing wizards and security features to provide secure access to Exchange when it's accessed from outside the safety of the corporate network. For more information about Forefront Unified Access Gateway 2010 and Forefront Threat Management Gateway 2010, see Publishing Exchange Server 2010 with Forefront Unified Access Gateway 2010 and Forefront Threat Management Gateway 2010.

ISA Server 2006 and Exchange 2010

ISA Server 2006 and Exchange 2010 coexist and provide an increased level of security for your messaging environment. When you use the New Exchange Publishing Rule Wizard to configure your ISA Server computer to allow client access, you automatically configure ISA Server settings that are required for the features in both Exchange 2010 and ISA Server 2006 to work correctly.

Earlier Versions of ISA Server and Exchange 2010

When you deploy Exchange 2010, we recommend that you upgrade any earlier versions of ISA Server that you're using. Deploying Exchange 2010 in an environment that was configured to use an earlier version of ISA Server, such as ISA Server 2004, requires changes to any ISA Server rules you configured for client access.

When you configure ISA Server 2004 or ISA Server 2000, you'll have to create new server or Web publishing rules for the Client Access servers you want your users to access. The following table describes the virtual directories to use as paths for the Web and server publishing rules you must create for client access to Exchange when you use an earlier version of ISA Server than ISA Server 2006. Make sure that you use only the paths for the client applications you plan to use. For example, if you don't plan to use Microsoft Exchange ActiveSync, you don't have to publish the Microsoft-Server-ActiveSync virtual directory.

Exchange 2010 virtual directories used as paths in ISA Server publishing rules

Path Name	Description
/owa	This virtual directory is used by Outlook Web App to access mailboxes on Exchange 2007 or Exchange 2010 Mailbox servers.
/public	This virtual directory is used by Outlook Web App to access public folders for mailboxes that are located on computers running Exchange 2010, Microsoft Exchange Server 2007, Exchange Server 2003, or Exchange 2000 Server.
/exchweb	This virtual directory is used by Outlook Web App for mailboxes on computers running Exchange 2003 or Exchange 2000.
/ecp	This virtual directory is used by the Exchange Control Panel.
/exchange	This virtual directory is used by Outlook Web App to access mailboxes on computers running Exchange 2003 or Exchange 2000.
/UnifiedMessaging	This virtual directory is used for access to Unified Messaging.
/Microsoft-Server-ActiveSync	This virtual directory is used by ActiveSync in Exchange 2007 or Exchange 2010.
/EWS	This virtual directory is used for Exchange Web Services.
/Autodiscover	This virtual directory is used by the Autodiscover service for the Exchange ActiveSync and Outlook clients.
/rpc	This virtual directory is used by the Outlook Anywhere feature in Outlook 2007 or Exchange 2010.

1.6.1.18 Understanding Load Balancing in Exchange 2010

Understanding Load Balancing in Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-29*

Load balancing is a way to manage which of your servers receive traffic. Load balancing provides failover redundancy to ensure your users continue to receive Exchange service in case of computer failure. It also enables your deployment to handle more traffic than one server can process while offering a single host name for your clients.

In addition to load balancing, Microsoft Exchange Server 2010 provides several solutions for switchover and failover redundancy. These solutions include the following:

- **High availability and site resilience** You can deploy two Active Directory sites in separate geographic locations, keep the mailbox data synchronized between the two, and have one of the sites take on the entire load if the other fails. Exchange 2010 uses database availability groups (DAGs) to keep multiple copies of your mailboxes on different servers synchronized.
- **Online mailbox moves** In an online mailbox move, end users can access their e-mail accounts during the move. Users are only locked out of their accounts for a brief time at the end of the process, when the final synchronization occurs. Online mailbox moves are supported between Exchange 2010 databases and between Exchange Server 2007 Service Pack 3 (SP3) or a later version of Exchange 2007 and Exchange 2010 databases. You can perform online mailbox moves across forests or in the same forest.
- **Shadow redundancy** Shadow redundancy protects the availability and recoverability of messages while they're in transit. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all the next hops for that message have completed. If any of the next hops fail before reporting successful delivery, the message is resubmitted for delivery to the hop that didn't complete.

Contents

Overview of Load Balancing

Load balancing serves two primary purposes. It reduces the impact of a single Client Access server failure within one of your Active Directory sites. In addition, load balancing ensures that the load on your Client Access server and Hub Transport computers is evenly distributed.

Architectural Changes in Exchange 2010 Load Balancing

Several changes in Exchange 2010 make load balancing important for your organization. The Exchange RPC Client Access service and the Exchange Address Book service on the Client Access server role improve the user's experience during Mailbox failovers by moving the connection endpoints for mailbox access from Outlook and other MAPI clients to the Client Access server role instead of to the Mailbox server role. In earlier versions of Exchange, Outlook connected directly to the Mailbox server hosting the user's mailbox, and directory connections were either proxied through the Mailbox server role or referred directly to a particular Active Directory global catalog server. Now that these connections are handled by the Client Access server role, both external and internal Outlook connections must be load balanced across the array of Client Access servers in a deployment to achieve fault tolerance.

A load-balanced array of Client Access servers is recommended for each Active Directory site and for each version of Exchange. It isn't possible to share one load-balanced array of Client Access servers for multiple Active Directory sites or to mix different versions of Exchange or service pack versions of Exchange within the same array.

When you install Exchange 2010 within your existing organization and configure a legacy namespace for coexistence with previous versions of Exchange, your clients will

automatically connect to the Exchange 2010 Client Access server or server array. The Exchange 2010 Client Access server or Client Access server array will then proxy or redirect client requests for mailboxes on older Exchange versions to either Exchange 2003 front-end servers or Exchange 2007 Client Access servers that match the mailbox version. For more information, see Understanding Upgrade to Exchange 2010.

Note:
You can mix Quick Fix Engineering (QFEs) and update rollups when you apply them to all or parts of an array. We recommend that you apply QFEs and update rollups to all computers within an array.

Your load balancing configuration will have a direct effect on the host names that your clients use to connect and the Secure Sockets Layer (SSL) certificates that you use. For more information about Exchange 2010 certificates, see Understanding Digital Certificates and SSL.

Configuring the Client Access Server Array

You can configure one Client Access server array per Active Directory site. As soon as the Client Access server array has been configured, you can configure the Mailbox database to use the Client Access server array as the MAPI endpoint instead of a specific Client Access server.

For more information about the Client Access server array and how to configure the Mailbox database to use the Client Access server array for the specific Active Directory site, see Understanding RPC Client Access.

Understanding Exchange 2010 Traffic Loads

Before you configure load balancing, you should understand the loads that are placed on an Exchange 2010 Client Access server. An Exchange 2010 Client Access server receives the following three types of traffic:

- Traffic from external clients
- Traffic from internal clients
- Proxy traffic from other Client Access servers

Proxy traffic from other Client Access servers is traffic that is originally sent by an external or internal client to one Client Access server but is then proxied to another Client Access server. This can happen for several reasons, but generally it happens because the originating client can't connect directly to the destination Client Access server. This can occur when a user is trying to access a mailbox from the Internet, but the mailbox is located in a non-Internet facing Active Directory site. For more information about proxying, see Understanding Proxying and Redirection.

Each of the types of traffic received by Client Access servers includes requests from a list of protocols and comes from client devices and computers with different characteristics. These differences affect which load balancing strategies can be used.

Return to top

Understanding Load Balancing Options

There are several key technology differences between the different load balancing solutions.

- **Performance** How many requests per second can the solution handle?
- **Manageability** How simple is it to configure and deploy the load balancing

solution?

- **Failover automation and detection** How smart is the load balancer about detecting when a Client Access server or service has failed?
- **Affinity** Which types of client to Client Access server affinity does the load balancing solution support?

Understanding Affinity

When a load balancing solution provides client-to-Client Access server affinity, it means that there is a long-standing association between a particular client and a particular Client Access server. The client can be Outlook running on a laptop, Microsoft Exchange ActiveSync running on a mobile device, Microsoft Office Outlook Web App, Exchange Web Services, or another client application.

This long-standing association, or affinity, ensures that all requests sent from the client go to the same Client Access server. Some Exchange 2010 protocols require affinity and other Exchange protocols do not.

Windows Network Load Balancing

Windows Network Load Balancing (WNLB) is the most common software load balancer used for Exchange servers. There are several limitations associated with deploying WNLB with Microsoft Exchange.

- WNLB can't be used on Exchange servers where mailbox DAGs are also being used because WNLB is incompatible with Windows failover clustering. If you're using an Exchange 2010 DAG and you want to use WNLB, you need to have the Client Access server role and the Mailbox server role running on separate servers.
- Due to performance issues, we don't recommend putting more than eight Client Access servers in an array that's load balanced by WNLB.
- WNLB doesn't detect service outages. WNLB only detects server outages by IP address. This means if a particular Web service, such as Outlook Web App, fails, but the server is still functioning, WNLB won’t detect the failure and will still route requests to that Client Access server. Manual intervention is required to remove the Client Access server experiencing the outage from the load balancing pool.
- WNLB configuration can result in port flooding, which can overwhelm networks.
- Because WNLB only performs client affinity using the source IP address, it's not an effective solution when the source IP pool is small. This can occur when the source IP pool is from a remote network subnet or when your organization is using network address translation.

Load Balancing Recommendations

There are several load balancing options available. The option you use depends on the size and configuration of your network.

Windows Network Load Balancing with Source IP Affinity

The first load balancing option is WNLB with source IP affinity. This solution is suitable if you have more than one Client Access server per Active Directory site but fewer than eight. This solution is built into Windows and doesn't require additional computers.

There are two scenarios in which you will not want to use WNLB.

- Your organization has a reverse proxy server that communicates directly with the Client Access server and not through the WNLB virtual IP address. The reverse proxy server hides the client IP addresses from the Client Access server array. Therefore, source IP affinity won't work as expected. However you may still want to use WNLB to load balance internal traffic.
- Your organization has many clients accessing your Client Access servers through a very small set of IP addresses. WNLB tends to affinitize an entire class C subnet to one Client Access server.

Hardware Load Balancing

If you have more than eight Client Access servers in a single Active Directory site, your organization will need a more robust load balancing solution. Although there are robust software load balancing solutions available, a hardware load balancing solution provides the most capacity. For more information about Exchange 2010 server load balancing solutions, see Microsoft Unified Communications Hardware Load Balancer Deployment.

Hardware load balancers support very high traffic throughput and can be configured to load balance in many ways. Most hardware load balancer vendors have detailed documentation about how their product works with Exchange 2010. The simplest way to configure hardware load balancers is to create a fallback list of the affinity methods that will be applied by the load balancer. For example, the load balancer will try cookie-based affinity first, then SSL session ID, and then source IP affinity.

Reverse Proxy Solutions

If you have a reverse proxy solution that can perform load balancing for the servers it publishes to the Internet, such as Microsoft Forefront Threat Management Gateway (TMG) or Forefront Unified Access Gateway (UAG), we recommend that you use it.

As traffic passes through the reverse proxy server to reach your Client Access servers, the client's original IP address is replaced by the IP address of the reverse proxy server. This breaks source IP affinity. There are ways to resolve this problem, including configuring the reverse proxy server to be the default gateway for the subnet it is proxying to.

However, most current reverse proxy servers can do load balancing for the services they publish to the Internet. These reverse proxy servers support load balancer-created cookie load balancing for the Exchange services that support this. This solution is more reliable than source IP load balancing. For this to work, the reverse proxy server must be able to read and modify the HTTP data stream. If you're using SSL, this means that the reverse proxy server must decrypt the traffic to read the contents and create the cookie within the stream. This decryption isn't possible in some circumstances, such as when you're using client certificate authentication, where the client connects to the Client Access server.

Return to top

Affinity Options

Different load balancing solutions offer different methods for associating clients with a specific Client Access server. There are several common types of affinity available in different load balancing products, both hardware and software. Not all types of affinity will be available in every load balancing option, as described in the following examples:

- WNLB only supports source IP affinity or no affinity.
- A software load balancer in a separate server array can use load balancer-created cookies for the protocols that support those cookies and source IP affinity for the remaining protocols.
- Hardware load balancers with SSL offloading let you configure more complex behavior. For example, you can configure a set of existing cookies that will take effect for protocols that support those cookies, as well as a load balancer-created cookie, SSL session ID, and source IP.

In addition to the options that are supported by the different load balancing solutions, you can also configure some of these steps to be applied only for certain Exchange protocols and services. Because each protocol behaves differently, this can help optimize performance.

Existing Cookies or HTTP Headers

Using existing cookies or HTTP headers is the most reliable way to identify a client and associate it with a specific Client Access server. These cookies and headers are created by the client or server as part of the communications protocol. This option also doesn't require the load balancer to modify the traffic, which helps performance.

When you use this affinity option, be aware of the following:

- Your load balancer must support this type of affinity. Currently only hardware load balancers support this affinity.
- This affinity only works for protocols that pass traffic on HTTP.
- There must be an existing cookie or header that remains constant during the client session and is unique to each specific client, or small set of clients, in the protocol.
- The load balancer solution must be able to read and interpret the HTTP data stream. If you're using SSL, this means that the load balancer must decrypt the traffic to read the contents. Sometimes this results in an increased load on the load balancer. Also, this decryption isn't possible in some circumstances, such as when you use client certificate authentication with the SSL session where the client connects to the Client Access server.

The existing cookies and HTTP headers suitable for load balancing that are available in Exchange 2010 protocols are the following:

- **HTTP Basic authentication authorization header** This header works when HTTP Basic authentication is used. Basic authentication is the default and most commonly used type of authentication for Exchange ActiveSync. This header is uncommon for other protocols and authentication methods. The Basic authentication authorization header sends all traffic that uses Basic authentication and that is from a specific user to the same Client Access server. This header is also used when Outlook traffic is transmitted completely via HTTP and clients are behind a reverse proxy server.
- **HTTP OWA UserContext cookie** This cookie works for Outlook Web App, which is the only client that uses it. When you use forms-based authentication (FBA) with Outlook Web App, which is the default configuration, a small set of requests are made at the start of an Outlook Web App session before the *UserContext* cookie is created. To ensure that those requests use affinity to connect the client to the same Client Access server, which is required for forms-based authentication to work, there has to be a fallback affinity option when you use the *UserContext* cookie. We recommend that you use the SSL session ID or source IP affinity as a fallback to provide affinity for those initial requests, before the load balancer gets the *UserContext* cookie to use.

  Note:

  Outlook Web App requests that use explicit logon to access a specific mailbox result in the use of a *UserContext* cookie with a different name and ID. The cookie starts with *UserContext*, but a string that identifies the individual mailbox is appended. This complicates load balancing with the *UserContext* cookie because the load balancer must first find a cookie starting with *UserContext*. This can result in decreased performance.

- **HTTP Exchange Control Panel msExchEcpCanary cookie** This cookie only works for the Exchange Control Panel.
- **HTTP Outlook 2010 OutlookSession cookie** Hardware load balancers support the OutlookSession cookie and other generic cookies. The following table describes the OutlookSession client cookie support requirements for Outlook RPC/HTTP:

	Windows XP	**Windows Vista**	**Windows 7**
Outlook 2003	Not supported	Not supported	Not supported
Outlook 2007	Not supported	Not supported	Not supported
Outlook 2007 Hosting Pack	Not supported	Supported	Supported

(KB2544404)			
Outlook 2010	Not supported	Supported	Supported

Note:
Microsoft Outlook running on Windows XP does not support the OutlookSession cookie for load balancing. In this scenario, we recommend that you use IP load balancing.

- **HTTP Remote PowerShell MS-WSMAN cookie** This method works only for Remote PowerShell.

Return to top

Load Balancer Created Cookie

The second most reliable way to associate a client session with a Client Access server is by using a load balancer-created cookie. The load balancer adds an HTTP cookie to the client/server protocol conversation and then uses that cookie to determine which Client Access server should handle an incoming request. The Exchange 2010 applications that support this method are Outlook Web App, Exchange Control Panel, and Remote PowerShell. This type of cookie has several limitations.

- The load balancer must support this type of affinity. Currently only hardware load balancers and software load balancers that run on a separate server tier support this affinity.
- This method only works for protocols that pass traffic on HTTP. You can't use this method for the RPC Client Access service, Exchange Address Book service, POP3, or IMAP4.
- The load balancer solution must be able to read and interpret the HTTP data stream. If you're using SSL, this means that the load balancer must decrypt the traffic to read the contents. Sometimes this results in a bigger load on the load balancer. In other cases, it isn't possible for the load balancer to interpret the HTTP data stream, such as when you use client certificate authentication on the Client Access server.
- The client must be able to receive arbitrary cookies from the server and must then include those cookies in all future requests sent from the client to the server. Exchange ActiveSync clients, Outlook Anywhere clients, and some Exchange Web Service clients such as Microsoft Office Communications Server 2007 devices don't support this.

SSL Session ID

Load balancing based on the SSL session ID provides more detail than source IP affinity and lets you split up traffic from different clients even if those clients are coming in from the same IP address. SSL session ID load balancing also has the advantage of letting you load balance without decrypting the SSL traffic. This is required when you use client certificate authentication and when you end the SSL connection at the Client Access server.

SSL session ID affinity isn't recommended in the following two situations:

- Some clients, such as Internet Explorer 8, re-create their SSL session for each browser process that runs on the client computer. This results in a new SSL session for each Outlook Web App window. Because this breaks client affinity for Outlook Web App, deploying load balancing in this manner is not supported for Exchange 2010. Some mobile devices, such as the Apple iPhone, also create new SSL sessions for some parts of their Exchange ActiveSync communication with Exchange.

Note:
When you use client certificate authentication, browsers will use the same SSL session for all traffic to a given host name. As long as client certificate authentication is enabled, SSL session ID is a valid affinity option for Outlook Web App and Exchange Control Panel.

- In the case of Outlook Anywhere, the Client Access servers will use the Windows RPC Proxy component to pair up the RPC_DATA_IN and the RPC_DATA_OUT connections. This can adversely affect performance.

Source IP

The most common way to provide affinity between clients and Client Access servers is by using source IP affinity. The load balancer examines a client's IP address and sends all traffic from a specific source IP to a specific Client Access server. This is the only type of affinity supported by WNLB. There are two important aspects to consider when you use source IP affinity.

- Affinity breaks when the client changes IP address. This can occur when a laptop is moved from a wired LAN to Wi-Fi or roams between different Wi-Fi networks. There is a user impact when the client changes IP address. For example, when they're using Outlook Web App, users will have to authenticate every time their computer obtains a new IP address.
- If many of your clients access your load balancing solution from the same IP address, the load distribution will become uneven. The impact of this depends on how many clients are masked behind a given IP address. For example, if you have four Client Access servers and 50 percent of your clients access your load balancer from the same IP address, at least 50 percent of your traffic will go to one Client Access server and the other three Client Access servers will handle the rest of the traffic. There are two main reasons why most clients will access your Exchange organization through a single IP address.
  - Network address translators (NATs) or outgoing proxy servers, such as Microsoft Forefront Threat Management Gateway (TMG). When there is a NAT or outgoing proxy server between your clients and your Client Access servers, the original client IP addresses are masked by the NAT or outgoing proxy server IP address.
  - Client Access server to Client Access server proxy traffic. In some scenarios, one Client Access server proxies traffic to another Client Access server. Typically, this happens between Active Directory sites because a client must access the Client Access server within the same Active Directory site as their mailbox. For more information about proxying, see Understanding Proxying and Redirection.

No Affinity

The last type of affinity is no affinity. When you don't use affinity, each request from a client is assigned to a random Client Access server. We don't recommend this option for protocols that require affinity or those that experience performance benefits from affinity.

It's recommended that you not use affinity for protocols that don't need affinity when SSL offloading is configured.

Return to top

Summary of Load Balancing Options

The following table provides a summary of the load balancing options that are available.

Solution	Client to Client Access server affinity	Failover method	Capacity	Cost
Hardware load balancer	Depending on the protocol and the client, fall back between the following: • Existing cookie • Load balancer-created cookie • SSL ID • Source IP	Automatic failover with minimal client downtime. Hardware load balancers also are able to provide failover for a	++++	$$$

		specific protocol.		
Software load balancer in a separate server layer Note: TMG and UAG are the only workable solutions for external traffic.	Either load balancer-created cookie or source IP, depending on the protocol and client.	Automatic failover with minimal client downtime.	++	$$
Software load balancer in the same server layer as the Client Access server (WNLB)	Source IP.	Automatic failover with minimal client downtime.	+	$
DNS round robin	Each client gets a random Client Access server IP address.	Manual steps to detect issues and recover. Browser and operating system DNS caching behavior may inhibit client connections even after recovery has been performed by an administrator. This solution breaks affinity for many protocols, including RPC Client Access, Outlook Web App, Exchange Web Services, and Exchange Control Panel.	+++	$
No load balancer	Separate host names are manually assigned for each Client Access server.	Manual steps to detect issues and failover. Client DNS caches cause slow failover.	+	N/A

There are several advantages and disadvantages to each of these options.

- Hardware load balancers usually include performance and security functionality such as SSL offloading and traffic inspection.
- Software load balancers in a separate server layer are usually included as parts of larger software packages, with reverse proxy capabilities like pre-authentication, SSL offloading, and extensive traffic inspection. When software load balancers pre-authenticate users, those users don't need to re-authenticate if the Client Access server they are affinitized to fails. However, some software load balancers require an affinity between the client and the reverse proxy server. In this case, you need an additional load balancing layer in front of the reverse proxy servers before those reverse proxy servers can perform load balancing duties for your Client Access servers.

1.6.1.18.1 Load Balancing Requirements of Exchange Protocols

Load Balancing Requirements of Exchange Protocols

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-02*

Microsoft Exchange protocols and client access services have different load balancing requirements. Some Microsoft Exchange protocols and client access services require client to Client Access server affinity. Others will work without it but will display performance improvements from such affinity. Other Exchange protocols don't require client to Client Access server affinity and performance doesn't decrease without affinity.

Contents

Exchange Protocols That Require Client to Client Access Server Affinity

The following Exchange protocols require client to Client Access server affinity. Affinity must last during a client session.

- **Outlook Web App and the Exchange Control Panel** Microsoft Office Outlook Web App and the Exchange Control Panel both require client to Client Access server affinity. When you use forms-based authentication, which is the default in Microsoft Exchange Server 2010, both Outlook Web App and the Exchange Control Panel must be affinitized to the same Client Access server. This is because they share the same authentication cookie and this cookie can only be decrypted by one specific Client Access server.
- **Exchange Web Services** Only a subset of Exchange Web Services requires affinity. Availability Service requests don't require affinity, but subscriptions do. All aspects of Exchange Web Services experience performance enhancements from affinity. An affinity timeout value of 45 minutes is recommended for

Exchange Web Services clients to ensure that periodic polling for events associated with a subscription are not directed to a new Client Access server resulting in inefficient new subscriptions for each request. We don't support the use of Exchange Web Services without affinity.

- **Outlook RPC over TCP on the Intranet** Outlook clients on the Intranet assume that all RPC connections are made to the same server. Outlook uses multiple sessions per user and assumes that all sessions connect to the same server.

Exchange Protocols That Benefit From Client to Client Access Server Affinity

The following Exchange protocols and services will work without affinity. However, performance is significantly reduced when they're deployed without affinity.

- **Outlook Anywhere** Outlook Anywhere connections are unidirectional and split a single RPC data connection into two HTTP connections. One connection is for incoming data and one is for outgoing data. When there's no affinity between these two types of connections, Outlook Anywhere tries to correlate the connections by coordinating with other members of the Client Access server array. This increases traffic between Client Access servers by about 50% for a two-server array and up to 100% for an array with a large number of servers.
- **Exchange ActiveSync** Microsoft Exchange ActiveSync transmits new mail notifications to clients through a long-standing HTTPS request from the client to the server. When an Exchange ActiveSync client is assigned to a new Client Access server, that server must re-create the notification subscription against the user's mailbox. This results in a significant performance penalty.
- **Exchange Address Book service** This is a new service in Exchange 2010 that provides directory access for clients. Not using affinity results in a significantly higher level of communication between the client and the Client Access servers.
- **Remote PowerShell** Without affinity, users will need to reauthenticate if a connection is interrupted.

Exchange Protocols That Don't Require Affinity

There are several Exchange protocols and services that don't require affinity because they're transactional. This means that the connection is established, the transaction is completed, and the connection is closed. These protocols don't experience performance benefits from affinity.

- Offline address book
- Autodiscover service
- POP3
- IMAP4

Understanding IP Ports

Most Exchange 2010 services are built on top of HTTP and use port 443 for Secure Sockets Layer (SSL) access and port 80 for non-SSL access. Outlook Web App, Exchange ActiveSync, Outlook Anywhere, and Exchange Web Services are such services. POP3 and IMAP4 use ports 110 and 143 respectively when not encrypted with SSL and ports 995 and 993 respectively when encrypted with SSL.

Other Exchange services, such as the RPC Client Access service and the Exchange Address Book service, are RPC services. When an Outlook client connects directly to the

Client Access server using these protocols, instead of using Outlook Anywhere, the endpoint TCP ports for these services are allocated by the RPC endpoint manager. Allocation occurs when the services are started. This requires a large range of destination ports to be configured for load balancing without the ability to specifically target traffic for these services based on port number. You can statically map these services to specific port numbers to simplify load balancing. If the ports for these services are statically mapped, the traffic will be restricted to port 135 and the two specific ports that were selected for these services.

Configuring Static Port Mapping for RPC-Based Services

The static port for the RPC Client Access service is configured in the registry. The following registry key should be configured on each Client Access server. Set the key to the value of the port that you want to use for TCP connections to the RPC Client Access service.

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeRPC\Parameter
Value: TCP/IP Port
Type: DWORD
```

Note:

This change will only affect internal connections via TCP and won't affect Outlook Anywhere connections that use RPC/HTTP tunneling. Outlook Anywhere connections to the RPC Client Access service occur on port 6001. This isn't configurable.

This process should also be performed on any public folder servers in your organization.

In Exchange 2010 SP1, the static ports for the two RPC endpoints maintained by the Exchange Address Book service are configured in the registry. Use the following registry key to configure these endpoints.

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeAB\Parameters
Value: RpcTcpPort
Type: REG_SZ (String)
```

Warning:

When you apply Exchange 2010 SP1 to a machine that previously had the static ports configured by editing the Microsoft.Exchange.AddressBook.Service.Exe.config file, the upgrade process will not recognize the static ports configured in the file. If you are planning to deploy Exchange 2010 SP1, we recommend you create the registry key before you install Exchange 2010 SP1. The registry key has no impact prior to SP1, so configuring it before installation can prevent service interruptions.

1.6.1.19 Understanding the Remote Connectivity Analyzer

Understanding the Remote Connectivity Analyzer

Exchange Server 2010 > Client Access > Understanding Client Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-22*

The Microsoft Exchange Remote Connectivity Analyzer (ExRCA) can help you confirm that connectivity for your Exchange servers is configured correctly and diagnose any connectivity issues. The Remote Connectivity Analyzer Web site offers tests for Microsoft Exchange ActiveSync, Exchange Web Services, Microsoft Office Outlook, and Internet e-mail.

Remote Connectivity Analyzer Tests

There are several tests that you can perform with the ExRCA. These tests work on Exchange Server 2003 Service Pack 2 and later versions.

The Remote Connectivity Analyzer performs tests for the following:

- Exchange ActiveSync
- Exchange Web Services
- Outlook
- Internet e-mail

Exchange ActiveSync Tests

There are two tests that you can run for Exchange ActiveSync, as follows:

- **Exchange ActiveSync** This test simulates the steps that a mobile device uses to connect to the Exchange server. It performs a full synchronization against a mailbox when you enter an e-mail address, user name, and password.
- **Exchange ActiveSync Autodiscover** This test doesn't perform a full synchronization. It validates the Autodiscover service settings for Exchange ActiveSync.

Exchange Web Services Tests

The Exchange Web Services tests validate settings for many of the Exchange Web Services. To troubleshoot external access to Exchange from Entourage, Web Services Edition, use the following tests:

- **Synchronization, Notification, Availability, and Automatic Replies (OOF**) This test determines whether programs that have to access this information can connect correctly. The test runs against a specific mailbox. To perform this test, the Inbox of the account that's used must be empty.
- **Service Account Access** This test determines whether developer connections to Exchange Web Services are configured correctly. The test verifies that a service account can access a mailbox, create and delete items in that mailbox, and access it through Exchange Impersonation.

Outlook Tests

To validate settings for connectivity to Outlook, use the following tests:

- **Outlook Anywhere (RPC over HTTP)** This test validates the connectivity for Outlook Anywhere for a specific mailbox. You can use the Autodiscover service to validate these settings or manually specify the server settings.
- **Outlook Autodiscover** This test verifies that the Autodiscover service is configured correctly for Outlook Anywhere. This test doesn't actually connect to a mailbox.

Internet E-Mail Tests

There are two Internet e-mail tests that you can run using the ExRCA, as follows:

- **Inbound SMTP E-Mail** This test confirms that you can receive an inbound SMTP message at a specified e-mail address.
- **Outbound SMTP E-Mail** This test checks your outbound IP address settings for Reverse DNS, Sender ID, and RBL checks.

1.6.1.20 Exchange 2010 and BlackBerry Enterprise Server Coexistence

Exchange 2010 and BlackBerry Enterprise Server Coexistence

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-08*

If you have BlackBerry devices in your organization and use a server running BlackBerry Enterprise Server to handle the communication between those devices and Microsoft Exchange Server 2010, there are specific updates that must be made to address known compatibility and performance issues.

Updates required for BlackBerry Enterprise Server and Exchange 2010

For Exchange 2010 and BlackBerry Enterprise Server to function together successfully, we recommend the following:

- Install the Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 update on the machines running BlackBerry Enterprise Server.
- Install the 5.0.2 Maintenance Release 4 of Blackberry Enterprise Server.
  - Download service packs and maintenance releases for BlackBerry Enterprise Server v5.0.
- Install the latest rollup for Exchange Server 2010 Service Pack 1 (SP1) on all of your Exchange 2010 Client Access servers and Mailbox servers or ensure that your Exchange 2010 Client Access servers and Mailbox servers have been upgraded to Exchange 2010 Service Pack 2 (SP2). Refer to Install the Latest Update Rollup for Exchange 2010 for more information about how to deploy the update rollup successfully.
- Install the following Windows Kernel Memory Manager hotfixes:
  - A computer that is running Windows 7 or Windows Server 2008 R2 becomes unresponsive when you run a large application
  - Poor performance occurs on a computer that has NUMA-based processors and that is running Windows Server 2008 R2 or Windows 7 if a thread requests lots of memory that is within the first 4 GB of memory

1.6.2 Managing Client Access Servers

Managing Client Access Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-09*

Services Used by a Client Access Server

Managing Outlook Web App

Managing Outlook Anywhere

Managing Exchange ActiveSync

Managing POP3 and IMAP4

Managing the Autodiscover Service

Managing the Availability Service

Managing External Client Access

Managing Client Access Server Virtual Directories

Maximum Client Access Service Sessions Per User

Configuring Kerberos Authentication for Load-Balanced Client Access Servers

1.6.2.1 Services Used by a Client Access Server

Services Used by a Client Access Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-20*

This topic describes the services used by a computer running Microsoft Exchange Server 2010 that has the Client Access server role installed. Depending on the protocols that are made available on the Client Access server and the Client Access method or methods used to access the Client Access server, some or all the following Exchange services may be required.

Enabling Services

To enable services used by a Client Access server, use the Services snap-in in the Microsoft Management Console (MMC). The following table shows the Exchange services that may be required.

Services that may be required by a Client Access server

Service name	Display name	Comments
W3SVC	World Wide Web Publishing Service	This service is required and must be started.
MSExchangeADTopology	Microsoft Exchange Active Directory Topology Service	This service provides Active Directory topology information to several Exchange Server components. This service doesn't have any dependencies.
POP3Svc	Microsoft Exchange POP3	By default, this service is stopped. For clients to use POP3 to connect to Microsoft Exchange, this service must be started. This service

		depends on the Microsoft Exchange Active Directory Topology service.
IMAP4Svc	Microsoft Exchange IMAP4	By default, this service is stopped. For clients to use IMAP4 to connect to Microsoft Exchange, this service must be started. This service depends on the Microsoft Exchange Active Directory Topology service.
IISAdmin	Internet Information Services Admin Service	This service manages the Internet Information Services (IIS) metabase and provides support for the World Wide Web Publishing Service (W3SVC) service, the POP3 service, and the IMAP4 service. These services are required by the Client Access server. IIS Admin also supports other applications, such as the metabase update service, which is an internal component of the system attendant.
MSExchangeServiceHost	Microsoft Exchange Service Host	This service configures the /rpc virtual directory in IIS and registry data for Outlook Anywhere. This service depends on the Microsoft Exchange Active Directory Topology service.
MSExchangeFDS	Microsoft Exchange File Distribution Service	This service is used to distribute offline address book and custom Unified Messaging prompts. This service depends on the Microsoft Exchange Active Directory Topology service.

1.6.2.2 Managing Outlook Web App

Managing Outlook Web App

Exchange Server 2010 > Client Access > Managing Client Access Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-01*

Managing Outlook Web App Virtual Directories

Managing Outlook Web App URLs

Managing File and Data Access for Outlook Web App

Managing Outlook Web App Advanced Features

Managing Outlook Web App Mailbox Policies

Managing Outlook Web App and Instant Messaging Integration

1.6.2.2.1 Managing Outlook Web App Virtual Directories

Managing Outlook Web App Virtual Directories

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-22*

Create an Outlook Web App Virtual Directory

View or Configure Outlook Web App Virtual Directories

Remove an Outlook Web App Virtual Directory

Rename an Outlook Web App Web Site

1.6.2.2.1.1 Create an Outlook Web App Virtual Directory

Create an Outlook Web App Virtual Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to create a Microsoft Office Outlook Web App virtual directory in Microsoft Exchange Server 2010.

By default, when Exchange 2010 is installed, a new virtual directory named "owa" is created in the default Web site in Internet Information Services (IIS). Alternatively, when you run the **New-OWAVirtualDirectory** cmdlet in the Shell, a new virtual directory named "owa" is created in the default IIS Web site on the local Exchange 2010 server.

To create a new Outlook Web App virtual directory, the following conditions must be true:

- The local Exchange 2010 server has the Client Access server role installed.
- There is a default IIS Web site, for example, */w3svc/1/root*.
- An Outlook Web App virtual directory named "owa" doesn't already exist.

If you have to create a new virtual directory for Outlook Web App, make sure that users are aware of the changes you're making. You'll be interrupting mail flow for your users.

Important:

When the default owa virtual directory is created, both forms-based authentication and

Secure Sockets Layer (SSL) encryption are enabled. However, when you create a new virtual directory by using the **New-OWAVirtualDirectory** cmdlet, neither forms-based authentication or SSL encryption is enabled.

Looking for other management tasks related to Outlook Web App virtual directories? Check out Managing Outlook Web App Virtual Directories.

Use the Shell to create an Outlook Web App virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example creates a new Outlook Web App virtual directory under the contoso.com Web site.

```
New-OwaVirtualDirectory -Name "Contoso" -WebSite "Contoso.com"
```

For more information about syntax and parameters, see New-OwaVirtualDirectory.

Other Tasks

After you create an Outlook Web App virtual directory, you may also want to:

- View or Configure Outlook Web App Virtual Directories
- Remove an Outlook Web App Virtual Directory

1.6.2.2.1.2 View or Configure Outlook Web App Virtual Directories

View or Configure Outlook Web App Virtual Directories

Managing Client Access Servers > Managing Outlook Web App > Managing Outlook Web App Virtual Directories >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the EMC or the Shell to view or configure the properties of an Outlook Web App virtual directory.

If you use the Shell to view the properties of an Outlook Web App virtual directory, the information returned is a subset of the information that's available. For example, if you use the **Get-OWAVirtualDirectory** cmdlet to view properties, Exchange returns the following information:

- Virtual directory name
- Server name
- Exchange server version

You can also retrieve information for a specific virtual directory on a specific server by using the available parameters. For more information about the **Get-OWAVirtualDirectory** cmdlet parameters, see Get-OwaVirtualDirectory.

If you use the EMC to view the properties of an Outlook Web App virtual directory, you'll be able to view a complete set of properties for the Exchange server that you're on.

Looking for other management tasks related to Outlook Web App? Check out Managing Outlook Web App.

What Do You Want to Do?

- Use the EMC to view or configure Outlook Web App virtual directory properties
- Use the Shell to configure Outlook Web App virtual directory properties
- Use the Shell to view Outlook Web App virtual directory properties

Use the EMC to view or configure Outlook Web App virtual directory properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the result pane, click the server you want.
3. In the work pane, click the **Outlook Web App** tab, right-click the virtual directory that you want to view or modify, and then click **Properties**.

4. On the **General** tab, you can view the properties of the Outlook Web App default Web site and specify an external URL and an internal URL. View or select the following options:
   - **Server** (Read-only.) **Server** displays the name of the server that hosts the Outlook Web App virtual directory.
   - **Web site** (Read-only.) **Web site** displays the name of the Web site.
   - **Version** (Read-only.) **Version** displays the version of Exchange that the virtual directory supports.
   - **Modified** (Read-only.) **Modified** displays the last date and time that the virtual directory was modified.
   - **Internal URL** In this text box, specify the URL used to access this Web site from an internal network. An internal URL is configured automatically during Exchange 2010 Setup. The default internal URL setting for an Internet-facing or non-Internet-facing Client Access server is https://<Computer Name>/owa.
   - **External URL** In this text box, specify the URL used to access the Web site from the Internet. By default, **External URL** is blank. For Internet-facing Client Access servers, **External URL** should be set to the value published in DNS for that Active Directory site. For Client Access servers that don't have an Internet presence, the **External URL** setting should remain blank.

5. On the **Authentication** tab, specify authentication methods, sign-in format, and sign-in domain:
   - **Use one or more standard authentication methods** Select this option to use one or more of the following standard authentication methods:
     Integrated Windows authentication This method requires that users have a valid Windows Server 2008, Windows Server 2003, or Microsoft Windows 2000 Server user account name and password to access information. Users aren't prompted for their account names and passwords. Instead, the server negotiates with the Windows security packages installed on the client computer. Integrated Windows authentication enables the server to authenticate users without prompting them for

information and without transmitting information that isn't encrypted over the network. For this method to work, the client computer must be a member of the same domain as the servers running Exchange, or of a domain that's trusted by the domain that the Exchange server is in.

Digest authentication for Windows domain servers This method transmits passwords over the network as a hash value for additional security. Digest authentication can be used only in Windows Server 2008, Windows Server 2003, and Windows 2000 Server domains for users who have an account that's stored in Active Directory. For more information about Digest authentication, see the Windows Server documentation.

Basic authentication (password is sent in clear text) This method is a simple authentication mechanism defined by the HTTP specification that encodes a user's sign-in name and password before the user's credentials are sent to the server. To make sure that the password is as secure as possible, you should use Secure Sockets Layer (SSL) encryption between client computers and the server that has the Client Access server role installed.

- **Use forms-based authentication** Forms-based authentication provides enhanced security for Outlook Web App virtual directories located on Client Access servers.

  Forms-based authentication creates a sign-in page for Outlook Web App. You can configure the type of sign-in prompt used by forms-based authentication. For example, you can configure forms-based authentication to require users to provide their domain and user name information, in the domain\user name format on the Outlook Web App sign-in page.

  Important:

  Forms-based authentication won't provide a secure channel unless SSL is enabled.

  Complete the following:

  Domain\user name Requires the user to enter their domain and user name in the format domain\user name. For example, for a user named Kweku in the domain Contoso, the sign-in would be contoso\kweku.

  User principal name (UPN) If the user principal name (UPN) sign-in format is specified, the **User Name** field on the Outlook Web App sign-in page guides users to enter their e-mail address, for example, kweku@contoso.com. If a user's UPN isn't identical to the e-mail address, the user can't access Outlook Web App by using the **PrincipalName** sign-in prompt. It's a best practice to use the **PrincipalName** sign-in prompt only if users' UPNs match their e-mail addresses.

  User name only The user enters their user name only, without the domain name, for example, Kweku. If you use the **UserName** sign-in prompt for forms-based authentication, you must also specify the **DefaultDomain** property. The **DefaultDomain** property determines the default domain to use when a user tries to access Outlook Web App. For example, if the default domain is Contoso, and a domain user named Kweku signs in to Outlook Web App, only Kweku must be entered as the user name. The server will use the default domain Contoso. If the user isn't a member of the Contoso domain, the domain and user name must be entered.

6. On the **Segmentation** tab, specify the features that you want to enable or disable for Outlook Web App users on a virtual directory.

Note:
Segmentation settings for individual users override virtual directory settings. You can change segmentation settings for individual users by using the **Set-CASMailbox** cmdlet or by using Outlook Web App mailbox policies. For more information, see Managing Outlook Web App Mailbox Policies.

View or specify the following:

- **Enable** Select a disabled feature in the list, and then click **Enable** to enable that feature.
- **Disable** Select an enabled feature in the list, and then click **Disable** to disable that feature.
- **Feature** The **Feature** column shows the list of features that are potentially available to Outlook Web App users on a virtual directory.
- **Status** The **Status** column shows whether each feature is enabled or disabled.
- **Description** This section displays a description for the selected feature in the list.

7. On the **Public Computer File Access** tab, configure the file access and viewing options available if users select **This is a public computer** while they're signing in to Outlook Web App. File access lets a user open or view the contents of files attached to an e-mail message.
   Direct file access
   - **Enable direct file access** Select this check box if you want to enable direct file access. Direct file access lets users open files attached to e-mail messages.
   - **Customize** After you select **Enable direct file access**, click **Customize** to customize the direct file access settings.

     Note:
     The direct file access settings are applied to private and public computer file access. Even though the settings can be set from either the **Private Computer File Access** tab or the **Public Computer File Access** tab, you can't have different settings on the two tabs.

     In the **Direct File Access Settings** dialog box, specify how files will be allowed, blocked, or handled in Outlook Web App. The Allow list overrides the Block list and the Force Save list. The Block list overrides the Force Save list. Select the following:
     Allow Click the **Allow** button to specify which types of files should always be allowed. The Allow list overrides the Block list and Force Save list.
     Block Click the **Block** button to specify which types of files should be blocked. The Block list overrides the Force Save list and is overridden by the Allow list.
     Force Save Click the **Force Save** button to specify which types of files the user must save to disk before opening. The Force Save list is overridden by the Allow and Block lists.
     Unknown Files Using the **Unknown Files** list, specify how Outlook Web App handles unknown files that aren't in the Allow list, Block list, or Force Save list.
     When you click **Allow**, **Block**, or **Force Save**, a new window opens in which you can add file name extensions and MIME types to the list you have selected, edit them, or remove them.
     After you have selected **Allow**, **Block**, or **Force Save**:
     To add a file name extension or MIME type, enter it in the appropriate box, and then click **Add**. File name extensions must be preceded by a period (**.**), for example, .exe.
     To edit a file name extension or MIME type, select it, and then click **Edit**.

To remove a file name extension or MIME type, select it, and then click **Remove**.
After you finish modifying the lists of file name extensions and MIME types, click **OK** to save your changes or click **Cancel** to discard your changes and return to the previous window.

WebReady Document Viewing

- **Enable WebReady Document Viewing** Select this check box if you want to enable supported documents to be converted to HTML and displayed in a Web browser.

> **Note:**
> WebReady Document Viewing settings are available for public and private computer file access, and can be different for each.

- **Force WebReady Document Viewing when a converter is available** Select this check box if you want to force documents to be converted to HTML and displayed in a Web browser before users can open them in the viewing application. Documents can be opened in the viewing application only if direct file access has been enabled.
- **Supported** After you select **Enable WebReady Document Viewing**, click **Supported** to select supported document types for **WebReady Document Viewing**.

Select document types to view from an Internet browser
To allow all supported document types to be viewed from an Internet browser, select **All supported document types**.
To allow only specific document types to be viewed, select **Specific document types**.
Add After you select **Specific document types**, click **Add** to add a document type to the list.
Remove After you select **Specific document types**, click the document type that you want to remove, and then click the remove icon.
Select the MIME types of documents Using this list, add the MIME types of documents to the list of types that can be viewed from an Internet browser or remove them from the list.
Add After you select **Specific document types**, click **Add** to add a MIME type to the list.
Remove After you select **Specific document types**, click the MIME type that you want to remove, and then click the remove icon.

8. On the **Private Computer File Access** tab, configure the file access and viewing options available if users select **This is a private computer** while they're signing in to Outlook Web App, or if users sign-in using an authentication method other than forms-based authentication. File access lets users open or view the contents of files attached to an e-mail message.

Direct file access

- **Enable direct file access** Select this check box if you want to enable direct file access. Direct file access lets users open files attached to e-mail messages.
- **Customize** After you select **Enable direct file access**, click **Customize** to customize the direct file access settings.

> **Note:**
> The settings for direct file access are divided into public computer file access settings and private computer file access settings. You can configure these settings on either the **Private Computer File Access** tab or the **Public Computer File Access** tab. However, you can't have different settings on the two tabs.

In the **Direct File Access Settings** dialog box, specify how files will be allowed, blocked, or handled in Outlook Web App. The

Allow list overrides the Block list and the Force Save list. The Block list overrides the Force Save list. Select the following:
Allow Click the **Allow** button to specify which types of files should always be allowed. The Allow list overrides the Block list and the Force Save list.
Block Click the **Block** button to specify which types of files should be blocked. The Block list overrides the Force Save list and is overridden by the Allow list.
Force Save Click the **Force Save** button to specify which types of files the user must save to disk before opening. The Force Save list is overridden by the Allow and Block lists.
Unknown Files Using the **Unknown Files** list, specify how Outlook Web App handles unknown files that aren't in the Allow list, Block list, or Force Save list.
When you click **Allow**, **Block**, or **Force Save**, a new window opens in which you can add file name extensions and MIME types to the list you have selected, edit them, or remove them.
After you have selected **Allow**, **Block**, or **Force Save**:
To add a file name extension or MIME type, enter it in the appropriate box, and then click **Add**. File name extensions must be preceded by a period (**.**), for example, .exe.
To edit a file name extension or MIME type, select it, and then click **Edit**.
To remove a file name extension or MIME type, select it, and then click **Remove**.
After you finish modifying the lists of file name extensions and MIME types, click **OK** to save your changes or click **Cancel** to discard your changes and return to the previous window.

WebReady Document Viewing

- **Enable WebReady Document Viewing** Select this check box if you want to enable supported documents to be converted to HTML and displayed in a Web browser.

  Note:
  WebReady Document Viewing settings are available for public and private computer file access, and can be different for each.

- **Force WebReady Document Viewing when a converter is available** Select this check box if you want to force documents to be converted to HTML and displayed in a Web browser before users can open them in the viewing application. Documents can be opened in the viewing application only if direct file access has been enabled.
- **Supported** After you select **Enable WebReady Document Viewing**, click **Supported** to select supported document types for **WebReady Document Viewing**.

  Select document types to view from an Internet browser
  To allow all supported document types to be viewed from an Internet browser, select **All supported document types**.
  To allow only specific document types to be viewed, select **Specific document types**.
  Add After you select **Specific document types**, click **Add** to add a document type to the list.
  Remove After you select **Specific document types**, click the document type that you want to remove, and then click the remove icon.
  Select the MIME types of documents Using this list, add the MIME types of documents to the list of types that can be viewed from an Internet browser or remove them from the list.
  Add After you select **Specific document types**, click **Add** to add a MIME type to the list.
  Remove After you select **Specific document types**, click the

MIME type that you want to remove, and then click the remove icon.

9. On the **Remote File Servers** tab, specify remote file server access. Outlook Web App accesses only internal Windows file shares. A file name can also be specified by using a fully qualified domain name (FQDN) that's internal or that's included in the list of sites that are to be treated as internal. Outlook Web App uses a simple set of criteria to determine whether an address is internal or external. If there are no dots in a URL that a user clicks, it's treated as internal. If there are one or more dots in the URL, it's treated as internal only if the domain suffix has been added to the list of sites to be treated as internal. Specify the following:
   - **Block** Click this button to specify the host names of servers that aren't allowed to be accessed through Outlook Web App.

     In the **Block List** dialog box, specify the types of files and the MIME types that you want to block from Outlook Web App. The options that you specify in the Block list override the settings that you specify in the Force Save list but are overridden by the settings in the Allow list.

     Note:
     The settings for direct file access are divided into public computer file access settings and private computer file access settings. You can configure these settings on either the **Private Computer File Access** tab or the **Public Computer File Access** tab. However, you can't have different settings for each tab.

     Enter the file extensions you want to block, one at a time In this section, do the following:
     To add a file name extension, enter it in the appropriate box, and then click **Add**. File name extensions must be preceded by a period (.), for example, .exe.
     To edit a file name extension, select it, and then click **Edit**.
     To remove a file name extension, select it, and then click **Remove**.
     After you finish modifying the lists of file name extensions, click **OK** to save your changes or click **Cancel** to discard your changes and return to the previous window.
     Enter the MIME types of files that are blocked In this section, do the following:
     To add a MIME type, enter it in the appropriate box, and then click **Add**.
     To edit a MIME type, select it, and then click **Edit**.
     To remove a MIME type, select it, and then click **Remove**.
     After you finish modifying the MIME types, click **OK** to save your changes or click **Cancel** to discard your changes and return to the previous window.
   - **Allow** Click this button to specify the host names of servers allowed to be accessed through Outlook Web App.

     In the **Allow List** dialog box, specify the types of files and the MIME types that you want to allow in Outlook Web App. The options that you specify in the Allow list override the settings that you specify in the Block list and Force Save list.

     Note:
     The settings for direct file access are divided into public computer file access settings and private computer file access settings. You can configure these settings on either the **Private Computer File Access** tab or the **Public Computer File Access** tab. However, you can't have different settings for each tab.

     Enter the file extensions you want to allow, one at a time In

this section, do the following:
To add a file name extension, enter it in the appropriate box, and then click **Add**. File name extensions must be preceded by a period (.), for example, .exe.
To edit a file name extension, select it, and then click **Edit**.
To remove a file name extension, select it, and then click **Remove**.
After you finish modifying the lists of file name extensions, click **OK** to save your changes or click **Cancel** to discard your changes and return to the previous window.
Enter the MIME types of files that are allowed In this section, do the following:
To add a MIME type, enter it in the appropriate box, and then click **Add**.
To edit a MIME type, select it, and then click **Edit**.
To remove a MIME type, select it, and then click **Remove**.
After you finish modifying the MIME types, click **OK** to save your changes or click **Cancel** to discard your changes and return to the previous window.

- **Unknown Servers** Select **Allow** or **Block** in the **Unknown Servers** list to specify how to handle accessing files from servers that aren't in the Block and Allow lists.
- **Configure** Click this button to specify the domain suffixes of sites that are to be treated as internal. You can also add FQDNs to this list of addresses that are to be treated as internal.

Note:
When you add host names to the Block and Allow lists, you must enter a server name. Entering a Windows file share name won't work.

Use the Shell to configure Outlook Web App virtual directory properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example enables forms-based authentication on the default Outlook Web App virtual directory on the server Contoso.

```
set-OwaVirtualDirectory -Identity "Contoso\owa (default web site)" -FormsAuthenti
```

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

Use the Shell to view Outlook Web App virtual directory properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "View Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example lets you view the properties for all Outlook Web App virtual directories in all Internet Information Services (IIS) Web sites on all computers that have the Client Access server role installed in an Exchange.

```
Get-OWAVirtualDirectory
```

This example lets you view the properties for an Outlook Web App virtual directory on the default IIS Web site on the local Exchange server.

```
Get-OWAVirtualDirectory -identity "<Exchange Server Name>\owa (default web site)"
```

This example lets you view the properties for all Outlook Web App virtual directories on an IIS Web site on a specific Exchange server.

```
Get-OWAVirtualDirectory -server <Exchange Server Name>
```

This example lets you view the values of the properties for every Outlook Web App virtual directory in all IIS Web sites on all Client Access servers in an Exchange organization.

```
Get-OWAVirtualDirectory | format-list
```

For more information about syntax and parameters, see Get-OwaVirtualDirectory.

1.6.2.2.1.3 Remove an Outlook Web App Virtual Directory

Remove an Outlook Web App Virtual Directory

Managing Client Access Servers > Managing Outlook Web App > Managing Outlook Web App Virtual Directories >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to remove a Microsoft Office Outlook Web App virtual directory.

Don't use Internet Information Services (IIS) Manager to remove an Outlook Web App virtual directory. Using IIS Manager to do this may result in what's known as an "orphan" virtual directory. Instead, use the procedure in this topic. You can use the same procedure to remove orphan virtual directories.

If the last Outlook Web App virtual directory to be removed was an orphan virtual directory, you must manually remove the Outlook Web App ISAPI filter from the associated Web site. See the procedures in this topic for how to find orphan virtual directories, and manually remove them.

Looking for other management tasks related to Outlook Web App virtual directories? Check out Managing Outlook Web App Virtual Directories.

Use the Shell to remove an Outlook Web App virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example deletes a virtual directory named `Legacy` from a site named "`second Web site`" on the server named `Contoso`.

```
Remove-OwaVirtualDirectory -identity "Contoso\Legacy (second Web site)"
```

Use the Shell to find orphan virtual directories

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example finds any orphan virtual directories.

```
Get-OwaVirtualDirectory | ? { ![DirectoryServices.DirectoryEntry]::Exists($_.Meta
```

Use IIS Manager to remove the ISAPI filter when the last Outlook Web App virtual directory to be removed was an orphan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "IIS Manager" entry in the Client Access Permissions topic.

1. Open IIS Manager.
2. Navigate to the Web site that hosted the Outlook Web App virtual directory, right-click the Web site name, and then click **Properties**.
3. Click the **ISAPI filters** tab.
4. Remove the *Exchange OWA Cookie Authentication ISAPI filter* entry.

For more information about syntax and parameters, see Remove-OwaVirtualDirectory.

Other Tasks

After you remove an Outlook Web App virtual directory, you may also want to:

- Create an Outlook Web App Virtual Directory
- View or Configure Outlook Web App Virtual Directories

1.6.2.2.1.4 Rename an Outlook Web App Web Site

Rename an Outlook Web App Web Site

Managing Client Access Servers > Managing Outlook Web App > Managing Outlook Web App Virtual Directories >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Internet Information Services (IIS) and the Shell to rename a Microsoft Office Outlook Web App Web site.

Looking for other management tasks related to Outlook Web App virtual directories? Check out Managing Outlook Web App Virtual Directories.

Use the Shell and IIS to rename an Outlook Web App Web site

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" and "IIS Manager" entries in the Client Access Permissions topic.

Important:

Don't rename the Web site that's used by Microsoft Exchange ActiveSync.

1. Remove the Outlook Web App virtual directories that are associated with the Web site that you want to rename. For more information, see Remove an Outlook Web App Virtual Directory.
2. Open IIS Manager, locate the Web Sites/*<Web site to be renamed>* directory. Right-click *<Web site to be renamed>*, and then click **Rename**.
3. Enter the new name and press ENTER.
4. Create new Outlook Web App virtual directories to replace the virtual directories that were deleted in step 1. For more information, see Create an Outlook Web App Virtual Directory.
5. Open a command prompt, and then type `iisreset /noforce` to stop and start IIS.

For more information about syntax and parameters, see Remove-OwaVirtualDirectory and New-OwaVirtualDirectory.

1.6.2.2.2 Managing Outlook Web App URLs

Managing Outlook Web App URLs

Client Access > Managing Client Access Servers > Managing Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-22*

Enable Explicit Sign-in in Outlook Web App

Simplify the Outlook Web App URL

Configure Redirection for Outlook Web App

1.6.2.2.2.1 Enable Explicit Sign-in in Outlook Web App

Enable Explicit Sign-in in Outlook Web App

Managing Client Access Servers > Managing Outlook Web App > Managing Outlook Web App URLs >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use either the EMC or the Shell to grant access to a user to open another user's mailbox or a resource mailbox.

Explicit sign-in enables a user to open another user's mailbox or a resource mailbox by using Outlook Web App. To use this feature, the user must have Full Access permission to the mailbox to be opened. Full Access permission doesn't give the user Send As permission or Delegate access to the mailbox.

When explicit sign-in is used to open a resource mailbox in Outlook Web App, there will be a set of options available to manage that resource.

Looking for other management tasks related to Outlook Web App URLs? Check out Managing Outlook Web App URLs.

Use the EMC to grant Full Access permission to a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. Right-click on the mailbox you want to grant access to, and then select **Manage Full Access Permission**.
3. Click **Add**, and then select the user or group you want to have Full Access permission to the mailbox. You can select multiple users or groups. Click **OK** after you've made your selection.
4. Click **Manage** to run the wizard.
5. Click **Finish** to close the wizard and return to the EMC.

Use the Shell to grant full access to a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

This example grants Full Access permission to the mailbox named `TestA` to the user named `TestB`.

```
Add-MailboxPermission -identity TestA -User TestB -AccessRights FullAccess
```

Open any mailbox from a URL

You must have Full Access permission for the mailbox that you want to open to perform this procedure.

1. Open a Web browser.
2. Enter the URL for your organization's Outlook Web App, and then add the SMTP address of the mailbox that you want to open to the end of the URL. For example, to open the mailbox `conferenceroom@contoso.com`, you would enter *<Outlook Web App URL>*`/conferenceroom@contoso.com`. A mailbox can have more than one SMTP address. You can use any of them to open the mailbox.
3. Sign in by using your user name and password.

Open another user's mailbox or a resource mailbox from Outlook Web App

You must have Full Access permission for the mailbox that you want to open to perform

this procedure.

1. Sign in to Outlook Web App.
2. At the top of the Outlook Web App window, click the drop-down arrow next to your mailbox name, and then click the **Open Other Mailbox** window.
3. Enter the name of the mailbox that you want to open, and then click **Open**.

Note:
To open another user's mailbox or a resource mailbox, your mailbox and the mailbox that you're opening must be Exchange 2010 mailboxes.

For more information about syntax and parameters, see Add-MailboxPermission.

1.6.2.2.2.2 Simplify the Outlook Web App URL

Simplify the Outlook Web App URL

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Internet Information Services (IIS) Manager to simplify the Microsoft Office Outlook Web App URL that users use to access their Microsoft Exchange Server 2010 mailbox.

The first procedure below configures a request that's sent to the root of the Web server (https://*server name*) to redirect to the Exchange virtual directory. For example, a request to https://*server*/ is directed to https://*server*/owa.

The second procedure redirects a request to http://*server* to https://*server*/owa. To help secure the information that's sent between the client and the server, the default Web site is set to require Secure Sockets Layer (SSL) at installation. To simplify access to Outlook Web App for your users, you may want to configure the Outlook Web App Web page, which is usually the default Web site in IIS, to automatically redirect users to https.

When you configure redirection from a top-level directory in Windows Server 2008, the settings are propagated to lower-level directories. For example, when you configure redirection on the Default Web Site to the /owa virtual directory, the settings that you configure also appear on the HTTP Redirect page of all the virtual directories, such as /Autodiscover, /Exchange, and /Public. Therefore, you must remove redirection from all the virtual directories except the one that you want redirected.

Looking for other management tasks related to Outlook Web App URLs? Check out Managing Outlook Web App URLs.

Use IIS Manager and Notepad to simplify the Outlook Web App URL when SSL isn't required

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "IIS Manager" entry in the Client Access Permissions topic.

1. Start IIS Manager.
2. Expand the local computer, expand Sites, and then click **Default Web Site**.
3. At the bottom of the Default Web Site Home pane, click **Features View** if this

option isn't already selected.
4. In the IIS section, double-click **HTTP Redirect**.
5. Select the **Redirect requests to this destination** check box, and then type /owa.
6. Under **Redirect Behavior**, select the **Only redirect requests to content in this directory (not subdirectories)** check box.
7. In the Status code list, click **Found (302)**.
8. In the Actions pane, click **Apply**.
9. Close IIS Manager
10. Find the Outlook Web App Web.config file on the Client Access server. The default location is *<drive>*\Program Files\Microsoft\Exchange Server*<version>*\ClientAccess\Owa.
11. Make a backup copy of the file.
12. Open the original file using an editor such as Notepad. Don't use IIS Manager to edit the Web.config file.
13. Find *httpCookies httpOnlyCookies="false" requireSSL="true" domain=""* and change the requireSSL flag to false.
14. Save and close the file.

Note:
If Outlook Web App is configured for plain-text HTTP only for the purpose of SSL offloading, then this additional step of modifying the web.config file is not required.

15. For the new settings to take effect, open a Command Prompt window, and then type *iisreset /noforce* to restart IIS.

Note:
If SSL is required, you must redirect HTTP to HTTPS and then also redirect to the /owa virtual directory. If you don't do this, users will receive an error message when they try to access Outlook Web App without specifying the virtual directory. To do this, use the following procedure.

Use IIS Manager to simplify the Outlook Web App URL when SSL is required

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "IIS Manager" entry in the Client Access Permissions topic.

1. Start IIS Manager.
2. Expand the local computer, expand Sites, and then click **Default Web Site**.
3. At the bottom of the Default Web Site Home pane, click **Features View** if this option isn't already selected.
4. In the **IIS** section, double-click **HTTP Redirect**.
5. Select the **Redirect requests to this destination** check box.
6. Type the absolute path of the /owa virtual directory. For example, type https://mail.contoso.com/owa.
7. Under **Redirect Behavior**, select the **Only redirect requests to content in this directory (not subdirectories)** check box.
8. In the **Status code** list, click **Found (302)**.
9. In the Actions pane, click **Apply**.
10. Click **Default Web Site**.
11. In the Default Web Site Home pane, click **SSL Settings**.
12. In SSL Settings, clear **Require SSL**.

Note:
If you don’t clear Require SSL, users won’t be redirected when they enter an unsecured URL. Instead, they’ll get an access denied error.

13. For the new settings to take effect, open a Command Prompt window, and then type *iisreset /noforce* to restart IIS.

Modify permissions on the Offline Address Book web.config file

After you've configured redirection for the Default Web Site, you have to edit the permissions on the Offline Address Book web.config file. If you don't complete this step, users won't be able to download the Offline Address Book when using Outlook.

1. Find the Offline Address Book Web.config file on the Client Access server. The default location is <*drive*>\Program Files\Microsoft\Exchange Server\<*version*>\ClientAccess\oab.
2. Right-click the file and click **Properties**.
3. Click the **Security** tab.
4. Click **Edit**.
5. Under **Group or user names**, select **Authenticated Users**. Under **Permissions for Authenticated Users**, click **Read & execute**.
6. Click **OK** twice to save your changes and close the properties window.

Use IIS Manager to remove redirection from a virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "IIS Manager" entry in the Client Access Permissions topic.

To remove redirection from a virtual directory, perform the following steps:

1. Start IIS Manager.
2. Navigate to the virtual directory.
3. Double-click the **HTTP Redirect** icon in the **Features** view of the virtual directory.
4. Clear the **Redirect requests to this destination** check box.
5. In the Actions pane, click **Apply**.
6. For the new settings to take effect, open a Command Prompt window, and then type *iisreset /noforce* to restart IIS.

You may not be able to use the procedure above to remove redirection from a virtual directory that doesn't have a physical path, such as /Exchange, /Exchweb, or /Public. Use the following procedure to remove redirection from a virtual directory that doesn't appear in IIS Manager.

1. Open a command window
2. Navigate to <Window directory>\System32\Inetsrv
3. Run the following commands:

```
3.a.appcmd set config "Default Web Site/autodiscover" /
  section:httpredirect /enabled:false -commit:apphost
3.b.appcmd set config "Default Web Site/ecp" /
  section:httpredirect /enabled:false -commit:apphost
3.c.appcmd set config "Default Web Site/ews" /
  section:httpredirect /enabled:false -commit:apphost
3.d.appcmd set config "Default Web Site/owa" /
  section:httpredirect /enabled:false -commit:apphost
3.e.appcmd set config "Default Web Site/oab" /
  section:httpredirect /enabled:false -commit:apphost
3.f.appcmd set config "Default Web Site/powershell" /
  section:httpredirect /enabled:false -commit:apphost
3.g.appcmd set config "Default Web Site/rpc" /
  section:httpredirect /enabled:false -commit:apphost
3.h.appcmd set config "Default Web Site/rpcwithcert" /
  section:httpredirect /enabled:false -commit:apphost
3.i.appcmd set config "Default Web Site/Microsoft-Server-
```

```
ActiveSync" /section:httpredirect /enabled:false -
commit:apphost
```

4. Finish by running the command `iisreset/noforce`.

When you configure redirection from a top-level directory, a web.config file may be created under <*drive*>\Program Files\Microsoft\Exchange Server\<*version*>\ClientAccess\oab. If this has happened and you later remove redirection, Outlook 2007 and Outlook 2010 may freeze when users click **Send and Receive**. To avoid this happening after you remove redirection, delete the web.config file from <*drive*>\Program Files\Microsoft\Exchange Server\<*version*>\ClientAccess\oab.

Other Tasks

After you simplify the Outlook Web App URL, you may also want to Enable Explicit Sign-in in Outlook Web App.

1.6.2.2.2.3 Configure Redirection for Outlook Web App

Configure Redirection for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

In a Microsoft Exchange Server 2010 organization, Microsoft Office Outlook Web App is provided by a Client Access server. If you have multiple Active Directory sites that have Client Access servers that can be reached from the Internet, you can use redirection to route users to the Client Access server that will give them the best Outlook Web App experience. If you have multiple Client Access servers in different Active Directory sites in an organization, and only one is exposed to the Internet, you can use Client Access server-to-Client Access server proxying to direct users to the Client Access server that will give them the best Outlook Web App experience.

1.6.2.2.3 Managing File and Data Access for Outlook Web App

Managing File and Data Access for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-21*

Configure Public and Private Computer File Access

Configure WebReady Document Viewing

Configure Maximum Message Size in Outlook Web App

Configure Public and Private Computer File Access

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Direct file access lets users open files that are attached to e-mail messages and files that are stored in Windows file shares. You can manage direct file access for Microsoft Office Outlook Web App in Microsoft Exchange Server 2010 for both public and private computers.

By default, public computer direct file access is enabled for new installations and upgrades of Outlook Web App. Therefore, when users in your organization select **This is a public or shared computer** or **This is a private computer** on the Outlook Web App sign-in page, they will be able to access files that are attached to e-mail messages.

When you enable private or public computer file access for users, you can use the EMC to specify individual file types and MIME types. The following table lists the file name extensions and MIME types that, by default, are set to Allow, Block, or Force Save for the \owa virtual directory.

- **Allow** File and MIME types in the Allow list can be opened from Outlook Web App if the application that's needed to open the files is installed on the client computer. Allow overrides Block and Force Save.
- **Block** File and MIME types in the Block list can't be opened. Block overrides Force Save and is overridden by Allow.
- **Force Save** File and MIME types in the Force Save list must be saved to the client computer before they can be opened. Force Save is overridden by Allow and Block.

Note:

Although it appears that you can set the values for private and public computer access individually, you can't. When you specify behavior for private access, you also set it for public access.

Default file name extensions and MIME values for the Allow, Block, and Force Save settings for the \owa virtual directory

Option	Description	Default file name extensions	Default MIME types
Allow	This option specifies the file types that are always enabled for direct file access.	.rpmsg, .xlsx, .xlsm, .xlsb, .pptx, .pptm, .ppsx, .ppsm, .docx, .docm, .xls, .wmv, .wma, .wav, vsd, .txt, .tif, .rtf, .pub, .ppt, .png, .pdf, .one, .mp3, .jpeg, .gif, .doc, .bmp, .avi	image/jpeg, image/png, image/gif, image/bmp
Block	This option specifies the file types that are always blocked from direct file access.	.ade, .adp, .asx, .app, .asp, .aspx, .bas, .bat, .cer, .chm, .cmd, .com, .cpl, .crt, .csh, .dir, .dcr, .der, .exe, .fxp, .hlp, .hta, .inf, .ins, .isp	application/x-javascript, application/javascript, application/msaccess, x-internet-signup, text/javascript,

		, .its, .js, .jse, .ksh, .lnk, .mad, .maf, .mag, .mam, .maq, .mar, .mas, .mat, .mau, .mav, .maw, .mda, .mdb, .mde, .mdt, .mdw, .mdz, .msc,.msh, .msh1, .mshxml, .msh1xml, .msi, .msp,.mst, .ops, .pcd, .pif, .plg, .prf,.prg, .ps1, .ps2, .psc1, .psc2, .ps1xml, .ps2xml, .pst, .reg, .scf, .scr, .sct, .shb, .shs, .spl, .swf, .tmp, .url, .vb, .vbe, .vbs, .vsmacros, .vss, .vst, .vsw, .ws, .wsc, .wsf, .wsh, .xml	application/prg, application/hta, text/scriptlet
Force Save	This option specifies the files that users can access only after they've saved them to the local computer.	.vsmacros, .mshxml, .aspx, .xml, .wsh, .wsf, .wsc, .vsw, .vst, .vss, .vbs, .vbe, .url, .tmp, .swf, .spl, .shs, .shb, .sct, .scr, .scf, .reg, .pst, .prg, .prf, .plg, .pif, .pcd, .ops, .mst, .msp, .msi, .msh, .msc, .mdz, .mdw, .mdt, .mde, .mdb, .mda, .maw, .mav, .mau, .mat, .mas, .mar, .maq, .mam, .mag, .maf, .mad, .lnk, .ksh, .jse, .its, .isp, .ins, .inf, .hta, .hlp, .fxp, .exe, .dir, .dcr, .csh, .crt, .cpl, .com, .cmd, .chm, .cer, .bat, .bas, .asx, .asp, .app, .adp, .ade, .ws, .vb, .js	Application/x-shockwave-flash, Application/octet-stream, Application/futuresplash, Application/x-director, Application/xml, text/xml

There is also a default setting for unknown file types. You can set the setting for unknown file types to one of the following values:

- Allow
- Block
- Force Save

Note:

By default, attachment types that are marked as **Force Save** will be excluded from security checks for XML or HTML. You can change this behavior by setting the *ForceSaveAttachmentFilteringEnabled* parameter to `$true` by using either the Set-OwaMailboxPolicy or the Set-OwaVirtualDirectory cmdlet.

Looking for other management tasks related to accessing files from Outlook Web App? Check out Managing File and Data Access for Outlook Web App.

Use the EMC to configure direct file access

policy settings for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the action pane, in **Outlook Web App**, click **Properties**.
3. On the **Outlook Web App Properties** page, click either the **Public Computer File Access** tab or the **Private Computer File Access** tab.
4. Under **Direct file access**, select the check box next to **Enable direct file access** to let users download attachments.
5. To modify the types of attachments that you want users to be able to access, click **Customize** next to **Customize direct file access**.
6. On the **Direct File Access Settings** page, do one of the following:
   - To set the file types and MIME types that you want users to access, click **Allow**, and then set the file name extensions and MIME values on the **Allow List** page.
   - To set the file types and MIME types that you want to block users from accessing, click **Block**, and then and set the file name extensions and MIME values on the **Block List** page.
   - To set the file types and MIME types that you want to force users to save before they access them, click **Force Save**, and then set the file name extensions and MIME values on the **Force Save List** page.
   - For unknown file types, select an option from the list in the **Unknown Files** box. Select **Allow**, **Block**, or **Force Save**.
7. Click **OK** to save your settings.

Use the Shell to configure attachments policy settings for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example prevents users on public computers from downloading files.

```
Set-OwaVirtualDirectory -identity "owa (Default Web Site)" -DirectFileAccessOnPub
```

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

Other Tasks

After you configure direct file access, you may also want to:

- Configure WebReady Document Viewing
- Configure Maximum Message Size in Outlook Web App

1.6.2.2.3.2 Configure WebReady Document Viewing

Configure WebReady Document Viewing

Managing Client Access Servers > Managing Outlook Web App > Managing File and Data Access for Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

WebReady Document Viewing lets users access file attachments in Microsoft Office Outlook Web App. Users can access common file types such as Microsoft Word documents without having the application installed.

You can manage WebReady Document Viewing for Outlook Web App in Microsoft Exchange Server 2010.

When you manage WebReady Document Viewing, you can specify files that you want users to be able to access within Outlook Web App for private and public computers. However, you can't specify individual settings for only private or public computers.

By default, public computer file access isn't enabled for Outlook Web App. Therefore, when users select the **This is a public or shared computer** option or the **This is a private computer** option on the Outlook Web App sign-in page, they won't be able to access files attached to e-mail messages.

Looking for other management tasks related to accessing files from Outlook Web App? Check out Managing File and Data Access for Outlook Web App.

Use the EMC to manage WebReady Document Viewing settings for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the work pane, select **owa (Default Web Site)**, and then, in the action pane, click **Properties**.
3. On the **Outlook Web App Properties** page, click the **Private Computer File Access** or **Public Computer File Access** tab.
4. Under **WebReady Document Viewing**, select the check box next to **Enable WebReady Document Viewing** to let users view common file types in Outlook Web App.
5. To modify the types of files that you want users to be able to view in Outlook Web App, click **Supported** under **WebReady Document Viewing**.
6. On the **WebReady Document Viewing Settings** page, select the default values or delete one or more of the file types.
7. Click **OK** to save your changes.

Use the Shell to configure attachment policy settings for Outlook Web App

You need to be assigned permissions before you can run this cmdlet. Although all parameters for this cmdlet are listed in this topic, you may not have access to some parameters if they're not included in the permissions assigned to you. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example uses the **Set-OwaVirtualDirectory** cmdlet to prevent users on public computers from downloading files.

```
Set-OwaVirtualDirectory -identity "owa (Default Web Site)" -WebReadyDocumentViewi
```

For information about syntax and parameters, see Set-OwaVirtualDirectory.

Other Tasks

After you configure WebReady Document Viewing settings, you may also want to:

- Configure Public and Private Computer File Access
- Configure Maximum Message Size in Outlook Web App

1.6.2.2.3.3 Configure Maximum Message Size in Outlook Web App

Configure Maximum Message Size in Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can edit the Web.config file on a Client Access server to enable large messages to be sent by using Outlook Web App. Outlook Web App is an application that uses ASP.NET and is affected by the configuration of ASP.NET settings.

The ASP.NET setting that determines the maximum amount of data that the Web browser can submit to the Client Access server is *maxRequestLength*. The *maxRequestLength* setting is found in the Web.config file. If the setting for the maximum message size for sending on a mailbox is more than the *maxRequestLength* setting, messages that are sent from Outlook Web App that exceed the *maxRequestLength* value will generate an error that might be confusing to users. To avoid this, you must configure the *maxRequestLength* to be at least as large as the largest maximum send size on the mailboxes in your organization.

Conditions and Associated Warnings

If a user tries to create or send a message that exceeds the maximum message size or *maxRequestLength*, a warning will appear in Outlook Web App. The text of the warning will vary, depending on the conditions that generated it.

- If a user tries to upload an attachment that's larger than the maximum message size, they receive the following error message in the upload dialog box: "Your attachment is larger than the maximum limit for attachments."
- If a user tries to upload one or more attachments that are larger than the ASP.NET *MaxRequestLength*, they receive the following error message in the Information Bar within the message: "The files *<file names>* weren't attached because they exceed the maximum size limit of *<size limit>* MB for attachments."
- If a user attaches several files, each of which is smaller than either the maximum message size or *maxRequestLength* but which, together, amount to more than the maximum message size, Outlook Web App displays the following message as a banner on the message form when the user clicks **Send**: "This message couldn't be sent because it exceeds the maximum size allowed."

- The default attachment size limit for a single attachment is 10 MB. To change this value for the organization, you can change the **Maximum receive size (KB)** and **Maximum send size (KB)** settings. After you change one or more these settings, you must restart the Exchange Information Store service for the changes to take effect.
  For more information about how to change the Exchange 2010 Transport Settings, see: Configure Transport Settings Properties.

Looking for other management tasks related to accessing files from Outlook Web App? Check out Managing File and Data Access for Outlook Web App.

Use Notepad to change the maxRequestLength value

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Text editor" entry in the Client Access Permissions topic.

1. Find the Outlook Web App Web.config file on the Client Access server. The default location is *<drive>*\Program Files\Microsoft\Exchange Server\V14 \ClientAccess\Owa.
2. Make a backup of the file.
3. Open the original file in a text editor, such as Notepad. Don't use Internet Information Services (IIS) Manager to edit the Web.config file.
   Change the requestLimits maxAllowedContentLength and httpRuntime maxRequestLength values to increase or decrease the message size
4. Find *maxRequestLength*, and change it to the value that you want. The value is stored in kilobytes (KB). The default value is 35000. The following example shows the *maxRequestLength* value in the Web.config file.
   `<httpRuntime maxRequestLength="35000" />`
5. Find *maxAllowedContentLength* and change it to the value that you want. The value is stored in bytes. The default value is 35000000, for example:
   `<requestLimits maxAllowedContentLength="35000000" />`
6. Save and close the file.

Caution:

Before you make changes to the Web.config file, make a copy of the file, and store it in a safe location.

Other Tasks

After you set the maximum message size, you may also want to do the following:

- Configure Public and Private Computer File Access
- Configure WebReady Document Viewing

1.6.2.2.4 Managing Outlook Web App Advanced Features

Managing Outlook Web App Advanced Features

Client Access > Managing Client Access Servers > Managing Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-12*

1.6.2.2.4.1 Configure Segmentation in Outlook Web App

Configure Segmentation in Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Segmentation lets you enable and disable many features in Outlook Web App. You can manage segmentation using the EMC or the Shell.

By default, segmentation changes take effect after 60 minutes of inactivity for users who are signed in to Outlook Web App, or when a user signs in to Outlook Web App. To force the changes to take effect immediately, restart Internet Information Services (IIS) by running the command `iisreset/noforce` on the Client Access server.

Looking for other advanced management tasks for Outlook Web App? Check out Managing Outlook Web App Advanced Features.

Segmentation in the EMC and the Shell

The following table lists the segmentation options that are available in the EMC and by using the Shell.

Segmentation options that can be set in the EMC and by using the Shell

EMC	Shell parameter	Description
All Address Lists	*AllAddressListsEnabled*	If it's enabled, this option lets users see all address lists in the Exchange organization. If it's disabled, the user will see only the

		default global address list.
Calendar	*CalendarEnabled*	If it's enabled, this option lets users see Calendar folders using Outlook Web App. If it's disabled, the Calendar is still available using Outlook but won't be visible from Outlook Web App.
Change Password	*ChangePasswordEnabled*	If it's enabled, this option lets users change their Active Directory account password using Outlook Web App.
Contacts	*ContactsEnabled*	If it's enabled, this option lets users see Contacts folders using Outlook Web App. If it's disabled, Contacts folders are still available using Outlook but won't be visible from Outlook Web App.
E-mail Signature	*SignaturesEnabled*	If it's enabled, this option lets users use the Outlook Web App **Options** to manage signatures for outgoing e-mail messages.
Exchange ActiveSync Integration	*ActiveSyncIntegrationEnabled*	If it's enabled, this option lets users manage a mobile phone by using the **Options** feature in Outlook Web App. If it's disabled, the option isn't visible.
Instant Messaging	*InstantMessagingEnabled*	If it's enabled, this option makes instant messaging in Outlook Web App available to users. This feature isn't available in the light version of Outlook Web App.
Journal	*JournalEnabled*	If it's enabled, this option lets users see the Journal folder using Outlook Web App. If it's disabled, the Journal is still available using Outlook but won't be visible from Outlook Web App.
Junk E-mail Filtering	*JunkEmailEnabled*	If it's enabled, this option enables users to control the junk e-mail settings for their mailbox from Outlook Web App. If it's disabled, the user

		won't be able to control the junk-email settings from Outlook Web App. But any settings that are set by an administrator or by using Outlook will still be applied.
Notes	*NotesEnabled*	If it's enabled, this option makes the Notes folder visible in Outlook Web App. Outlook Web App provides view-only access to Notes.
Premium Client	*PremiumClientEnabled*	If it's enabled, this option lets users access the standard Outlook Web App client. If it's disabled, only the light version of Outlook Web App will be available.
Public Folders	*PublicFoldersEnabled*	If it's enabled, this option lets users browse or read items in public folders using Outlook Web App.
Recover Deleted Items	*RecoverDeletedItemsEnabled*	If it's enabled, this option lets users view, recover, or permanently delete items that were deleted from the Deleted Items folder by using Outlook Web App.
Reminders and Notifications	*RemindersAndNotificationsEnabled*	If it's enabled, this option lets users receive reminders for calendar items and tasks and notifications for new messages. If it's disabled, users won't receive reminders and notifications. Reminders and notifications are not available in the light version of Outlook Web App.
Rules	*RulesEnabled*	If it's enabled, this option lets users view, create, or modify server-side rules using Outlook Web App.
S/MIME	*SMimeEnabled*	If it's enabled, this option lets users download the S/MIME control for Outlook Web App and use it to read and compose signed and encrypted messages.
Search Folders	*SearchFoldersEnabled*	If it's enabled, this option lets users see the **Search Folders** icon in the Outlook Web App navigation pane

		and lets them access any search folders that exist on the server. If it's disabled, the **Search Folders** icon remains visible in Outlook Web App. But the folders won't be available. For more information about how to create search folders, see the Outlook Help.
Spelling Checker	*SpellCheckerEnabled*	If it's enabled, this option lets users check spelling in Outlook Web App. This feature isn't available in the light version of Outlook Web App.
Tasks	*TasksEnabled*	If it's enabled, this option makes the **Tasks** features in Outlook Web App available to users. This feature isn't available in the light version of Outlook Web App.
Text Messaging	*TextMessagingEnabled*	If it's enabled, this option lets user send and receive text messages in Outlook Web App. This feature isn't available in the light version of Outlook Web App.
Theme Selection	*ThemeSelectionEnabled*	If it’s enabled, this parameter allows users to select a theme in Outlook Web App.
Unified Messaging Integration	*UMIntegrationEnabled*	If it's enabled, this option lets users manage their Unified Messaging settings by using Outlook Web App.

Use the EMC to configure Outlook Web App segmentation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the work pane, select the server that hosts the Outlook Web App virtual directory you want to modify.
3. From the work pane, on the **Outlook Web App** tab, select **owa (Default Web Site)**, and then, in the action pane, click **Properties**.
4. On the **owa (Default Web Site) Properties** page, click the **Segmentation** tab.
5. The **Segmentation** window provides a list of features for Outlook Web App that you can enable or disable for all users.
6. To enable or disable a feature for Outlook Web App for all users, select a

feature, and then click **Enable** or **Disable**.
7. The status for all features is displayed in the center section in the **Segmentation** window.

Use the Shell to configure Outlook Web App segmentation

For a detailed description and examples of how to use the Shell to configure Outlook Web App segmentation, see Set-OwaVirtualDirectory.

1.6.2.2.4.2 Configure Gzip Compression Settings

Configure Gzip Compression Settings

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to configure Gzip compression for Microsoft Office Outlook Web App in Microsoft Exchange Server 2010. Gzip compression improves performance over slow network connections by compressing content on the server. Gzip compression might slow performance on the server.

Note:
By default, Gzip compression is set to low.

Looking for other advanced management tasks for Outlook Web App? Check out Managing Outlook Web App Advanced Features.

Use the Shell to configure Gzip compression

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example configures Gzip compression to `High` on an Outlook Web App virtual directory that's named `owa` in the default Internet Information Services (IIS) Web site on the local server.

```
Set-OwaVirtualDirectory -identity "owa (Default Web Site)" -GzipLevel High
```

This example sets Gzip compression to `Off` on an Outlook Web App virtual directory that's named `owa` in the default IIS Web site on the local server.

```
Set-OwaVirtualDirectory -identity "owa (Default Web Site)" -GzipLevel Off
```

Note:
You must restart IIS by using the command `iisreset/noforce` for these changes to take effect.

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

1.6.2.2.4.3 Configure Character Settings for Outlook Web App

Configure Character Settings for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to configure the character settings on Microsoft Office Outlook Web App virtual directories in Microsoft Exchange Server 2010. For more information about character settings in Outlook Web App, see Managing Outlook Web App Advanced Features.

Looking for other advanced management tasks for Outlook Web App? Check out Managing Outlook Web App Advanced Features.

Use the Shell to configure character settings for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example configures Outlook Web App to always use UTF-8 encoded UNICODE characters on all outgoing e-mail messages.

```
Set-OwaVirtualDirectory -identity "Owa (Default Web Site)" -OutboundCharset Alway
```

Note:
The *AlwaysUTF8* character setting on the Outlook Web App virtual directory takes precedence over user-defined settings. Outlook Web App sets the UTF-8 character on all outgoing e-mail messages, regardless of the user's language choice in Outlook Web App.

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

Other Tasks

After you configure character settings for Outlook Web App, you may also want to Configure Language Settings for Outlook Web App.

1.6.2.2.4.4 Configure Language Settings for Outlook Web App

Configure Language Settings for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The language setting determines the language of the Microsoft Office Outlook Web App sign-in page and error messages. It can be changed by the user at any time. You can use Outlook Web App or the Microsoft to configure language settings for Outlook Web App.

About Language Settings

You can configure three language settings for Outlook Web App.

- The sign-in and error language setting applies to individual Outlook Web App virtual directories. The sign-in and error language is the language that will be used for errors and the forms-based authentication sign-in page. If a value isn't set for this language, the default value is *0*. This means that the default sign-in and error language isn't defined. If the sign-in and error language isn't defined, Outlook Web App will default first to the language set on the Web browser on the client computer. If the language set on the Web browser on the client computer isn't supported by Outlook Web App, Outlook Web App will use the language of the Client Access server.
- The default client language setting applies to individual Outlook Web App virtual directories. The default client language is the client language that's used by Outlook Web App unless the user uses **Regional Settings** in Outlook Web App to change the language and time zone. The default value for this setting is *0*. This means the default client language isn't defined. If the default client language isn't defined, users will be prompted to choose a language and time zone the first time that they sign in to Outlook Web App. If the default client language value is defined, users won't be prompted to choose a language and the Outlook Web App time zone will use the time zone of the Client Access server. Defining the default client language causes the default folders to be renamed based on the specified language. Users can change the client language and time zone by using **Regional Settings** in Outlook Web App and can rename the default folders after they sign in.
- The client languages are set on individual mailboxes and affect the language that's used in Outlook and Outlook Web App. If multiple languages are configured, the first language in the list that's supported by the Web browser will be used. If none of the languages in the default languages list are supported by the Web browser, the Client Access server language will be used.
- To support labels such as **To** and **From** in languages other than English, the appropriate language pack must be installed on the Client Access server and the Mailbox server.

Looking for other advanced management tasks for Outlook Web App? Check out Managing Outlook Web App Advanced Features.

Prerequisites

Note:
For all Arabic, Hebrew, and Urdu text to be displayed correctly in Outlook Web App, support for languages that are read from right-to-left and for script languages must be installed on the client computer. Asian languages might also require that the East Asian language support be installed on the client computer.

The following table lists the languages and locales that can be configured in the Shell, and their associated codes.

Available languages and locales and their associated codes

Language (Locale)	Code

Arabic (Algeria)	5121
Arabic (Bahrain)	15361
Arabic (Egypt)	3073
Arabic (Iraq)	2049
Arabic (Jordan)	11265
Arabic (Kuwait)	13313
Arabic (Lebanon)	12289
Arabic (Libya)	4097
Arabic (Morocco)	6145
Arabic (Oman)	8193
Arabic (Qatar)	16385
Arabic (Saudi Arabia)	1025
Arabic (Syria)	10241
Arabic (Tunisia)	7169
Arabic (U.A.E.)	14337
Arabic (Yemen)	9217
Basque	1069
Bulgarian	1026
Catalan	1027
Chinese (Hong Kong S.A.R)	3076
Chinese (Macau S.A.R)	5124
Chinese (People's Republic of China)	2052
Chinese (Singapore)	4100
Chinese (Taiwan)	1028
Croatian	1050
Czech	1029
Danish	1030
Dutch (Belgium)	2067
Dutch (Netherlands)	1043
English (Australia)	3081
English (Belize)	10249
English (Canada)	4105
English (Caribbean)	9225

English (Ireland)	6153
English (Jamaica)	8201
English (New Zealand)	5129
English (Republic of the Philippines)	13321
English (South Africa)	7177
English (Trinidad)	11273
English (United Kingdom)	2057
English (United States)	1033
English (Zimbabwe)	12297
Estonian	1061
Filipino (Philippines)	1124
Finnish	1035
French (Belgium)	2060
French (Canada)	3084
French (France)	1036
French (Luxembourg)	5132
French (Principality of Monaco)	6156
French (Switzerland)	4108
German (Austria)	3079
German (Germany)	1031
German (Liechtenstein)	5127
German (Luxembourg)	4103
German (Switzerland)	2055
Greek	1032
Hebrew	1037
Hindi	1081
Hungarian	1038
Icelandic	1039
Indonesian	1057
Italian (Italy)	1040
Italian (Switzerland)	2064
Japanese	1041
Kazakh	1087

Korean	1042
Latvian	1062
Lithuanian	1063
Malay	1086
Norwegian (Bokmål)	1044
Persian	1065
Polish	1045
Portuguese (Brazil)	1046
Portuguese (Portugal)	2070
Romanian	1048
Russian	1049
Serbian (Cyrillic)	3098
Serbian (Latin)	2074
Slovak	1051
Slovenian	1060
Spanish (Argentina)	11274
Spanish (Bolivia)	16394
Spanish (Chile)	13322
Spanish (Colombia)	9226
Spanish (Costa Rica)	5130
Spanish (Dominican Republic)	7178
Spanish (Ecuador)	12298
Spanish (El Salvador)	17418
Spanish (Guatemala)	4106
Spanish (Honduras)	18442
Spanish (Mexico)	2058
Spanish (Nicaragua)	19466
Spanish (Panama)	6154
Spanish (Paraguay)	15370
Spanish (Peru)	10250
Spanish (Puerto Rico)	20490
Spanish (International Sort)	3082
Spanish (Traditional Sort)	1034

Spanish (Uruguay)	14346
Spanish (Venezuela)	8202
Swedish (Finland)	2077
Swedish (Sweden)	1053
Thai	1054
Turkish	1055
Ukrainian	1058
Urdu	1056
Vietnamese	1066

Use the Outlook Web App client to configure language settings

1. Use a Web browser to sign in to a mailbox that you have full access permission to via Outlook Web App.
2. Click **Options**, and then click **Regional Settings**.
3. Under **Language**, in the **Choose language** list, click the language that you want to use.

   Note:
   The language that you select will determine the date and time settings in the **Date and Time Formats** section.

4. Click **Save** to save your language settings.

Use the Shell to configure language settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

Use the Shell to configure the sign-in and error language settings for Outlook Web App

This example sets the sign-in and error language setting.

```
Set-OwaVirtualDirectory -identity "Owa (Default Web Site)" -LogonAndErrorLanguage
```

Use the Shell to configure the default client language setting for an Outlook Web App virtual directory

This example sets the default client language setting.

```
Set-MailboxRegionalConfiguration -Identity <Username> -Language <language code>
```

Use the Shell to configure the client language setting for an individual mailbox

This example sets the client languages setting for an individual mailbox.

```
Set-Mailbox -identity <mailbox identity> -languages <language code>
```

For more information about syntax and parameters, see Set-OwaVirtualDirectory and Set-

Mailbox.

Other Tasks

After you configure language settings, you may also want to Configure Character Settings for Outlook Web App.

1.6.2.2.4.5 Configure Web Beacon and HTML Form Filtering for Outlook Web App

Configure Web Beacon and HTML Form Filtering for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to disable Web beacons and HTML forms on Outlook Web App. A Web beacon is a file object, such as a transparent graphic or an image, that's put on a Web site or in an e-mail message. Web beacons are typically used together with HTML cookies to monitor user behavior on a Web site or to validate a recipient's e-mail address when an e-mail message that contains a Web beacon is opened. Web beacons and HTML forms can also contain harmful code and can be used to circumvent e-mail filters.

By default, Web beacons and HTML forms are set to *UserFilterChoice*. This blocks all Web beacons and HTML forms but lets the user unblock them on individual messages. An administrator can use the Shell to change the type of filtering that's used for Web beacon and HTML form content in Outlook Web App.

Web beacon configuration is set on a per virtual directory basis for each Outlook Web App virtual directory in your organization.

For more information about Web beacons, see Managing Outlook Web App Advanced Features.

Looking for other advanced management tasks for Outlook Web App? Check out Managing Outlook Web App Advanced Features.

Use the Shell to block Web beacons and HTML forms in Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example blocks all Web beacon and HTML form content on an Outlook Web App virtual directory named `Owa` in the default Internet Information Services (IIS) Web site on the local server.

```
Set-OwaVirtualDirectory -identity "Owa (Default Web Site)" -FilterWebBeaconsAndHt
```

The possible values for `FilterWebBeaconsandHtmlforms` are as follows:

- `UserFilterChoice` By default, this value blocks Web beacons and HTML

forms, but lets the user allow Web beacons and HTML forms on individual messages.
- `ForceFilter` This value blocks all Web beacons and HTML forms.
- `DisableFilter` This value allows Web beacons and HTML forms.

Note:
Both `UserFilterChoice` and `ForceFilter` give the user an option to unblock blocked content on individual messages. If the parameter has been set to `ForceFilter`, the content will remain blocked regardless of the user's choice.

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

1.6.2.2.4.6 Specify Address Lists in Outlook Web App

Specify Address Lists in Outlook Web App

Managing Client Access Servers > Managing Outlook Web App > Managing Outlook Web App Advanced Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use ADSI Edit to control which address lists are available to users when they use Outlook Web App for Microsoft Exchange Server 2010.

Looking for other advanced management tasks for Outlook Web App? Check out Managing Outlook Web App Advanced Features.

Use ADSI Edit to limit the address lists that are available to a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. Open ADSI Edit.
2. Locate the user for whom you want to set an address list value.
3. Open the properties for that user, and then add the appropriate value for the *querybaseDN* parameter.
4. Save the changes to that user's properties.

How QuerybaseDN Is Used

The *querybaseDN* parameter is found on Active Directory user objects. By setting the value of *querybaseDN*, you can control which address list a user has access to through Outlook Web App. You do this by assigning the distinguished name of an address list or organizational unit (OU) to the *querybaseDN* parameter.

The following conditions apply to the use of *querybaseDN*:

- If the *querybaseDN* parameter isn't used, the user will have access to the first global address list (GAL) that's listed in the **globalAddressList** attribute for that user.
- If the *querybaseDN* parameter is set to a specific address list, the user will have access only to that address list.
  - If the user uses **Select Rooms** in the Scheduling Assistant, they'll see only resources from the specified address list.
- If the *querybaseDN* parameter is set to a specific OU and the

displayAddressLists parameter is set to `$false`, the user won't have access to any address lists. If the *querybaseDN* parameter is set to a specific OU and the *displayAddressLists* parameter is set to `$true`, the user will have access only to users in the OU that is specified by the *querybaseDN* parameter.

- If the user uses **Select Rooms** in the Scheduling Assistant, they'll see only resources from the specified OU.

Use ADSI Edit to find the distinguished name of an address list or organizational unit

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. Open ADSI Edit.
2. Find the address list or OU that you want to use, right-click it, and then click **Properties**.
3. Find the distinguished name of the address list or OU.

Use the Shell to find address lists in your organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

Enter **Get-AddressList** to return all the address lists under the All Address Lists container.

For more information about syntax and parameters, see Get-AddressList.

1.6.2.2.4.7 Configuring the Change Password Feature in Outlook Web App

Configuring the Change Password Feature in Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Change Password feature in Microsoft Office Outlook Web App enables domain users to change their password when they're using Outlook Web App. This topic discusses the Change Password feature and how it's implemented in Microsoft Exchange Server 2010.

Password Overview

Three types of Account policies are found in Windows Server 2008 or Windows Server 2003 domains: password policies, account lockout policies, and Kerberos authentication protocol policies. A single domain will have one of each of these policies. In Active Directory domains, you can apply one password and account lockout policy. This password is specified in the Default Domain Policy for the domain. The settings that are configured will apply to all users within the domain. This includes Outlook Web App users.

Password and account lockout settings protect accounts and data in your organization by

preventing a person from guessing another user's account password. You can use the Account Lockout and Password Policy nodes of the Default Domain policy settings to configure the account lockout policies and password policy settings that will affect the Outlook Web App users in your Exchange organization and be enforced. Password policies include the following settings:

- Password Complexity
- Password History
- Minimum Password Length
- Maximum Password Age
- Minimum Password Age

When you create a user account and mailbox-enable the user, the password policies and the settings on the user's account will be applied to the user. However, there are other user password settings that may also affect Outlook Web App users, such as **User Must Change Password at First Logon** and **User Cannot Change Password**.

Change Password Feature in Outlook Web App

By default, the domain password that's used by the user to access a Windows-based network is the same as the password that's used to access Outlook Web App. A user can change their domain password using a Web browser by using the Change Password feature within Outlook Web App.

Outlook Web App provides the functionality to change passwords that haven't expired yet. However, if a password has already expired or is required to be changed at the first sign-in, the password can't be changed via Outlook Web App unless you make a configuration change on the Client Access server to enable changing expired passwords.

If you don't enable changing expired passwords, a user whose password must be changed will have to contact their administrator to have their password reset. When the password is reset, the administrator must clear the **User must change password at next logon** check box.

If you haven't enabled changing expired passwords and are using forms-based authentication, a user who must change their password will be returned to the sign-in page, and the following error message will be displayed: **The user name or password you entered isn't correct. Try entering it again**. If forms-based authentication isn't used for Outlook Web App, the user will be returned to the sign-in window but won't see any error message.

Important:

When Basic authentication or forms-based authentication is used with Outlook Web App, the Change Password feature may not work correctly when a user uses a password that includes extended ASCII or Unicode characters. This happens because passwords that use extended ASCII or Unicode characters aren't transmitted correctly between IIS and some Web browsers. We recommend that Outlook Web App users use only ASCII characters if they'll be using the Change Password feature in Outlook Web App.

You can enable or disable the Change Password feature for a single user by configuring the user's mailbox, or for multiple users by configuring the /owa virtual directory or another virtual directory that's used for Outlook Web App. You can enable or disable the Change Password feature by using segmentation. For more information, see Configure Segmentation in Outlook Web App.

Enable Users to Change Expired Passwords

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App Registry Editor" entry in the Client Access Permissions topic.

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

1. Log on to the Client Access server.
2. Start Registry Editor (regedit).
3. Locate the following registry subkey: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA**.
4. Create the following DWORD value if it doesn't already exist: **ChangeExpiredPasswordEnabled**. The value type will be **REG_DWORD**.
5. Set the value of **ChangeExpiredPasswordEnabled** to **1**.
6. Exit Registry Editor.

Note:

You must make this change on each Client Access server that supports Outlook Web App.

1.6.2.2.4.8 Using Outlook Web App Web Parts

Using Outlook Web App Web Parts

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Microsoft Office Outlook Web App Web Parts to specify the mailbox to open, the folder within that mailbox to open, and the content view to use.

Outlook Web App Web Parts let you access Outlook Web App content directly from a URL. The URL can be entered into a Web browser or embedded in an application. Generally, Web Parts aren't created manually. Instead, they're created programmatically based on selections made in a user interface (UI), or they're embedded directly in an application, such as a Microsoft Office SharePoint Server 2007 or SharePoint Server 2010 page. The code behind the UI then creates the URL. One use for Outlook Web App Web Parts is to display a user's Inbox or Calendar on a SharePoint Server 2007 or SharePoint Server 2010 page.

Note:

To use Outlook Web App Web Parts, both the user's mailbox and the mailbox being opened through a Web Part must be located in the same Active Directory forest.

Permissions for Using Outlook Web Access Web Parts

To use Outlook Web App Web Parts, you must, at a minimum, be delegated "Reviewer"

access to the content that you're opening. If you've embedded an Outlook Web App Web Part that requires authentication into an application, you must pass authentication information through together with the request for the Web Part. One way to do this is by configuring the Outlook Web App virtual directory to use Integrated Windows authentication. Integrated Windows authentication lets users who've already logged on by using their Active Directory account use Outlook Web App without having to enter their credentials again.

Outlook Web App Web Parts Syntax

Outlook Web App in Microsoft Exchange Server 2010 has a new URL format to use for requests to the /owa virtual directory. These requests can be made by typing a URL directly into a Web browser or by embedding the URL in a Web application, such as a SharePoint Server page.

Outlook Web App Web Parts can be used to create URLs of varying complexity. A simple Web Part URL can be used to open the Inbox of any mailbox. A more complex Web Part URL could be used to specify the mailbox to open, the folder within that mailbox to open, and the content view to use.

For example, the simple Web Part URL https://<*server name*>/owa/?cmd=contents will open the Inbox of the mailbox that's determined by the user's logon. The more complex Web Part URL https://<*server name*>/owa/<SMTP address>/?cmd=contents&fpath=inbox%2fProjects&view=by%20subject will open the mailbox that's specified by the SMTP address to the subfolder Projects, sorted by subject.

Depending on the security measures that have been applied to your network, you may have to configure encoding for the Web Parts URL. After you configure the encoding, the code behind the UI will create the URL by using the URL-encoded parameters. URL-encoded parameters use %20 in place of spaces and %2f in place of the path delimiter "/". All examples in this topic use encoded parameters.

The following table lists the parameters of a Web Part and examples of how they're used.

Web Part parameters and how they're used

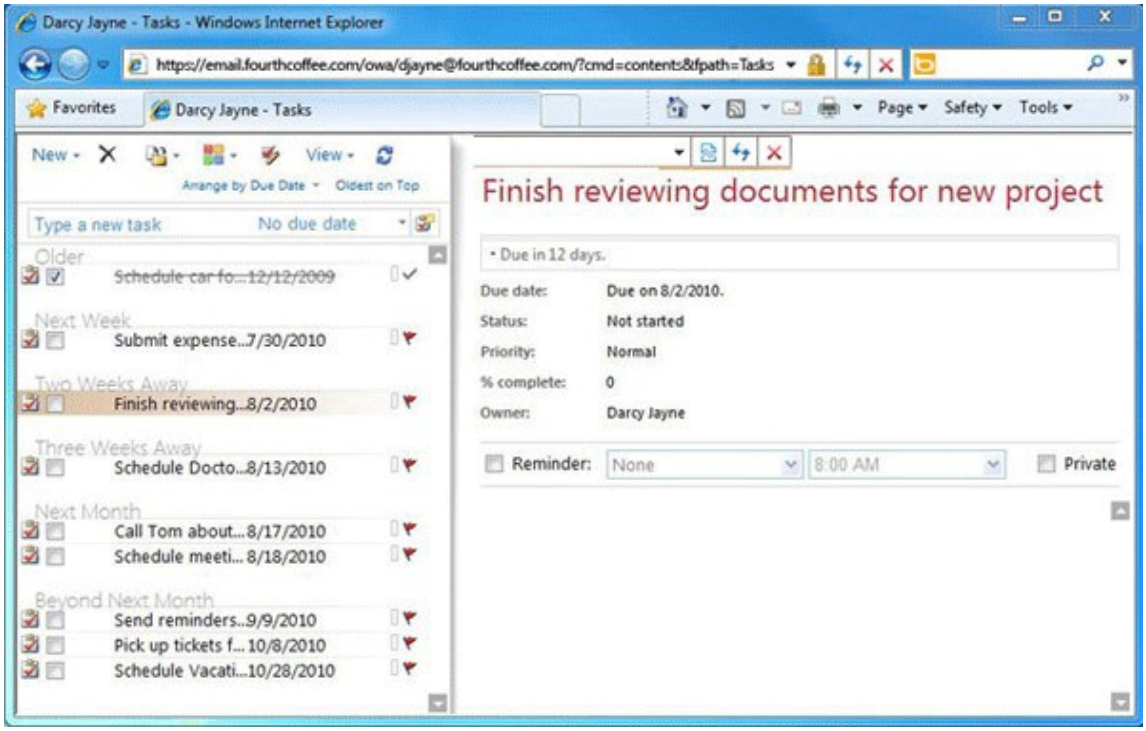
URL parameter	Description	Values and examples
Server name and directory (required)	The URL of the Outlook Web App virtual directory.	This may be the same URL that users use to sign in to Outlook Web App, for example: https://<*server name*>/owa
Exchange 2010 explicit logon mailbox identification (optional)	Any SMTP address that's associated with the mailbox to be opened. If this section of the URL is missing, the default mailbox of the authenticated user is opened. If no additional parameters are specified, the default behavior is to open the Inbox.	To open the mailbox with the SMTP address tsmith@fourthcoffee.com, use the following URL: https://<*server name*>/owa/tsmith@fourthcoffee.com
cmd (required if you're specifying any parameter other than the	?cmd=contents displays the Outlook Web App Web Part that's specified by the parameters instead of the full Outlook Web	If no mailbox is specified, the cmd parameter comes after the sign-in address, as follows: https://<*server name*>/owa/?

explicit logon mailbox identification)	App user interface.	cmd=contents If a mailbox is specified, the cmd parameter comes after the explicit mailbox identification, as follows: https://*<server name>*/owa/*<SMTP address>*/?cmd=contents If no additional parameters are specified, the default behavior is to open the Inbox.
id (optional)	The folder ID of the folder from which the Web Part should display contents. This can be obtained by using Web services and can be used in applications to dynamically select which folder to open.	The folder ID is the Base64-encoded PR_ENTRY_ID of the folder, for example: https://*<server name>*/owa/?cmd=contents&id=*<PR_ENTRY_ID>*
fpath (optional)	A string that specifies the mailbox folder to be shown in the Web Part. The Web Part URL may have to be written by using URL encoding so that it can pass through firewalls. When you use URL encoding, a space becomes %20, and a path delimiter (/) becomes %2f. The folder hierarchy should start from the mailbox root. This folder path can point to ordinary folders or search folders.	To open the subfolder Projects in the Inbox, use the following URL: https://*<server name>*/owa/?cmd=contents&fpath= inbox%2fprojects
module (optional)	This parameter can be used to specify any of the four default folders without knowing the localized name.	Values for the module parameter aren't case sensitive, and include the following: • Inbox • Calendar • Contacts • Tasks • Publicfolders To open the calendar of a mailbox regardless of localization, use the following URL: https://*<server name>*/owa/?cmd=contents&module=calendar
view (optional)	This parameter specifies the view to be displayed for the folder. The default views when this parameter is not present are as	The views available vary according to the folder type. Calendar views: • Daily The daily

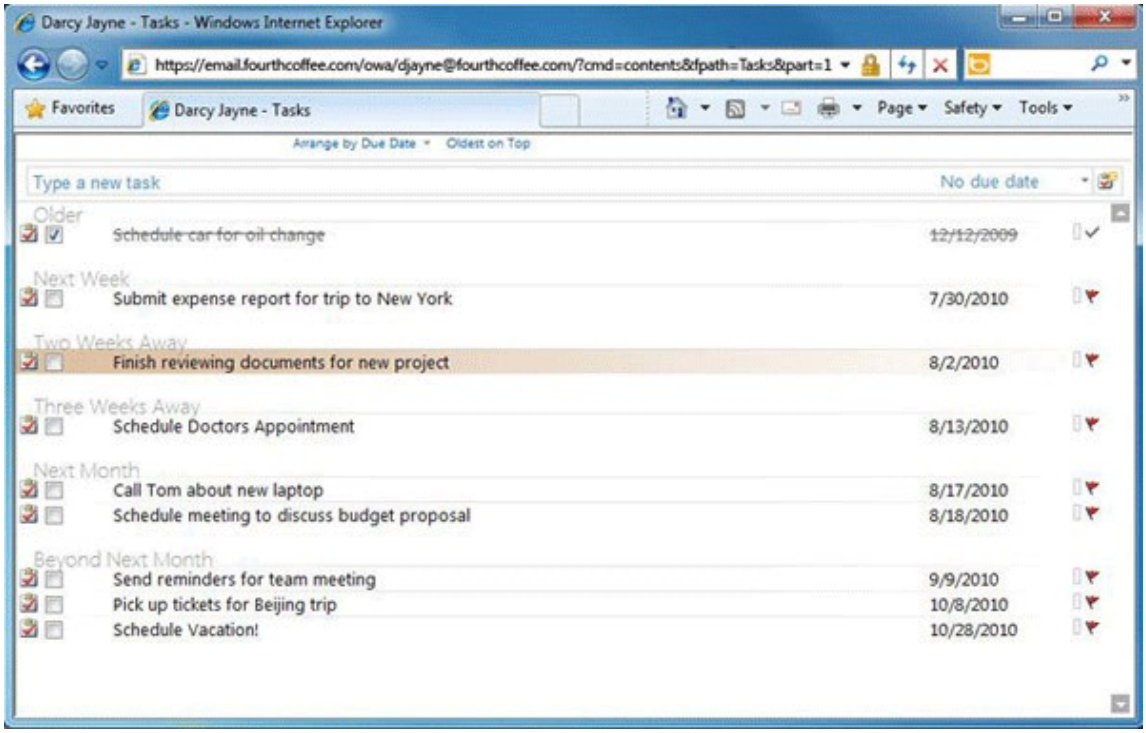
	follows: • Calendar Daily • Messages Messages • Contacts Two%20Line • Tasks By%20Due%20Date **Note:** The strings for the default views are automatically URL encoded. The default sort for a view is the way the folder would be sorted if it was opened in the Outlook Web App client. The strings identifying the views aren't localized and not case sensitive.	calendar view • Weekly The weekly calendar view • Monthly The monthly calendar view Message views: • Messages Message view, with default sort • By%20Sender Message view sorted by From with sender names that begin with "a" on top • By%20Subject Message view sorted by Subject with subjects that begin with "a" on top • By%20Conversation%20Topic Conversation View, not available in the light version of Outlook Web App Contact Views: • Phone%20List Contact view, with default sort Tasks: • By%20Due%20Date Tasks view with default sort • By%20Subject Tasks view sorted by subject, with a on top https://<*server name*>/owa/?cmd=contents&fpath=Calendar&view=Weekly will display the requested calendar in Weekly view.
d, m, y (optional)	Specifies the date for which the calendar should be displayed. These parameters can be entered in any order and can be used singly or together. If any of these parameters aren't specified, the default values are the current day, month, and year values. For example, if the current day is May 3, 2010 and you specify a month value of "9" for September, the date displayed will be September 3, 2010.	The valid values for the data parameters are as follows: d=[1-31] m=[1-12] y=[four digit year] To open a calendar to the date May 3, 2007, you would use the following URL: https://<*server name*>/owa/?cmd=content&fpath=calendar&view=daily&d=3&m=5&y=2007

part (optional)	Specifies that Outlook Web App should display a smaller Web Part.	When you use Web Parts to access Outlook Web App content, the UI that is displayed will be smaller than the full Outlook Web App UI. The part parameter reduces the UI further. The following example URL shows the Tasks list in the smallest Web Part format: https://*<server name>*/owa/?cmd=contents&fpath=tasks&part=1 The part parameter doesn't apply to the calendar module.

The following figure shows the Outlook Web App Tasks Web Part without the parameter *part=1*.



The following figure shows the Outlook Web App Tasks Web Part with the parameter *part=1*.



You can use multiple parameters to specify the folder to be displayed and the format to display it in. If more than one folder parameter is used, the precedence order is *id*, *f*, and then *module*. If none of these parameters is present, the Inbox will be shown by default.

Note:

If a feature has been turned off by using segmentation, that feature won't be available as a Web Part. For example, if the Outlook Web App calendar has been disabled, you won't be able to access calendars by using Outlook Web App Web Parts.

Enter Outlook Web App Web Parts manually

Outlook Web App Web Parts can be also be entered manually in a Web browser. For example, a user can use an Outlook Web App Web Part URL to open another user's calendar.

To open a specific calendar in Weekly view:

1. Open a Web browser window.
2. Enter the URL for Outlook Web App and add the following string to the end of the URL: *<mailbox SMTP address>*/?cmd=contents&fpath=calendar&view=weekly.
3. Enter sign-in credentials, if you're prompted to do this.

For example, if the URL of Outlook Web App is https://email.fourthcoffee.com/owa, then the following URL will open the calendar that belongs to the user tsmith in Weekly view: https://email.fourthcoffee.com/owa/tsmith@fourthcoffee.com/?cmd=contents&fpath=calendar&view=weekly

For More Information

- Web Parts (How Do I...in SharePoint Foundation)

- Plan Web pages

1.6.2.2.4.9 Customize the Outlook Web App Sign-In and Sign-Out Pages

Customize the Outlook Web App Sign-In and Sign-Out Pages

Managing Client Access Servers > Managing Outlook Web App > Managing Outlook Web App Advanced Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to create custom sign-in and sign-out pages for Outlook Web App.

Looking for other advanced management tasks for Outlook Web App? Check out Managing Outlook Web App Advanced Features.

Customize the sign-in and sign-out pages

The Outlook Web App sign-in, language selection, and sign-out pages are created based on graphics and the logon.css file in the base theme folder. Therefore, to use custom sign-in and sign-out pages, you must modify the files in the base theme folder. You can find the base theme folder in the Exchange installation directory at \V14\Client Access \OWA\<version number>\themes\base.

Note:

In Exchange Server 2010 SP1, the path is \V14\Client Access\OWA\<version number> \themes\resources.

The sign-in, language selection, and sign-out pages use the logon.css file to define text styles and colors. The pages are created by combining several images for the border top, bottom, and sides and also include repeating images and corners for expansion. The following files create the sign-in page:

- logon.css
- lgnbotl.gif
- lgnbotm.gif
- lgnbotr.gif
- lgnexlogo.gif
- lgnleft.gif
- lgnright.gif
- lgntopl.gif
- lgntopm.gif
- lgntopr.gif

It is easiest to create a new look by using a solid color because the same collection of images is used for three pages: the sign-in page, the language selection page that is shown on the first sign-in per mailbox, and the sign-out page. The pages resize horizontally and vertically based on the contents of the page.

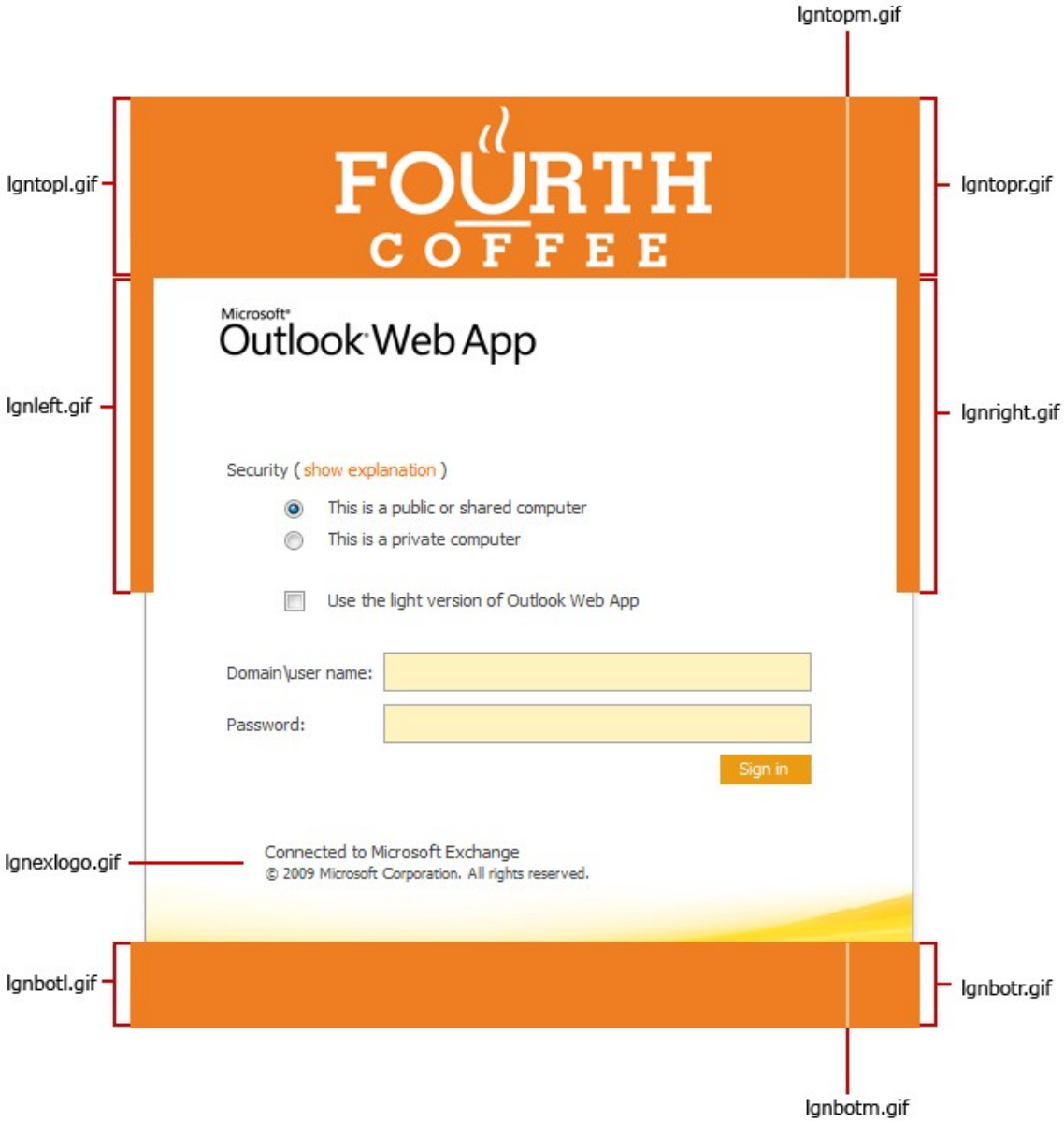
If you have multiple Client Access servers and want them all to use the same sign-in and sign-out pages, you must copy the modified sign-in and sign-out files to each Client Access server. You should also create a back-up copy of your customized files. If you reinstall or upgrade Exchange, all files in the themes folders will be overwritten. You'll have to copy your customized files back to the appropriate theme folder after the

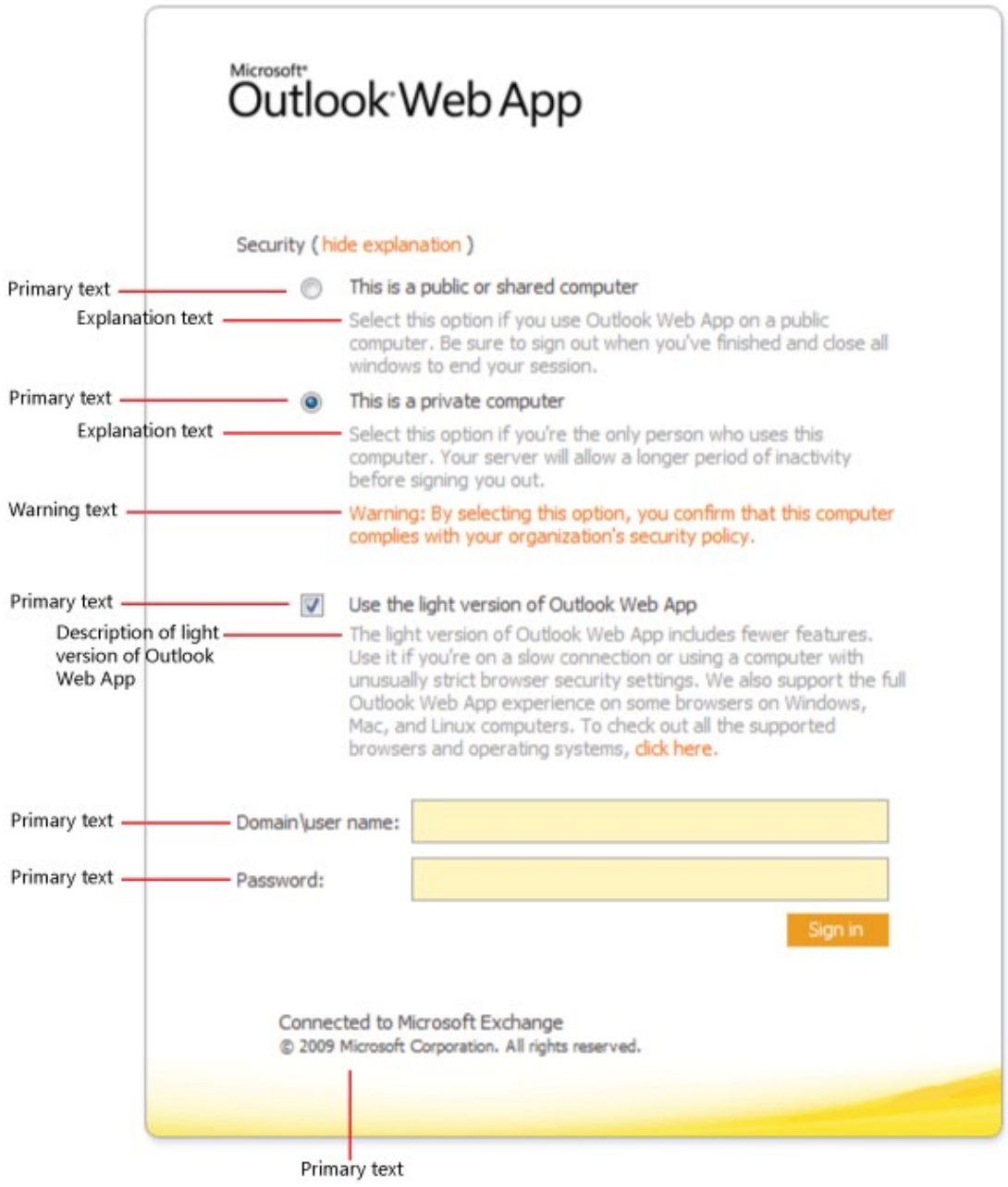
reinstallation or upgrade is complete.

Caution:

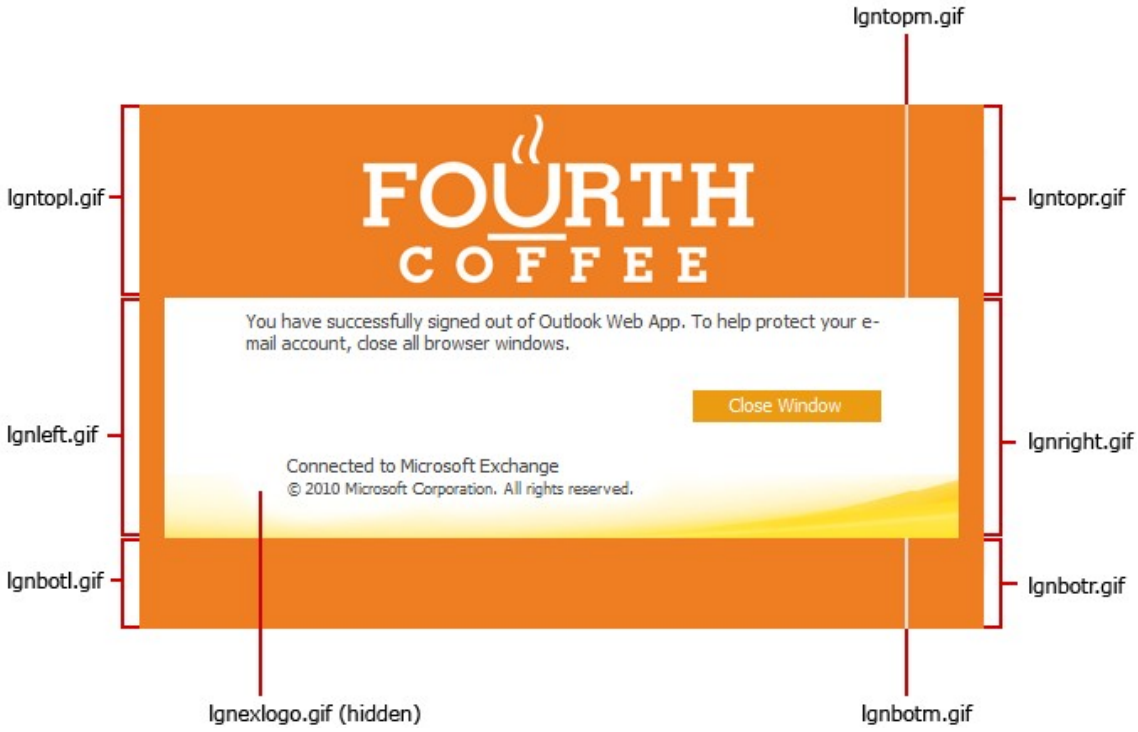
Before you change the files to create custom sign-in and sign-out pages, back up copies of all the files that you'll be changing before you start to create your custom sign-in and sign-out pages.

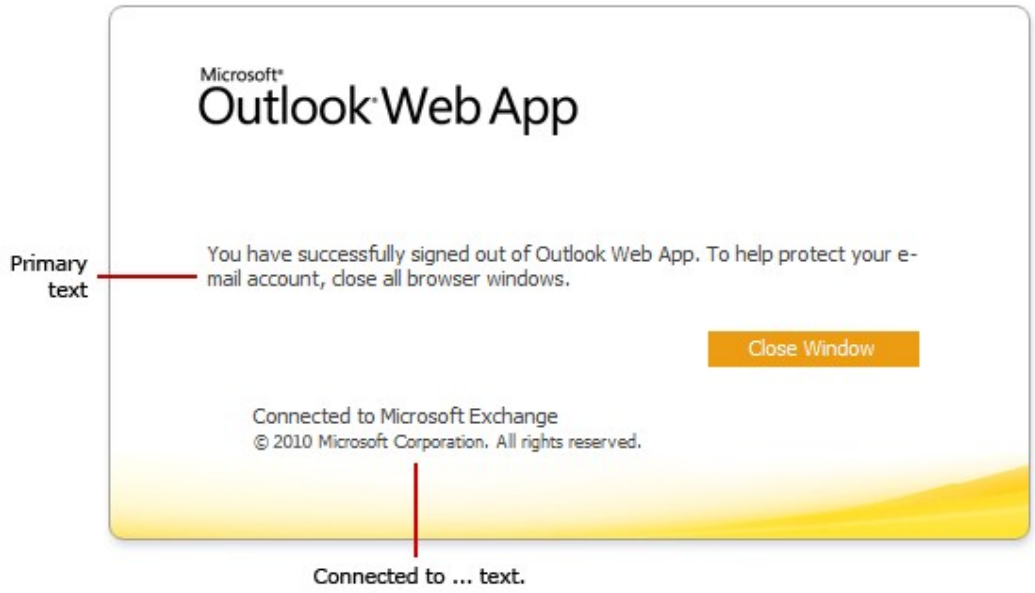
The following figures illustrate the default Outlook Web App sign-in page as it appears if the user clicks **show explanation** and selects **This is a private computer** and **Use the light version of Outlook Web App**. One figure shows how the graphics files that create the page fit together. The other figure shows how the logon.css file determines the colors of the background and text on the sign-in page.





The following figures illustrate the default Outlook Web App sign-out page. One figure shows how the graphic files that create the page fit together. The other shows how the logon.css file determines the colors of the background and text on the sign-out page.





Test changes to the sign-in and sign-out pages

After you've opened the Outlook Web App sign-in or sign-out page in Microsoft Internet Explorer, you can test your changes without having to reset IIS or exit Internet Explorer.

1. Open the Outlook Web App sign-in or sign-out page in Internet Explorer.
2. On the toolbar, click **Tools**, and then click **Internet Options**.
3. On the **General** tab, under **Browsing history**, click **Delete**.

4. Under **Temporary Internet Files**, click **Delete files**, and then click **Yes** when you are asked whether you are sure that you want to delete all temporary Internet Explorer files
5. Click **OK** to close **Internet Options**.
6. Click **Refresh** to see your changes.

Repeat these steps to see your changes every time that you make a change to the sign-in or sign-out page files. If you're making several changes, you can leave the sign-in or sign-out page open and repeat the steps to see your changes.

Change the logo in Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Graphics editor" entry in the Client Access Permissions topic.

To customize Outlook Web App, you can change the Outlook Web App logo on the sign-in and sign-out pages to your organization's logo.

1. Create copies of the files that you want to change, and then save them to a safe location so that you can restore the original pages, if it's necessary.
2. Open the lgntopl.gif file by using an image editing tool, and then modify it to create the logo that you want to use.
3. Save your changes, and then click the **Refresh** button to see your changes.

Note:
If you've changed the background color of lgntopl.gif, we recommend that you modify the remaining files that are used to create the sign-in and sign-out pages to match.

Change the font styles and colors

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Text editor" entry in the Client Access Permissions topic.

You can edit the logon.css file to change font styles and some of the colors that are used on the pages. This includes the background color that's behind the controls in the center of the sign-in page and the language selection page. If you've changed the color of these pages, we recommend that you change the background color to match.

To change the background and font colors of the sign-in, language selection, and sign-out pages, you must find the values in the sign-in style sheet (logon.css) and then determine the HTML RGB values for the colors that you want to use. The HTML RGB color values are defined by a seven-character string in the format of the number sign (#) followed by a string of six characters. To find the HTML RGB values for many colors, see the Color Table in the MSDN Library. If you must match a specific color and you can't find a match for the color online, you can use an image editing tool to sample a color and determine its HTML RGB value.

To test your changes, open Internet Explorer and enter the URL for Outlook Web App. If you're testing the changes to the Default Web site on the Client Access server that is hosting the Outlook Web App virtual directory, you can test them by opening Internet Explorer and entering the URL https://localhost/owa.

Note:
The language selection page appears only the first time that a user signs in to Outlook Web App.

The following table lists the elements of the sign-in and sign-out pages and a description for each element.

Sign-in and sign-out page elements and their descriptions

Element to change	String to search for	Description
Background color of the Web browser window	`body{background-color:#FFFFCC`	The background color of the Web browser window. This controls the color of the window that borders the sign-in and sign-out pages.
Background color the sign-in and sign-out pages	`Background: #FFFFCC`	The background color of the sign-in and sign-out pages. If you change the background color of the graphics files, you should change the background color to match.
Warning text	`wrng{color:#ff6c00;`	The color of the warning text that appears when a user selects **This is a private computer**. On the existing Outlook Web App sign-in page, this warning text is orange and stands out well against the white background. If you change the background color of the sign-in page, you may also want to change the color of the warning text so that it's readable.
Primary text color	`select, table {color:#444444;}`	The primary text color is black. It indicates options that can be selected and entry fields on the Outlook Web App sign-in page. Examples include the labels for the user name and password fields, and the text next to the security options. If you've chosen a light color for your sign-in pages, black will still work well for this text.
Show explanation/hide explanation	`a{color:#ff6c00;`	Link on the sign-in page that a user can click to show or hide the explanation of Private and Public sign-ins.
Explanation text	`expl{color:#999999;`	The color of the text that appears when the user clicks **show explanation**.
Description of the light version of Outlook Web App	`disBsc{color:#999999;`	When a user selects **Use the light version of Outlook Web App**, a short explanation about the light version of Outlook Web App is displayed.

After you've decided which elements you want to change the color of and identified the HTML RGB color values that you'll be changing those elements to, use the following procedure to change the color of any element that is defined by a .css file.

Change the color of an element

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Text editor" entry in the Client Access Permissions topic.

1. Open logon.css.
2. Use the table of sign-in and sign-out page elements included earlier in this topic to find the string that matches the element that you want to change.
3. Replace the HTML RGB color value of the element that you want to change with the new HTML RGB color value that you want to use for that element.
4. Save your changes and close logon.css.
5. Test your changes by opening Internet Explorer and entering the URL for the Outlook Web App sign-in page.

Note:

If you've already opened the Outlook Web App sign-in URL, you can test your changes by deleting the temporary Internet files and refreshing Internet Explorer. To do this, click **Tools**, and then click **Internet Options**. On the **General** tab, under **Browsing history**, click **Delete**. Under **Temporary Internet Files**, click **Delete files**, and then click **Yes** when you're asked whether you're sure that you want to delete all temporary Internet Explorer files Click **OK** to close **Internet Options**, and then press F5 to refresh the sign-in page.

1.6.2.2.4.10 Create a Theme for Outlook Web App

Create a Theme for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to create a custom theme for Microsoft Office Outlook Web App. A theme is a collection of media files and cascading style sheets (.css files) that control the appearance of Outlook Web App.

By default, multiple themes are installed when you install the Client Access server role on a computer that's running Microsoft Exchange Server 2010, as follows:

- .css files -- Define colors, gradients, and fonts.
- Image (.png) files -- Provide the icons and other graphic elements. If you edit any of the icons, don't change their size. If you change the size of any graphic elements, test your changes to verify that the elements still fit together correctly.

These files are stored on the Client Access server in the installation directory in \Client Access\OWA\<*version*>\themes. Each theme is stored in a subdirectory of themes. You can create additional themes by copying an existing theme and modifying the copy.

Note:

The light version of Outlook Web App doesn't support themes.

Recommendations

Many elements of an Outlook Web App theme can be changed. To avoid creating instability in Outlook Web App, we recommend that you change only the files directly related to your custom theme.

As a best practice, follow these guidelines:

- Always make backup copies of the original files before you edit them.
- Before you apply upgrades or hotfixes to a Client Access server that has custom themes, make backup copies of those themes.
- Make only one or two changes at a time and test your changes before you make additional changes.
- Don't change files in \Client Access\OWA\<*version*>\themes\resources. Fonts and other settings defined by those files are used by every theme in Outlook Web App. The files can't be changed without affecting every theme.
- Themes are saved on each Client Access server. If you have more than one Client Access server, and you want a custom theme to be available on all servers, you must copy the theme to the themes directory on each Client Access server.

Looking for other management tasks related to customizing the appearance of Outlook Web App? Check out Customize the Outlook Web App Sign-In and Sign-Out Pages.

What Do You Want to Do?

- Create a new Outlook Web App theme
- Name your custom theme
- Create a custom icon for your theme
- Create a custom header
- Use the Internet Explorer Developer Tools to determine colors
- Change colors in a theme
- Change icons and logos in a theme
- Set the default Outlook Web App theme

Create a new Outlook Web App theme

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Graphics editor" entry in the Client Access Permissions topic.

1. On the Client Access server that hosts Outlook Web App, open Windows Explorer, and then find the Exchange server installation directory.
2. In \Client Access\OWA\<*version*>\themes, find a theme that uses a color scheme similar to what you want, and then make a copy of it.
3. Give the copy you just created a short name similar to the name you want to give the theme.
4. Create back-up copies of the following files in your new theme folder, in addition to any others that you'll have to change to create your theme. These copies will preserve your original settings if you have to undo your changes:
   - premium.css
   - csssprites.png
   - csssprites2.png
   - headerbgmain.png
   - headerbgright.png
5. Follow the steps in the next sections to modify the files in the new theme folder to create your theme.
6. Restart Internet Information Services (IIS) by using the **iisreset/noforce**

command.
7. Test the new theme by signing in to Outlook Web App and selecting the new theme.

Name your custom theme

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Graphics editor" entry in the Client Access Permissions topic.

1. Open the copy of themeinfo.xml that's in the custom theme folder.
2. Find the `displayname` value for the theme, and then change the value to the name you want the theme to have.
   Example: To name your theme Fourth Coffee, the file should read as follows: `theme displayname = "Fourth Coffee"`.
3. Change the `sortorder` value to place your theme where you want it in the theme picker in Outlook Web App.
   Example: To set your theme to appear first, the file should read `sortorder = 1`.
4. Save your changes, and then close themeinfo.xml.
5. Stop and start IIS on the Client Access server by opening a Command Prompt window and using the command **iisreset/noforce**.
6. To test your changes, sign in to Outlook Web App, click **Options**, and then look for your new theme in the theme picker. If you don't see your theme listed, use Internet Options in Microsoft Internet Explorer to delete the temporary files. Then refresh the browser and try again to view the theme picker.

Create a custom icon for your theme

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Graphics editor" entry in the Client Access Permissions topic.

To create a custom icon for your theme, you must edit the themepreview.png file. This file is the icon for your theme in the theme picker in Outlook Web App.

1. Open themepreview.png in an image editing tool and make the changes you want. Don't modify the dimensions. The image is 32x32 pixels.
2. To test your changes, sign in to Outlook Web App, click **Options**, and then look for your new theme in the theme picker. If you don't see the new icon, use Internet Options in Internet Explorer to delete the temporary files. Then refresh the browser and try again to view the theme picker.

Create a custom header

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Graphics editor" entry in the Client Access Permissions topic.

To change the header in Outlook Web App, you must edit the following files that are used to create the header at the top of Outlook Web App:

- headerbgmain.png
- headerbgright.png
- headerbgmainrtl.png (You only need to edit this file if you support right-to-left languages).

1. Open the .png files in an image editing tool and make the changes you want. Don't modify the dimensions.
2. To change the logo, use an image-editing tool that supports transparent backgrounds, such as Paint.NET or Photoshop, to open and modify csssprites.png. This file has a transparent background. Don't move or change

the size of images in the file because Outlook Web App pulls each icon or logo from a specific location on cssprites.png. When you edit something in the file, you must line up the new image exactly on top of the image you're replacing.

3. After you edit the files, save your changes.
4. To test the changes to your custom theme, sign in to Outlook Web App, click **Options**, and then select your theme from the theme picker. If you don't see your new theme, use Internet Options in Internet Explorer to delete the temporary files. Then refresh the browser and try again to select your custom theme.

Use the Internet Explorer developer tools to determine colors

Internet Explorer 8 and Internet Explorer 9 include developer tools that let you determine the colors and fonts of specific elements and test modifications to those values. You can then use the information from the developer tools to locate those values in the .css files and modify them there to customize a theme.

1. Sign in to Outlook Web App and select any theme.
2. Go to a module that shows the element you want to customize. For example, if you want to customize the highlight color in Mail, go to Mail.
3. In Internet Explorer, go to the program toolbar and select Tools > Developer Tools, or press F12.
4. Arrange your windows so that Outlook Web App and the Developer Tools windows don't overlap.
5. In Developer Tools, click the select arrow at the left of the toolbar or press CTRL+B.
6. Move the pointer over the section of Outlook Web App that you want to customize. You'll see an outline around each element as the pointer passes over it. Click when the element you want to change is outlined.
7. Look in the Developer Tools window. You'll see the code that's used to build the page, and the element you selected will be highlighted in the left window.
8. Look in the right window for the color of that element. It will be an RGB value, which is expressed as a seven-character string starting with a # and followed by six alphanumeric characters. For example, white is expressed as #FFFFCC.
9. If you don't see an RGB value, repeat the preceding steps and try again.
10. When you find an RGB value, change it to the value you want, and then press Enter. The change will show up in Outlook Web App almost immediately. This doesn't change the theme, only the local settings and only for the current session.
11. The right pane of Developer Tools shows you what file the value is in and where to find it in that file.
12. After you find the value that you want to change, you must go the folder for your custom theme on the Client Access server and modify that value in premium.css.

Note:

To find the HTML RGB values for many colors, see the Color Table in the MSDN Library. If you must match a specific color and you can't find a match for the color online, you can use an image-editing tool to sample a color and determine its HTML RGB value. The Developer Tools have a useful color picker tool. Select **Tools** > **Show Color Picker** from the menu. To determine the RGB value of a color you want, position the mouse pointer over an element that has that color.

Change colors in a theme

After you find the color you want to change and determine the RGB value that you want

to change it to, you must find that property in the premium style sheet (premium.css) on the Client Access server and replace the existing value with the new value.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Graphics editor" entry in the Client Access Permissions topic.

1. Open the premium.css file in your custom theme by using a text editor such as Notepad.
2. In the file, search for the value that you found using the Internet Explorer tools.
3. Replace the RGB value with the RGB value of the color that you want.
4. To test the changes to your custom theme, sign in to Outlook Web App, click **Options**, and then select your theme from the theme picker. If you don't see your changes, use Internet Options in Internet Explorer to delete the temporary files. Then refresh the browser and try again to select your custom theme.

Change icons and logos in a theme

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Graphics editor" entry in the Client Access Permissions topic.

To change the icons and logos in a theme, use an image editing tool that supports transparent backgrounds, such as Paint.NET or Photoshop, to open and modify csssprites.png and csssprites2.png. These files have a transparent background that must be preserved to correctly display the individual elements. Don't move or change the size of images in the file because Outlook Web App pulls each image from a specific location in the file. When you edit something in the file, you must place the new image in exactly the same location as the image you're replacing.

To change an image:

1. Use an image editing tool that supports transparent backgrounds to open the file that contains the graphic elements you want to change.
2. Edit the element that you want to change, being careful to preserve the location and size of the original element.
3. Save and close the file.
4. To test the changes to your custom theme, sign in to Outlook Web App, click **Options**, and then select your theme from the theme picker. If you don't see your changes, use Internet Options in Internet Explorer to delete the temporary files. Then refresh the browser and try again to select your custom theme.

Set the default Outlook Web App theme

When you set a default theme, only users who haven't previously signed in to Outlook Web App and selected a new theme will be forced to use the default theme.

To force all users to use the default theme, you must disable theme selection in addition to setting a new default theme.

Use the Shell to set the default theme for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example sets the default theme for Outlook Web App where the server name is "FourthCoffee", the virtual directory name is "owa", the Web site name is "Default Web site", and the theme is in the folder named "Custom".

```
set-owavirtualdirectory -identity "fourthcoffee\owa (default web site)" -defaultt
```

For detailed syntax and parameter information, see Set-OwaVirtualDirectory.

Use the Shell to disable theme selection for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example disables theme selection in Outlook Web App where the server name is "FourthCoffee", the virtual directory name is "owa", and the Web site name is "Default Web site".

```
set-owavirtualdirectory -identity "fourthcoffee\owa (default web site)" -themesel
```

You can also complete both commands at the same time as shown in the following example:

```
set-owavirtualdirectory -identity "fourthcoffee\owa (default web site)" -defaultt
```

For detailed syntax and parameter information, see Set-OwaVirtualDirectory.

Other Tasks

After you create a theme, you may also want toCustomize the Outlook Web App Sign-In and Sign-Out Pages.

1.6.2.2.5 Managing Outlook Web App Mailbox Policies

Managing Outlook Web App Mailbox Policies

Client Access > Managing Client Access Servers > Managing Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-22*

Create Outlook Web App Mailbox Policy

View or Configure Outlook Web App Mailbox Policy Properties

Remove an Outlook Web App Mailbox Policy from Exchange

Apply an Outlook Web App Mailbox Policy to a Mailbox

1.6.2.2.5.1 Create Outlook Web App Mailbox Policy

Create Outlook Web App Mailbox Policy

Managing Client Access Servers > Managing Outlook Web App > Managing Outlook Web App Mailbox Policies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-07-21*

You can create an Outlook Web App mailbox policy to apply a common set of policy settings, such as attachment settings. Outlook Web App mailbox policies are useful for applying and standardizing settings for specific groups of users.

When the Client Access server role is installed, a default Outlook Web App mailbox policy is created. You can create additional Outlook Web App mailbox policies as needed. You apply Outlook Web App mailbox policies by changing the properties of mailboxes.

Looking for other management tasks related to Outlook Web App mailbox policies? Check out Managing Outlook Web App Mailbox Policies.

Prerequisites

The Client Access server role has been installed.

What Do You Want to Do?

- Use the EMC to create an Outlook Web Access mailbox policy
- Use the Shell to create an Outlook Web Access mailbox policy

Use the EMC to create an Outlook Web App mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App mailbox policies" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Client Access**.
2. In the work pane, click the **Outlook Web App Mailbox Policies** tab.
3. In the action pane, click **New Outlook Web App Mailbox Policy**.
4. In the New UM Mailbox Policy wizard, complete the following fields:
   - **Outlook Web App mailbox policy name** Use this text box to specify a unique name for the Outlook Web App mailbox policy. This is a display name that appears in the Exchange Management Console.
     The Outlook Web App mailbox policy name is required, but it is used for display only. Because your organization may use multiple Outlook Web App mailbox policies, we recommend that you use meaningful names for your Outlook Web App mailbox policies. The maximum length of an Outlook Web App mailbox policy name is 64 characters, and it can include spaces. However, it can't include any of the following characters: " / \ [ ] : ; | = , + * ? < >.
   - **Select the features that you want to enable or disable for the Outlook Web App mailbox policy** Select the features that you want to enable or disable, and then click **Enable** or **Disable** to set them.
   - Click **New** to create your policy.
5. On the **Completion** page, confirm whether the Outlook Web App mailbox policy was successfully created:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to complete the New Outlook Web App Mailbox Policy wizard.

Use the Shell to create an Outlook Web App mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App mailbox policies" entry in the Client Access Permissions topic.

This example creates an Outlook Web App mailbox policy named `Policy1`:

```
New-OwaMailboxPolicy -Name Policy1
```

For more information about syntax and parameters, see New-OwaMailboxPolicy.

Other Tasks

After you create an Outlook Web App mailbox policy, you may also want to View or Configure Outlook Web App Mailbox Policy Properties.

For More Information

Understanding Outlook Web App Mailbox Policies

1.6.2.2.5.2 View or Configure Outlook Web App Mailbox Policy Properties

View or Configure Outlook Web App Mailbox Policy Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After you create an Outlook Web App mailbox policy, you can configure a variety of options to control the features available to users in Outlook Web App. For example, you can enable or disable Inbox rules or create a list of allowed file types for attachments.

Looking for other management tasks related to Outlook Web App? Check out Managing Outlook Web App.

What Do You Want to Do?

- Use the EMC to view or configure Outlook Web App mailbox policies
- Use the Shell to configure Outlook Web Access mailbox policies
- Use the Shell to view Outlook Web App mailbox policies

Use the EMC to view or configure Outlook Web App mailbox policies

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App mailbox policies" entry in the Client

Access Permissions topic.

1. In the console tree, click **Organization Configuration** > **Client Access**. Click the **Outlook Web App Mailbox Policies** tab.
2. In the work pane, select the Outlook Web App mailbox policy that you want to view or configure, and then click **Properties**.
3. On the **General** tab, you can view and edit the name of the policy and view the modified date.
4. On the **Segmentation** tab, specify the features you want to enable or disable for Outlook Web App users.

Note:
Segmentation settings for mailbox policies override virtual directory settings. You can change segmentation settings for individual users by using the **Set-CASMailbox** cmdlet or by using Outlook Web App policies. For more information, see Managing Outlook Web App Mailbox Policies.

- **Enable** Select a disabled feature in the list, and then click **Enable** to enable that feature.
- **Disable** Select an enabled feature in the list, and then click **Disable** to disable that feature.
- **Feature** The **Feature** column shows the list of features that are potentially available to Outlook Web App users on a virtual directory.
- **Status** The **Status** column shows whether each feature is enabled or disabled.
- **Description** This section displays a description for the selected feature in the list.

5. On the **Public Computer File Access** tab, configure the file access and viewing options available if users select **This is a public computer** while they're signing in to Outlook Web App. File access lets a user open or view any file attached to an e-mail message.
Direct file access
- **Enable direct file access** Select this check box if you want to enable direct file access. Direct file access lets users open files attached to e-mail messages.
- **Customize** After you select **Enable direct file access**, click **Customize** to customize the direct file access settings.

Note:
The direct file access settings are applied to private and public computer file access. Even though the settings can be set from either the **Private Computer File Access** tab or the **Public Computer File Access** tab, you can't have different settings on the two tabs.

In the **Direct File Access Settings** dialog box, specify how files will be allowed, blocked, or handled in Outlook Web App. The Allow list overrides the Block list and the Force Save list. The Block list overrides the Force Save list. Select the following:
Allow Click the **Allow** button to specify which types of files should always be allowed. The Allow list overrides the Block list and the Force Save list.
Block Click the **Block** button to specify which types of files should be blocked. The Block list overrides the Force Save list and is overridden by the Allow list.
Force Save Click the **Force Save** button to specify which types of files the user must save to disk before opening them. The Force Save list is overridden by the Allow and Block lists.
Unknown Files Using the **Unknown Files** list, specify how Outlook Web App will handle unknown files that aren't in the

Allow, Block, or Force Save lists.
When you click **Allow**, **Block**, or **Force Save**, a new window opens in which you can add file name extensions and MIME types to the list you have selected, edit them, or remove them.
After you have selected **Allow**, **Block**, or **Force Save**:
To add a file name extension or MIME type, enter it in the appropriate box, and then click **Add**. File name extensions must be preceded by a period (**.**), for example, .exe.
To edit a file name extension or MIME type, select it, and then click **Edit**.
To remove a file name extension or MIME type, select it, and then click **Remove**.
After you finish modifying the lists of file name extensions and MIME types, click **OK** to save your changes or click **Cancel** to discard your changes and return to the previous window.

WebReady Document Viewing
WebReady Document Viewing enables Outlook Web App documents to be converted to HTML and displayed in a Web browser. Configure WebReady Document Viewing on the **WebReady Document Viewing Settings** tab. These settings are available for public and private computer file access, and can be different for each:

- **Enable WebReady Document Viewing** Select this check box if you want to enable supported documents to be converted to HTML and displayed in a Web browser.
- **Force WebReady Document Viewing when a converter is available** Select this check box if you want to force documents to be converted to HTML and displayed in a Web browser before users can open them in the viewing application. Documents can be opened in the viewing application only if **Direct File Access** is enabled.
- **Supported** After you select **Enable WebReady Document Viewing**, click **Supported** to select supported document types for **WebReady Document Viewing**.

  Select document types to view from an Internet browser
  To allow all supported document types to be viewed from an Internet browser, select **All supported document types**.
  To allow only specific document types to be viewed, select **Specific document types**.
  Add After you select **Specific document types**, click **Add** to add a document type to the list.
  Remove After you select **Specific document types**, click the document type that you want to remove, and then click the remove icon.
  Select the MIME types of documents Using this list, add the MIME types of documents to the list of types that can be viewed from an Internet browser or remove them from the list.
  Add After you select **Specific document types**, click **Add** to add a MIME type to the list.
  Remove After you select **Specific document types**, click the MIME type that you want to remove, and then click the remove icon.

6. On the **Private Computer File Access** tab, configure the file access and viewing options available if users select **This is a private computer** while they're signing in to Outlook Web App, or if users sign in using an authentication method other than forms-based authentication. File access lets users open any file attached to an e-mail message and files available through Windows file shares and Windows SharePoint Services document libraries.
   Direct file access
   - **Enable direct file access** Select this check box if you want to enable

direct file access. Direct file access lets users open files available through Outlook Web App. This includes files attached to e-mail messages and files in Windows SharePoint Services document libraries and on Windows file shares.

- **Customize** After you select **Enable direct file access**, click **Customize** to customize the direct file access settings.

Note:
The settings for direct file access are divided into public computer file access settings and private computer file access settings. You can configure these settings on either the **Private Computer File Access** tab or the **Public Computer File Access** tab. However, you cannot have different settings for each tab.

In the **Direct File Access Settings** dialog box, specify how files will be allowed, blocked, or handled in Outlook Web App. The Allow list overrides the Block list and the Force Save list. The Block list overrides the Force Save list. Select the following:
Allow Click the **Allow** button to specify which types of files should always be allowed. The Allow list overrides the Block list and Force Save list.
Block Click the **Block** button to specify which types of files should be blocked. The Block list overrides the Force Save list and is overridden by the Allow list.
Force Save Click the **Force Save** button to specify which types of files the user must save to disk before opening them. The Force Save list is overridden by the Allow and Block lists.
Unknown Files Using the **Unknown Files** list, specify how Outlook Web App handles unknown files that aren't in the Allow, Block, or Force Save lists.
When you click **Allow**, **Block**, or **Force Save**, a new window opens in which you can add file name extensions and MIME types to the list you have selected, edit them, or remove them.
After you have selected **Allow**, **Block**, or **Force Save**:
To add a file name extension or MIME type, enter it in the appropriate box, and then click **Add**. File name extensions must be preceded by a period (**.**), for example, .exe.
To edit a file name extension or MIME type, select it, and then click **Edit**.
To remove a file name extension or MIME type, select it, and then click **Remove**.
After you finish modifying the lists of file name extensions and MIME types, click **OK** to save your changes or click **Cancel** to discard your changes and return to the previous window.

WebReady Document Viewing

WebReady Document Viewing enables Outlook Web App documents to be converted to HTML and displayed in a Web browser. Configure WebReady Document Viewing using the **WebReady Document Viewing Settings** tab. These settings are available for public and private computer file access, and can be different for each:

- **Enable WebReady Document Viewing** Select this check box if you want to enable supported documents to be converted to HTML and displayed in a Web browser.
- **Force WebReady Document Viewing when a converter is available** Select this check box if you want to force documents to be converted to HTML and displayed in a Web browser before users can open them in the viewing application. Documents can be opened in the viewing application only if **Direct File Access** is enabled.
- **Supported** After you select **Enable WebReady Document Viewing**, click **Supported** to select supported document types for **WebReady Document Viewing**.

Select document types to view from an Internet browser
To allow all supported document types to be viewed from an Internet browser, select **All supported document types**.
To allow only specific document types to be viewed, select **Specific document types**.
Add After you select **Specific document types**, click **Add** to add a document type to the list.
Remove After you select **Specific document types**, click the document type that you want to remove, and then click the remove icon.
Select the MIME types of documents Using this list, add the MIME types of documents to the list of types that can be viewed from an Internet browser or remove them from the list.
Add After you select **Specific document types**, click **Add** to add a MIME type to the list.
Remove After you select **Specific document types**, click the MIME type that you want to remove, and then click the remove icon.

Use the Shell to configure Outlook Web App mailbox policies

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App mailbox policies" entry in the Client Access Permissions topic.

This example enables calendar access in the default mailbox policy.

```
Set-OwaMailboxPolicy -Identity Default -CalendarEnabled $true
```

For more information about syntax and parameters, see Set-OwaMailboxPolicy.

Use the Shell to view Outlook Web App mailbox policies

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "View Outlook Web App mailbox policies" entry in the Client Access Permissions topic.

This example retrieves the properties of the Outlook Web App mailbox policy `Executives` in the organization `Fabrikam`.

```
Get-OwaMailboxPolicy -Identity Fabrikam\Executives
```

For more information about syntax and parameters, see Get-OwaMailboxPolicy.

1.6.2.2.5.3 Remove an Outlook Web App Mailbox Policy from Exchange

Remove an Outlook Web App Mailbox Policy from Exchange

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove a Microsoft Office Outlook Web App mailbox policy from an Exchange organization by using either the EMC or the Shell.

Looking for other management tasks related to Outlook Web App mailbox policies? Check out Managing Outlook Web App Mailbox Policies.

Prerequisites

The Client Access server role has been installed.

Use the EMC to remove an Outlook Web App mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App mailbox policies" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Client Access**.
2. In the work pane, click the **Outlook Web App Mailbox Policies** tab.
3. Right-click the Outlook Web App mailbox policy you want to remove, and then click **Remove**.
4. In the confirmation window, click **Yes** to remove the mailbox policy, or click **No** to cancel.

Use the Shell to remove an Outlook Web App mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App mailbox policies" entry in the Client Access Permissions topic.

This example removes an Outlook Web App mailbox policy named `Policy1`.

```
Remove-OwaMailboxPolicy -Name Policy1
```

For more information about syntax and parameters, see Remove-OwaMailboxPolicy.

1.6.2.2.5.4 Apply an Outlook Web App Mailbox Policy to a Mailbox

Apply an Outlook Web App Mailbox Policy to a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can apply an Outlook Web App mailbox policy to one or more mailboxes or remove one using either the EMC or the Shell.

Looking for other management tasks related to Outlook Web App mailbox policies? Check out Managing Outlook Web App Mailbox Policies.

Prerequisites

The Client Access server role has been installed and the Outlook Web App mailbox policies you want have been created.

Use the EMC to apply an Outlook Web App mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App mailbox policies" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the work pane, select the mailbox that you want to apply an Outlook Web App mailbox policy to. You can also select multiple mailboxes.
3. Right-click your selection, then click **Properties**.
4. Click the **Mailbox Feature** tab.
5. Click **Outlook Web App**, and then click **Properties** to view the Outlook Web App Properties window.
6. Select the **Outlook Web App mailbox policy** check box, and then click **Browse** to view available Outlook Web App mailbox policies.
7. Click the policy you want to apply and then click **OK**. You'll be taken back to the Outlook Web App mailbox properties window.
8. Click **OK** to apply the policy.
9. If you've selected more than one recipient, you'll see a Bulk Edit Summary. Click **OK** to accept the change, or **Cancel** to cancel.
10. Click **OK** in the mailbox properties window to accept your changes.

Use the EMC to remove an Outlook Web App mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App mailbox policies" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the work pane, select the mailbox that you want to apply an Outlook Web App mailbox policy to. You can also select multiple mailboxes.
3. Right-click your selection, then click **Properties**.
4. Click the **Mailbox Feature** tab.
5. Click **Outlook Web App**, and then click **Properties** to view the Outlook Web App Properties window.
6. Clear the **Outlook Web App mailbox policy** check box.
7. Click **OK** to remove the policy.
8. If you've selected more than one recipient, you'll see a Bulk Edit Summary. Click **OK** to accept the change, or click **Cancel** to cancel.
9. Click **OK** in the mailbox properties window to accept your changes.

Use the Shell to apply an Outlook Web App mailbox policy to an existing mailbox.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access user settings" entry in the Client Access Permissions topic.

This example applies the Outlook Web App mailbox policy named "Calendar" to the

mailbox of the user tony@contoso.com.

```
Set-CASMailbox -Identity tony@contoso.com -OwaMailboxPolicy:Calendar
```

For more information about syntax and parameters, see Set-CASMailbox.

Use the Shell to remove an Outlook Web App mailbox policy from an existing mailbox.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access user settings" entry in the Client Access Permissions topic.

This example removes the Outlook Web App mailbox policy from mailbox of the user tony@contoso.com.

```
Set-CASMailbox -Identity tony@contoso.com -OwaMailboxPolicy:$null
```

For more information about syntax and parameters, see Set-CASMailbox.

1.6.2.2.6 Managing Outlook Web App and Instant Messaging Integration

Managing Outlook Web App and Instant Messaging Integration

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-01*

Configure Outlook Web App and Office Communications Server 2007 Integration

Configure Outlook Web App and Lync Server 2010 Integration

1.6.2.2.6.1 Configure Outlook Web App and Office Communications Server 2007 Integration

Configure Outlook Web App and Office Communications Server 2007 Integration

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

To enable Microsoft Office Outlook Web App and Microsoft Office Communications Server 2007 integration, you must complete the following steps.

Note:

All references to Communications Server 2007 in this topic refer to Communications

Server 2007 R2.

Prerequisites

You must have:

- Deployed Microsoft Exchange Server 2010 in your organization.
- A working Communications Server 2007 R2 environment.
- A certificate that's trusted by the Communications Server 2007 server and the Client Access server and is issued by the same authority.
- A certificate that has the Client Access server namespace as the subject on the Subject line. The namespace may be the name of a particular Client Access server, or it may be a DNS name that's used for load balancing across multiple Client Access servers.
- The Client Access server namespace must be in the Communications Server 2007 trusted hosts list.
- The fully qualified domain name (FQDN) of the Communications Server 2007 server or the Communications Server 2007 pool.
- Enabled your users to use Communications Server 2007 via the Communications Server 2007 user administration tools.

Download and Install the Web Service Provider

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. On the Client Access server running Windows Server 2008 or a later version, download and install UCMA 2.0 from Unified Communications Managed API 2.0, Core Runtime (64-bit).

   Note:
   UCMA must be version 6907.210 or a later version. If you have installed a previous version of UCMA, you should uninstall it before you install the later version.

2. On the Client Access server, download and extract the CWAOWASSPMain.msi file from: Microsoft Office Communications Server 2007 R2 Web Service Provider.
   2.a. The following files are extracted to the Web Service Provider installer package location:
   CWAOWAASSP.msi
   Donnetfx35setup.exe
   UcamRedist.msi
   Vcredist_x64.exe
3. Double-click **CWAOWASSP.msi** to install the Microsoft Office Communications Server 2007 R2 Web Service Provider.
4. Download and install the hotfix from OCS 2007 R2 Web Service Provider Hotfix version 6907.202.

Use the following checklist to make sure that the installation was successful:

- Look for the **InstantMessaging** key in the registry under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA**. The string under **InstantMessaging** with the name **ImplementationDLLPath** and the value "<Your Exchange Install Path>\ClientAccess\owa\bin\Microsoft.Rtc.UCWeb.dll" should have been created.
- The Microsoft.Rtc.UCWeb.dll file should be present in the directory <install drive>\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa\Bin.
- The files SIPEPS.dll and Microsoft.Rtc.Collaboration.dll should be present in the

Microsoft .NET Framework Global Assembly Cache.

Obtain Certificate Information

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Certificate management" entry in the Exchange and Shell Infrastructure Permissions topic.

The Client Access server must be configured to use a certificate that's trusted by Communications Server 2007.

Note:
The certificate on the Client Access server and the Communications Server 2007 server must be from the same issuer.

Note:
If all your Client Access servers are in the same namespace, you can use a single certificate for all of them.

After the certificate is in place on the Client Access server, use the Exchange Management Shell to get the certificate information by running the following command on the Client Access server.

```
get-ExchangeCertificate | fl
```

Locate the certificate you want to use, and then record the *thumbprint*.

When you configure the Communications Server 2007 host authorization list, you'll add the certificate subject as the name of an authorized host.

For information about how to obtain and configure a certificate for a Client Access server, see Obtain a Server Certificate from a Certification Authority.

Select a Communications Server 2007 Pool

Select the same Communications Server 2007 pool you used for the next hop server for Microsoft Office Communicator Web Access server. This server will proxy all SIP requests to the destination pool. For more information about the next hop server, see Creating a Communicator Web Access Virtual Server.

Use the Shell to configure the Communications Server 2007 server used by the Client Access server and to enable integration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example configures which Communications Server 2007 pool to connect to, the certificate to be used, and enables the Client Access server to use Communications Server 2007 for instant messaging.

```
Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -InstantMessagingServerName <na
```

Note:
You may have to restart Internet Information Services (IIS). You can do this by opening a Command Prompt window and using the iisreset/noforce command.

For detailed syntax and parameter information, see Set-OwaVirtualDirectory.

Configure Communications Server 2007

For information about how to configure Communications Server 2007 to work with Outlook Web App, see Administering Web Service Provider in the Communications Server 2007 documentation.

Other Tasks

After you enable Communications Server 2007 integration on the Client Access server, you may also want to use segmentation or Outlook Web App mailbox policies to enable or disable IM for users.

- Managing Outlook Web App Mailbox Policies
- Set-CASMailbox

1.6.2.2.6.2 Configure Outlook Web App and Lync Server 2010 Integration

Configure Outlook Web App and Lync Server 2010 Integration

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

To enable Microsoft Office Outlook Web App and Microsoft Lync Server 2010 integration, you must complete the following steps.

Prerequisites

You must have:

- Deployed Microsoft Exchange Server 2010 in your organization.
- Deployed Lync Server 2010.
- Obtained a certificate that's trusted by the Lync Server 2010 server and the Client Access server and is issued by the same authority. The certificate must have the Client Access server namespace as the subject on the Subject line. The namespace may be the name of a particular Client Access server, or it may be a DNS name that's used for load balancing across multiple Client Access servers.
- Recorded the fully qualified domain name (FQDN) of the Lync Server 2010 server or the Lync Server 2010 pool that the Client Access server will connect to. The server or pool should be geographically close to the Client Access server.
- Enabled your users to use Lync Server 2010 via the Lync Server 2010 user

administration tools.

Step 1: Download and install the Web Service Provider

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. On the Client Access server running Windows Server 2008 or a later version, download and install UCMA 2.0 from Unified Communications Managed API 2.0, Core Runtime (64-bit).

   Note:
   Unified Communications Managed API v. 2.0 (UCMA) must be version 6907.210 or a later version. If you've installed a previous version of UCMA, you should uninstall it before you install the later version.

2. On the Client Access server, download and extract the CWAOWASSPMain.msi file from Microsoft Office Communications Server 2010 R2 Web Service Provider. The following files are extracted to the Web Service Provider installer package location:
   - CWAOWAASSP.msi
   - Donnetfx35setup.exe
   - UcamRedist.msi
   - Vcredist_x64.exe
3. Double-click **CWAOWASSP.msi** to install the Microsoft Office Lync Server 2010 R2 Web Service Provider.
4. Download and install the hotfix from OCS 2007 R2 Web Service Provider Hotfix.

Use the following checklist to make sure that the installation was successful:

- Look for the **InstantMessaging** key in the registry under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA**. The string under **InstantMessaging** with the name **ImplementationDLLPath** and the value "<Your Exchange Install Path>\ClientAccess\owa\bin\Microsoft.Rtc.UCWeb.dll" should have been created.
- The Microsoft.Rtc.UCWeb.dll file should be present in the directory *<installation drive>*\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa\Bin.
- The files SIPEPS.dll and Microsoft.Rtc.Collaboration.dll should be present in the Microsoft .NET Framework Global Assembly Cache.

Step 2: Use the Shell to verify certificate information

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Certificate management" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
If all your Client Access servers are in the same namespace, you can use a single certificate for all of them.

1. Run the following cmdlet on the Client Access server to obtain certificate information for that server:

   ```
   get-ExchangeCertificate | fl
   ```

2. Locate the certificate you want to use, and then record its thumbprint and subject.

When you configure the Lync Server 2010 host authorization list, you'll add the certificate subject as the name of an authorized host.

For detailed syntax and parameter information, see Get-ExchangeCertificate.

For information about how to obtain and configure a certificate for a Client Access server, see Obtain a Server Certificate from a Certification Authority.

Step 3: Use the Shell to set the Lync Server 2010 server used by the Client Access server and to enable integration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

Note:
Step 3 can be performed before or after step 4, but both steps are required.

This example configures which Lync Server 2010 server or pool to connect to, the certificate to be used, and enables the Client Access server to use Lync Server 2010 for instant messaging.

```
Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -InstantMessagingServerName <na
```

Note:
You may have to restart Internet Information Services (IIS). You can do this by opening a Command Prompt window and using the **iisreset/noforce** command.

For detailed syntax and parameter information, see Set-OwaVirtualDirectory.

Step 4: Configure Lync Server 2010

Note:
Step 3 can be performed before or after step 4, but both steps are required.

This example creates an Outlook Web App pool entry on the Lync Server 2010 server. Use the Lync Server Management Shell on the Lync Server 2010 server to perform the following steps:

1. Run the **Get-CsSite** cmdlet to get the `siteID` for the `siteName` in which you are creating the pool.
2. Run the **New-CsTrustedApplicationPool** cmdlet to create the trusted application pool. This also creates the external service entry in Lync Server 2010.

```
New-CsTrustedApplicationPool -Identity <OwaPoolfqdn same as what is us
```

Note:
Running the cmdlet with these parameters will create a pool with a computer FQDN that's the same as the pool FQDN. This allows you to keep adding new Outlook Web App servers to the Exchange organization without going through this process to add each of them to the Lync server.

1. Run the **New-CsTrustedApplication** cmdlet to add a trusted service port for the application.

```
New-CsTrustedApplication -ApplicationId <ApplicationIDForOWA> -Trusted
```

Note:
The ApplicationID for Outlook Web App can't include spaces, but otherwise it can be any string that allows the Lync Server administrator to recognize the trusted application as Outlook Web App, for example: Outlook Web App Pool.

1. Run the **Enable-CsTopology** cmdlet in the Shell to enable the topology.

```
Enable-CsTopology
```

Other Tasks

After you enable Lync Server 2010 integration on the Client Access server, you may also want to use segmentation or Outlook Web App mailbox policies to enable or disable instant messaging for users.

- Managing Outlook Web App Mailbox Policies
- Set-CASMailbox

1.6.2.3 Managing Outlook Anywhere

Managing Outlook Anywhere

Exchange Server 2010 > Client Access > Managing Client Access Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-13*

Configure Outlook Anywhere in an Environment with Earlier Versions of Exchange

Enable Outlook Anywhere

Disable Outlook Anywhere

Configure an External Host Name for Outlook Anywhere

Managing Certificates for Outlook Anywhere

Configure Client Access Server Properties

Install the Windows RPC Over HTTP Proxy Component

Test Outlook Anywhere Connectivity

1.6.2.3.1 Configure Outlook Anywhere in an Environment with Earlier Versions of Exchange

Configure Outlook Anywhere in an Environment with Earlier Versions of Exchange

Client Access > Managing Client Access Servers > Managing Outlook Anywhere >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-05-18*

When you deploy the Outlook Anywhere feature (formerly known as RPC over HTTP) on a Microsoft Exchange Server 2010 Client Access server that will provide access to Microsoft Exchange Server 2007 or Exchange Server 2003, you must disable Outlook Anywhere for the earlier versions. You need to do this because Exchange 2003 and Exchange 2007 can't provide access to a mailbox that's hosted on an Exchange 2010 server.

After you enable Outlook Anywhere on Exchange 2010 and disable Outlook Anywhere on Exchange 2003 and Exchange 2007, you should make sure that users who have mailboxes on computers running Exchange 2003 and Exchange 2007 can access their mailboxes through Exchange 2010. To do this, create a test mailbox on each computer running Exchange 2003 and Exchange 2007. Then, perform an Outlook Anywhere (RPC over HTTP) connectivity test on each test mailbox by using Microsoft Exchange Remote Connectivity Analyzer. For more information about testing Outlook Anywhere, see Test Outlook Anywhere Connectivity.

Looking for other management tasks related to Exchange 2010 Outlook Anywhere? Check out Managing Outlook Anywhere.

Looking for other tasks related to upgrading client access from Exchange 2003 to Exchange 2010? Check out Upgrade from Exchange 2003 Client Access.

Looking for other tasks related to upgrading client access from Exchange 2007 to Exchange 2010? Check out Upgrade from Exchange 2007 Client Access.

Configure Outlook Anywhere for Exchange Server 2003

You can configure Outlook Anywhere for the original release version of Exchange 2003 and for Exchange 2003 with Service Pack 1 (SP1) or SP2 by following the configuration steps for RPC over HTTP for these versions of Microsoft Exchange. For detailed steps, see How to Configure Outlook Anywhere with Exchange 2003.

Configure Outlook Anywhere for Exchange Server 2007

Use the EMC or the Shell in Exchange Server 2007 to enable or disable Outlook Anywhere for your organization. For detailed steps, see How to Enable Outlook Anywhere.

Other Tasks

After you configure Outlook Anywhere for earlier versions of Exchange, you may also want to:

- Test Outlook Anywhere Connectivity
- Configure an External Host Name for Outlook Anywhere

1.6.2.3.2 Enable Outlook Anywhere

Enable Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the Enable Outlook Anywhere wizard on the Exchange Server 2010 Client Access server to allow users to connect to their Exchange mailbox from the Internet. Outlook Anywhere eliminates the need for users in remote offices or mobile users to use a virtual private network (VPN) to connect to their Exchange servers.

Outlook Anywhere will be enabled on your Client Access server after a configuration period of approximately 15 minutes. To verify that Outlook Anywhere has been enabled, check the application event log on the Client Access server.

Prerequisites

- Install a valid Secure Sockets Layer (SSL) certificate from a certification authority (CA) that the client trusts.
- Install the Microsoft Windows RPC over HTTP Proxy component if it wasn't already installed by default in Windows Server 2008. For detailed steps, see Install the Windows RPC Over HTTP Proxy Component.
- Enable Outlook Anywhere on the Client Access server.

When you install Exchange 2010, you can install a default SSL certificate that's created by Exchange Setup. However, this certificate isn't a valid SSL certificate that's trusted by the client. To use Outlook Anywhere, you must install an SSL certificate that's trusted by the client.

What Do You Want to Do?

- Use the EMC to enable Outlook Anywhere
- Use the Shell to enable Outlook Anywhere

Use the EMC to enable Outlook Anywhere

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the action pane, click **Enable Outlook Anywhere**.
3. In the Enable Outlook Anywhere wizard, type the external host name or URL for your organization in the box under **External host name**.
   This is the URL, for example site.contoso.com, that users will use to connect to the Exchange server by using Outlook Anywhere.
4. Select an available external authentication method. You can select **Basic authentication** or **NTLM authentication**.
   Basic authentication sends the user name and password in clear text. It also requires that users enter domain, user name, and password every time that they connect to the Exchange server. When you use NTLM authentication, the user's credentials are never sent over the network. Instead, the client computer and the server exchange hashed values of the user's credentials. NTLM can also use the current Windows operating system logon information.

Even though it's more secure, NTLM may not work with firewalls that examine and modify traffic. You can use an advanced firewall server such as Microsoft Internet Security and Acceleration (ISA) Server 2006 together with NTLM authentication for Outlook Anywhere.

Caution:

Negotiate Ex authentication is an authentication type that's reserved for future Microsoft use and should not be used. Use of this setting will cause authentication to fail.

5. If you're using an SSL accelerator and you want to use SSL offloading, select the check box next to **Allow secure channel (SSL) offloading**.
   Select this check box if you'll be using a separate server to handle Secure Sockets Layer (SSL) encryption and decryption. When you use SSL offloading, the firewall in front of the Client Access server ends the SSL session and then establishes a new non-SSL session to the Exchange server.

   Important:

   Don't use this option unless you're sure that you have an SSL accelerator that can handle SSL offloading. If you don't have an SSL accelerator that can handle SSL offloading, and you select this option, Outlook Anywhere won't function correctly.

6. Click **Enable** to apply these settings and enable Outlook Anywhere.

7. Click **Finish** to close the Enable Outlook Anywhere wizard.

Use the Shell to enable Outlook Anywhere

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration settings" entry in the Client Access Permissions topic.

In this example, the Client Access server named `Exch1` is enabled for Outlook Anywhere with its external host name as `site.contoso.org`, the default authentication set to Basic, and SSL offloading not selected.

```
Enable-OutlookAnywhere -Server 'Exch1' -ExternalHostname 'site.contoso.org' -Defa
```

This example enables the server named `Server01` for Outlook Anywhere. The external host name is set to `mail.contoso.com`, both Basic and NTLM authentication are used, and SSL offloading is set to `$true`. The `ClientAuthenticationMethod` parameter specifies the authentication method that the Autodiscover service provides to the Outlook Anywhere clients to authenticate to the Client Access server. The authentication method can be set to Basic or NTLM.

```
Enable-OutlookAnywhere -Server:Server01 -ExternalHostname:mail.contoso.com -Clien
```

For more information about syntax and parameters, see Enable-OutlookAnywhere.

Other Tasks

After you enable Outlook Anywhere, you may want to Configure Client Access Server Properties.

1.6.2.3.3 Disable Outlook Anywhere

Disable Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to disable Outlook Anywhere on the Microsoft Exchange Server 2010 Client Access server for your organization.

Looking for other management tasks related to Outlook Anywhere? Check out Managing Outlook Anywhere.

Prerequisites

If you want to disable Outlook Anywhere access for your whole organization, you must disable it on the Exchange 2010 Client Access server that's enabled for Outlook Anywhere in all sites in your organization. However, you can disable access to Outlook Anywhere on a site-by-site basis by disabling Outlook Anywhere only on each Client Access server in the site in which you want to disable Outlook Anywhere access to Mailbox servers.

Use the EMC to disable Outlook Anywhere

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the action pane, click **Disable Outlook Anywhere**.
3. Click **Yes** when you're asked if you want to disable Outlook Anywhere for this server.

Use the Shell to disable Outlook Anywhere

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration" entry in the Client Access Permissions topic.

This example disables Outlook Anywhere on the specified Client Access server.

```
disable-OutlookAnywhere -Server:'ServerName'
```

For more information about syntax and parameters, see Disable-OutlookAnywhere.

Other Tasks

After you disable Outlook Anywhere, you may also want to:

- Enable Outlook Anywhere
- Test Outlook Anywhere Connectivity

Configure an External Host Name for Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can create an external host name for Outlook Anywhere on a Microsoft Exchange Server 2010 Client Access server.

If you manage more than one Exchange site, we recommend that you create separate external host names for each site that has a Client Access server that's enabled for Outlook Anywhere. When you create a separate external host name for each site, Microsoft Office Outlook 2007 clients automatically use the Client Access server that's closest to their mailbox.

Note:
Users who are using Outlook 2003 must have their profiles manually updated to use the external host name that is closest to their mailbox.

Looking for other management tasks related to Outlook Anywhere? Check out Managing Outlook Anywhere.

Prerequisites

To successfully complete this procedure, either the Client Access server must be enabled for Outlook Anywhere or the external host name must be specified by using the Enable Outlook Anywhere wizard. To enable Outlook Anywhere, see Enable Outlook Anywhere.

Use the EMC to configure an external host name for Outlook Anywhere

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration (enable, disable, change, view)" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the action pane, click **Properties**.
3. On the **Exchange (Default Web Site) Properties** page, click the **Outlook Anywhere** tab.
4. In the text box under **External host name**, enter the external host name to use for this site.
5. Click **OK** to save your changes.

Use the Shell to configure an external host name for Outlook Anywhere

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration (enable, disable, change, view)" entry in the Client Access Permissions topic.

This example configures an external host name for Outlook Anywhere.

```
set-OutlookAnywhere -Identity:'CAS01' -ExternalHostName:'site.contoso.com'
```

For more information about syntax and parameters, see Configure an External Host Name for Outlook Anywhere.

Other Tasks

After you configure an external host name for Outlook Anywhere, you may also want to:

- Configure Authentication for Outlook Anywhere
- Configure SSL for Outlook Anywhere
- Configure SSL Offloading for Outlook Anywhere

1.6.2.3.5 Managing Certificates for Outlook Anywhere

Managing Certificates for Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-07*

Configure Outlook Anywhere to Use an SSL Certificate with Redirection

Configure Outlook Anywhere to Use Multiple SSL Certificates

1.6.2.3.5.1 Configure Outlook Anywhere to Use an SSL Certificate with Redirection

Configure Outlook Anywhere to Use an SSL Certificate with Redirection

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you can't use multiple Secure Sockets Layer (SSL) certificates for your Outlook Anywhere deployment, you can set up your Outlook Anywhere deployment to use a single SSL certificate with redirection. Microsoft Office Outlook 2007 and Outlook 2010 clients that aren't joined to your domain or don't have direct access to Active Directory in your Microsoft Exchange Server 2010 forest will be redirected to another Domain Name System (DNS) address to obtain their user profile information by using the Autodiscover service.

For more information about how a single SSL certificate works with redirection in an Outlook Anywhere deployment, see Understanding Redirection for Outlook Anywhere with a Single SSL Certificate.

Looking for other tasks for managing Outlook Anywhere? Check out Managing Outlook Anywhere.

Configure your Outlook Anywhere deployment to use an SSL certificate with redirection

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "SSL for Outlook Anywhere" and "IIS Manager" entries in the Client Access Permissions topic.

1. Configure a valid SSL certificate. You must obtain a valid SSL certificate from a certification authority (CA) that's trusted by the client computer's operating system. For more information, see Obtain a Server Certificate from a Certification Authority. After you obtain a valid SSL certificate, apply the certificate to the default Web site of your Client Access server. For more information, see Install an SSL Certificate on a Client Access Server.
2. Configure the URLs for Exchange services. You must configure the external and internal URLs for your available Exchange services to point to the default Web site, for example, mail.contoso.com. For more information about how to set the URLs for the Exchange services, see Configure Exchange Services for the Autodiscover Service.
3. Configure the service connection point object to use a site dedicated to handling e-mail, for example, mail.contoso.com. You can do this by running the following command:

```
Set-ClientAccessServer -id <CAS01>  -AutoDiscoverServiceInternalUri ht
```

4. Configure the IP address for the default Web site. You must set the default Web site to listen on only one IP address. After you have done this, bind any additional IP addresses to the network adapter, also known as a NIC, for the Client Access server. For more information about how to do this, see your Windows server documentation.
5. Create a new Web site in Internet Information Services (IIS) Manager for the Autodiscover service redirection by doing the following:
   5.a. In IIS Manager, expand your Client Access server name to select and right-click **Sites**, then select **Add Web Site**. Enter your domain name under **Site name**.
   5.b. Under **Physical path**, navigate to %SystemDrive%\inetpub\. Under inetpub, create a new folder called Autodiscover_redirect.

   Note:
   You must allow the **Users** group **Read & execute** access to the Web site that you create.
6. Create the Autodiscover redirect. Use Windows Explorer to locate the folder that you created named Autodiscover_redirect. Create a new folder named Autodiscover in the Autodiscover redirect folder, and then use a text editor, such as Notepad, to create a new blank text file named Autodiscover.xml in the Autodiscover folder.
7. Configure the new Web site to redirect to the site that's dedicated to handling e-mail, for example, mail.contoso.com. In IIS Manager, right-click the Autodiscover.xml file that you created, and then click **Properties**. On the Properties page, select **A redirection to a URL**, and then enter the same URL that you used to configure the server connection point object. For example, https://mail.contoso.com/autodiscover/autodiscover.xml.
8. Test your results to make sure that the site that you're using to handle e-mail, for example, mail.contoso.com, can be resolved internally and externally by using your Outlook 2010 or Outlook 2007 client.

Other Tasks

After you configure Outlook Anywhere to use an SSL certificate with redirection, you may

also want to:

- Configure SSL Offloading for Outlook Anywhere

1.6.2.3.5.2 Configure Outlook Anywhere to Use Multiple SSL Certificates

Configure Outlook Anywhere to Use Multiple SSL Certificates

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use multiple Secure Sockets Layer (SSL) certificates for Outlook Anywhere and the Microsoft Exchange services that Microsoft Office Outlook 2007 and Outlook 2010 use, such as Unified Messaging and the offline address book.

After your Outlook Anywhere deployment has been configured correctly to use multiple SSL certificates, your domain-joined clients will contact Active Directory and obtain the site address for the Autodiscover service from the service connection point (SCP) object. Clients that aren't domain joined or that don't have direct access to Active Directory will contact the DNS server to obtain the site address for the Autodiscover service SCP object. After a client connects to the Autodiscover service, the client will receive the URLs for the available Microsoft Exchange services. The client won't be prompted with a certificate warning because a valid certificate is provided at each point during the connection process.

Looking for management tasks related to Outlook Anywhere? See Managing Outlook Anywhere.

Configure your Outlook Anywhere deployment to use multiple SSL certificates

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "SSL for Outlook Anywhere", "IIS Manager", and "Autodiscover service virtual directory settings" entries in the Client Access Permissions topic.

The following are the steps required to configure your Outlook Anywhere deployment to use multiple SSL certificates.

1. **Obtain two valid SSL certificates** You must obtain two valid SSL certificates from a certification authority (CA) that's trusted by the client's operating system. One SSL certificate will be used for the site that will handle e-mail and the other will be used for the site dedicated to the Autodiscover service. For example, you can create one SSL certificate named mail.contoso.com and another certificate named autodiscover.contoso.com. For more information, see Obtain a Server Certificate from a Certification Authority.
2. **Configure a second IP address** After you've obtained the certificates, you must assign an additional IP address to the network adapter, also known as a NIC, on the Microsoft Exchange Server 2010 Client Access server. This will enable the Client Access server to have two public IP addresses. For more

information, see the Windows Server 2008 documentation about configuring networks and servers.

3. **Create an A record** Create a Host (A) resource record using the DNS manager for the second site that's dedicated to the Autodiscover service, for example, autodiscover.contoso.com, and point it to the new IP address that you created on the Client Access server. For more information, see the Windows Server 2008 DNS documentation about adding resource records.
4. **Create a new Autodiscover Web site** On the Client Access server, use Internet Information Services (IIS) Manager to create a new Web site that points to an empty directory. Then assign this new Web site the IP address for the second site that's dedicated to the Autodiscover service (for example, autodiscover.contoso.com). Follow these steps:
   4.a. From IIS Manager, expand your server name > **Sites**, and select the new Web site
   4.b. In the **Actions** pane, select **Bindings**.
   4.c. From the **Site Bindings** dialog box, in the **Types** column, select **http**, and then click **Edit**.
   4.d. In the **Edit Site Binding** dialog box, assign the dedicated IP address, enter the host name, for example autodiscover.contoso.com, and then click **OK**.
5. **Create a new Autodiscover virtual directory** Use the **New-AutodiscoverVirtualDirectory** cmdlet to create the new Autodiscover virtual directory on this second Web site that's dedicated to the Autodiscover service. For more information, see Create an Autodiscover Virtual Directory.
6. **Remove the Autodiscover virtual directory for the default Web site** You must correctly identify and remove the Autodiscover virtual directory that you created during Exchange Setup by using the **Remove-AutoDiscoverVirtualDirectory** cmdlet. For more information, see Delete the Default Autodiscover Virtual Directory.
7. **Assign the SSL certificates to the correct Web sites** You must assign the first SSL certificate, for example, the certificate for mail.contoso.com, to the default Web site, and then assign the second SSL certificate to the site that's dedicated to the Autodiscover service, for example, the autodiscover.contoso.com Web site. Follow these steps:
   7.a. From IIS Manager, expand your server name > **Sites**, and then select the Web site.
   7.b. In the **action** pane, select **Bindings**.
   7.c. In the **Site Bindings** dialog box, click **Add**.
   7.d. In the **Add Site Bindings** dialog box, set the binding type as **https**.
   7.e. Under SSL certificate, select the SSL certificate to be used for this site, and then click **OK**.
8. **Change the URLs for the Exchange services** You must change the external and internal URLs for your available Exchange services to point to the site that's dedicated to handling e-mail, for example, mail.contoso.com. For more information about how to set the URLs for the Exchange services, see Configure Exchange Services for the Autodiscover Service.
9. **Configure the SCP object** You must configure the SCP object to use the site that's dedicated to the Autodiscover service, for example, autodiscover.contoso.com. This example sets the Active Directory SCP object to direct users to the autodiscover.contoso.com URL using the **Set-ClientAccessServer** cmdlet on CAS1:

```
Set-ClientAccessServer -Identity CAS1 -AutoDiscoverServiceInternalUri
```

10. **Test your results** After you've completed these steps, you must make sure that the sites that are dedicated to handling e-mail and the Autodiscover service can be resolved internally and externally by your Outlook client. For more information, see Test Outlook Anywhere Connectivity and Test Outlook Autodiscover Connectivity.

Other Tasks

After you've configured Outlook Anywhere to use multiple SSL certificates, you may also want to:

- Configure Outlook Anywhere to Use an SSL Certificate with Redirection
- Test Outlook Anywhere Connectivity
- Test Outlook Autodiscover Connectivity

1.6.2.3.6 Configure Client Access Server Properties

Configure Client Access Server Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the **Outlook Anywhere** tab to configure settings after you enable Outlook Anywhere on your Microsoft Exchange Server 2010 Client Access server.

Looking for other tasks for managing Outlook Anywhere? Check out Managing Outlook Anywhere.

What Do You Want to Do?

- Use the EMC to configure Outlook Anywhere on the Client Access server properties
- Use the Shell to configure Outlook Anywhere on the Client Access server properties

Prerequisites

Outlook Anywhere has been enabled. For detailed steps, see Enable Outlook Anywhere.

Use the EMC to configure Outlook Anywhere on the Client Access server properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration settings" entry in the Client Access Permissions topic.

Note:

You can also use the Shell to view general information about a server. For more information, see Get-ExchangeServer.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the work pane, select the server that you want to configure.
3. In the action pane, click **Properties**.

4. On the **General** tab, you can view general information about the server:
   - **Version** This field displays the version of Exchange installed on the server.
   - **Edition** This field displays the Exchange Server edition. The edition is either Standard Edition or Enterprise Edition.
   - **Role(s)** This field displays the Exchange server roles installed on the server.
   - **Product ID** This field displays the product ID for the Exchange server. If you haven't yet entered the product key for the server, the product ID displayed is **Unlicensed**. To license an unlicensed version of Exchange, see Enter Product Key.
   - **Modified** This field displays the last date and time that a configuration change was made on this server.

5. On the **System Settings** tab, view the domain controller servers and global catalog servers. You can also enable an error reporting feature:
   - **Domain controller servers being used by Exchange** This read-only box displays a list of domain controller servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.
   - **Global catalog servers being used by Exchange** This read-only box displays a list of global catalog servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.
   - **Automatically send fatal service error report to Microsoft** Select this check box if you want to enable the error reporting feature and automatically send an error report to Microsoft in the event of a fatal error.
     If you enable the error reporting feature, information about fatal service errors is sent to Microsoft over encrypted channels. The information is used to improve Microsoft products. When this feature is enabled and the issue reported has a known solution, the server receives feedback from Microsoft. This feedback contains a link to information that may help resolve the problem.

6. On the **Customer Feedback Options** tab, you can enroll the selected server into the Customer Experience Improvement Program. For more information, see Opt-in or Opt-out of the Customer Experience Improvement Program.

7. Use the **Outlook Anywhere** tab to view or configure Outlook Anywhere settings. This tab is available only on servers that have the Client Access server role installed.
   - **Status** This read-only field displays whether Outlook Anywhere is enabled or disabled for the server.
   - **External host name** Use this text box to type the external host name or URL for your organization. Users will use this name to connect to the Exchange server by using Outlook Anywhere.
   - **Client authentication method** There are three authentication options available for Outlook Anywhere.
     Basic authentication Click this button to use Basic authentication. Basic authentication sends the user's user name and password in clear text. Basic authentication also requires the user to enter their domain, user name, and password every time they connect to the Client Access server.
     NTLM authentication Click this button to use NTLM authentication. NTLM authentication is also known as Integrated Windows authentication. When NTLM authentication is used, the user's credentials aren't sent over the network. Instead, the client computer and the server exchange hashed

values of the user's credentials. NTLM can also use the current Microsoft Windows operating system logon information.
Even though it is more secure, NTLM may not work with firewalls that examine and modify traffic. For more information about whether you can use NTLM with your firewall, see your firewall manufacturer's documentation. We recommend that you choose NTLM authentication with SSL when you're using an advanced firewall server such as Microsoft Internet Security and Acceleration (ISA) Server 2006. ISA Server 2006 allows NTLM authentication to be used with Outlook Anywhere.
Negotiate Ex authentication Do not click this button. Negotiate Ex authentication is an authentication type reserved for future Microsoft use and shouldn't be used. Use of this setting will cause authentication to fail.

- **Allow secure channel (SSL) offloading** Select this check box if you will be using a separate server to handle Secure Sockets Layer (SSL) encryption and decryption. When you use SSL offloading, the firewall in front of the Client Access server ends the SSL session and then establishes a new non-SSL session to the Client Access server.

Use the Shell to configure Outlook Anywhere on the Client Access server properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration settings" entry in the Client Access Permissions topic.

This example sets the client authentication method to NTLM for a Client Access server named CAS01.

```
Set-OutlookAnywhere -Identity:CAS01\Rpc (Default Web Site) -ClientAuthenticationM
```

This example turns on SSL offloading on the Client Access server named CAS01.

```
Set-OutlookAnywhere -Identity:CAS01\Rpc (Default Web Site) -SSLOffloading:$true
```

For more information about syntax and parameters, see Set-OutlookAnywhere.

For More Information

Managing Outlook Anywhere

1.6.2.3.7 Install the Windows RPC Over HTTP Proxy Component

Install the Windows RPC Over HTTP Proxy Component

Client Access > Managing Client Access Servers > Managing Outlook Anywhere >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

For Outlook Anywhere to work correctly, the Windows RPC over HTTP Proxy component must be installed on your Microsoft Exchange Server 2010 Client Access server that's

running Windows Server 2008. If the component isn't installed, follow these steps to install it before you enable Outlook Anywhere. You can install the Windows RPC over HTTP Proxy component using Server Manager or the command line.

Looking for other management tasks related to Outlook Anywhere? Check out Managing Outlook Anywhere.

Install the RPC over HTTP Proxy component using Server Manager

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "RPC over HTTP Proxy component" entry in the Client Access Permissions topic.

1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. Under Server Manager, right-click **Features**, and then click **Add Features**.
3. In the **Add Features Wizard**, on the **Features** page, select the check box for **RPC over HTTP Proxy**, and then click **Next**.
4. On the **Confirmation** page, click **Install**.
5. On the **Results** page, click **Close**.

Install the RPC over HTTP Proxy component using the command line

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "RPC over HTTP Proxy component" entry in the Client Access Permissions topic.

Open a Command Prompt window, and then type the following command:

```
ServerManagerCmd -i RPC-over-HTTP-proxy
```

Other Tasks

After you install the RPC over HTTP Proxy component, you may also to want to:

- Enable Outlook Anywhere
- Test Outlook Anywhere Connectivity

1.6.2.3.8 Test Outlook Anywhere Connectivity

Test Outlook Anywhere Connectivity

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

After you enable Outlook Anywhere (formerly known as RPC over HTTP) in your Microsoft Exchange Server 2010 organization, you can test for end-to-end client Outlook Anywhere connectivity in either of the following ways:

- Perform the test in the Shell by running the **Test-OutlookConnectivity** cmdlet on the Exchange Client Access server enabled for Outlook Anywhere.

- Run the Outlook Anywhere connectivity test from a Web browser using the Exchange Remote Connectivity Analyzer (ExRCA).

If the cmdlet test fails, the output notes the step that failed. The ExRCA also returns a detailed summary showing where the test failed and what steps you can take to fix issues. Both tests attempt to sign in to the specified user mailbox via Outlook Anywhere after obtaining server settings from the Autodiscover service.

Looking for other management tasks related to Outlook Anywhere? Check out Managing Outlook Anywhere.

Prerequisites

- Outlook Anywhere must be enabled on the Client Access server. For more information, see Enable Outlook Anywhere.
- Before running the test using the cmdlet, you must create a test user using the New-TestCasConnectivityUser.ps1 script.

Use the Shell to test Outlook Anywhere connectivity

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Test Outlook Anywhere connectivity" entry in the Client Access Permissions topic.

This example tests Outlook Anywhere connectivity by setting the `Protocol` parameter to HTTP.

```
Test-OutlookConnectivity -Protocol:Http -GetDefaultsFromAutoDiscover:$true -verbo
```

Note:

The `verbose` parameter returns a detailed output that notes each action the cmdlet performs.

For more information about cmdlet syntax, parameters, and examples, see Test-OutlookConnectivity.

Use the ExRCA to test Outlook Anywhere connectivity

1. From your Web browser, navigate to the Exchange Remote Connectivity Analyzer Web site.
2. Follow the wizard instructions for testing Outlook Anywhere.

Other Tasks

After you test Outlook Anywhere connectivity, you may also want to:

- Configure Client Access Server Properties
- Test Outlook Autodiscover Connectivity

1.6.2.4 Managing Exchange ActiveSync

Managing Exchange ActiveSync

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-17*

Managing the Exchange ActiveSync Virtual Directory

Managing Exchange ActiveSync Users

Managing an Exchange ActiveSync Server

Managing Exchange ActiveSync Devices

Managing Exchange ActiveSync with Policies

1.6.2.4.1 Managing the Exchange ActiveSync Virtual Directory

Managing the Exchange ActiveSync Virtual Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-12*

Create an Exchange ActiveSync Virtual Directory

Remove an Exchange ActiveSync Virtual Directory

View or Configure Exchange ActiveSync Virtual Directory Properties

1.6.2.4.1.1 Create an Exchange ActiveSync Virtual Directory

Create an Exchange ActiveSync Virtual Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Exchange Management Shell to create a Microsoft Exchange ActiveSync virtual directory in Microsoft Exchange Server 2010.

By default, when Exchange 2010 is installed, a new virtual directory is created in the default Web site in Internet Information Services (IIS). This virtual directory is named Microsoft-Server-ActiveSync. You can create additional Exchange ActiveSync virtual directories under Web sites other than the default Web site. All Exchange ActiveSync virtual directories you create will have the name Microsoft-Server-ActiveSync.

Note:
You can also use this procedure to create a new Exchange ActiveSync virtual directory if you've removed the virtual directory because it's become corrupted.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Use the Shell to create an Exchange ActiveSync virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync server settings" entry in the Client Access Permissions topic.

This example creates the Exchange ActiveSync virtual directory under the contoso.com Web site.

```
New-ActiveSyncVirtualDirectory -Identity "Contoso.com\Microsoft-Server-ActiveSync
```

For more information about syntax and parameters, see New-ActiveSyncVirtualDirectory.

Other Tasks

After you create an Exchange ActiveSync virtual directory, you may also want to:

- Remove an Exchange ActiveSync Virtual Directory
- View or Configure Exchange ActiveSync Virtual Directory Properties

1.6.2.4.1.2 Remove an Exchange ActiveSync Virtual Directory

Remove an Exchange ActiveSync Virtual Directory

Managing Client Access Servers > Managing Exchange ActiveSync > Managing the Exchange ActiveSync Virtual Directory >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to remove a Microsoft Exchange ActiveSync virtual directory in Microsoft Exchange Server 2010.

By default, when Exchange 2010 is installed, a new virtual directory is created in the default Web site in Internet Information Services (IIS). This virtual directory is named Microsoft-Server-ActiveSync. You can create additional Exchange ActiveSync virtual directories under Web sites other than the default Web site. All Exchange ActiveSync virtual directories you create will have the name Microsoft-Server-ActiveSync. You can remove the default Exchange ActiveSync virtual directory or any additional Exchange ActiveSync virtual directories you create.

Note:
You can also use this procedure to remove an Exchange ActiveSync virtual directory if the virtual directory settings become corrupted.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Use the Shell to remove an Exchange ActiveSync virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync server settings" entry in the Client Access Permissions topic.

This example removes the Exchange ActiveSync virtual directory under the contoso.com Web site.

```
Remove-ActiveSyncVirtualDirectory -Identity "Contoso.com\Microsoft-Server-ActiveS
```

For more information about syntax and parameters, see Remove-ActiveSyncVirtualDirectory.

Other Tasks

After you remove an Exchange ActiveSync virtual directory, you may also want to:

- Create an Exchange ActiveSync Virtual Directory
- View or Configure Exchange ActiveSync Virtual Directory Properties

1.6.2.4.1.3 View or Configure Exchange ActiveSync Virtual Directory Properties

View or Configure Exchange ActiveSync Virtual Directory Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After you have installed the Client Access server role on an Exchange Server 2010 computer, Exchange ActiveSync is enabled by default. An Exchange ActiveSync virtual directory is created on the Exchange 2010 Client Access server. You can configure a variety of options on that virtual directory.

Looking for other management tasks related to Exchange ActiveSync virtual directories? Check out Managing the Exchange ActiveSync Virtual Directory.

Prerequisites

The Client Access server role has been installed on an Exchange 2010 computer. For more information, see Install Exchange Server 2010.

What Do You Want to Do?

Use the EMC to view or configure the Exchange ActiveSync virtual directory properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync virtual directory settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the work pane, click the **Exchange ActiveSync** tab, and then click the **Microsoft-Server-ActiveSync** virtual directory.
3. In the action pane, under click **Microsoft-Server-ActiveSync**, click **Properties**.

4. Use the **General** tab to view display-only information about the Exchange ActiveSync virtual directory and to modify the Internal and External URLs.
   - **Server** This read-only field shows the name of the server the virtual directory is located on.
   - **Web site** This read-only field shows the name of the Web site that holds the virtual directory. Normally, this will be the **Default Web Site**.
   - **SSL Enabled** This read-only field shows the Secure Sockets Layer (SSL) status of the virtual directory. The default is **True**.
   - **Modified** This read-only field shows the date and time that the virtual directory was last modified.
   - **Internal URL** This field shows the `InternalURL` setting for the virtual directory. In most cases, you shouldn't change this setting.
   - **External URL** This field shows the `ExternalURL` setting for the virtual directory. In an Internet-facing Active Directory site, this field will be populated with the external DNS endpoint for Exchange ActiveSync, for example, http://contoso.com/Microsoft-Server-ActiveSync.

5. Use the **Authentication** tab to control the authentication methods for the Exchange ActiveSync virtual directory.
   - **Basic authentication (password is sent in clear text)** Select this check box if you want the mobile device to send the user name and password in clear text.

     Important Because passwords are sent in clear text with Basic authentication, you should configure SSL to encrypt data transferred between your mobile clients and the Exchange ActiveSync virtual directory.
   - **Client Certificate authentication** Select whether you want to ignore, accept, or require client certificate authentication.

     Certificates can reside in the certificate store on a mobile device or on a smart card. A certificate authentication method uses the Extensible Authentication Protocol (EAP) and Transport Layer Security (TLS) protocols. In EAP-TLS certificate authentication, the client and the server prove their identities to each other. For example, an Exchange ActiveSync client presents its user certificate to the Client Access server, and the Client Access server presents its computer certificate to the mobile device to provide mutual authentication.

     Note Requiring client certificates will force you to configure SSL on the Web site that's hosting the Exchange ActiveSync virtual

directory.

6. Exchange ActiveSync clients can access files and Web sites that are located on Windows SharePoint Services and Windows file shares. Use the **Remote File Servers** tab to specify allowed and blocked host names for your Exchange ActiveSync clients. This tab also allows you to configure which domains are treated as internal.
   - **Block List** Click **Block** to configure a list of host names of servers to which clients are denied access.
     The Block list takes precedence over the Allow list. To add a host name to the Block list, type the host name in the **Block List** dialog box, and then click **Add**. To remove a host name from the Block list, select the host name, and then click **Delete** in the **Block List** dialog box.
   - **Allow List** Click the **Allow** button to configure a list of host names of servers from which clients are allowed to access files.
     To add a host name to the Allow list, type the host name in the **Allow List** dialog box, and then click **Add**. To remove a host name from the Allow list, select the name, and then click **Delete** in the **Allow List** dialog box.
     If a host name is specified in the Allow list and the Block list, clients will be blocked from accessing files from that host name.
   - **Unknown Servers** Use this list to specify how to access files from host names that aren't listed in either the Block list or the Allow list. The default value is Allow.
   - **Enter the domain suffixes that should be treated as internal** Use this option to configure specific host names as internal host names. Click **Configure** to add host names to the **Internal Domain Suffix List**.
     When clients try to access files on one of these host names, Exchange ActiveSync uses the internal network to access these files instead of trying to access them over the Internet.

Use the Shell to configure the Exchange ActiveSync virtual directory properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync virtual directory settings" entry in the Client Access Permissions topic.

This example configures the Exchange ActiveSync virtual directory with Basic authentication and an *External URL* of http://contoso.com/Microsoft-Server-ActiveSync.

```
Set-ActiveSyncVirtualDirectory -Identity "http://contoso/microsoft-server-actives
```

This example configures the Exchange ActiveSync virtual directory with Basic authentication and adds a site to the blocked list.

```
Set-ActiveSyncVirtualDirectory -Identity "contoso\microsoft-server-activesync" -B
```

For syntax and parameter information, see Set-ActiveSyncVirtualDirectory.

Use the Shell to view the Exchange ActiveSync virtual directory properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync virtual directory settings" entry in the Client Access Permissions topic.

This example returns the settings for the Exchange ActiveSync virtual directory on the server CAS-01.

```
Get-ActiveSyncVirtualDirectory -Server "CAS-01"
```

This example returns the settings for a specific Exchange ActiveSync virtual directory on the server CAS-01.

```
Get-ActiveSyncVirtualDirectory -Server "CAS-01" -Identity "Microsoft-Server-Activ
```

This example returns the settings for the Exchange ActiveSync virtual directory on the server CAS-01, for the domain controller DOM-01.

```
Get-ActiveSyncVirtualDirectory -Server "CAS-01" -DomainController "DOM-01"
```

For syntax and parameter information, see Get-ActiveSyncVirtualDirectory.

Other Tasks

After you configure Exchange ActiveSync virtual directory properties, you may also want to View or Configure Exchange ActiveSync Mailbox Policy Properties.

For More Information

Managing the Exchange ActiveSync Virtual Directory

Configure Exchange ActiveSync to Access Windows SharePoint Services Sites and Windows File Shares

Managing Exchange ActiveSync

Understanding Exchange ActiveSync

1.6.2.4.2 Managing Exchange ActiveSync Users

Managing Exchange ActiveSync Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-18*

Enable Exchange ActiveSync for a User

Disable Exchange ActiveSync for a User

Configure Synchronization Options for Users

Enable Exchange ActiveSync for a User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable a user for Microsoft Exchange ActiveSync. By default, in Microsoft Exchange Server 2010, all new users are enabled for Exchange ActiveSync. If Exchange ActiveSync is disabled for a user, it can be manually enabled.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync Users.

Prerequisites

Exchange ActiveSync is enabled on the Exchange 2010 Client Access server.

Note:

By default, Exchange ActiveSync is enabled on a Client Access server.

Use the EMC to enable a user for Exchange ActiveSync

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync user settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. Select **Properties** from the action pane, or right-click the user's mailbox and then click **Properties**.
3. Click the **Mailbox Features** tab.
4. Select **Exchange ActiveSync**, and then click **Enable**.
5. Click **OK**.

Use the Shell to enable a user for Exchange ActiveSync

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync user settings" entry in the Client Access Permissions topic.

This example enables Exchange ActiveSync for a user.

```
Set-CASMailbox -Identity <SMTP Address of user> -ActiveSyncEnabled $true
```

For more information about syntax and parameters, see Set-CASMailbox.

1.6.2.4.2.2 Disable Exchange ActiveSync for a User

Disable Exchange ActiveSync for a User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can disable Microsoft Exchange ActiveSync for a user. By default, in Microsoft Exchange Server 2010, users are enabled for Exchange ActiveSync.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync Users.

Prerequisites

Exchange ActiveSync has been enabled on the Exchange 2010 server that has the Client Access server role installed.

Note:

By default, Exchange ActiveSync is enabled on a Client Access server.

Use the EMC to disable Exchange ActiveSync for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync user settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. Select **Properties** from the action pane, or right-click the user's mailbox and then click **Properties**.
3. Click the **Mailbox Features** tab.
4. Select **Exchange ActiveSync**, and then click **Disable**.
5. Click **OK**.

Use the Shell to disable Exchange ActiveSync for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync user settings" entry in the Client Access Permissions topic.

This example disables Exchange ActiveSync for a user.

```
Set-CASMailbox -Identity<SMTP Address of user> -ActiveSyncEnabled $false
```

For more information about syntax and parameters, see Set-CASMailbox.

Configure Synchronization Options for Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Windows Mobile to configure synchronization options for users.

Microsoft Exchange ActiveSync can synchronize e-mail messages, contacts, calendar items, and tasks between a user's Microsoft Exchange mailbox and the user's mobile phone. Exchange ActiveSync can't synchronize Microsoft Outlook Notes to a mobile phone.

There are many different phones that use Exchange ActiveSync and synchronize with Microsoft Exchange Server 2010. The steps in this topic are designed for Windows Mobile 6.0.

Note:
For information about how to configure phones that don't use Windows Mobile, or phones that use versions of Windows Mobile other than Windows Mobile 6.0 to synchronize with Exchange, see the documentation for your mobile phone.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync Users.

Prerequisites

- You've reviewed the manufacturer's documentation for the mobile phone you want to configure.
- Exchange ActiveSync is enabled on the Exchange 2010 Client Access server.
- You've established a partnership with the Exchange server. For more information about how to establish a partnership, see Configure a Mobile Phone for Synchronization.

Use ActiveSync on a mobile phone to configure synchronization options

1. On the mobile phone, select **Start**, select **Programs**, and then select **ActiveSync** to start the ActiveSync application.
2. Select **Menu**, and then select **Options** to display the **Options** screen.
3. Select or clear **Contacts**, **Calendar**, **E-mail**, or **Tasks**.
4. To configure options for any of these data types, select the data type, and then select **Settings**.

Use Pocket Outlook on a mobile phone to configure e-mail synchronization options

Note:
The exact steps will vary depending on the version of your mobile phone's software.

1. On the mobile phone, select **Outlook E-mail** to start the Pocket Outlook application.
2. Select **Menu**, select **Tools,** and then select **Manage Folders** to display the

folder list screen.
3. Select or clear the check box next to the folder name. Selecting the check box enables the folder for synchronization. Clearing the check box disables synchronization for that folder.

For more information about how to manage Windows Mobile phones, visit the Windows Mobile Center Web site.

1.6.2.4.3 Managing an Exchange ActiveSync Server

Managing an Exchange ActiveSync Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-18*

Enable Exchange ActiveSync

Disable Exchange ActiveSync

Configure Direct Push to Work Through Your Firewall

Configure Autodiscover for Exchange ActiveSync

Monitor Exchange ActiveSync

Define the SMTP Gateway to the Exchange Server

1.6.2.4.3.1 Disable Exchange ActiveSync

Disable Exchange ActiveSync

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can disable Microsoft ActiveSync. When you disable ActiveSync on a Microsoft Exchange Server 2010 Client Access server, you disable the application pool ActiveSync uses. An application pool is a group of processes that Internet Information Services (IIS) uses to perform a task. For more information, see Understanding Exchange ActiveSync.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Prerequisites

- The IIS component ASP.NET is installed.
- The ASP.NET Web service extension status is set to **Allowed**, not **Prohibited**. You can verify the status of the ASP.NET Web service extension in IIS Manager by expanding the server name and then clicking **Web Service Extensions**. If the **ASP.NET** Web service extension isn't set to **Allowed**, right-click the Web

service extension to change the status.

Use IIS Manager to disable Exchange ActiveSync

To perform these steps you must have Local Administrator permissions on the Client Access server.

Click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

1. Double-click to expand the server name, and then double-click to expand the **Application Pools** folder.
2. Right-click **MSExchangeSyncAppPool**, and then click **Stop** to disable ActiveSync.

Note:

If the **Stop** command is unavailable, ActiveSync is already disabled on this server.

1.6.2.4.3.2 Enable Exchange ActiveSync

Enable Exchange ActiveSync

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable Microsoft ActiveSync. By default, ActiveSync is enabled when you install the Client Access server role on the computer that's running Microsoft Exchange Server 2010.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Prerequisites

- The Internet Information Services (IIS) component ASP.NET is installed.
- The ASP.NET Web service extension status is **Allowed**, not **Prohibited**. You can verify the status of the ASP.NET Web service extension in IIS Manager by expanding the server name and then clicking **Web Service Extensions**. If the **ASP.NET** Web service extension isn't set to **Allowed**, right-click the Web service extension to change the status.

Use IIS Manager to enable Exchange ActiveSync

To perform the following procedures, you must have Local Administrator privileges on the Client Access server.

1. Click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. Double-click to expand the server name, and then double-click to expand the **Application Pools** folder.
3. Right-click **MSExchangeSyncAppPool**, and then click **Start** to enable ActiveSync.

Note:
If the **Start** command isn't available, ActiveSync is already enabled on this server.

1.6.2.4.3.3 Configure Direct Push to Work Through Your Firewall

Configure Direct Push to Work Through Your Firewall

Managing Client Access Servers > Managing Exchange ActiveSync > Managing an Exchange ActiveSync Server >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure your firewall to support Direct Push. Direct Push lets your mobile phone stay current with your Microsoft Exchange Server 2010 mailbox.

Direct Push operates by maintaining a long-standing HTTPS request between the mobile phone and the Exchange Client Access server. This request tells the Exchange Client Access server to immediately notify the mobile phone if any items in synchronized folders change during the life of the request. If any items change, the mobile phone issues a synchronization request, synchronizes with the server, and then reissues the HTTPS request. If no items change during the life of the request, the request is reissued.

Configure your firewall for Direct Push

Because the request and the response travel over an HTTPS connection, the only port that you have to open on your firewall is port 443 for HTTPS traffic. No additional ports are required for Direct Push to operate.

To verify that port 443 is open, see your firewall documentation. You should also configure your firewall time-out value to be between 15 and 30 minutes. This ensures that the long-standing HTTPS request can stay open without expiring. The exact steps for this configuration will vary, depending on your firewall hardware and software.

1.6.2.4.3.4 Configure Autodiscover for Exchange ActiveSync

Configure Autodiscover for Exchange ActiveSync

Managing Client Access Servers > Managing Exchange ActiveSync > Managing an Exchange ActiveSync Server >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to enable the Autodiscover service in Microsoft Exchange ActiveSync. You can't configure the Autodiscover service for Exchange ActiveSync using the EMC.

Note:
The ability to use Autodiscover depends on the operating system of the mobile phone.

Not all mobile phone operating systems that support synchronization with Microsoft Exchange Server 2010 support Autodiscover. For more information about operating systems that support Autodiscover, contact the manufacturer of the mobile phone.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Use the Shell to configure Autodiscover in Exchange ActiveSync

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync mobile phone settings" entry in the Client Access Permissions topic.

This example configures Autodiscover for Exchange ActiveSync and sets the **ExternalURL** property.

```
Set-ActiveSyncVirtualDirectory -Identity "COMPUTERNAME\Microsoft-Server-ActiveSyn
```

For more information about syntax and parameters, see Set-ActiveSyncVirtualDirectory.

1.6.2.4.3.5 Monitor Exchange ActiveSync

Monitor Exchange ActiveSync

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-12-03*

The performance of Microsoft Exchange ActiveSync is affected by many factors. These include the number of users who are synchronizing with Exchange ActiveSync, the types of mobile phones that are synchronizing, and how much data each user synchronizes between the Microsoft Exchange server and the mobile phone. By using monitoring, you can understand the factors that affect the performance of Exchange ActiveSync. You can examine Internet Information Services (IIS) log files and use the **Export-ActiveSyncLog** cmdlet to generate reports in comma-separated value format. You can also create several graphs from the data in these reports to analyze traffic and usage patterns.

By monitoring Exchange ActiveSync errors and events, you can understand problems your users encounter when they synchronize their mobile phones with Microsoft Exchange.

For More Information

For more information about how to monitor Exchange ActiveSync, see the following topics:

- Generate Exchange ActiveSync Reports
- Understanding Exchange ActiveSync Reporting Services

Generate Exchange ActiveSync Reports

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to generate a compiled set of reports for Microsoft Exchange ActiveSync. The **Export-ActiveSyncLog** cmdlet compiles a set of Internet Information Services (IIS) logs and processes them to create a series of output files. Each file is a separate report that can help you understand your Exchange ActiveSync deployment.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Prerequisites

You have read-only access to the directory that contains the IIS log files.

Use the Shell to generate Exchange ActiveSync reports

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync server settings" entry in the Client Access Permissions topic.

This example exports the Exchange ActiveSync log for the date range 06/08/09 to 06/09/09. The times on the report are in Coordinated Universal Time (UTC), and the report is saved in c:\exreports\easreports.

```
Export-ActiveSyncLog -Filename: "c:\Windows\System32\LogFiles\W2SVC1\ex060809.log
```

For more information about syntax and parameters, see Export-ActiveSyncLog.

Other Tasks

After you generate Exchange ActiveSync reports, you may also want to learn about:

- Managing Exchange ActiveSync Devices
- Configuring Exchange ActiveSync Policies

1.6.2.4.3.6 Configure Exchange ActiveSync to Access Windows SharePoint Services Sites and Windows File Shares

Configure Exchange ActiveSync to Access Windows SharePoint Services Sites and Windows File Shares

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to manage the list of Microsoft Windows SharePoint Services sites and Windows file shares that Microsoft Exchange ActiveSync users can access from their mobile phones.

Note:
The lists of Windows SharePoint Services sites and Windows file shares that are allowed and blocked apply to the whole Exchange ActiveSync virtual directory. You can't configure these lists for individual users. But you can disable Windows SharePoint Services sites and Windows file share access for individual users by using Exchange ActiveSync policies.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Use the EMC to configure access to Windows SharePoint Services sites and Windows file shares

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync user settings" entry in the Client Access Permissions topic.

1. Open the EMC.
2. In the console tree, navigate to **Server Configuration** > **Client Access**.
3. Select **Exchange ActiveSync**.
4. In the action pane, under **Microsoft-Server-ActiveSync**, click **Properties**.
5. Click the **Remote File Servers** tab.
6. Click **Block** to add host names of sites that clients are prohibited from accessing.
7. Click **Allow** to add host names of sites that clients are permitted to access.
8. Use the list in the **Unknown Servers** section to specify the default action that should be taken when a client tries to access a file from a server that's not entered in either the Allow List or Block List.
9. Click **Configure** to enter the domain suffixes that should be treated as internal.

   Note:
   If you specify that a domain suffix should be treated as internal, the Exchange ActiveSync client will access the content through an intranet connection instead of an Internet connection.

Use the Shell to configure access to Windows SharePoint Services sites and Windows file shares

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the " Exchange ActiveSync user settings" entry in the Client Access Permissions topic.

This example adds two sites to the Block list and one to the Allow list, specifies an internal domain suffix, and configures the default action to take when a client tries to access a file from a server that's not entered in the Allow or Block lists.

```
Set-ActiveSyncVirtualDirectory -Identity:"ServerName\Microsoft-Server-ActiveSync
```

For more information about syntax and parameters, see Set-ActiveSyncVirtualDirectory.

1.6.2.4.3.7 Define the SMTP Gateway to the Exchange Server

Define the SMTP Gateway to the Exchange Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-30*

Microsoft Exchange Server 2010 uses an SMTP-to-SMS gateway to send text messaging notifications from an Exchange mailbox to a user's mobile phone. This functionality notifies a user by sending them a text message whenever a new e-mail message is received. An SMTP-to-SMS gateway is required for each mobile phone provider. Several common SMTP-to-SMS gateways are included with Exchange 2010 Service Pack (SP1). These SMTP-to-SMS gateways are stored in an XML file and a copy of that file is included on each Client Access server and each Hub Transport server. If your organization requires an SMTP-to-SMS gateway for a mobile phone provider that isn't included in Exchange 2010 SP1, you can create a customized XML file using the instructions included in this topic.

Creating a Customized SMTP Gateway XML File

The SMTP gateway XML file is located in the Exchange Server\V14\Bin folder. The file name is TextMessagingHostingData-System.xml. In order to create your own customized XML file, must create a second customized XML file named TextMessagingHostingData-Site.xml in the same location on the Client Access servers and the Hub Transport servers in your Exchange organization.

Note:
If your Exchange organization includes multiple Client Access servers and Hub Transport servers, you must copy this customized XML file to all of these servers.

As soon as the file has been copied to all applicable servers, the next time your users try to configure SMS notifications in the Exchange Control Panel (ECP), they'll see the new SMTP-to-SMS gateways you have defined.

Note:
Because changes to the customized XML file are visible without a service restart, we recommend that you don't edit the customized XML file in the target location. Copy it to another location for editing, and then copy the completed file to the target folder.

SMTP Gateway XML File Format

The name of customized XML file must be TextMessagingHostingData-Site.xml. Three types of information are stored in this file:

- Country and region information, which is stored in the Regions section of the XML file.
- SMTP gateway carrier information.
- SMTP gateway detailed specifications.

Every SMTP gateway requires both a country or region and a carrier. One carrier can have multiple SMTP gateways, but each SMTP gateway can have only one carrier. Each combination of these three types of information must be unique. Therefore, if you define a

combination in the customized file that's the same as the combination in the default file, the information in the default file will be overwritten.

Regions Section

The Regions section of the XML file is made up of three pieces of information.

- **ISO2 two-letter country code** This is the two-letter code from ISO 3166-1 alpha-2.
- **Country code** This code is obtained from the List of ITU-T Recommendation E.164 Assigned Country Codes.
- **Phone number example** This example format is optional.
- The regions section in the XML file might look like the following:

```
<Regions>
    <Region Iso2="CN">
      <CountryCode>86</CountryCode>
      <PhoneNumberExample>139 0000 0000</PhoneNumberExample>
    </Region>
</Regions>
```

Note:

If the custom XML file tries to define the same region as one contained in the default file, the entry in the default file will be overwritten.

Carriers Section

The carrier information section contains the following two pieces of information:

- **ID** This is a 5-digit number that's unique within the default and customized SMTP configuration XML files.
- **Carrier localized name** Each carrier can have multiple names. This is the localized name for the carrier in the local region. You can specify display names for a variety of localities. An English display name should always be specified as a default.

The carriers section of the XML file might look like the following:

```
<Carriers>
    <Carrier Identity="30344">
        <LocalizedInfo Culture="en">
            <DisplayName>Gold Systems, Inc.</DisplayName>
        </LocalizedInfo>
    </Carrier>
    <Carrier Identity="30345">
        <LocalizedInfo Culture="en">
            <DisplayName>China Mobile</DisplayName>
        </LocalizedInfo>
        <LocalizedInfo Culture="zh">
            <DisplayName>中国移动</DisplayName>
        </LocalizedInfo>
    </Carrier>
</Carriers>
```

Note:

If the XML file contains Unicode text for the localized carrier name, you must save the XML file in a UTF-8 or Unicode encoding format.

Service Section

The service section defines the SMTP gateway specification. Three types of information are included in this section of the XML file.

- **Region ISO** The Region ISO you are specifying must have been previously defined in the Region section of the XML file.
- **Carrier** The Carrier identity must have been previously defined in the Carriers section of the XML file.
- **SMTPToSMSGateway** This section of the file contains the following information:
  - **SMTP address** This is the SMTP address for the message to be routed to

when an SMS notification is generated. There are two keywords in this field. %c is the country code specified in region section and %n is the local phone number.

- **MessageRendering** This container defines how the message is rendered. It includes several parameters. The *Container* parameter can have one of two values. If the value is body, then the SMS message content is stored in the message body. If the value is subject, then the SMS message content is stored in the message subject. The *Capacity* parameter specifies how many characters can be contained in one SMS message. The **CodingScheme** property of the *Capacity* parameter can be either GSMDefault, Unicode, or Euc-KR.

An example service section might look like the following.

```
<Service>
        <RegionIso2>CN</RegionIso2>
        <CarrierIdentity>30345</CarrierIdentity>
        <Type>SmtpToSmsGateway</Type>
        <SmtpToSmsGateway>
            <RecipientAddressing>
                <SmtpAddress>%n@139.com</SmtpAddress>
            </RecipientAddressing>
            <MessageRendering Container="Body">
                <Capacity CodingScheme="GsmDefault">140</Capacity>
                <Capacity CodingScheme="Unicode">50</Capacity>
            </MessageRendering>
        </SmtpToSmsGateway>
    </Service>
```

For a GSM network, GsmDefault capacity should always be specified, while Unicode is optional. When Unicode is not specified, all Unicode characters will be automatically converted to ? in the system.

For a CDMA network, at least one capacity should be specified.

Note:

Typically, the SMTP gateway will use some characters for extra information, such as the from field. Set aside enough buffer when specifying message length for some of this extra information.

XML File Example

This is an example of a complete TextMessagingHostingData-Site.xml file.

```
<?xml version="1.0" ?>
<TextMessagingHostingData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" x
<Regions>
    <Region Iso2="CN">
      <CountryCode>86</CountryCode>
      <PhoneNumberExample>139 0000 0000</PhoneNumberExample>
    </Region>
</Regions>
<Carriers>
    <Carrier Identity="30344">
        <LocalizedInfo Culture="en">
            <DisplayName>Gold Systems, Inc.</DisplayName>
        </LocalizedInfo>
    </Carrier>
    <Carrier Identity="30345">
        <LocalizedInfo Culture="en">
            <DisplayName>China Mobile</DisplayName>
        </LocalizedInfo>
        <LocalizedInfo Culture="zh">
            <DisplayName>中国移动</DisplayName>
        </LocalizedInfo>
    </Carrier>
</Carriers>
<Services>
```

```
    <Service>
        <RegionIso2>US</RegionIso2>
        <CarrierIdentity>30344</CarrierIdentity>
        <Type>SmtpToSmsGateway</Type>
        <SmtpToSmsGateway>
            <RecipientAddressing>
                <SmtpAddress>%n@paging.goldsys.com</SmtpAddress>
            </RecipientAddressing>
            <MessageRendering Container="Body">
                <Capacity CodingScheme="GsmDefault">140</Capacity>
            </MessageRendering>
        </SmtpToSmsGateway>
    </Service>
    <Service>
        <RegionIso2>CN</RegionIso2>
        <CarrierIdentity>30345</CarrierIdentity>
        <Type>SmtpToSmsGateway</Type>
        <SmtpToSmsGateway>
            <RecipientAddressing>
                <SmtpAddress>%n@139.com</SmtpAddress>
            </RecipientAddressing>
            <MessageRendering Container="Body">
                <Capacity CodingScheme="GsmDefault">140</Capacity>
                <Capacity CodingScheme="Unicode">50</Capacity>
            </MessageRendering>
            </SmtpToSmsGateway>
    </Service>
</Services>
</TextMessagingHostingData>
```


1.6.2.4.4 Managing Exchange ActiveSync Devices

Managing Exchange ActiveSync Devices

Client Access > Managing Client Access Servers > Managing Exchange ActiveSync >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-18*

Exchange ActiveSync Mobile Phones and Compatible Features

Configure a Mobile Phone for Synchronization

Disable a Mobile Phone for Exchange ActiveSync

Enable a Device for Exchange ActiveSync

View a List of Devices for a User

Configure Device Password Locking

Recover a Device Password

Perform a Remote Wipe on a Mobile Phone

Install SSL Certificates on a Windows Mobile Phone

Configure Mobile Phones to Synchronize with Exchange Server

Manage a Mobile Device

1.6.2.4.4.1 Exchange ActiveSync Mobile Phones and Compatible Features

Exchange ActiveSync Mobile Phones and Compatible Features

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-06*

Microsoft Exchange ActiveSync in Microsoft Exchange Server 2010 enables users to synchronize their mobile phones with their Exchange mailbox. Users can synchronize e-mail messages, calendar information, contact and task data, and manage their Deleted Items folder, their e-mail signature, and automatic-reply settings to let people know they're away. This topic provides information about the different types of mobile phones that synchronize with Exchange 2010.

Note:

Although we consistently refer to devices that access Exchange 2010 as mobile phones, there are many personal digital assistant devices that can access Exchange 2010 but don't have cellular phone functionality. The term "mobile phone" in this documentation refers to those devices, as well.

Devices Enabled for Exchange ActiveSync

Users can take advantage of Exchange ActiveSync by selecting mobile phones that are compatible with Exchange ActiveSync. These mobile phones are available from many manufacturers. For more information, see the device documentation.

Mobile phones that are compatible with Microsoft Exchange include the following:

- **Apple** The Apple iPhone, iPod Touch, and iPad all support Exchange ActiveSync.
- **Nokia** Nokia offers Mail for Exchange on their Eseries mobile phones. E-mail, calendar, and contact data can be synchronized over a cellular network or a wireless LAN.
- **Sony Ericsson** Sony Ericsson offers Exchange ActiveSync support on several of their newer smartphones. They also support Direct Push through a third-party program.
- **Palm** Palm offers some models of mobile phones that have the Windows Mobile operating system. These devices support Direct Push.
- **Motorola** Motorola has its own synchronization framework that enables over-the-air synchronization through Exchange ActiveSync on many of its devices.
- **Symbian** Symbian Limited licenses Exchange ActiveSync for use in the Symbian operating system. This operating system is an open standard operating system for mobile phones.
- **Android** Many mobile phones with the Android operating system support Exchange ActiveSync. However, these mobile phones may not support all available Exchange ActiveSync mailbox policies. For more information see Understanding Exchange ActiveSync Mailbox Policies.

Windows Mobile Software Features

Mobile phones that have a version of Windows Mobile software as their operating system offer the greatest functionality when synchronizing with Exchange 2010. The following table shows some features that are available with different versions of Windows Mobile software.

Windows Mobile software features

Operating system	Features
Windows Mobile 6.0 and later versions	• Direct Push • HTML e-mail support • Message flags • Quick message retrieval • Task synchronization • Global address book lookup • Enhanced calendar views • Meeting attendee information • Management of Automatic Replies • Exchange search • Windows SharePoint Services and Windows file share (UNC) document access • Enforcement of Exchange ActiveSync mailbox policies • Remote device wipe • Basic authentication • Integration with Internet Security and Acceleration (ISA) Server • Certificate-based authentication • S/MIME support (with Exchange 2010) • Device storage card encryption • Support for rights management **Important:** Windows Phone 7 mobile phones only support a subset of all Exchange ActiveSync mailbox policy settings. For a complete list, see Understanding Exchange ActiveSync.

For More Information

For more information about how to manage Windows Mobile phones, see the Windows Mobile Center Web site.

1.6.2.4.4.2 Configure a Mobile Phone for Synchronization

Configure a Mobile Phone for Synchronization

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure a mobile phone to synchronize with your Microsoft Exchange Server 2010 mailbox. When you provision a mobile phone, you configure it to synchronize with Microsoft Exchange. Perform this procedure on each mobile phone in your organization.

Looking for other management tasks related to mobile phones? Check out Managing Exchange ActiveSync Devices.

Prerequisites

- You've reviewed the manufacturer's documentation for the mobile phone you want to configure.
- Exchange ActiveSync is enabled on the Exchange 2010 Client Access server.

Configure a mobile phone to use Exchange ActiveSync

To configure a mobile phone to use Exchange ActiveSync, you must be able to sign in to the user's Exchange mailbox with the user's credentials.

1. On the mobile phone, from the home screen, click **Start**, and then click **ActiveSync**.
2. Click **Menu**, and then click **Configure Server**.
3. Enter the server address. This is the same address as your Microsoft Office Outlook Web App server address.
4. If you've configured Exchange ActiveSync to require Secure Sockets Layer (SSL), select the **This server requires an encrypted (SSL) connection** check box.
5. Click **Next**.
6. Enter your user name, password, and domain.
7. Select the **Save password** check box.
8. Click **Next**.
9. Select the check box next to each type of information that you want to synchronize with the server, and then click **Finish**.

For more information about how to manage Windows Mobile phones, visit the Windows Mobile Center Web site.

Windows Phone 7 synchronization

If you have Windows Phone 7 mobile phones in your organization, these phones will experience synchronization problems if certain Exchange ActiveSync mailbox policy properties are configured. To allow Windows Phone 7 mobile phones to synchronize with an Exchange mailbox, either set the **AllowNonProvisionableDevices** property to true or only configure the following Exchange ActiveSync mailbox policy properties:

- PasswordRequired
- MinPasswordLength
- IdleTimeoutFrequencyValue
- DeviceWipeThreshold
- AllowSimplePassword
- PasswordExpiration
- PasswordHistory
- DisableRemovableStorage
- DisableIrDA
- DisableDesktopSync
- BlockRemoteDesktop
- BlockInternetSharing

If you have Windows Phone 7 mobile phones in your organization, you can set **AllowNonProvisionalDevices** property to True or you can create a separate Exchange ActiveSync mailbox policy for users with Windows Phone 7 mobile phones. This new Exchange ActiveSync mailbox policy should either have the **AllowNonProvisionalDevices** property set to True or only have the preceding list of policy properties configured. For more information about Exchange ActiveSync Mailbox Policy properties and Windows Phone 7, see Understanding Exchange ActiveSync Mailbox Policies.

Disable a Mobile Phone for Exchange ActiveSync

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-09*

Microsoft Exchange Server 2010 lets you restrict access to Exchange ActiveSync by using the device ID. This feature prevents users from synchronizing unauthorized devices with Exchange 2010. You can configure this restriction on each user's mailbox. By default, if Microsoft Exchange ActiveSync is enabled for a user, the user can synchronize their Exchange mailbox with any device. To restrict a user to a specific device, populate the `ActiveSyncAllowedDeviceIDs` parameter from the **Set-CASMailbox** cmdlet. To prevent a single device or set of devices, populate the `ActiveSyncBlockedDeviceIDs` parameter from the **Set-CASMailbox** cmdlet.

The *ActiveSyncBlockedDeviceIDs* parameter accepts a list of device IDs that are restricted from synchronizing with the mailbox.

Note:

When you use the **set-ActiveSyncOrganizationSettings –DefaultAccessLevel** cmdlet, devices can still be blocked if they do not comply with a specific Exchange ActiveSync policy, regardless of whether the device is allowed by the list that is provided to *ActiveSyncAllowedDeviceIDs*.

For more information about the **set-ActiveSyncOrganizationSettings –DefaultAccessLevel** cmdlet, see Set-ActiveSyncOrganizationSettings.

If Exchange ActiveSync isn't enabled for the user, the user won't be able to synchronize any device with Exchange. You can prevent a specific device from synchronizing with Exchange, but only by using the Exchange Management Shell.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Prerequisites

Exchange ActiveSync is enabled for the user.

Use the Shell to disable a device for Exchange ActiveSync

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync device settings" entry in the Client Access Permissions topic.

This example adds the device ID to the `ActiveSyncBlockedDeviceIDs` parameter list to prevent the device from synchronizing with Microsoft Exchange.

```
Set-CASMailbox -Identity: "EmailAlias" -ActiveSyncBlockedDeviceIDs: "<DeviceID_1>
```

Note:

There's no built-in functionality for retrieving the device ID before the user synchronizes with the Exchange server.

This example retrieves the device ID after the user has synchronized the device with the Exchange server.

```
Get-ActiveSyncDeviceStatistics -Mailbox:"<EmailAlias>" |fl DeviceID
```

For more information about syntax and parameters, see Set-CASMailbox.

For more information about how to manage Windows Mobile phones, visit the Windows Mobile Center Web site.

1.6.2.4.4.4 Enable a Device for Exchange ActiveSync

Enable a Device for Exchange ActiveSync

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 enables you to restrict access to Microsoft Exchange ActiveSync by using the device ID. This feature prevents users from synchronizing unauthorized mobile phones with Exchange 2010. You can configure this restriction on each user's mailbox. By default, if Exchange ActiveSync is enabled for a user, the user can synchronize the Exchange mailbox with any mobile phone. To restrict a user to a specific mobile phone, populate the `ActiveSyncAllowedDeviceIDs` parameter from the **Set-CASMailbox** cmdlet.

The *ActiveSyncAllowedDeviceIDs* parameter accepts a list of device IDs that are allowed to synchronize with the mailbox. However, devices are not blocked from synchronizing unless this parameter is used together with settings that are defined by the **set-ActiveSyncOrganizationSettings –DefaultAccessLevel** cmdlet.

Note:

When you use the **set-ActiveSyncOrganizationSettings –DefaultAccessLevel** cmdlet, devices can still be blocked if they do not comply with a specific ActiveSync policy, regardless of whether the device is allowed by the list that is provided to *ActiveSyncAllowedDeviceIDs*.

For more information about the **set-ActiveSyncOrganizationSettings –DefaultAccessLevel** cmdlet, see Set-ActiveSyncOrganizationSettings

If Exchange ActiveSync isn't enabled for users, users won't be able to synchronize any mobile phone with Exchange. You can enable a specific mobile phone for Exchange ActiveSync, but only by using the Exchange Management Shell.

Looking for other management tasks related to Exchange ActiveSync mobile phones? Check out Managing Exchange ActiveSync Devices.

Prerequisites

Exchange ActiveSync is enabled for the user.

Use the Shell to enable a mobile phone for

Exchange ActiveSync

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync Device Settings" entry in the Client Access Permissions topic.

This example adds two mobile phones to a list of allowed mobile phones for the user with the alias *tonysmit*. The mobile phones are added through a property called the *DeviceID*, which is a unique identifier associated with every mobile phone.

```
Set-CASMailbox -Identity: "tonysmit" -ActiveSyncAllowedDeviceIDs: "<DeviceID_1>",
```

Note:
There is no built-in functionality for retrieving the device ID before the user synchronizes with the Exchange server. After the user has synchronized the mobile phone with the Exchange server, this example will enable you to retrieve the device ID: `Get-ActiveSyncDeviceStatistics -Mailbox:"<EmailAlias>" |fl DeviceID`

For more information about syntax and parameters, see Set-CASMailbox.

For more information about how to manage Windows Mobile phones, visit the Windows Mobile Center Web site.

1.6.2.4.4.5 View a List of Devices for a User

View a List of Devices for a User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Users can configure multiple devices for synchronization with Microsoft Exchange Server 2010. You can use the EMC or the Shell to view a list of mobile phones that are associated with a specific user.

Note:
This topic also provides instructions for how to use Microsoft Office Outlook Web App to view a list of mobile phones associated with a user's mailbox. The user must be signed in to Outlook Web App to view a list of devices that are associated with their mailbox.

Looking for other management tasks related to Exchange ActiveSync mobile phones? Check out Managing Exchange ActiveSync Devices.

Use Outlook Web App to view a list of mobile phones for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync device settings" entry in the Client Access Permissions topic.

1. In Outlook Web App, click **Options**.
2. In the Navigation pane, select **Phone**.
3. Click the **Mobile Phones** tab.
4. The list displays several device statistics including the mobile phone name,

last synchronization time, and status.

Note:
All mobile phones the user has configured for Exchange ActiveSync are displayed in this list. To determine the correct mobile phone, use the device name and the last synchronization time from the list of mobile phones.

Use the EMC to view a list of mobile phones for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync device settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. Select a user, and then select **Manage Mobile Device** from the action pane. The **Manage Mobile Device** dialog box will display a list of all devices that are configured for synchronization.

Note:
The **Manage Mobile Device** link is only available in the action pane for users who've established a mobile phone partnership with the Exchange server.

Use the Shell to view a list of devices for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync settings" entry in the Client Access Permissions topic.

This example retrieves a list of mobile phones and their associated statistics for a user, where "alias" is the user's alias. These statistics include last synchronization time and identifying mobile phone characteristics such as the name of the mobile phone.

```
Get-ActiveSyncDeviceStatistics -Mailbox:"alias"
```

For more information about syntax and parameters, see Get-ActiveSyncDeviceStatistics.

Other Tasks

After you view a list of devices for a user, you may also want to:

- Perform a Remote Wipe on a Mobile Phone
- Configure Device Password Locking

1.6.2.4.4.6 Configure Device Password Locking

Configure Device Password Locking

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure device password locking. You can require users to lock their mobile phones by using a password. You can also enforce a variety of policy settings that guide the usage of mobile phone passwords. The settings you can configure include the following:

- Enforcing an alphanumeric password.
- Enabling password recovery.
- Requiring encryption on the mobile phone.
- Specifying a minimum password length.
- Specifying a period of inactivity before you must re-enter a password on a mobile phone. This is known as device password locking.

Looking for other management tasks related to managing mobile phones? Check out Managing Exchange ActiveSync Devices.

Prerequisites

An Exchange ActiveSync mailbox policy has been created. For detailed steps, see Create a New Exchange ActiveSync Mailbox Policy.

Use the EMC to configure device password locking

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync device settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Client Access**.
2. In the work pane, click the **Exchange ActiveSync Mailbox Policies** tab, select an existing mailbox policy, and then click **Properties** in the action pane.
3. Click the **Password** tab.
4. Select the **Require password** check box.
5. Select the **Time without user input before password must be entered (in minutes)** check box.
6. Enter the inactivity time-out value in minutes.
7. Click **OK**.

Use the Shell to configure device password locking

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync device settings" entry in the Client Access Permissions topic.

This example configures the Exchange ActiveSync mailbox policy named `Default` for device password locking after 15 minutes.

```
Set-ActiveSyncMailboxPolicy -Identity "Default" -DevicePasswordEnabled: $true -Ma
```

For more information about syntax and parameters, see Set-ActiveSyncMailboxPolicy.

Other Tasks

After you configure device password locking, you may also want to:

- Recover a Device Password
- Perform a Remote Wipe on a Mobile Phone

1.6.2.4.4.7 Recover a Device Password

Recover a Device Password

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC, the Shell, or Microsoft Office Outlook Web App to recover a device password.

You can require a device password through Microsoft Exchange ActiveSync policies. A user can configure a device password even if your Exchange ActiveSync policies don't require one. If users forget their password, you can obtain a recovery password using the EMC or the Shell. The recovery password unlocks the device and lets the user create a new password. Users can also recover their device passwords by using Outlook Web App.

Looking for other management tasks related to mobile phones? Check out Managing Exchange ActiveSync Devices.

Prerequisites

To use Outlook Web App to recover a user's device password, you must be able to sign in to Outlook Web App using the user's credentials.

Use the EMC to display the device recovery password

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync server settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the details pane, select a user, and then select **Manage Mobile Device** from the action pane. The device recovery password is displayed in the **Manage Mobile Device** dialog box.

Use the Shell to display the device recovery password

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync device settings" entry in the Client Access Permissions topic.

This example displays the recovery password for the mobile phone on the mailbox that belongs to Tony Smith.

```
Get-ActiveSyncDeviceStatistics -Mailbox:"tonysmith" -ShowRecoveryPassword:$true
```

For more information about syntax and parameters, see Get-ActiveSyncDeviceStatistics.

Use Outlook Web App to recover a device password

1. In Outlook Web App, click **Options**.
2. Select **Phones** from the Navigation Pane.
3. Select the mobile phone from the list.

   Note:
   All mobile phones the user has configured for Exchange ActiveSync are displayed in this list. To determine the correct mobile phone, use the device name and the last synchronization time displayed in the list of devices.

4. Click **Display Device Password**.

Other Tasks

After you recover a password, you may also want to:

- Configure Mobile Phones to Synchronize with Exchange Server
- Disable a Mobile Phone for Exchange ActiveSync

1.6.2.4.4.8 Perform a Remote Wipe on a Mobile Phone

Perform a Remote Wipe on a Mobile Phone

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 lets you send a command to a mobile phone to perform a remote device wipe of that phone. This process removes all the information that's stored on the phone. This includes Exchange information. This process then completes a full reset of the device. You can use the EMC or the Exchange Management Shell to perform a remote wipe on a mobile phone.

You can use this procedure to clear data from a stolen phone or to clear data from a phone before you assign it to another user.

Note:
This topic also provides instructions for a user to use Microsoft Office Outlook Web App to perform a remote wipe on a phone. The user must be signed in to Outlook Web App to perform a remote wipe.

Looking for other management tasks related to Exchange ActiveSync device? Check out Managing Exchange ActiveSync Devices.

Use the EMC to perform a remote wipe on a mobile phone

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync device settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. Select the user from the **Mailbox** window.
3. In the action pane, click **Manage mobile device**, or right-click the user's mailbox, and then click **Manage mobile device**.
4. Select the mobile phone you want to clear all data from.
5. In the **Actions** section, click **Clear**.
6. Click **Clear** again.

Use Outlook Web App to perform a remote wipe on a mobile phone

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync device settings" entry in the Client Access Permissions topic.

1. Open Outlook Web App.
2. Sign in to the device owner's mailbox.
3. Click **Options**.
4. In the Navigation Pane, select **Phone**.
5. Click the **Mobile Phones** tab.
6. Select the ID of the mobile phone that you want to wipe and remove from the list.
7. Click **Wipe device**.
8. Click **OK**.
9. Click **Remove Device**.

Use the Shell to perform a remote wipe on a mobile phone

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync device settings" entry in the Client Access Permissions topic.

This example obtains the identity of the device.

```
Get-ActiveSyncDeviceStatistics - Mailbox jeffhays | fl Identity
```

This example performs the remote wipe of the device.

```
Clear-ActiveSyncDevice -Identity WM_jeffhayes
```

For more information about syntax and parameters, see Get-ActiveSyncDeviceStatistics and Clear-ActiveSyncDevice.

Install SSL Certificates on a Windows Mobile Phone

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

It is possible to save a digital certificate to a file and install a digital certificate on a Windows Mobile phone. Microsoft Exchange ActiveSync enables a variety of mobile phones to synchronize with an Exchange mailbox. A digital certificate might need to be installed on a user's mobile phone if Exchange ActiveSync is required to use Secure Sockets Layer (SSL) and your organization uses a certificate that isn't from a trusted commercial certification authority (CA).

Instructions for installing a certificate on a Windows Mobile phone are included here. For more information about how to install a certificate on a phone that isn't running Windows Mobile software, see the documentation for the specific phone.

Note:

If your organization uses an SSL certificate from a trusted commercial CA, your users might not have to install the certificate on their phone. Most phones have certificates from several trusted commercial CAs preinstalled in the root store of the phone. For a list of certificates that are preinstalled on Windows Mobile 6.0 and Windows Mobile 5.0 phones, see the Windows Mobile Center Web site.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync Devices.

Prerequisites

To perform the following procedures on a Windows Mobile phone, your users may need an ActiveSync connection between the phone and a desktop or portable computer. For Windows XP, use desktop ActiveSync to form this connection. For Windows Vista computers, use the Windows Mobile Center Web site. Your users must be able to copy the certificate file to the phone before they install the certificate. They can copy the certificate to the phone by using desktop ActiveSync or the Windows Mobile Center web site. Alternatively, your users can copy the certificate to a storage card and access the storage card from the mobile phone.

Use Internet Information Services Manager to save a certificate to a file

1. Right-click the **Default Web Site** or the **Microsoft-Server-ActiveSync** virtual directory, and then click **Properties**.
2. Click the **Directory Security** tab.
3. Under **Secure Communications**, click **View Certificate**.
4. In the **Certificate** dialog box, click the **Details** tab.
5. Click **Copy to File**.
6. In the **Certificate Export Wizard**, click **Next**.
7. Select **No, do not export the private key**, and then click **Next**.
8. Select **DER encoded binary X.509 (.CER)**, and then click **Next**.
9. Type a file name, click **Next**, and then click **Finish**.

After your users have saved their certificate to a file, they can install it on their phone. The procedure for installing the certificate on a phone will vary depending on the operating system of the phone. Choose the procedure that matches the operating system of the phone.

Use ActiveSync to install a certificate on a Windows Mobile 5.0 phone

1. With your user's phone connected to their computer, click **Tools**, and then click **Explore Smartphone**.
2. Drag the .cer file that was created in the previous procedure into a folder on the phone.
3. On the phone, click **Start**, and then click **File Explorer**.
4. Locate the folder that you selected in step 2.
5. Open the .cer file and, when you're prompted, select **Yes**.

Many Windows Mobile 5.0 phones implement a security policy that prevents the installation of certificate files directly from a .cer file. If the previous procedure fails, use the following procedure.

Use the SmartPhoneAddCert tool to install root certificates on a Windows Mobile 5.0 phone

1. Download the SmartPhoneAddcert.exe tool.

   Note:

   Some mobile service providers provide a signed version of this tool. If a signed version is available for the phone, download the signed version from the mobile service provider.

2. Run **SmartPhoneAddCert.exe** and extract the contents to a folder on your user's computer.
3. Copy SmartPhoneAddCert.exe to your user's phone through desktop ActiveSync or the Windows Mobile Center Web site.
4. On your user's phone, create a folder named **Storage**.
5. Copy the .cer file to the **Storage** folder on your user's phone.
6. Run SmartPhoneAddCdert.exe. Select the .cer file that you copied to the **Storage** folder and install the root certificate.

Note:

If you create a .cab file that includes the .cer file, you can also copy this .cab file to your user's phone and run the .cab file to install the certificate.

Use ActiveSync or the Windows Mobile Center Web site to install a certificate on a Windows Mobile 6.0 phone

1. With your user's phone connected to their computer, click **Tools**, and then click **Explore Smartphone**.
2. Drag the .cer file that was created in the previous procedure into a folder on the phone.

3. On the phone, click **Start**, and then click **File Explorer**.
4. Locate the folder that you selected in step 2.
5. Open the .cer file and, when you are prompted, select **Yes**.

Note:
You don't have to use ActiveSync or the Windows Mobile Center Web site to install the certificate on a Windows Mobile 6.0 phone. The certificate file can be copied to a storage card and installed directly from the storage card.

1.6.2.4.4.10 Configure Mobile Phones to Synchronize with Exchange Server

Configure Mobile Phones to Synchronize with Exchange Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure a mobile phone, such as a Windows Mobile phone, to use Microsoft Exchange ActiveSync. You should perform this procedure on each mobile phone in your organization.

Looking for other management tasks related to mobile phones? Check out Managing Exchange ActiveSync Devices.

Prerequisites

- You have reviewed the manufacturer's documentation for the mobile phone you want to configure.
- Exchange ActiveSync is enabled on the Microsoft Exchange Server 2010 Client Access server.

Configure a mobile phone to use Exchange ActiveSync

To perform these steps, you must be able to sign in to the user's account with their credentials on a mobile phone.

1. On the mobile phone, from the home screen, click **Start**, and then click **ActiveSync**.
2. Click **Menu**, and then click **Configure Server**.
3. Enter the server address. This is the same address as your Outlook Web App server address.
4. If you've configured ActiveSync to require Secure Sockets Layer (SSL), select the **This server requires an encrypted (SSL) connection** check box.
5. Click **Next**.
6. Enter your user name, password, and domain.
7. Select the **Save password** check box.
8. Click **Next**.
9. Select the check box next to each type of information you want to synchronize with the server, and then click **Finish**.

Windows Phone 7 synchronization

If you're configuring a Windows Phone 7 mobile phone to synchronize with an Exchange mailbox using Exchange ActiveSync, synchronization will fail under the following conditions:

- If the **AllowNonProvisionableDevices** property of the Exchange ActiveSync mailbox policy is set to False.
- If any policy properties that aren't included in the following list are configured for the Exchange ActiveSync mailbox policy:
  - PasswordRequired
  - MinPasswordLength
  - IdleTimeoutFrequencyValue
  - DeviceWipeThreshold
  - AllowSimplePassword
  - PasswordExpiration
  - PasswordHistory
  - DisableRemovableStorage
  - DisableIrDA
  - DisableDesktopSync
  - BlockRemoteDesktop
  - BlockInternetSharing

If you have Windows Phone 7 mobile phones in your organization, you can set the **AllowNonProvisionalDevices** property to True or you can create a separate Exchange ActiveSync mailbox policy for users who have Windows Phone 7 mobile phones. This new Exchange ActiveSync mailbox policy should either have the **AllowNonProvisionalDevices** property set to True or only have the preceding list of policy properties configured. For more information about Exchange ActiveSync mailbox policy properties and Windows Phone 7, see Understanding Exchange ActiveSync Mailbox Policies.

1.6.2.4.4.11 Manage a Mobile Device

Manage a Mobile Device

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After a user has synchronized a mobile phone with their mailbox, the Manage Mobile Device wizard lets you view and manage the mobile phones for that user.

Looking for other management tasks related to mobile phones? Check out Managing Exchange ActiveSync Devices.

Prerequisites

A user has synchronized a mobile phone with their mailbox.

What Do You Want to Do?

- Use the EMC to manage a mobile phone
- Use the Shell to manage a mobile phone

Use the EMC to manage a mobile phone

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync user settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. Select a mailbox and then, in the action pane, click **Manage Mobile Device** to open the **Manage Mobile Device** wizard.
   - This wizard helps you view mobile phones associated with a user's mailbox and remove a mobile phone from a user's mailbox. To remove a mobile phone from a user's mailbox, select the mobile phone, and then click **Remove Device**.
3. On the **Completion** page, confirm whether the mobile phone has been removed from the user's mailbox.
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
4. Click **Finish** to complete the Manage Mobile Device wizard.

Use the Shell to manage a mobile phone

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync user settings" entry in the Client Access Permissions topic.

This example removes a mobile phone from Tony Smith's mailbox.

```
Remove-ActiveSyncDevice -Identity iPhone_TonySmith
```

Other Tasks

In addition to using the Manage Mobile Device wizard, you may also want to Perform a Remote Wipe on a Mobile Phone.

For More Information

View a List of Devices for a User

Managing Exchange ActiveSync Devices

1.6.2.4.5 Managing Exchange ActiveSync with Policies

Managing Exchange ActiveSync with Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-12*

Create a New Exchange ActiveSync Mailbox Policy

Add Users to an Exchange ActiveSync Mailbox Policy

View or Configure Exchange ActiveSync Mailbox Policy Properties

1.6.2.4.5.1 Add Users to an Exchange ActiveSync Mailbox Policy

Add Users to an Exchange ActiveSync Mailbox Policy

Managing Client Access Servers > Managing Exchange ActiveSync > Managing Exchange ActiveSync with Policies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

After you create a Microsoft Exchange ActiveSync mailbox policy, you can add users to that policy. By default, users aren't assigned to an Exchange ActiveSync mailbox policy. You can add a user to only one Exchange ActiveSync mailbox policy at a time. If you add a user to an Exchange ActiveSync mailbox policy, and that user is a member of another Exchange ActiveSync mailbox policy, that user is removed from the original Exchange ActiveSync mailbox policy and added to the new Exchange ActiveSync mailbox policy. You can add users individually or add a filtered group of users to an Exchange ActiveSync mailbox policy.

Prerequisites

The Client Access server role has been installed on a Microsoft Exchange Server 2010 computer.

Use the EMC to add users to an Exchange ActiveSync mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync mailbox policy settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the work pane, right-click the user who you want to assign to a policy, and then click **Properties**.
3. In the user's **Properties** dialog box, click **Mailbox Features**.
4. Click **Exchange ActiveSync**, and then click **Properties**.
5. Select the **Apply an Exchange ActiveSync mailbox policy** check box.
6. Click **Browse** to view the **Select Exchange ActiveSync Mailbox Policy** dialog box.
7. Select an available policy, and then click **OK** three times to apply your changes.
   - **Note** You can add multiple users to a policy at the same time. However, that task must be accomplished by using the Exchange Management Shell.

Use the Shell to add users to an Exchange ActiveSync mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync mailbox policy settings" entry in the

Client Access Permissions topic.

This example adds a user with the username TonySmith to an Exchange ActiveSync mailbox policy named Sales.

```
Set-CASMailbox TonySmith -ActiveSyncMailboxPolicy(Get-ActiveSyncMailboxPolicy "Sa
```

This example adds all users to an Exchange ActiveSync mailbox policy named Corporate.

```
Get-Mailbox | Set-CASMailbox -ActiveSyncMailboxPolicy(Get-ActiveSyncMailboxPolicy
```

This example adds a filtered list of users to an Exchange ActiveSync mailbox policy named Contoso.

```
Get-Mailbox | where { $_.CustomAttribute1 -match "Manager"
 } | Set-CASMailbox -activesyncmailboxpolicy(Get-ActiveSyncMailboxPolicy "Contoso
```

Note:

You can substitute `CustomAttribute1` for any of the properties on the **Get-Mailbox** object. To view the full list, type: `Get-Mailbox username |fl`

For more information about syntax and parameters, see Set-CASMailbox.

1.6.2.4.5.2 View or Configure Exchange ActiveSync Mailbox Policy Properties

View or Configure Exchange ActiveSync Mailbox Policy Properties

Managing Client Access Servers > Managing Exchange ActiveSync > Managing Exchange ActiveSync with Policies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can create an Exchange ActiveSync mailbox policy to configure a variety of security options for users. In addition to password requirements and settings, you can use the **General** tab to specify the types of mobile phones that can connect to the Exchange server and whether attachments can be synchronized.

Looking for other management tasks related to Exchange ActiveSync mailbox policies? Check out Managing Exchange ActiveSync with Policies.

Important:

Windows Phone 7 mobile phones only support a subset of all Exchange ActiveSync mailbox policy settings. For more information, see Understanding Exchange ActiveSync Mailbox Policies.

What Do You Want To Do?

- Use the EMC to view or configure Exchange ActiveSync mailbox properties
- Use the Shell to view Exchange ActiveSync mailbox properties
- Use the Shell to configure Exchange ActiveSync Mailbox properties

Use the EMC to view or configure mailbox user properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync mailbox policy settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Client Access**.
2. In the result pane, click the **Exchange ActiveSync Mailbox Policies** tab, and then select the policy you want to view or configure.
3. In the action pane, click **Properties**.
4. Use the **General** tab to specify the types of mobile phones that can connect to the Exchange server and whether attachments can be synchronized.
   - **Allow non-provisionable devices** Select this check box to allow mobile phones that can't be provisioned automatically. These mobile phones may be unable to enforce all the Exchange ActiveSync policy settings. By selecting this box, you're allowing these mobile phones to synchronize even though some policy settings may not be applied.
   - **Refresh interval** Select this check box to force the server to resend the policy to clients at a fixed interval defined in the number of hours between policy refresh events.
5. Use the **Password** tab to set password requirements for Exchange ActiveSync clients.
   - **Require password** Select this checkbox to require a password for the mobile phone. If passwords are required, the following options become available.
   - **Require alphanumeric password** Select this check box to specify that the mobile phone password must include non-numeric characters. Requiring non-numeric characters in passwords increases the strength of password security.
   - **Minimum number of character sets** Use this text box to specify the complexity of the alphanumeric password and force users to use a number of different sets of characters from among the following: lower case letters, upper case letters, symbols and numbers.
   - **Enable password recovery** Select this check box to enable password recovery for the mobile phone. Users can use Outlook Web App to look up their recovery password and unlock their mobile phone. Administrators can use the EMC to look up a user's recovery password.
   - **Require encryption on device** Select this check box to require encryption on the mobile phone. This increases security by encrypting all information on the mobile phone.
   - **Require encryption on storage cards** Select this check box to require encryption on the mobile phone’s removable storage card. This increases security by encrypting all information on the storage cards for the mobile phone.
   - **Allow simple password** Select this check box to allow users to lock their mobile phones with simple passwords such as 1111 or 1234. If you clear this check box, users will be required to use more secure password sequences.
   - **Number of failed attempts allowed** Use this text box to limit the number of failed password attempts a mobile phone accepts before all information on the mobile phone is deleted and the mobile phone is automatically returned to the original factory settings. This reduces the chance of an unauthorized user accessing information on a lost or stolen mobile phone that has a password.
   - **Minimum password length** Use this text box to specify a minimum password length for the mobile phone password. Long passwords can provide increased security. However, long passwords can decrease mobile phone usability. A moderate password length of four to six characters is recommended.
   - **Time without user input before password must be re-entered (in minutes)** When a mobile phone password is required, you can use this

text box to prompt the user for the password after the mobile phone has been inactive for a specified period of time. For example, if this setting is set to 15 minutes, the user must enter the mobile phone password every time that the mobile phone is idle for 15 minutes. If the mobile phone is idle for 10 minutes, the user won't have to re-enter the password.

- **Password expiration (days)** Use this text box to force users to reset their mobile phone's password at a given interval. The interval is set in a number of days.
- **Enforce password history** Select this check box to force the mobile phone to prevent the user from re-using their previous passwords. The number you set determines how many past passwords the user won't be allowed to reuse.

6. Use the **Sync Settings** tab to specify a variety of synchronization-specific settings.
   - **Include past calendar items** Use this drop-down list to select the date range of calendar items to synchronize to the mobile phone. The available options include the following: **All**, **Two Weeks**, **One Month**, **Three Months**, and **Six Months**. If you have to specify other options, use the Shell to configure this setting.
   - **Include past e-mail items** Use this drop-down list to select the date range of e-mail items to synchronize to the mobile phone. The available options include the following: **All**, **One Day**, **Three Days**, **One Week**, **Two Weeks**, and **One Month**. If you have to specify other options, use the Shell to configure this setting.
   - **Limit e-mail size to (KB)** Select this check box to limit the message size that can be downloaded to the mobile phone. After you've selected the check box, use the text box to specify a maximum message size, in kilobytes (KB).
   - **Allow Direct Push when roaming** Select this check box to enable the mobile phone to synchronize as new items arrive when you're roaming with your phone. You're roaming when you're outside your normal service area. Check with your mobile service provider to determine your normal service area. Clearing this check box forces you to manually launch synchronization when you're roaming with the phone and data rates are traditionally higher.
   - **Allow HTML-formatted e-mail** Select this check box to enable e-mail messages that are formatted in HTML to be synchronized to the mobile phone. If this check box isn't selected, all e-mail messages will be converted to plain text before synchronization. Use of this check box doesn't affect whether or not messages are received on the mobile phone.
   - **Allow attachments to be downloaded to device** Select this check box to enable attachments to be downloaded to the mobile phone. If this check box is cleared, the name of the attachment is visible within the e-mail message but can't be downloaded to the mobile phone.
   - **Maximum attachment size (KB)** Select this check box to specify a maximum size for attachments that are downloaded to the mobile phone. After you select the check box, use the text box to enter a maximum attachment size, in KB. If this check box is selected, attachments that are larger than the specified size can't be downloaded to the device.

7. Use the **Device** tab to specify a variety of device-specific settings. All settings that you access on the **Device** tab of the Exchange ActiveSync policy **Properties** page are premium features of Exchange ActiveSync. For these features to be implemented on a mobile phone, the mailbox requires an Exchange Enterprise client access license (CAL).
   - **Allow removable storage** Select this check box to allow storage cards to be accessed from a mobile phone. If this check box isn't selected, storage cards can't be accessed from a mobile phone.
   - **Allow camera** Select this check box to allow the mobile phone camera to

be used.

- **Allow Wi-Fi** Select this check box to allow the mobile phone to use a Wi-Fi connection for Internet access. Direct Push isn't supported over Wi-Fi.
- **Allow infrared** Select this check box to allow the mobile phone to establish an infrared connection with other devices or computers.
- **Allow Internet sharing from device** Select this check box to allow another device to share the Internet connection of the mobile phone. Internet sharing is frequently used when the device functions as a modem for a laptop or desktop computer.
- **Allow remote desktop from device** Select this check box to allow the mobile phone to establish a remote desktop connection to another computer.
- **Allow desktop synchronization** Select this check box to allow the mobile phone to synchronize with a desktop computer through desktop ActiveSync or the Windows Mobile Device Center.
- **Allow Bluetooth** Use this drop-down list to control the Bluetooth functionality of the mobile phone. You can choose to **Allow**, **Disable**, or enable Bluetooth for **Handsfree only**.

8. Use the **Device Applications** tab to enable or disable specific features on a mobile phone. All settings that you access on the **Device Applications** tab of the Exchange ActiveSync policy Properties pages are premium features of Exchange ActiveSync. For these features to be implemented on a mobile phone, the mailbox requires an Exchange Enterprise client access license (CAL).
   - **Allow browser** Select this check box to allow mobile phones to use Pocket Internet Explorer.

     Note:
     This check box doesn't control access to third-party mobile phone browsers.

   - **Allow consumer mail** Select this check box to allow the mobile phone to access e-mail accounts other than Microsoft Exchange accounts. Consumer e-mail accounts include accounts that are accessed through POP3 and IMAP4.

     Note:
     This check box doesn't control access to third-party mobile phone e-mail applications.

   - **Allow unsigned applications** Select this check box to allow unsigned applications to be installed on the mobile phone.
   - **Allow unsigned installation packages** Select this check box to allow unsigned installation packages to be run on the mobile phone.
9. Use the **Other** tab to specify allowed and blocked applications. All settings that you access on the **Other** tab of the Exchange ActiveSync policy Properties pages are premium features of Exchange ActiveSync. For these features to be implemented on a mobile phone, the mailbox requires an Exchange Enterprise client access license (CAL).
   - **Allowed Applications** You can add applications to or remove them from the **Allowed Applications** list. Allowed applications can be installed and run on the mobile phone. Click **Add** to add an application, and click **Delete** to remove an application.
   - **Blocked Applications** You can add applications to or remove them from the **Blocked Applications** list. Blocked applications are prohibited from running on the mobile phone. Click **Add** to add an application, and click **Delete** to remove an application.

Use the Shell to view Exchange

ActiveSync mailbox policy settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync mailbox policy settings" entry in the Client Access Permissions topic.

This example returns all the settings for the Exchange ActiveSync mailbox policy named `Sales Policy`.

```
Get-ActiveSyncMailboxPolicy -Identity "SalesPolicy"
```

For more information about syntax and parameters, see Get-ActiveSyncMailboxPolicy.

Use the Shell to configure Exchange ActiveSync mailbox policy settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync mailbox policy settings" entry in the Client Access Permissions topic.

This example sets a variety of settings for the Exchange ActiveSync mailbox policy named `MyPolicy`. The settings that are configured include the following:

- Allowing non-provisionable devices
- Requiring an alphanumeric password
- Setting the device password to expire every 12 days
- Allowing password recovery
- Locking the device after 15 minutes of inactivity

```
Set-ActiveSyncMailboxPolicy -Identity MyPolicy -AllowNonProvisionableDevices $tru
```

For more information about syntax and parameters, see Set-ActiveSyncMailboxPolicy.

Other Tasks

After you configure Exchange ActiveSync mailbox policies, you may also want to Perform a Remote Wipe on a Mobile Phone.

1.6.2.4.5.3 Create a New Exchange ActiveSync Mailbox Policy

Create a New Exchange ActiveSync Mailbox Policy

Managing Client Access Servers > Managing Exchange ActiveSync > Managing Exchange ActiveSync with Policies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the New Exchange ActiveSync Mailbox Policy wizard to create a new Exchange ActiveSync mailbox policy. An Exchange ActiveSync mailbox policy contains a variety of settings, including password settings, attachment settings, and device settings.

Looking for other management tasks related to mobile phones? Check out Managing Exchange ActiveSync Devices.

Prerequisites

The Client Access server role has been installed on an Exchange Server 2010 computer.

What Do You Want to Do?

- Use the EMC to create an Exchange ActiveSync mailbox policy
- Use the shell to create an Exchange ActiveSync mailbox policy

Use the EMC to create an Exchange ActiveSync mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync mailbox policy settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Client Access**.
2. Select the **Exchange ActiveSync Mailbox Policies** tab and then, in the action pane, click **New Exchange ActiveSync Mailbox Policy**.
3. On the **New Exchange ActiveSync Mailbox Policy** page, enter a Mailbox policy name, and then choose from a variety of options including the following:
   - **Allow non-provisionable devices** Select this check box to allow mobile phones that can't be provisioned automatically. These mobile phones may be unable to enforce all the Exchange ActiveSync policy settings. By selecting this box, you are allowing these mobile phones to synchronize even though all policy settings may not be applied.
   - **Allow attachments to be downloaded to device** Select this option to allow attachments to be downloaded to the mobile phone. If selected, files that are attached to synchronized e-mail messages can be downloaded to the mobile phone. Users must select the attachment to mark it for download. After the attachment is selected, it's downloaded at the next scheduled synchronization for users who don't have Direct Push. For users who have Direct Push, the attachment is downloaded immediately.
   - **Require password** Select this option to require users to enter a password to access information on their mobile phones. If you select this option, you can also select a variety of other password options, including settings for password length, password time-out settings, and password recovery.
4. The **Completion** page will confirm whether your new Exchange ActiveSync mailbox policy was successfully created and will also display the syntax for the **New-ActiveSyncMailboxPolicy** cmdlet.

Use the Shell to create an Exchange ActiveSync mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync mailbox policy settings" entry in the Client Access Permissions topic.

This example creates a new Exchange ActiveSync mailbox policy that requires a password of four characters, encryption, and also a new password every 30 days.

```
New-ActiveSyncMailboxPolicy -Name 'All Users' -AllowNonProvisionableDevices $fals
```

Other Tasks

In addition to using the New Exchange ActiveSync Policy wizard, you may also want toPerform a Remote Wipe on a Mobile Phone.

For More Information

View a List of Devices for a User

Managing Exchange ActiveSync Devices

1.6.2.5 Managing POP3 and IMAP4

Managing POP3 and IMAP4

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-04*

Start and Stop the POP3 Service

Start and Stop the IMAP4 Service

Enabling POP3 and IMAP4 on a Client Access Server

Enable or Disable POP3 Access for a User

Enable or Disable IMAP4 Access for a User

View or Configure POP3 Properties

View or Configure IMAP4 Properties

Configure Calendar Options for POP3

Enable POP3 and IMAP4 Users to Use Default Protocol Settings

Configure Calendar Options for POP3

Configure Calendar Options for IMAP4

Configure POP3 and IMAP4 Message Retrieval Format Options

Set Connection Time-Out Limits for POP3

Set Connection Time-Out Limits for IMAP4

Configure IP Addresses and Ports for POP3 and IMAP4 Access

Set Connection Limits for POP3

Set Connection Limits for IMAP4

Configure Protocol Logging for POP3 and IMAP4

Allow POP3, IMAP4, and SMTP Server Settings to be Viewed By End Users in Outlook Web App

1.6.2.5.1 Start and Stop the POP3 Service

Start and Stop the POP3 Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

By default, POP3 is disabled in Microsoft Exchange Server 2010. After you enable POP3, Exchange 2010 accepts unsecured POP3 client communications on port 110 and over Port 995 using Secure Sockets Layer (SSL).

You can start and stop the POP3 service by using either Microsoft Management Console or net start on the Exchange 2010 Client Access server. You can also check to verify whether the service is running on the Client Access server.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use Microsoft Management Console to start or stop the POP3 service

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**.
   - To start the service, in the results pane, right-click **Microsoft Exchange POP3**, and then click **Start**.
   - To stop the service, in the results pane, right-click **Microsoft Exchange POP3**, and then click **Stop**.

Use net start to start or stop the POP3 service

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. On the Exchange server that has the Client Access server role installed, open a Command Prompt window.
   - To start the service, at the command prompt, type **net start MSExchangePOP3**, and then press **Enter**.
   - To stop the service, at the command prompt, type **net stop MSExchangePOP3**, and then press **Enter**.
2. Close the Command Prompt window.

Verify that the POP3 service is running

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. On the Exchange Client Access server, open a Command Prompt window.
2. At the command prompt, type **telnet localhost 110**, and then press **ENTER**. POP3 is working correctly if Telnet returns "+OK Microsoft Exchange POP3 server ready".
3. Close Telnet, and then close the Command Prompt window.

Other Tasks

After you start and stop the POP3 service, you may also want to:

- Set Connection Limits for POP3
- Set Connection Time-Out Limits for POP3

1.6.2.5.2 Start and Stop the IMAP4 Service

Start and Stop the IMAP4 Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

By default, IMAP4 is disabled in Microsoft Exchange Server 2010. After you enable IMAP4, Exchange 2010 accepts unsecured IMAP4 client communications on port 143 and over port 993 using Secure Sockets Layer (SSL).

You can start and stop the IMAP4 service by using either Microsoft Management Console or net start on the Exchange 2010 Client Access server. You can also check to verify whether the service is running on the Client Access server.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use Microsoft Management Console to start or stop the IMAP4 service

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**.
   - To start the Microsoft Exchange IMAP4 service, in the results pane, right-click **Microsoft Exchange IMAP4**, and then click **Start**.
   - To stop the Microsoft Exchange IMAP4 service, in the results pane, right-click **Microsoft Exchange IMAP4**, and then click **Stop**.

Use net start to start or stop the IMAP4 service

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. On the Exchange server that has the Client Access server role installed, open

a Command Prompt window.
- To start the service, at the command prompt, type **net start MSExchangeIMAP4**, and then press **ENTER**.
- To stop the service, at the command prompt, type **net stop MSExchangeIMAP4**, and then press **ENTER**.

2. Close the Command Prompt window.

Verify that the IMAP4 service is running

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. On the Exchange Client Access server, open a Command Prompt window.
2. At the command prompt, type **telnet localhost 143**, and then press **ENTER**. IMAP4 is working correctly if Telnet returns "+OK Microsoft Exchange IMAP4 server ready."
3. Close Telnet, and then close the Command Prompt window.

Other Tasks

After you start and stop the IMAP4 service, you may also want to:

- Set Connection Time-Out Limits for IMAP4
- Set Connection Limits for IMAP4

1.6.2.5.3 Enabling POP3 and IMAP4 on a Client Access Server

Enabling POP3 and IMAP4 on a Client Access Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-06*

Enable POP3 in Exchange 2010

Enable IMAP4 in Exchange 2010

1.6.2.5.3.1 Enable POP3 in Exchange 2010

Enable POP3 in Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you install Microsoft Exchange Server 2010, the POP3 service isn't started. You can set it to start automatically by using the Services snap-in in Microsoft Management Console (MMC) or by using the Shell.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use Microsoft Management Console to enable POP3

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the **Services** snap-in, in the console tree, click **Services (Local)**.
2. In the result pane, right-click **Microsoft Exchange POP3**, and then click **Properties**.
3. On the **General** tab, under **Startup type**, select **Automatic**, and then click **Apply**.
4. Under **Service status**, click **Start**, and then click **OK**.

Use the Shell to enable POP3

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example enables POP3 on the local Client Access server.

1. Run this command to configure the POP3 service to start automatically.

```
Set-service msExchangePOP3 -startuptype automatic
```

2. Run this command to start the POP3 service.

```
Start-service -service msExchangePOP3
```

Other Tasks

After you enable POP3, you may also want to:

- Enable or Disable POP3 Access for a User
- Set Connection Limits for POP3
- Allow POP3, IMAP4, and SMTP Server Settings to be Viewed By End Users in Outlook Web App

1.6.2.5.3.2 Enable IMAP4 in Exchange 2010

Enable IMAP4 in Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you install Microsoft Exchange Server 2010, the IMAP4 service isn't started. You can set it to start automatically by using the Services snap-in in Microsoft Management Console (MMC) or by using the Shell.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use Microsoft Management Console to enable IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the **Services** snap-in, in the console tree, click **Services (Local)**.
2. In the result pane, right-click **Microsoft Exchange IMAP4**, and then click **Properties**.
3. On the **General** tab, under **Startup type**, select **Automatic**, and then click **Apply**.
4. Under **Service status**, click **Start**, and then click **OK**.

Use the Shell to enable IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example enables IMAP4 on the local Client Access server.

1. This command configures the IMAP4 service to start automatically.

```
Set-service msExchangeIMAP4 -startuptype automatic
```

2. This command starts the IMAP4 service.

```
Start-service msExchangeIMAP4
```

Other Tasks

After you enable IMAP4, you may also want to:

- Enable or Disable IMAP4 Access for a User
- Set Connection Limits for IMAP4
- Allow POP3, IMAP4, and SMTP Server Settings to be Viewed By End Users in Outlook Web App

1.6.2.5.4 Enable or Disable POP3 Access for a User

Enable or Disable POP3 Access for a User

Client Access > Managing Client Access Servers > Managing POP3 and IMAP4 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable POP3 for a user.

Note:

After you've enabled or disabled POP3 for a user, you must restart the Microsoft Exchange POP3 service. For more information about how to restart the POP3 service, see Start and Stop the IMAP4 Service.

Looking for other management tasks related to managing user mailboxes? Check out

Managing User Mailboxes.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to enable or disable POP3 for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient provisioning permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the user for whom you want to enable or disable POP3.
3. In the action pane, under the name of the user, click **Properties**.
4. In **<User> Properties**, on the **Mailbox Features** tab, click **POP3**, and then click either **Enable** or **Disable**.
5. Click **OK**.

Use the Shell to enable or disable POP3 for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient provisioning permissions" section in the Mailbox Permissions topic.

This example enables POP3 for the user John Smith.

```
Set-CASMailbox -Identity "John Smith" -POPEnabled $true
```

This example disables POP3 for the user John Smith.

```
Set-CASMailbox -Identity "John Smith" -POPEnabled $false
```

For detailed information about syntax and parameters, see Set-CASMailbox.

Other Tasks

After you enable or disable POP3 for a user, you may also want to:

- Enable POP3 in Exchange 2010
- Configure Authentication for POP3

1.6.2.5.5 Enable or Disable IMAP4 Access for a User

Enable or Disable IMAP4 Access for a User

Client Access > Managing Client Access Servers > Managing POP3 and IMAP4 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable IMAP4 for a user.

Note:
After you've enabled or disabled IMAP4 for a user, you must restart the Microsoft Exchange IMAP4 service. For more information about how to restart the IMAP4 service, see Start and Stop the IMAP4 Service.

Looking for other management tasks related to managing user mailboxes? Check out Managing User Mailboxes.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to enable or disable IMAP4 for a user mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient provisioning permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the user for which you want to enable or disable IMAP4.
3. In the action pane, under the name of the user, click **Properties**.
4. In **<User> Properties**, on the **Mailbox Features** tab, click **IMAP4**, and then click either **Enable** or **Disable**.
5. Click **OK**.

Use the Shell to enable or disable IMAP4 for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient provisioning permissions" section in the Mailbox Permissions topic.

This example enables IMAP4 for the user John Smith.

```
Set-CASMailbox -Identity "John Smith" -IMAPEnabled $true
```

This example disables IMAP4 for the user John Smith.

```
Set-CASMailbox -Identity "John Smith" -IMAPEnabled $false
```

For detailed information about syntax and parameters, see Set-CASMailbox.

Other Tasks

After you enable or disable IMAP4 for a user, you may also want to:

- Enable IMAP4 in Exchange 2010
- Configure Authentication for IMAP4

View or Configure POP3 Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can view or configure the settings that apply to your POP3 users. You can specify the message you want POP3 users to see when they sign in, set connection limits, and make sure that the POP3 service is retrieving messages using the settings you have chosen.

Note:
After you change any settings for the POP3 service by using either the EMC or the Shell, you must restart the POP3 service.

Looking for other management tasks related to POP3? Check out Managing POP3 and IMAP4.

What Do You Want to Do?

- Use the EMC to view or configure POP3 properties
- Use the Shell to configure POP3 properties
- Use the Shell to view POP3 properties

Use the EMC to view or configure POP3 properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access** > **POP3 and IMAP4**.
2. In the work pane, select **POP3**, and then, in the action pane, under **POP3**, click **Properties**.
3. On the **General** tab, in the **Banner string** box, specify a banner string for your POP3 clients to see when they log on to their Exchange mailbox. The default banner string for POP3 is "The Microsoft Exchange POP3 service is ready."

   Note:
   After you change a banner string for the POP3 service, you must restart the POP3 service.

4. On the **Binding** tab, specify the IP addresses and TCP ports on the Receive connector that accepts connections from POP3 clients. You can also configure the IP address ranges from which the Receive connector accepts connections from POP3 clients.

   Note:
   If Microsoft Exchange Server 2010 is deployed on a computer running the Windows Server 2008 operating system, enter IP addresses and IP address ranges in the Internet Protocol Version 4 (IPv4) format, Internet Protocol Version 6 (IPv6) format, or both formats. A default installation of Windows Server 2008 enables support for IPv4 and IPv6.

Specify the following:

- **TLS or Unencrypted Connections** In this section, specify the IP addresses and port numbers for POP3 connections that use Transport Layer Security (TLS) or unencrypted connections. For each entry, you must specify a different set of IP addresses or specify all available IP addresses. To add a new IP address or port number, click **Add**. To edit an existing IP address, select the IP address, and then click **Edit**. To remove an existing IP address, select the IP address, and then click  .

  The following options are available in the **TLS or Unencrypted Connection Settings** dialog box:

  Use all IP addresses available on this server Select this option to use all IP addresses associated with this computer.

  Specify an IP address Select this option if the following conditions are true:

  * More than one IP address is associated with the computer.
  * You want to bind the Receive connector to a specific IP address.

  Then, in the text box, type the IP address on which this server accepts connections.

  Note:
  You must specify a local IP address that's valid for the Client Access server that's providing POP3 access.

  Port This text box identifies the TCP port number on which this Receive connector listens for incoming mail. TCP port 110 is the default port used for POP3.

  Note:
  After you configure IP addresses and ports for the Receive connector to accept connections from POP3 clients, you must restart the POP3 service.

- **Secure Sockets Layer (SSL) Connections** Using this list, specify the IP address or IP address range for POP3 connections that use SSL. For each entry, you must specify a different set of IP addresses or specify all available IP addresses. To add a new IP address or port number, click **Add**. To edit an existing IP address, select the IP address, and then click **Edit**. To remove an existing IP address, select the IP address, and then click  .

  The following options are available in the **SSL Connection Settings** dialog box:

  Use all IP addresses available on this server Select this option to use all IP addresses associated with this computer.

  Specify an IP address Select this option if the following conditions are true:

  * More than one IP address is associated with the computer.
  * You want to bind the Receive connector to a specific IP address.

  Then, in the text box, type the IP address on which this server accepts connections.

  Note:
  You must specify a local IP address that's valid for the Client Access server that's providing POP3 access.

  Port This text box identifies the TCP port number on which this Receive connector listens for incoming mail. SSL port 995 is the default port used for POP3.

  Note:
  After you configure IP addresses and ports for the Receive connector to accept connections from POP3 clients, you must restart the POP3 service.

5. On the **Authentication** tab, specify the method by which your POP3 users will log on.
   - **Plain text logon (Basic authentication)** Select this option if you want to send user names and passwords in clear text. Using this option enables user names and passwords to be sent to the server without a TLS or SSL connection.
   - **Plain text authentication logon (Integrated Windows authentication)** Select this option if you want to use Integrated Windows authentication without a TLS or SSL connection.
   - **Secure logon** Select this option if you want to require a TLS or SSL connection.
   - **X.509 certificate name** Use this text box to specify the X.509 certificate name to use for a TLS or SSL session.

   Note:
   After you configure the authentication settings, you must restart the POP3 service.

6. On the **Connection** tab, configure the time-out settings, connection limit settings, and the proxy target port for POP3.
   - **Time-out Settings** Configure the following settings:
     Authenticated time-out (seconds) In this text box, specify the amount of time to wait before closing idle authenticated connections. The default setting is 1800 seconds, and the valid input range is 30 to 86400 seconds.
     Unauthenticated time-out (seconds) In this text box, specify the amount of time to wait before closing idle unauthenticated connections. The default setting is 60 seconds, and the valid input range is 30 to 3600 seconds.
   - **Connection Limits** Configure the following settings:
     Maximum connections In this text box, specify the total number of connections the Client Access server will accept. This includes authenticated and unauthenticated connections. The default value is 2000, and the valid input range is 1 to 25000.
     Maximum connections from a single IP address In this text box, specify the number of connections that the Client Access server will accept from a single IP address. The default value is 2000, and the valid input range is 1 to 25000.
     Maximum connections from a single user In this text box, specify the maximum number of connections the Client Access server will accept from a particular user. The default value is 16, and the valid input range is 1 to 25000.
     Maximum command size In this text box, specify the maximum size of a single command. The default value is 45 bytes, and the valid input range is 40 to 1024.
   - **Command Relay** In the **Proxy target port** text box, specify the port on the Microsoft Exchange Server 2003 back-end server for which POP3 will relay commands. The default port is 110. The valid input range is from 0 through 65535. Using a value of 0 will disable proxying commands to the Exchange 2003 back-end server.

   Note:
   After you configure connection settings for the POP3 service, you must restart the POP3 service.

7. On the **Retrieval Settings** tab, specify the message and calendar retrieval settings for your POP3 clients:
   - **Message Retrieval** Configure the following settings:
     Message MIME format Using this drop-down list, specify the

format of the messages retrieved by the Client Access server. You can select from one of the following message format options:
* Text
* HTML
* HTML and alternative text
* Enriched text
* Enriched text and alternative text
* Best body format
* TNEF

Message sort order Using this drop-down list, select the message sort order. You can select **Ascending** or **Descending**.

- **Calendar Retrieval** Configure the following settings:

  iCalendar Configure this setting so users can use the iCalendar standard for calendar items. The iCalendar standard is a standard for exchanging calendar information.
  Intranet URL Specify an internal URL for users to use to access their calendar information.
  Internet URL Specify an external URL for users to use to access their calendar information.
  Custom Specify the URL of the Outlook Web App server for users to use to access their calendar information.
  URL of Outlook Web App server Specify the Outlook Web App server for custom Outlook Web App calendar items. If you've selected the custom setting for Calendar retrieval, you must specify the Outlook Web App server URL.

Note:
After you configure the message retrieval settings for the POP3 service, you must restart the POP3 service.

Use the Shell to configure POP3 properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 settings" entry in the Client Access Permissions topic.

This example sets the IP address for communication over a TLS-encrypted connection or a connection that isn't encrypted on a Client Access server named CAS01.

```
Set-PopSettings -Server "CAS01" -UnencryptedOrTLSBindings IPaddress:953
```

For syntax and parameter information, see Set-PopSettings.

Use the Shell to view POP3 properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 settings" entry in the Client Access Permissions topic.

This example returns the POP3 settings for the server CAS01.

```
Get-POPSettings -Server CAS01
```

For syntax and parameter information, see Get-POPSettings.

For More Information

Managing POP3 and IMAP4

Start and Stop the POP3 Service

Configure IP Addresses and Ports for POP3 and IMAP4 Access

Managing POP3 and IMAP4 Security

Configuring TLS and SSL for POP3 and IMAP4 Access

Set Connection Time-Out Limits for POP3

Configure Calendar Options for POP3

1.6.2.5.7 View or Configure IMAP4 Properties

View or Configure IMAP4 Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can view or configure the settings that apply to your IMAP4 users. You can specify the message you want IMAP4 users to see when they sign in, set connection limits, and make sure that the IMAP4 service is retrieving messages using the settings you have chosen.

Note:

After you change any settings for the IMAP4 service by using either the EMC or the Shell, you must restart the IMAP4 service.

Looking for other management tasks related to IMAP4? Check out Managing POP3 and IMAP4.

What Do You Want to Do?

- Use the EMC to view or configure IMAP4 properties
- Use the Shell to configure IMAP4 properties
- Use the Shell to view IMAP4 properties

Use the EMC to view or configure IMAP4 properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "IMAP4 settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access** > **POP3 and IMAP4**.
2. In the work pane, select **IMAP4**, and then, in the action pane, under **IMAP4**, click **Properties**. The **IMAP Properties** page will open.
3. On the **General** tab, in the **Banner string** box, specify a banner string for

your IMAP4 clients to see when they log on to their Exchange mailbox. The default banner string for IMAP4 is "The Microsoft Exchange IMAP4 service is ready."

Note:
After you change a banner string for the IMAP4 service, you must restart the IMAP4 service.

4. On the **Binding** tab, specify the IP addresses and TCP ports on the Receive connector that accepts connections from IMAP4 clients. You can also configure the IP address ranges from which the Receive connector accepts connections from IMAP4 clients.

Note:
If Microsoft Exchange Server 2010 is deployed on a computer running the Windows Server 2008 operating system, enter IP addresses and IP address ranges in the Internet Protocol Version 4 (IPv4) format, Internet Protocol Version 6 (IPv6) format, or both formats. A default installation of Windows Server 2008 enables support for IPv4 and IPv6.

Specify the following:

- **TLS or Unencrypted Connections** In this section, specify the IP addresses and port numbers for IMAP4 connections that use Transport Layer Security (TLS) or unencrypted connections. For each entry, you must specify a different set of IP addresses or specify all available IP addresses. To add a new IP address or port number, click **Add**. To edit an existing IP address, select the IP address, and then click **Edit**. To remove an existing IP address, select the IP address, and then click  .

  The following options are available in the **TLS or Unencrypted Connection Settings** dialog box:

  Use all IP addresses available on this server Select this option to use all IP addresses associated with this computer.

  Specify an IP address Select this option if the following conditions are true:

  * More than one IP address is associated with the computer.
  * You want to bind the Receive connector to a specific IP address.

  Then, in the text box, type the IP address on which this server accepts connections.

  Note:
  You must specify a local IP address that's valid for the Client Access server that's providing IMAP4 access.

  Port This text box identifies the TCP port number on which this Receive connector listens for incoming mail. TCP port 143 is the default port used for IMAP4.

  Note:
  After you configure IP addresses and ports for the Receive connector to accept connections from IMAP4 clients, you must restart the IMAP4 service.

- **Secure Sockets Layer (SSL) Connections** Using this list, specify the IP address or IP address range for IMAP4 connections that use SSL. For each entry, you must specify a different set of IP addresses or specify all available IP addresses. To add a new IP address or port number, click **Add**. To edit an existing IP address, select the IP address, and then click **Edit**. To remove an existing IP address, select the IP address, and then click  .

  The following options are available in the **SSL Connection Settings** dialog box:

  Use all IP addresses available on this server Select this option to use all IP addresses associated with this computer.

Specify an IP address Select this option if the following conditions are true:
* More than one IP address is associated with the computer.
* You want to bind the Receive connector to a specific IP address.
Then, in the text box, type the IP address on which this server accepts connections.

Note:
You must specify a local IP address that's valid for the Client Access server that's providing IMAP4 access.

Port This text box identifies the TCP port number on which this Receive connector listens for incoming mail. SSL port 993 is the default port used for IMAP4.

Note:
After you configure IP addresses and ports for the Receive connector to accept connections from IMAP4 clients, you must restart the IMAP4 service.

5. On the **Authentication** tab, specify the method by which your IMAP4 users will log on.
   - **Plain text logon (Basic authentication)** Select this option if you want to send user names and passwords in clear text. Using this option enables user names and passwords to be sent to the server without a TLS or SSL connection.
   - **Plain text authentication logon (Integrated Windows authentication)** Select this option if you want to use Integrated Windows authentication without a TLS or SSL connection.
   - **Secure logon** Select this option if you want to require a TLS or SSL connection.
   - **X.509 certificate name** Use this text box to specify the X.509 certificate name to use for a TLS or SSL session.

     Note:
     After you configure the authentication settings, you must restart the IMAP4 service.

6. On the **Connection** tab, configure the time-out settings, connection limit settings, and the proxy target port for IMAP4.
   - **Time-out Settings** Configure the following settings:
     Authenticated time-out (seconds) In this text box, specify the amount of time to wait before closing idle authenticated connections. The default setting is 1800 seconds, and the valid input range is 30 to 86400 seconds.
     Unauthenticated time-out (seconds) In this text box, specify the amount of time to wait before closing idle unauthenticated connections. The default setting is 60 seconds, and the valid input range is 30 to 3600 seconds.
   - **Connection Limits** Configure the following settings:
     Maximum connections In this text box, specify the total number of connections the Client Access server will accept. This includes authenticated and unauthenticated connections. The default value is 2000, and the valid input range is 1 to 25000.
     Maximum connections from a single IP address In this text box, specify the number of connections the Client Access server will accept from a single IP address. The default value is 2000, and the valid input range is 1 to 25000.
     Maximum connections from a single user In this text box, specify the maximum number of connections the Client Access

server will accept from a particular user. The default value is 16, and the valid input range is 1 to 25000.
Maximum command size In this text box, specify the maximum size of a single command. The default value is 10240 bytes, and the valid input range is 1024 to 16384.

- **Command Relay** In the **Proxy target port** text box, specify the port on the Microsoft Exchange Server 2003 back-end server for which IMAP4 will relay commands. The default port is 143. The valid input range is from 0 through 65535. Using a value of 0 will disable proxying commands to the Exchange 2003 back-end server.

Note:
After you configure connection settings for the IMAP4 service, you must restart the IMAP4 service.

7. On the **Retrieval Settings** tab, specify the message and calendar retrieval settings for your IMAP4 clients.
   - **Message Retrieval** Configure the following settings:
     Message MIME format Using this drop-down list, specify the format of the messages retrieved by the Client Access server. You can select from one of the following message format options:
     * Text
     * HTML
     * HTML and alternative text
     * Enriched text
     * Enriched text and alternative text
     * Best body format
     * TNEF
   - **Calendar Retrieval** Configure the following settings:
     iCalendar Configure this setting so users can use the iCalendar standard for calendar items. The iCalendar standard is a standard for exchanging calendar information.
     Intranet URL Specify an internal URL for users to use to access their calendar information.
     Internet URL Specify an external URL for users to use to access their calendar information.
     Custom Specify the URL of the Outlook Web App server for users to use to access their calendar information.
     URL of Outlook Web App server Specify the Outlook Web App server for custom Outlook Web App calendar items. If you've selected the custom setting for Calendar retrieval, you must specify the Outlook Web App server URL.

Note:
After you configure the message retrieval settings for the IMAP4 service, you must restart the IMAP4 service.

Use the Shell to configure IMAP4 properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "IMAP4 settings" entry in the Client Access Permissions topic.

This example sets the IP address for communication over a TLS-encrypted connection or a connection that isn't encrypted on a Client Access server named CAS01.

```
Set-ImapSettings -Server "CAS01" -UnencryptedOrTLSBindings IPaddress:953
```

For syntax and parameter information, see Set-ImapSettings.

Use the Shell to view IMAP4 properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "IMAP4 settings" entry in the Client Access Permissions topic.

This example returns the IMAP4 settings for the server CAS01.

```
Get-IMAPSettings -Server CAS01
```

For syntax and parameter information, see Get-IMAPSettings.

For More Information

Managing POP3 and IMAP4

Start and Stop the IMAP4 Service

Configure IP Addresses and Ports for POP3 and IMAP4 Access

Managing POP3 and IMAP4 Security

Configuring TLS and SSL for POP3 and IMAP4 Access

Set Connection Time-Out Limits for IMAP4

Configure Calendar Options for IMAP4

1.6.2.5.8 Enable POP3 and IMAP4 Users to Use Default Protocol Settings

Enable POP3 and IMAP4 Users to Use Default Protocol Settings

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable POP3 and IMAP4 users to use the default protocol settings on the Microsoft Exchange Server 2010 Client Access server that has the IMAP4 service or POP3 service enabled.

Using the Exchange Management Shell to Enable POP3 and IMAP4 Users to Use the Default Protocol Settings

In addition to using the **Set-PopSettings** or **Set-ImapSettings** cmdlets to manage POP3 and IMAP4 settings for all your users, you can also use the **Set-CASMailbox** cmdlet to specify individual POP3 and IMAP4 settings for your users. You can also use the **Set-CASMailbox** cmdlet to enable a user to use the default protocol settings for a server when you use the **Set-PopSettings** or **Set-ImapSettings** cmdlets.

The following table shows the parameters to use to configure a POP3 or IMAP4 user to use the protocol default settings as specified on the Client Access server.

POP3 and IMAP4 parameters for the Set-CASMailbox cmdlet

Parameter	Value	Description
PoPopUseProtocolDefaults	• $true • $false	This parameter lets you use the default protocol settings as specified by the **Set-PopSettings** cmdlet.
ImImapUseProtocolDefaults	• $true • $false	This parameter lets you use the default protocol settings as specified by the **Set-ImapSettings** cmdlet.

For more information about the **Set-CASMailbox** cmdlet, see Set-CASMailbox.

Looking for other management tasks related to setting up POP 3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the Shell to enable a POP3 user to use the default protocol settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example enables a POP3 user to use the default protocol settings for the server CAS01:

```
Set-CASMailbox -Identity CAS01 -PopProtocolDefaults $true
```

This example disables the default protocol settings for a POP3 user on the server CAS01:

```
Set-CASMailbox -Identity CAS01 -PopProtocolDefaults $false
```

Use the Shell to configure an IMAP4 user to use the default protocol settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example enables an IMAP4 user to use the default protocol settings for the server CAS01.

```
Set-CASMailbox -Identity CAS01 -ImapProtocolDefaults $true
```

This example disables the default protocol settings for an IMAP4 user on the server CAS01.

```
Set-CASMailbox -Identity CAS01 -ImapProtocolDefaults $false
```

For more information about syntax and parameters, see Set-CASMailbox.

Other Tasks

After you enable POP3 and IMAP4 users to use the default protocol settings, you may also want to:

- Configure IP Addresses and Ports for POP3 and IMAP4 Access
- Enable IMAP4 in Exchange 2010
- Enable POP3 in Exchange 2010

1.6.2.5.9 Configure Calendar Options for POP3

Configure Calendar Options for POP3

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to set the calendaring options that are available on the Microsoft Exchange Server 2010 server that has the POP3 service enabled.

The following table describes the `CalendarItemRetrievalOption` parameter for your POP3 users.

POP3 calendar options for Exchange 2010

Setting	Value	Description
iCalendar	0	This setting lets users use the iCalendar standard for calendar items. The iCalendar standard is a standard for exchanging calendar information.
IntranetUrl	1	This setting lets you specify an internal URL for users to use to access their calendar information.
InternetUrl	2	This setting lets you specify an external URL for users to use to access their calendar information.
Custom	3	This setting lets you specify an Outlook Web App server for users to use to access their calendar information.

Note:

After you've specified the calendar options for POP3, you must restart the POP3 service. For information about how to restart the POP3 service, see Start and Stop the POP3 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out

Managing POP3 and IMAP4.

Use the EMC to set the calendar options for POP3

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. In the action pane, under **POP3**, click **Properties**.
4. On the **POP3 Properties** page, click the **Retrieval Settings** tab.
5. Under **Calendar Retrieval**, select one of the following options:
   - iCalendar
   - Intranet URL
   - Internet URL
   - Custom
6. To apply the calendar retrieval option that you selected, click **Apply**, and then click **OK**.

Use the Shell to set the calendar options for POP3

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example enables POP3 to use iCalendar.

```
Set-PopSettings -Identity CAS01 -CalendarItemRetrievalOption 0
```

This example enables POP3 users to access internal calendar information from an internal server.

```
Set-PopSettings -Identity CAS01 -CalendarItemRetrievalOption 1 -IntranetUrl "Serv
```

This example enables POP3 users to access calendar information from the Internet on an external server.

```
Set-PopSettings -CalendarItemRetrievalOption 2 InternetUrl "https://Server01"
```

This example enables POP3 users to access calendar information by using Outlook Web App.

```
Set-PopSettings -CalendarItemRetrievalOption 3 -OwaServerUrl "https://OwaServer01
```

For more information about syntax and parameters, see Set-PopSettings.

Other Tasks

After you set the calendar options for POP3, you may also want to:

- Configure POP3 and IMAP4 Message Retrieval Format Options
- Set Connection Time-Out Limits for POP3

Configure Calendar Options for IMAP4

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to set the calendaring options that are available on the Microsoft Exchange Server 2010 server that has the IMAP4 service enabled.

These settings allow you to set different calendar options for your organization when you're using IMAP4 as the e-mail protocol for your users. You can use the `CalendarItemRetrievalOption` parameter for the Set-ImapSettings cmdlet in the Shell to set different calendar options.

The following table describes the `CalendarItemRetrievalOption` parameter for IMAP4 users.

IMAP4 calendar options for Exchange 2010

Setting	Value	Description
iCalendar	0	This setting lets users use the iCalendar standard for calendar items. The iCalendar standard is a standard for exchanging calendar information.
IntranetUrl	1	This setting lets you specify an internal URL for users to access their calendar information.
InternetUrl	2	This setting lets you specify an external URL for users to access their calendar information.
Custom	3	This setting lets you specify an Outlook Web App server for users to access their calendar information.

Note:

After you've specified the calendar options for IMAP4, you must restart the IMAP4 service. For information about how to restart the IMAP4 service, see Start and Stop the IMAP4 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to set the calendar options for IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions

topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. In the action pane, under **IMAP4**, click **Properties**.
4. On the **IMAP4 Properties** page, click the **Retrieval Settings** tab.
5. Under **Calendar Retrieval**, select one of the following options:
   - iCalendar
   - Intranet URL
   - Internet URL
   - Custom
6. To apply the calendar retrieval option that you selected, click **Apply**, and then click **OK**.

Use the Shell to set the calendar options for IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example enables IMAP4 to use iCalendar.

```
Set-ImapSettings -Identity CAS01 -CalendarItemRetrievalOption 0
```

This example enables IMAP4 users to access internal calendar information from an internal server.

```
Set-ImapSettings -Identity CAS01 -CalendarItemRetrievalOption 1 -IntranetUrl "Ser
```

This example enables IMAP4 users to access calendar information from the Internet on an external server.

```
Set-ImapSettings -CalendarItemRetrievalOption 2 InternetUrl "https://Server01"
```

This example enables IMAP4 users to access calendar information by using Outlook Web App.

```
Set-ImapSettings -CalendarItemRetrievalOption 3 -OwaServerUrl "https://OwaServer0
```

For more information about syntax and parameters, see Set-ImapSettings.

Other Tasks

After you set the calendar options for IMAP4, you may also want to:

- Configure POP3 and IMAP4 Message Retrieval Format Options
- Set Connection Time-Out Limits for IMAP4

1.6.2.5.11 Configure POP3 and IMAP4 Message Retrieval Format Options

Configure POP3 and IMAP4 Message Retrieval Format Options

Client Access > Managing Client Access Servers > Managing POP3 and IMAP4 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can manage message retrieval format options for users on a Microsoft Exchange Server 2010 Client Access server that has the POP3 service or the IMAP4 service enabled.

You can use the EMC or the Shell to manage the message retrieval options for IMAP4 and POP3 access for an individual user's mailbox. The following table describes the format options available for POP3 and IMAP4 users.

Note:

After you've specified message retrieval format options for POP3 or IMAP4, you must restart whichever service you're using: POP3 or IMAP4. For more information about how to restart the POP3 and IMAP4 services, see Start and Stop the POP3 Service and Start and Stop the IMAP4 Service.

Message retrieval format options for POP3 and IMAP4

Setting	Value	Description
PopMessagesRetrievalMimeFormat	• 0:Text Only • 1:HTML Only • 2:HTML and Alternative Text • 3:Enriched Text Only • 4:Enriched Text and Alternative Text • 5:Best Body Format • 6:TNEF	This setting lets you set the POP3 message retrieval format for an individual user.
ImapMessagesRetrievalMimeFormat	• 0:Text Only • 1:HTML Only • 2:HTML and Alternative Text • 3:Enriched Text Only • 4:Enriched Text and Alternative Text • 5:Best Body Format • 6:TNEF	This setting lets you set the IMAP4 message retrieval format for an individual user.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to set the message retrieval format for a POP3 user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4 Permissions" section in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **POP3** and then, in the result pane, under **POP3**, click **Properties**.
4. On the **POP3 Properties** page, click the **Retrieval Settings** tab.
5. Under **Message Retrieval**, select a message format from the drop-down list under **Message MIME format**.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to set the message retrieval format for a POP3 user

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "POP3 and IMAP4 Permissions" section in the Client Access Permissions topic.

This example sets the message retrieval format for POP3 access for USER01.

```
Set-CASMailbox -Identity USER01 -PopMessagesRetrievalMimeFormat value
```

Use one of the message retrieval format options listed in the Value column in the "Message retrieval format options for POP3 and IMAP4" table.

For more information about syntax and parameters, see Set-CASMailbox.

Use the EMC to set the message retrieval format for an IMAP4 user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4 Permissions" section in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **IMAP4** and then, in the result pane, under **IMAP4**, click **Properties**.
4. On the **IMAP4 Properties** page, click the **Retrieval Settings** tab.
5. Under **Message Retrieval**, select a message format from the drop-down list under **Message MIME format**.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to set the message retrieval format for an IMAP4 user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4 Permissions" section in the Client Access Permissions topic.

This example sets the message retrieval format for IMAP4 access for USER01.

```
Set-CASMailbox -Identity USER01 -ImapMessagesRetrievalMimeFormat value
```

Use one of the message retrieval format options listed in the Value column in the "Message retrieval format options for POP3 and IMAP4" table.

For more information about syntax and parameters, see Set-CASMailbox.

Other Tasks

After you set the message retrieval format for IMAP4 and POP3 users, you may also want to:

- Enable or Disable POP3 Access for a User
- Enable or Disable IMAP4 Access for a User
- Configure Calendar Options for IMAP4
- Configure Calendar Options for POP3

Set Connection Time-Out Limits for POP3

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure the connection time-out limits for idle authenticated and unauthenticated POP3 connections.

Note:

After you've set the connection time-out limits for POP3, you must restart the POP3 service for the settings to take effect. For information about how to restart the POP3 service, see Start and Stop the POP3 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to set connection time-out limits for POP3

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **POP3** and then, in the action pane, under **POP3**, click **Properties**.
4. On the **POP3 Properties** page, click the **Connection** tab.
5. Under **Time-out Settings**, do one of the following:
   - To set the connection time-out limit for idle authenticated connections, enter a number between 1 and 18,000 in the box next to **Authenticated time-out (seconds)**.
   - To set the connection time-out limit for idle unauthenticated connections, enter a number between 1 and 200 in the box next to **Unauthenticated time-out (seconds)**.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to set connection time-out limits for POP3

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example sets the connection time-out limit for idle authenticated connections.

```
Set -PopSettings -Identity CAS01 -AuthenticatedConnectionTimeout TimeValue
```

This example sets the connection time-out limit for idle unauthenticated connections.

```
Set -PopSettings -Identity CAS01 -PreAuthenticatedConnectionTimeout TimeValue
```

For more information about syntax and parameters, see Set-PopSettings.

Other Tasks

After you set connection time-out limits for POP3, you may also want to:

- Enable POP3 in Exchange 2010
- Set Connection Limits for POP3

1.6.2.5.13 Set Connection Time-Out Limits for IMAP4

Set Connection Time-Out Limits for IMAP4

Client Access > Managing Client Access Servers > Managing POP3 and IMAP4 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure the connection time-out limits for idle authenticated and unauthenticated IMAP4 connections.

Note:

After you've set the connection time-out limits for IMAP4, you must restart the IMAP4 service. For information about how to restart the IMAP4 service, see Start and Stop the IMAP4 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to set connection time-out limits for IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **IMAP4** and then, in the action pane, under **IMAP4**, click **Properties**.
4. On the **IMAP4 Properties** page, click the **Connection** tab.
5. Under **Time-out Settings**, do one of the following:
   - To set the connection time-out limit for idle authenticated connections, enter a number between 1 and 18,000 in the box next to **Authenticated time-out (seconds)**.
   - To set the connection time-out limit for idle unauthenticated connections, enter a number between 1 and 200 in the box next to **Unauthenticated time-out (seconds)**.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to set connection time-out limits for IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions

topic.

This example sets the connection time-out limit for idle authenticated connections.

```
Set -ImapSettings -Identity CAS01 -AuthenticatedConnectionTimeout Timespan
```

This example sets the connection time-out limit for idle unauthenticated connections.

```
Set -ImapSettings -Identity CAS01 -PreAuthenticatedConnectionTimeout Timespan
```

For more information about syntax and parameters, see Set-ImapSettings.

Other Tasks

After you set authentication time-out limits for IMAP4, you may also want to:

- Enable IMAP4 in Exchange 2010
- Set Connection Limits for IMAP4

1.6.2.5.14 Configure IP Addresses and Ports for POP3 and IMAP4 Access

Configure IP Addresses and Ports for POP3 and IMAP4 Access

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to configure Microsoft Exchange to use ports other than the default ports on the Microsoft Exchange Server 2010 server that has the POP3 and IMAP4 services enabled.

Note:
Enter IP addresses and IP address ranges in the Internet Protocol Version 4 (IPv4) format, Internet Protocol Version 6 (IPv6) format, or both formats. A default installation of Windows Server 2008 enables support for IPv4 and IPv6.

Note:
After you configure IP addresses and ports for POP3 and IMAP4 access, you must restart the POP3 or IMAP4 service. For information about how to restart the POP3 and IMAP4 services, see Start and Stop the POP3 Service and Start and Stop the IMAP4 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to configure IP addresses and ports for POP3 and IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select either **POP3** or **IMAP4**, and then under **POP3** or **IMAP4**, click

Properties in the action pane.
4. On the **Binding** tab, under **TLS or Unencrypted Connections**, click **Add**.
5. On the **TLS or Unencrypted Connection Settings** page, under **IP address to Use**, do one of the following:
   - To use all available IP addresses for a server, select **Use all IP addresses available on this server**.
   - To manually specify an address, select **Specify an IP address**, and then enter an IP address in the dialog box.
6. Under **Port to Use**, in the box next to **Port**, enter a port number, or accept the default port.
7. Click **OK** to save your changes.

Use the Shell to configure IP addresses and ports for POP3 and IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example sets the IP address and port for communicating with Exchange by using POP3 with Secure Sockets Layer (SSL).

```
Set-PopSettings -SSLBindings: IPaddress:Port
```

This example sets the IP address and port for communicating with Exchange by using POP3 with no encryption or Transport Layer Security (TLS) encryption.

```
Set-PopSettings -UnencryptedOrTLSBindings IPaddress:Port
```

This example sets the IP address and port for communicating with Exchange by using IMAP4.

```
Set-ImapSettings -SSLBindings: IPaddress:Port
```

This example sets the IP address and port for communicating with Exchange by using IMAP4 with no encryption or TLS encryption.

```
Set-ImapSettings -UnencryptedOrTLSBindings IPaddress:Port
```

For more information about syntax and parameters, see the following topics:

- Set-PopSettings
- Set-ImapSettings

Other Tasks

After you configure IP addresses and ports for POP3 and IMAP4, you may also want to:

- Enable POP3 and IMAP4 Users to Use Default Protocol Settings
- Enable IMAP4 in Exchange 2010
- Enable POP3 in Exchange 2010

1.6.2.5.15 Set Connection Limits for POP3

Set Connection Limits for POP3

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to set the connection limits on the computer running Microsoft Exchange Server 2010 that has the POP3 service enabled.

When you specify connection limits for POP3, you can select connection limits for the server, IP address, or a specific user. The following table describes the three settings for connection limits.

Descriptions of commands for setting connection limits for POP3

Command	Description	Default value	Limits
`MaxConnections`	Specifies the total number of connections the specified server will accept. This includes authenticated and unauthenticated connections.	2,000	1-25,000
`MaxConnectionsFromSingleIP`	Specifies the number of connections that the server will accept from a single IP address.	2000	1-25,000
`MaxConnectionsPerUser`	Specifies the maximum number of connections that the server will accept from a particular user.	16	1-25,000

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Note:
After you set connection limits, you must restart the POP3 service. For information about how to restart the POP3 service, see Start and Stop the POP3 Service.

Use the EMC to set POP3 connection limits for a server, an IP address, or a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **POP3** and then, in the action pane, under **POP3**, click **Properties**.
4. On the **POP3 Properties** page, click the **Connection** tab.
5. Under **Connection Limits**, specify the following:
   - To set the connection limit for a server, enter a value between 1 and 25,000 in the box next to **Maximum connections**.
   - To set the connection limit for an IP address, enter a value between 1 and 25,000 in the box next to **Maximum connections from a single IP address**.
   - To set the connection limit for a single user, enter a value between 1 and 25,000 in the box next to **Maximum connections from a single user**.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to set POP3 connection limits for a server, an IP address, or a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example sets the connection limit for a server.

```
Set-PopSettings -Identity CAS01 -MaxConnections Value
```

This example sets the connection limit for an IP address.

```
Set-PopSettings -Identity CAS01 -MaxConnectionsFromSingleIP Value
```

This example sets the connection limit for a user.

```
Set-PopSettings -MaxConnectionsPerUser Value
```

For more information about syntax and parameters, see Set-PopSettings.

Other Tasks

After you set POP3 connection limits for a server, IP address, or a user, you may also want to:

- Enable POP3 in Exchange 2010
- Set Connection Time-Out Limits for POP3

1.6.2.5.16 Set Connection Limits for IMAP4

Set Connection Limits for IMAP4

Client Access > Managing Client Access Servers > Managing POP3 and IMAP4 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to set the connection limits on a computer running Microsoft Exchange Server 2010 that has the IMAP4 service enabled.

When you specify connection limits for IMAP4, you can select connection limits for the server, IP address, or a specific user.

The following table describes the three settings for connection limits.

Descriptions of commands for setting connection limits for IMAP4

Command	Description	Default value	Limits
MaxConnections	Specifies the total number of	2,000	1-25,000

	connections the specified server will accept. This includes authenticated and unauthenticated connections.		
MaxConnectionsFromSingleIP	Specifies the number of connections that the server will accept from a single IP address.	2000	1-25,0000
MaxConnectionsPerUser	Specifies the maximum number of connections that the server will accept from a particular user.	16	1-25,000

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Note:

After you set connection limits, you must restart the IMAP4 service. For information about how to restart the IMAP4 service, see Start and Stop the IMAP4 Service.

Use the EMC to set IMAP4 connection limits for a server, an IP address, or a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **IMAP4** and then, in the action pane, under **IMAP4**, click **Properties**.
4. On the **IMAP4 Properties** page, click the **Connection** tab.
5. Under **Connection Limits**, specify the following:
   - To set the connection limit for a server, enter a value between 1 and 25,000 in the box next to **Maximum connections**.
   - To set the connection limit for an IP address, enter a value between 1 and 25,000 in the box next to **Maximum connections from a single IP address**.
   - To set the connection limit for a single user, enter a value between 1 and 25,000 in the box next to **Maximum connections from a single user**.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to set IMAP4 connection limits for a server, an IP address, or a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example sets the connection limit for a server.

```
Set-ImapSettings -Identity CAS01 -MaxConnections Value
```

This example sets the connection limit for an IP address.

```
Set-ImapSettings -Identity CAS01 -MaxConnectionsFromSingleIP Value
```

This example sets the connection limit for a user.

```
Set-ImapSettings -MaxConnectionsPerUser Value
```

For more information about syntax and parameters, see Set-ImapSettings.

Other Tasks

After you set IMAP4 connection limits for a server, IP address, or a user, you may also want to:

- Enable IMAP4 in Exchange 2010
- Set Connection Time-Out Limits for IMAP4

1.6.2.5.17 Configure Protocol Logging for POP3 and IMAP4

Configure Protocol Logging for POP3 and IMAP4

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure protocol logging settings for POP3 and IMAP4 on a Microsoft Exchange Server 2010 Client Access server. By default, protocol logging isn't enabled. You can use protocol logging to review the POP3 and IMAP4 connections in your Exchange environment. This can be useful if you're troubleshooting issues related to POP3 or IMAP4 performance. For more information, see Understanding Protocol Logging for POP3 and IMAP4.

You can enable, disable, and modify protocol logging options by using the Exchange Management Shell.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the Shell to enable protocol logging for POP3 or IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example enables protocol logging for IMAP4 or POP3 on the Client Access server CAS01.

```
Set-IMAPSettings -Server "CAS01" -ProtocolLogEnabled $true
Set-POPSettings -Server "CAS01" -ProtocolLogEnabled $true
```

You must restart the POP3 service or the IMAP4 service after you change these settings. The settings will take effect as soon as you restart the service.

For detailed syntax and parameter information, see Set-ImapSettings and Set-PopSettings.

Use the Shell to disable protocol logging for POP3 or IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example disables protocol logging for IMAP4 or POP3 on the Client Access server CAS01.

```
Set-IMAPSettings -Server "CAS01" -ProtocolLogEnabled $false
Set-POPSettings -Server "CAS01" -ProtocolLogEnabled $false
```

You must restart the POP3 service or the IMAP4 service after you change these settings. The settings will take effect as soon as you restart the service.

For detailed syntax and parameter information, see Set-ImapSettings and Set-PopSettings.

Use the Shell to modify protocol logging for POP3 or IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

To modify POP3 or IMAP4 logging settings, run the **Set-IMAPSettings** or **Set-POPSettings** cmdlets with one or more of the following parameters. You must restart the POP3 service or the IMAP4 service after you change these settings. The settings will take effect as soon as you restart the service.

- *LogFileLocation* This parameter specifies the location for the POP3 or IMAP4 protocol log files. By default, POP3 protocol log files are located in the C:\Program Files\Microsoft\Exchange Server\V14\Logging\Pop3 directory. This example turns on POP3 protocol logging on the Client Access server CAS01. It also changes the POP3 protocol logging directory to C:\Pop3Logging.

  ```
  Set-POPSettings -Server "CAS01" -ProtocolLogEnabled $true -LogFileLocat
  ```

- *LogFileRollOverSettings* This parameter defines how frequently POP3 or IMAP4 protocol logging creates a new log file. By default, a new log file is created every hour. The possible values are:
  Hourly
  Daily
  Weekly
  Monthly
  This setting applies only when the value for the parameter *LogPerFileSizeQuota* is set to 0. This example changes the POP3 protocol logging on the Client

Access server CAS01 to create a new log file every hour.

```
Set-POPSettings -Server "CAS01" -LogPerFileSizeQuota 0 -LogFileRollOver
```

- *LogPerFileSizeQuota* This parameter defines the maximum size of a POP3 or IMAP4 protocol log file in bytes. By default, this value is set to 0. When this value is set to zero, a new protocol log file is created at the frequency specified by the *LogFileRollOverSettings* parameter.
  This example changes the POP3 protocol logging on the Client Access server CAS01 to create a new log file when a log file reaches 2 MB.

```
Set-POPSettings -Server "CAS01" -LogPerFileSizeQuota 2000000
```

This example changes the POP3 protocol logging on the Client Access server CAS01 to use the same log file regardless of its creation date and size.

```
Set-POPSettings -Server "CAS01" -LogPerFileSizeQuota unlimited
```

For detailed syntax and parameter information, see Set-ImapSettings and Set-PopSettings.

Other Tasks

After you configure protocol logging settings for POP3 and IMAP4, you may also want to do the following:

- Start and Stop the IMAP4 Service
- Start and Stop the POP3 Service

1.6.2.5.18 Allow POP3, IMAP4, and SMTP Server Settings to be Viewed By End Users in Outlook Web App

Allow POP3, IMAP4, and SMTP Server Settings to be Viewed By End Users in Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-10*

If you have users who use POP3 or IMAP4 to connect to their Microsoft Exchange Server 2010 mailboxes, they have to know the correct server settings to connect to these mailboxes. You can configure Exchange so that your users can look up their own settings.

POP and IMAP e-mail programs require that users enter their incoming POP3 or IMAP4 server settings and their outgoing SMTP server settings. You can allow your users to connect from inside the corporate network (using internal server settings) or over the Internet (using external server settings).

Note:

After a default Exchange 2010 installation, your users can look up their internal POP3 and IMAP4 server settings using Microsoft Office Outlook Web App. However, you must make changes to the settings on your Exchange server if you want users to be able to look up their own external POP3 and IMAP4 server settings or their internal or external SMTP server settings.

For more information about how to manage POP3 and IMAP4, see Managing POP3 and IMAP4.

Use the Shell to allow POP3, IMAP4, and SMTP server settings to be viewed by end users in Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 settings" and "IMAP4 settings" entries in the Client Access Permissions topic and "Receive connectors" entry in the Transport Permissions topic.

This example allows external POP3 server settings to be viewed by end users.

```
set-popsettings -ExternalConnectionSettings {CAS01:995:SSL}
```

For detailed syntax and parameter information, see Set-PopSettings.

This example allows external IMAP4 server settings to be viewed by end users.

```
set-imapsettings -ExternalConnectionSettings {CAS01:993:SSL}
```

For detailed syntax and parameter information, see Set-ImapSettings.

This example allows internal and external SMTP server settings to be viewed by end users using Outlook Web App. **Client CAS01** is the send connector.

```
Set-ReceiveConnector "Client CAS01" -advertiseclientsettings $true
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

After you run these commands, your users can look up their server settings in Outlook Web App, as follows:

- If you're running Exchange 2010 SP1, your users can look up their external POP3, IMAP4, and SMTP server settings by clicking **Options** > **All Options** > **Account** > **My Account** > **Settings for POP, IMAP, and SMTP access**.
- If you're running the RTM version of Exchange 2010, your users can look up their external POP3, IMAP4, and SMTP server settings by clicking the drop-down arrow next to the Help question mark, and then clicking **About**.
- If you're running Exchange 2010 SP1 or Exchange 2010 RTM, your users can look up their internal POP3, IMAP4, and SMTP server settings in Outlook Web App by clicking the drop-down arrow next to the Help question mark, and then clicking **About**.

Other Tasks

After you make it possible for end users to view their POP3, IMAP4, and SMTP settings, you may also want to:

- Enable or Disable POP3 Access for a User
- Enable or Disable IMAP4 Access for a User

1.6.2.6 Managing the Autodiscover Service

Managing the Autodiscover Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-13*

1.6.2.6.1 Create an Autodiscover Virtual Directory

Create an Autodiscover Virtual Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to create a new Autodiscover virtual directory for Microsoft Exchange Server 2010. This can't be done using the EMC. The Autodiscover virtual directory provides the internal and external URLs that connecting Outlook clients require to access Exchange services, including the Availability service, the offline address book, and Unified Messaging.

Note:

The ability to use the Autodiscover service on a mobile phone depends on the operating system that's running on the mobile phone. Not all mobile phone operating systems that support synchronization with Exchange 2010 also support the Autodiscover service. For more information, contact the manufacturer of your mobile phone.

Looking for other management tasks related to the Autodiscover service? Check out Managing the Autodiscover Service.

Use the Shell to create a new Autodiscover virtual directory

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Autodiscover virtual directory settings" entry in the Client Access Permissions topic.

This example creates an Autodiscover virtual directory under the Default Web Site in the Internet Information Services (IIS) Manager, with client authentication set to allow Basic and Integrated Windows authentication.

```
New-AutodiscoverVirtualDirectory -Websitename <websitename> -BasicAuthentication:
```

For more information about syntax and parameters, see New-AutodiscoverVirtualDirectory.

Other Tasks

After you create a new Autodiscover virtual directory, you may also want to:

- Delete the Default Autodiscover Virtual Directory
- Configure the Autodiscover Service for Internet Access

1.6.2.6.2 Delete the Default Autodiscover Virtual Directory

Delete the Default Autodiscover Virtual Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to delete the default Autodiscover virtual directory for Microsoft Exchange Server 2010. You can't use the EMC to do this.

Looking for other management tasks related to the Autodiscover service? Check out Managing the Autodiscover Service.

Use the Shell to delete the default Autodiscover virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Autodiscover virtual directory settings" entry in the Client Access Permissions topic.

This example removes the default Autodiscover virtual directory.

```
Remove-AutodiscoverVirtualDirectory -Identity "MyServer\autodiscover(autodiscover
```

For more information about syntax and parameters, see Remove-AutodiscoverVirtualDirectory.

Other Tasks

After you delete the default Autodiscover virtual directory, you may also want to:

- Create an Autodiscover Virtual Directory
- Configure the Autodiscover Service for Internet Access

1.6.2.6.3 Test Outlook Autodiscover Connectivity

Test Outlook Autodiscover Connectivity

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to verify that the Autodiscover service settings for Outlook clients are configured correctly.

Looking for other management tasks related to the Autodiscover service? Check out Managing the Autodiscover Service.

Use the Shell to test Autodiscover connectivity

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Test Autodiscover service connectivity" entry in the Client Access Permissions topic.

This example tests that the Outlook provider settings for the Autodiscover service are configured correctly on the Client Access server CASServer01.

```
Test-OutlookWebServices -ClientAccessServer "CASServer01"
```

For detailed syntax and parameter information, see the Test-OutlookWebServices reference topic.

Other Tasks

After you test connectivity for the Autodiscover service, you may also want toTest Outlook Anywhere Connectivity.

1.6.2.6.4 Configure the Autodiscover Service for Internet Access

Configure the Autodiscover Service for Internet Access

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the Autodiscover service for Internet access on a Microsoft Exchange Server 2010 Client Access server.

If you've deployed Exchange 2010 in your messaging environment, you can let the Autodiscover service automatically configure Microsoft Office Outlook 2007 or Outlook

2010 clients for features such as the Availability service, Unified Messaging, and Outlook Anywhere. If you plan to allow external access to the Autodiscover service for Outlook 2007 or Outlook 2010 clients that connect from the Internet, you must configure a valid Secure Sockets Layer (SSL) certificate from a certification authority (CA) that's trusted by the client computer's operating system.

You can create a separate Internet Information Services (IIS) Web site to host Autodiscover traffic. Consider hosting the Autodiscover service on a separate IIS Web site if either of the following is true:

- Your primary Web site is visited frequently
- Your primary Web site hosts your e-mail traffic

Looking for other management tasks related to the Autodiscover service? Check out Managing the Autodiscover Service.

Configure Internet access to the Autodiscover service

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Autodiscover service virtual directory settings" entry in the Client Access Permissions topic.

To allow external access to the Autodiscover service for Outlook 2010 or Outlook 2007 clients that are connected from the Internet, we recommend that you perform these steps in the following order.

1. **(Optional) Configure a separate IIS Web site on a Client Access server to host the Autodiscover service** You can create a separate site to host Autodiscover service traffic by using the **New-AutodiscoverVirtualDirectory** cmdlet. This step is recommended if the domain in the Simple Mail Transfer Protocol (SMTP) address is the same as the corporate Web site address and your corporate Web site is visited frequently. For example, if the corporate Web site is www.contoso.com, the e-mail SMTP domain is contoso.com, and the corporate Web site (www.contoso.com) is visited frequently, we recommend that you create a separate site and host the Autodiscover service on autodiscover.contoso.com. For more information, see Create an Autodiscover Virtual Directory.

   Note:
   You must use one IP address per site.

2. **(Required) Configure a valid SSL certificate** You must configure a valid SSL certificate from a CA that the client computer trusts. We recommend that you use the Exchange 2010 Certificate wizard to configure a valid SSL certificate. For information about how to create an SSL certificate, see Create a New Exchange Certificate. If you've decided to host the Autodiscover service on a separate Web site, see Configure SSL Certificates to Use Multiple Client Access Server Host Names.
3. **(Optional) Update the SCP Object** You only need to perform this step if you want internal Exchange clients to connect to the Autodiscover service through the Internet. Service connection points (SCPs) are only used for internal Exchange clients. If you've created a separate IIS Web site for the Autodiscover service, you must update the SCP object in Active Directory to specify which Client Access server and Autodiscover virtual directory you want clients to connect to. For more information about how to configure SCP objects, see Publishing with Service Connection Points.
4. **(Required) Configure the firewall and SSL certificate** You should configure the firewall for the address space and configure the SSL certificate for the Autodiscover service. For more information, check your firewall documentation. If your firewall server is ISA Server 2006, see Publishing

Exchange Server 2007 with ISA Server 2006. For information about how to configure Outlook Anywhere to use multiple SSL certificates, see Configure Outlook Anywhere to Use Multiple SSL Certificates.

5. **(Optional) Create a new Web site for the Autodiscover service** Follow these steps:
   5.a. In IIS Manager, expand your Client Access server name, select and right-click **Sites**, and then select **Add Web Site**. Enter your SMTP domain name under **Site name**.
   5.b. Under **Physical path**, navigate to %SystemDrive%\inetpub\. Under inetpub, create a new folder called Autodiscover.

   Note:
   You must allow the **Users** group **Read & execute** access to the Web site that you create.

6. **(Optional) Create an Autodiscover virtual directory for the new Web site** You can use the Shell to create an Autodiscover virtual directory for the new Web site in IIS by running the following command.
   You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Autodiscover virtual directory settings" entry in the Client Access Permissions topic.

   ```
   New-AutodiscoverVirtualDirectory -Websitename <websitename> -BasicAuth
   ```

   Note:
   A Web site that uses SSL requires that you use a unique IP address.

   For more information about syntax and parameters, see New-AutodiscoverVirtualDirectory.
7. **(Optional) Configure a trusted third-party SSL certificate on the new Web site** If you created a new Web site to host the Autodiscover service, configure a trusted third-party SSL certificate on the Web site. We recommend that you use the Exchange 2010 Certificate wizard to configure a valid SSL certificate. For information about how to create an SSL certificate, see Create a New Exchange Certificate. For more information, see Understanding Digital Certificates and SSL.

Other Tasks

After you configure a new Web site for the Autodiscover service, you may also want to:

- Configure Exchange Services for the Autodiscover Service
- Configure the Autodiscover Service for Multiple Forests

1.6.2.6.5 Configure the Autodiscover Service for Multiple Forests

Configure the Autodiscover Service for Multiple Forests

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to configure the Autodiscover service when your Microsoft Exchange deployment has two or more trusted forests.

To configure the Autodiscover service when your deployment has two or more trusted forests, you must update Active Directory so that users who are running Microsoft Office

Outlook 2007 or Outlook 2010 in one forest can access the Client Access servers in the remote (or target) forest to use the Autodiscover service. To do this, you run the **Export-AutodiscoverConfig** cmdlet in each forest that contains the Client Access servers that provide the Autodiscover service against the target forests. This configures the service connection point (SCP) information for the Autodiscover pointer in Active Directory.

Looking for other management tasks related to the Autodiscover service? Check out Managing the Autodiscover Service.

Use the Shell to configure the Autodiscover service for multiple forests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Autodiscover service virtual directory settings" entry in the Client Access Permissions topic.

The procedures in the following examples must be performed on an Exchange 2010 Client Access server in the source forest.

This example retrieves the credentials from the Client Access server in the target forest. Use the target server's credentials to run the cmdlet **Export-AutodiscoverConfig**.

```
$a = Get-Credential
```

This example updates a service connection point for an Autodiscover service pointer on the Client Access server in the source forest for the target Exchange forest.

```
Export-AutoDiscoverConfig -DomainController <FQDN> -TargetForestDomainController
```

For more information about syntax and parameters, see Export-AutoDiscoverConfig.

Other Tasks

After you configure the Autodiscover service for multiple forests, you may also want to:

- Configure the Autodiscover Service to Use Site Affinity

1.6.2.6.6 Configure the Autodiscover Service to Use Site Affinity

Configure the Autodiscover Service to Use Site Affinity

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to configure site affinity for the Autodiscover service on the Microsoft Exchange Server 2010 Client Access server. When you configure site affinity on the Client Access server, you enable clients using Outlook 2007 and Outlook 2010 to get Autodiscover information from the closest Active Directory site. This provides Autodiscover information to the Outlook clients more quickly than if site affinity hasn't been set.

To configure the Autodiscover service to use site affinity, use the **Set-ClientAccessServer**

cmdlet.

Looking for other management tasks related to the Autodiscover service? Check out Managing the Autodiscover Service.

Use the Shell to configure site affinity for the Autodiscover service

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Autodiscover service site affinity" entry in the Client Access Permissions topic.

This example sets the Autodiscover URL for Outlook clients in the specified Active Directory site to get Autodiscover information.

```
Set-ClientAccessServer -Identity "ServerName" -AutodiscoverServiceInternalURI "ht
```

For more information about syntax and parameters, see Set-ClientAccessServer.

Other Tasks

After you configure site affinity for the Autodiscover service, you may also want to:

- Configure Exchange Services for the Autodiscover Service
- Configure the Autodiscover Service for Internet Access

1.6.2.6.7 Configure Exchange ActiveSync Autodiscover Settings

Configure Exchange ActiveSync Autodiscover Settings

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Autodiscover service to provision mobile phones for users. The Autodiscover service returns an XML file that's used to provision a user's phone when the user's e-mail address and password are supplied. The Autodiscover service returns the address to a Microsoft Exchange Server 2010 Client Access server. By default, the Autodiscover service is enabled. You can use the Shell to enable the Autodiscover service in Microsoft Exchange ActiveSync.

Note:

The ability to use the Autodiscover service depends on the mobile phone operating system that you're using. Not all mobile phone operating systems that support synchronization with Exchange 2010 support Autodiscover. For more information about mobile phone operating systems that support Autodiscover, contact the manufacturer of your mobile phone.

Looking for other management tasks related to the Autodiscover service? Check out Managing the Autodiscover Service.

Use the Shell to configure the Autodiscover service in Exchange ActiveSync

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access Server settings" entry in the Client Access Permissions topic.

This example configures the Autodiscover service and sets the **ExternalURL** property.

```
Set-ActiveSyncVirtualDirectory -Identity "COMPUTERNAME\Microsoft-Server-ActiveSyn
```

This example configures the Exchange ActiveSync server property on the Client Access server.

```
Set-ActiveSyncVirtualDirectory -Identity "COMPUTERNAME\Microsoft-Server-ActiveSyn
```

For more information about syntax and parameters, see Set-ActiveSyncVirtualDirectory.

1.6.2.6.8 Configure Exchange Services for the Autodiscover Service

Configure Exchange Services for the Autodiscover Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure Microsoft Exchange services, such as the Availability service, for the Autodiscover service on a Microsoft Exchange Server 2010 Client Access server.

When you enable Outlook Anywhere, you must also configure external client access to Microsoft Exchange services for the Autodiscover service. Other external URLS you must configure include the URLs for the Availability service, Exchange Web Services, Unified Messaging (UM), and the offline address book.

If you don't configure the external URL values, the Autodiscover service information provided to the Microsoft Office Outlook 2007 or Outlook 2010 clients may be incorrect for users who are connecting from outside your network. They may be able to connect to their Exchange mailbox. However, they won't be able to use Exchange features such as Automatic Replies, the Availability service, Unified Messaging, or offline address book downloads.

Generally, the internal URL is configured by Exchange Setup. However, the external URLs must be configured by using the virtual directory cmdlet for each component.

Looking for other management tasks related to the Autodiscover service? Check out Managing the Autodiscover Service.

Use the Shell to configure the Outlook Anywhere external host name for the

Autodiscover service

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration (enable, disable, change, view)" entry in the Client Access Permissions topic.

This example sets the external host name for Outlook Anywhere on the Client Access server CAS01.

```
Enable-OutlookAnywhere -Server CAS01 -ExternalHostname "mail.contoso.com" -Defaul
```

For more information about syntax and parameters, see Enable-OutlookAnywhere.

Use the Shell to configure the offline address book external URL for the Autodiscover service

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "OAB virtual directory" entry in the Mailbox Permissions topic.

This example sets the external URL for the offline address book virtual directory on the Client Access server CAS01.

```
Set-OABVirtualDirectory -identity "CAS01\OAB (Default Web Site)" -externalurl htt
```

For more information about syntax and parameters, see Set-OABVirtualDirectory.

Use the Shell to configure the Exchange Web Services external URL for the Autodiscover service

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Web Services settings" entry in the Client Access Permissions topic.

This example sets the external URL for the Exchange Web services virtual directory on the Client Access server CAS01.

```
Set-WebServicesVirtualDirectory -identity "CAS01\EWS (Default Web Site)" -externa
```

For more information about syntax and parameters, see Set-WebServicesVirtualDirectory.

Other Tasks

After you configure Exchange services for the Autodiscover service, you may also want to:

- Configure the Autodiscover Service for Internet Access
- Configure the Autodiscover Service to Use Site Affinity

Modify the Time Limit for Autodiscover Operations

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-09-14*

The Cross-Forest Availability service has a time limit for performing an AutoDiscover operation for cross-forest users in the Active Directory directory service. By default, the time-out value is 10 seconds. If the Autodiscover request does not finish in 10 seconds, the Availability service request for the cross-forest user may time out.

To control the time-out value, use the **RecipientResolutionTimeoutInSeconds** property. The **RecipientResolutionTimeoutInSeconds** property is set in the ASP.NET Web.config file. The ASP.NET Web.config file exists in two locations.

Caution:

We recommend that you set this property to a value of no more than 25 seconds.

Change the value of the RecipientResolutionTimeoutInSeconds property

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the Exchange Server configuration settings entry in the Exchange and Shell Infrastructure Permissions topic.

Note:

The ASP.NET Web.config file exists in two locations. Therefore, the same procedure applies to both locations.

1. Locate the Web.config file in the following directory:

   drive:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews\web.config

2. Copy the existing Web.config file, and then rename the copy file **Web.config.bak1**.
3. Open the Web.config file in Notepad.
4. Look for a section that is named **<appSettings>**. If **<appSettings>** exists, add the following entry to this section between **<appSettings>** and **</appSettings>**:

   ```
   <add key="RecipientResolutionTimeoutInSeconds" value="24"/>
   ```

   If the **<appSettings>** section does not exist, add the following section directly beneath the **<Configuration>** section:

   ```
   <appSettings>
        <add key="RecipientResolutionTimeoutInSeconds" value="24"/>
   </appSettings>
   ```

   Important:

   - This entry is case-sensitive, and must be entered exactly as shown. However, you can change the value from 24 to the value that you want to use. We recommend that you set the value for this property to between 20 and 24 seconds.

- Do not add this section under any other section of the Web.config file. If the new section does not immediately follow **<Configuration>**, it will not work.

1. Save the Web.config file.
2. Locate the Web.config file in the following directory:

   drive:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa\web.config

3. Copy the existing Web.config file, and then rename the copy file **Web.config.bak1**.
4. Open the Web.config file in Notepad.
5. Look for a section that is named **<appSettings>**. If **<appSettings>** exists, add the following entry to this section between **<appSettings>** and **</appSettings>**:

```
<add key="RecipientResolutionTimeoutInSeconds" value="24"/>
```

If the **<appSettings>** section does not exist, add the following section directly under the **<Configuration>** section:

```
<appSettings>
     <add key="RecipientResolutionTimeoutInSeconds" value="24"/>
</appSettings>
```

Important:

- This entry is case-sensitive, and must be entered exactly as shown. However, you can change the value from 24 to the value that you want to use. We recommend that you set the value for this property to between 20 and 24 seconds.
- Do not add this section under any other section of the Web.config file. If the new section does not immediately follow **<Configuration>**, it will not work.

1. Save the Web.config file.

For More Information

Configure the Availability Service for Cross-Forest Topologies

1.6.2.7 Managing the Availability Service

Managing the Availability Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-01*

Configure the Availability Service for Network Load Balanced Computers

Configure the Availability Service for Cross-Forest Topologies

Diagnose Availability Service Issues

Configure the Availability Service for Network Load Balanced Computers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Outlook 2007 discovers the Availability service URL using the Autodiscover service. To use network load balancing with the Availability service, you must make changes to your configuration. Specifically, for the Autodiscover and Availability services to work, DNS needs to be configured so that mail.<*domain name*>.com and autodiscover.<*domain name*>.com point to the Network Load Balancing (NLB) array of Client Access servers. In the previous sentence, <*domain name*> is a placeholder for your domain name.

You can configure the Availability service for network load balanced computers using the Exchange Management Shell.

Looking for other management tasks related to managing the Availability service? See Managing the Availability Service.

Prerequisites

Review the section "Availability Service Network Load Balancing" in the topic Understanding the Availability Service.

Use the Shell to configure the Availability service for network load balanced computers

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Availability service permissions" entry in the Client Access Permissions topic.

This example configures the Availability service for load balancing for a domain named Contoso.com.

```
Set-WebServicesVirtualDirectory -Identity "EWS*" -ExternalUrl "Https:// mail.cont
```

Note:

If you have a set of load balanced Client Access servers, you don't have to specify the name of each server when you run this command. You only need to use the name of one of the servers in the set of load balanced servers.

For information about syntax and parameters, see Set-WebServicesVirtualDirectory.

Other Tasks

After you configure the Availability service for network load balanced computers, you may also want to:

- Diagnose Availability Service Issues
- Configure the Availability Service for Cross-Forest Topologies

1.6.2.7.2 Configure the Availability Service for Cross-Forest Topologies

Configure the Availability Service for Cross-Forest Topologies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-23*

The Availability service improves information workers' free/busy information by providing secure, consistent, and up-to-date free/busy information to clients who are running Microsoft Office Outlook 2007. By default, this service is installed with Microsoft Exchange Server 2010. In cross-forest topologies where all connecting clients are running Outlook 2007, the Availability service is the only method of retrieving free/busy information. You can use the Exchange Management Shell to configure the Availability service for cross-forest topologies.

Note:
You can't use the EMC to configure the Availability service for cross-forest topologies.

Note:
The terms *Source forest* and *Target forest* are used in this topic to identify each forest. These terms are defined as follows:

- **Source forest** Exchange forest from which the Availability Service makes the free/busy inquiry
- **Target forest** Exchange forest from which the free/busy information is being retrieved

Looking for other management tasks related to the Availability service? Check out Managing the Availability Service.

Using the Availability Service in Trusted and Untrusted Forests

You can use the Availability service in cross-forest topologies across trusted or untrusted forests. The type of free/busy information that's available depends on if you're using a trusted or untrusted forest.

Trusted Forests In trusted forests, you can configure the Availability service to retrieve free/busy information on a per-user basis. When the Availability service is configured to retrieve free/busy information on a per-user basis, the service can make cross-forest requests on behalf of a particular user. This allows a user in a remote forest to retrieve detailed free/busy information for someone who is not in the same forest.

Untrusted Forests In untrusted forests, you can configure the Availability service only to retrieve free/busy information on an organization-wide basis. When the Availability service makes free/busy cross-forest requests at the organizational level, free/busy information is returned for each user in the organization. In untrusted forests, it isn't possible to control the level of free/busy information that's returned on a per-user basis.

Configure Active Directory for Cross-Forest Topologies

To configure Active Directory in Microsoft Windows for a cross-forest topology, you must install and configure GAL Synchronization (GALSync). For information about how to install and configure the GALSync feature in Microsoft Identity Integration Server (MIIS), see the following resources:

- Microsoft Identity Integration Server 2003 Scenarios
- Microsoft Identity Integration Server 2003

Note:
If you want to use the *PerUserFB* parameter together with the **Add-AvailabilityAddressSpace** cmdlet, GALSync must be configured to synchronize the **msExchMasterAccountSid** attribute for the contacts and mail users that are synchronized to the target forest. This is not required for OrgWideFB.

If you're running Office Outlook 2003 or an earlier version, you must use the Microsoft Exchange Inter-Organization Replication tool to synchronize free/busy information across multiple forests. For more information about the Microsoft Exchange Inter-Organization Replication tool, see Microsoft Exchange Server Inter-Organization Replication.

Note:
To use the Microsoft Exchange Inter-Organization Replication tool, a Microsoft Exchange Server 2003 server or a Microsoft Exchange Server 2007 server must be the target server. The Microsoft Exchange Inter-Organization Replication tool is not supported when a Microsoft Exchange Server 2010 server is the target server.

Note:
Microsoft Exchange Server 2010 Service Pack 2 (SP2) Update Rollup 1 uses the external URL for Exchange Web Services to connect to the target forest. The external URL for Exchange Web Services cannot be returned by the AutoDiscover service if Outlook Anywhere is not enabled in the target forest. In this case, the cross-forest lookup fails. To work around this issue, enable Outlook Anywhere in the target forest, and then verify that the external URL for Exchange Server Web Services is configured correctly.

1. Enable Outlook Anywhere in the target forest. For information about how to enable Outlook Anywhere, see Enable Outlook Anywhere.
2. Configure the external URL for Exchange Web Services for the target forest. To do this, run the following command in Windows PowerShell for Exchange: **Set-WebServicesVirtualDirectory -identity "server_name\EWS (Default Web Site)" -ExternalURL https://mail.contoso.com/ews/Exchange.asmx**

   Note:
   In this command, contoso is a placeholder for the appropriate domain name.
3. Enable Outlook Anywhere for the organization mailboxes that should make incoming remote availability requests.

   Note:
   If an administrator disables Outlook Anywhere on an individual mailbox, that mailbox's information cannot be retrieved by a remote forest because Autodiscover will not return an Exchange Web Services ExternalURL for that mailbox.

Use the Shell to configure per-user free/busy information in a trusted cross-forest topology

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Availability Service Permissions" entries in the Client Access Permissions topic.

This example configures the Availability service to retrieve per-user free/busy information

on a Client Access server in the target forest.

Target Forest

```
Get-ClientAccessServer | Add-ADPermission -Accessrights Extendedright -Extendedri
EPI-Token-Serialization"  -User "<Remote Forest Domain>\Client Access servers"
```

This example defines the free/busy access method that the Availability service uses on the local Client Access server in the source forest. The local Client Access server is configured to access free/busy information from the <*Target_Forest*>.com forest on a per-user basis. The following example uses the service account to retrieve free/busy information.

Source Forest

```
Add-AvailabilityAddressSpace -Forestname <Target_Forest> -AccessMethod PerUserFB
```

Note:
To configure bidirectional cross-forest availability, repeat these steps in the target forest.

If you choose to configure cross-forest availability with trust, and also choose to use a service account (instead of specifying organization-wide or per-user credentials), you must extend permissions, as shown in the example in the "Use the Shell to configure trusted cross-forest availability with a service account" section. Performing that procedure in the target forest gives Client Access servers in the source forest permission to serialize the original user context.

Use the Shell to configure trusted cross-forest availability with a service account

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Availability Service Permissions" entries in the Client Access Permissions topic.

This example configures trusted cross-forest availability with a service account in the source forest.

Source Forest

```
$a = Get-Credential (Type the credential  "TargetForest\User"  for organization-w
Add-AvailabilityAddressSpace -ForestName <Target_Forest> -AccessMethod OrgWide -C
```

This example configures trusted cross-forest availability with a service account in the target forest.

Target Forest

```
Set-AvailabilityConfig -OrgWideAccount "TargetForest\User"
```

For detailed information about syntax and parameters, see the following topics:

- Get-ClientAccessServer
- Add-ADPermission
- Add-AvailabilityAddressSpace
- Set-AvailabilityConfig

Use the Shell to configure organization-

wide free/busy information in an untrusted cross-forest topology

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Availability Service Permissions" entries in the Client Access Permissions topic.

This example sets the organization-wide account on the availability configuration object to configure the access level for free/busy information in the target forest.

Target Forest

```
Set-AvailabilityConfig -OrgWideAccount "TargetForestDomain\User"
```

This example adds the Availability address space configuration object for the source forest.

Source Forest

```
$a = get-credential  (Enter the credentials for organization-wide user in SourceF
Add-AvailabilityAddressspace -Forestname SourceForestDomain -Accessmethod OrgWide
```

Configuring Cross-Forest Availability in Forests that Include Exchange 2003

For Outlook 2007 and Exchange 2010 users to view the free/busy information of Exchange Server 2003 users in another forest, you must configure the Availability service by using the **Add-AvailabilityAddressSpace** cmdlet.

You only have to run this command once on any server in the Exchange 2010 forest. You can run this cmdlet from any computer running Exchange 2007 or Exchange 2010.

Use the Shell to configure cross-forest availability in forests that include Exchange 2003

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Availability Service Permissions" entries in the Client Access Permissions topic.

This example sets public folder free/busy availability in the source forest.

Source Forest

```
Add-AvailabilityAddressSpace -ForestName SourceForestDomain -AccessMethod PublicF
```

Note:

To replicate free/busy information and public folder content between Exchange organizations you must use the Microsoft Exchange Inter-Organization Replication tool. For more information about the Microsoft Exchange Inter-Organization Replication tool, see Microsoft Exchange Server Inter-Organization Replication.

Cross-Forest Availability with Shared

name space

Important:
When you set up cross forest availability together with a shared name space, the availability services uses the target address on the contacts.

To configure SMTP namespace sharing, you must create an accepted domain that configured as internal relay domain for the SMTP namespace that you want to share. Then, create an SMTP connector that has the address space of the internal SMTP domain. The destination e-mail server must be a Hub Transport Server.

For more information, see Configure Exchange 2010 to Route Messages for a Shared Address Space.

Other Tasks

After you configure the Availability service for cross-forest topologies, you may also want to:

- Diagnose Availability Service Issues
- Configure the Availability Service for Network Load Balanced Computers

1.6.2.7.3 Diagnose Availability Service Issues

Diagnose Availability Service Issues

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to diagnose Availability service issues in Exchange Server 2010, as follows:

- For an individual user
- On a Client Access server
- Across different sites

The Autodiscover service provides Microsoft Office Outlook 2007 with configuration information that's needed to connect to Exchange. The **Test-OutlookWebServices** cmdlet verifies whether the Autodiscover service and the Availability service are correctly configured and can service Outlook client requests.

Before you perform these procedures, consider trying to diagnose your Availability service issues using Event Viewer. Specifically, search Event Viewer on your Client Access server for event logs that contain the event source "MSExchange Availability".

Looking for other management tasks related to managing the Availability service? See Managing the Availability Service.

Prerequisites

You must create a test account before you can diagnose Availability service issues using the **Test-OutlookWebServices** cmdlet. To create the test mailbox, log on to the Exchange Server 2007 or Exchange 2010 Mailbox server. Open the Shell, and then locate the **Scripts** directory under the installation path on the Exchange server. For Exchange 2007, the folder is located at C:\Program Files\Microsoft\Exchange Server\Scripts, where C:\ is the directory to which you installed Exchange. For Exchange 2010, the folder is located at C:\Program Files\Microsoft\ExchangeServer\V14\Scripts, where C:\ is the directory to which you installed Exchange 2010. Run the script New-TestCasConnectivityUser.ps1. Repeat this process on each Exchange 2007 or Exchange 2010 Mailbox server that is to be tested.

Use the Shell to diagnose Availability service issues for an individual user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Availability service permissions" entry in the Client Access Permissions topic.

This example tests access to the Availability service for user User1@Contoso.com.

```
Test-OutlookWebServices -Identity: User1@Contoso.com
```

Use the Shell to diagnose Availability service issues for a Client Access server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Availability service permissions" entry in the Client Access Permissions topic.

This example tests user access to the Availability service on the Client Access server ClientAccessServer01.

```
Test-OutlookWebServices -ClientAccessServer ClientAccessServer01
```

Use the Shell to diagnose Availability service issues across different sites

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Availability service permissions" entry in the Client Access Permissions topic.

This example tests Availability service connectivity between users in two different Active Directory sites.

```
Test-OutlookWebServices -Identity User1@Site1.Contoso.com -TargetAddress User2@Si
```

For information about syntax and parameters, see Test-OutlookWebServices.

Other Tasks

After you diagnose Availability service issues, you may also want to:

- Configure the Availability Service for Cross-Forest Topologies
- Configure the Availability Service for Network Load Balanced Computers

1.6.2.8 Managing External Client Access

Managing External Client Access

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-12*

Configure External Client Access Namespaces

Using ISA Server with Outlook Web App

Using ISA Server with Outlook Anywhere

Using ISA Server with Exchange ActiveSync

Using ISA Server with POP3 and IMAP4

1.6.2.8.1 Configuring External Client Access

Configuring External Client Access

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-09*

By allowing remote access to Microsoft Exchange to users who are based outside the corporate network, an organization enables its employees to take full advantage of the technology their company provides. Remote access lets employees use many types of devices to communicate with their peers and customers from any place and at any time.

When an organization allows access to corporate resources from any location—perhaps with devices that aren't controlled by the organization—it risks the security of the data and services that are accessed. Therefore it's critical to take measures to ensure that the data is accessed securely. This means you must implement technologies such as certificates, implement firewalls, and enforce pre-authentication and device or endpoint validation. This process is known as publishing Exchange.

When you publish Exchange, Microsoft offers two primary software-based options: Microsoft Forefront Threat Management Gateway 2010 (Forefront TMG) and Microsoft Forefront Unified Access Gateway 2010 (Forefront UAG). Both options offer publishing wizards and security features to provide secure access to Exchange when it's accessed from outside the safety of the corporate network. For more information about these two solutions, see Publishing Exchange Server 2010 with Forefront UAG and TMG.

Configuring Client Access Protocols for External Access

In addition to configuring your chosen firewall and security solution, you must configure

the individual Client Access server protocols for external access. For more information about how to configure the various Client Access server protocols for external access, see the following topics.

- Configure External Client Access Namespaces
- Using ISA Server with Outlook Web App
- Using ISA Server with Outlook Anywhere
- Using ISA Server with Exchange ActiveSync
- Using ISA Server with POP3 and IMAP4

1.6.2.8.1.1 Using ISA Server with Outlook Web App

Using ISA Server with Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

Outlook Web App for Microsoft Exchange Server 2010 is designed to take full advantage of the features that are available in Microsoft Internet Security and Acceleration (ISA) Server 2006. Exchange 2010 is also designed to integrate with earlier versions of ISA Server. When you deploy Exchange 2010 in an environment where ISA Server 2006 is being used to help secure your corporate network, the full set of features for Exchange Client Access are available.

Looking for more tasks related to external access? See Managing External Client Access.

Contents

Benefits of Using ISA Server 2006 with Outlook Web Access

The following table lists features in ISA Server 2006 that can help you secure your Exchange messaging environment that includes Outlook Web App.

Using ISA Server 2006 as a reverse proxy server for Outlook Web App

Feature	Description
Link Translation	ISA Server 2006 redirects Outlook Web App requests for internal URLs that are contained in the body of any object in Outlook Web App, such as an e-mail message or calendar

	entry. Users no longer have to remember the external namespaces for internal corporate information that is mapped to an external namespace. For example, if a user sends a link in an e-mail message to an internal namespace such as http://contoso, and this internal URL is mapped to an external namespace such as http://www.contoso.com, the internal URL is automatically translated into the external URL when the user clicks the internal URL.
Web Publishing Load Balancing	ISA Server 2006 can load balance client requests and send them to an array of Client Access servers. When ISA Server 2006 receives a request for a connection to Outlook Web App, it selects a Client Access server and then sends the name of the Client Access server back to the Web browser in a cookie.
HTTP Compression	In the past, if you used forms-based authentication on the ISA Server computer that had Exchange Server 2003 and ISA Server 2004 or ISA Server 2000 installed, it was not possible to use Gzip compression. This was because ISA Server could not decompress and recompress the information correctly. ISA Server 2006 can decompress, inspect, and then recompress data before it sends the data to your Exchange servers. **Note:** Gzip compression is available in ISA Server 2004, Service Pack 2 (SP2).
Exchange server locations are hidden	When you publish an application through ISA Server, you're protecting the server from direct external access because the name and IP address of the server can't be viewed by the user. The user accesses the ISA Server computer. The ISA Server computer then creates a connection to the Client Access server according to the conditions of the server publishing rule.
SSL bridging and inspection	Secure Sockets Layer (SSL) bridging protects against attacks that are hidden in SSL-encrypted connections. For SSL-enabled Web applications, after ISA Server receives the client's request, ISA Server decrypts the request, inspects it, and acts as the endpoint for the SSL connection with the client computer. The Web publishing rules determine how ISA Server communicates the request for the object to the published Web server. When you use SSL bridging, the secure Web publishing rule is configured to forward the request by using Secure HTTP (HTTPS). ISA Server then initiates a new SSL connection with the published server.

	Because the ISA Server computer has become an SSL client, it requires the published Web server to respond with a certificate. An additional advantage of SSL bridging is that an organization has to buy SSL certificates from an external certification authority only for the ISA Server computers. Servers that use ISA Server as a reverse proxy can either not require SSL or use SSL certificates that are generated internally. You can also terminate the SSL connection at the ISA Server computer and continue to the Client Access server with a connection that isn't encrypted. This is known as SSL offloading. If you do this, the internal URL for Outlook Web App must be set to use HTTP and the external URL must be set to use HTTPS. The internal URL and external URL can be configured through the Exchange Management Console, or by using the **Set-OwaVirtualDirectory** cmdlet with the *InternalURL* parameter and *ExternalURL* parameter in the Exchange Management Shell. For more information about how to use the **Set-OwaVirtualDirectory** cmdlet and the EMC to manage Outlook Web App virtual directories, see Set-OwaVirtualDirectory and Managing Outlook Web App Virtual Directories.
Single sign-on	Single sign-on enables users to access a group of published Web sites without being required to authenticate with each Web site. When you use ISA Server 2006 as a reverse proxy server for Outlook Web App, ISA Server 2006 can be configured to obtain the user's credentials and pass them to the Client Access server so that users are prompted for their credentials only one time.

For more information about ISA Server 2006 when it is used with Exchange 2010, see What's New and Improved in ISA Server 2006.

Return to top

Deployment Options

When you deploy ISA Server 2006 together with Exchange 2010, you won't have to do any additional configuration to your Exchange infrastructure. However, ISA Server 2006 can be configured in different ways to enable Exchange client access using Outlook Web App, POP3 or IMAP access, Exchange ActiveSync, and Outlook Anywhere. The configuration options depend on the authentication method that you want to use to access Exchange.

Earlier versions of ISA Server, including ISA Server 2004 and ISA Server 2000 when they are deployed with Exchange 2010, don't have the same deployment options for authentication. Additionally, if you're deploying Exchange 2010 with both ISA Server 2006 and an earlier version of ISA Server, you can use the following authentication options:

- **Basic authentication for Outlook Web App** If you plan to use Basic authentication for Outlook Web App, ISA Server 2006 and earlier versions of ISA Server should all use Web Publishing to publish Outlook Web App.
- **Client certificate authentication** If you plan to use a client certificate-based authentication method, ISA Server will automatically perform authentication on the computer that is running ISA Server. Earlier versions of ISA Server, including ISA Server 2004 and ISA Server 2000, require server publishing to use client certificate authentication. If you use client certificate authentication, you can't use ISA Server to inspect the SSL packets before they are sent to the Client Access server.

Return to top

For More Information

ISA Server Web site

ISA Server 2006 Features at a Glance

Configure Reverse Proxy Servers for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use ISA Server 2006 as a reverse proxy server for Outlook Web App.

Use ISA Server 2006 to configure a reverse proxy server for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "ISA Server 2006" entry in the Client Access Permissions topic.

1. In the ISA Server 2006 console, use the **Publish Exchange Web Client Access** wizard to publish Outlook Web App.
2. Configure ISA Server to authenticate users when they connect to the Outlook Web App virtual directories (optional).
   For more information about how to configure ISA Server, see ISA Server 2006.

If you've configured the ISA Server computer to authenticate users, it's recommended that you configure the Outlook Web App virtual directories to use either Integrated Windows authentication or Basic authentication, depending on which type of authentication is required by your organization. When you use Basic authentication or Integrated Windows authentication, users are prompted for their sign-in information only one time.

Note:
Integrated Windows authentication prohibits access to documents on Windows file shares or in Windows SharePoint Services document libraries from Outlook Web App. If you must access documents from Outlook Web App, you must use Basic authentication.

Other Tasks

After you configure a reverse proxy server for Outlook Web App, you may also want toConfigure Outlook Web App Virtual Directories to Use SSL.

Deploy ISA Server 2006 for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you deploy ISA Server 2006 for Outlook Web App, you use the New Exchange Publishing Rule wizard on the firewall policy tasks. This wizard shows you the specific settings that you must configure to enable access to Exchange.

Important:
If you have multiple versions of Exchange in your organization, you must create an Exchange publishing rule for each version that you support.

Steps

Here are the basic steps for deploying ISA Server 2006 for Outlook Web App:

Step 1: Create a new Exchange publishing rule

Step 2: Configure additional options

Step 3: Install a server certificate for ISA Server 2006

See the following sections for information about each step.

Step 1: Create a new Exchange publishing rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "ISA Server 2006" entry in the Client Access Permissions topic.

During this process, you must provide the following information:

- **Exchange publishing rule name** Provide a friendly name for your publishing rule, such as "Exchange E-mail Access".
- **Supported client access services** On the **Select Services** page, select the version of Exchange that you're deploying and the client access services that you want to support for your users. By default, when you select Exchange 2010, Outlook Web App is selected.
- **Publishing type** On the **Publishing Type** page, select an option to use

depending on whether you plan to publish a single site or an external load balancer, a Web server farm, or multiple Web sites.

- **Server connection security** This page lets you select whether to use SSL or non-secured connections from the ISA Server computer to Exchange.
- **Internal publishing details** On the **Internal Publishing Details** page, enter the internal site name of Outlook Web App or select the option to use a computer name or IP address to connect to Exchange.
- **Public name details** The **Public name details** page lets you select which domains you will accept requests from. You must also provide a public name, for example, www.contoso.com.
- **Select web listener** The **Select web listener** page lets you specify the listener for the Exchange server to which you're connecting. A listener is used to specify the authentication type that will be used when the client first contacts the ISA Server computer. The listener contains information about how the ISA Server computer accepts requests from clients, such as the encryption, compression, and authentication that's used on the external connection. You can use this page to create a new listener or edit existing listeners.
- **Authentication delegation** The **Authentication delegation** page lets you specify the type of authentication mechanism that the Client Access server should expect from ISA Server. Select from the following:
  - No delegation, but client may authenticate directly
  - Basic authentication
  - NTLM authentication
  - Negotiate (Kerberos/NTLM)
  - Kerberos constrained delegation
- **User sets** The **User sets** page lets you select which users can use this rule to connect to Exchange.

If you have configured the ISA Server computer to authenticate users, you should configure the Outlook Web App virtual directories to use either Integrated Windows authentication or Basic authentication, depending on which type of authentication is required by your organization. When you use Basic authentication or Integrated Windows authentication on the Outlook Web App virtual directories together with ISA Server 2006 authentication, users are prompted for their sign in information only one time.

Note:
If you select forms-based authentication for the ISA Server listener, the user will be prompted to reenter authentication credentials if the Outlook Web App session times out.

However, Integrated Windows authentication disallows access from Outlook Web App to documents on Windows file shares or in Windows SharePoint Services document libraries. If you must access documents from Outlook Web App, you must use Basic authentication on the Outlook Web App virtual directory.

After you complete the wizard, the wizard creates the Exchange publishing rule. The rule you create appears in the **Firewall Policy Rules** list on the **Firewall Policy** tab.

Note:
After you finish creating your publishing rule, you must wait for the settings to take effect. You can monitor ISA Server 2006 publishing rule progress by using the Monitoring node in the ISA Server 2006 Management console.

Step 2: Configure additional options (optional)

You can configure additional features, such as link translation and HTTP compression, for the new rule that you created in the ISA Server 2006 Management console. Additional settings for link translation and HTTP compression are managed under the General node

on the ISA Server 2006 Management console.

- **Configure Link Translation** To configure link translation, you must select the Exchange publishing rule that you created, and then click **Edit Selected Rule** under **Policy Editing Tasks**. On the **Link Translation** tab, you can configure link translation based on the needs of your users.
- **Configure HTTP Compression** The HTTP compression option can be configured in the General node under **Configuration** in the ISA Server 2006 Management console. Click **Define HTTP compression preferences**, and then select the options that you want to support for your users.

After you finish configuring these options, the ISA Server configuration for Exchange is complete.

Step 3: Install a server certificate for ISA Server 2006

To enable an encrypted channel by using SSL between the client computer and the ISA Server computer, you must install a server certificate on the ISA Server computer. This certificate should be issued by a public certification authority (CA) because it will be accessed by users on the Internet. If a private CA is used, the root CA certificate from the private CA must be installed on any computer that has to create an encrypted channel (HTTPS) to the ISA Server computer. Otherwise, users will receive a warning that the certificate isn't trusted.

For more information about how to install a server certificate on ISA Server 2006, see Publishing Exchange Server 2007 with ISA Server 2006.

Other Tasks

After you deploy ISA Server, you may also want to Configure Reverse Proxy Servers for Outlook Web App.

For More Information

ISA Server Web site

ISA Server 2006 Features at a Glance

1.6.2.8.1.2 Using ISA Server with Outlook Anywhere

Using ISA Server with Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-12*

This topic describes how you can use Microsoft Internet Security and Acceleration (ISA) Server 2006 with Outlook Anywhere. We recommend that you use ISA Server 2006 for all available client access methods in Microsoft Exchange Server 2010. When you publish Outlook Anywhere client access with ISA Server 2006, communications from the Outlook clients located on the Internet to the ISA Server computer and from the ISA Server

computer to the Client Access server are encrypted using Secure Sockets Layer (SSL).

In many organizations, users need to have access to their mailbox when they're away from the office. Outlook Anywhere ensures that users can interact with their Exchange information from any location. To support this client access method, specific paths must be published on the ISA Server computer.

Looking for management tasks related to Outlook Anywhere? See Managing Outlook Anywhere.

Contents

Exchange 2010 Services Used with ISA Server 2006

The following table lists the Exchange services that are supported by ISA Server 2006 for Exchange 2010 and used by Outlook Anywhere clients.

Exchange 2010 services used with ISA Server 2006

Feature	Path	Description
Outlook Anywhere	/rpc/*	Internet-based access to an Exchange deployment by using RPC over HTTP or RPC over HTTPS.
Unified Messaging	/unifiedmessaging/*	Exchange 2010 Unified Messaging puts all e-mail, voice mail, and fax messages into one Exchange 2010 mailbox that can be accessed from a variety of devices.
Offline Address Book	/OAB/*	An offline address book (OAB) is a copy of an address book that's been downloaded so that an Outlook user can access address book information while disconnected from the server.
Exchange Web Services	/ews/*	This virtual directory is used for the Autodiscover service and the Availability service to provide free/busy information.
Autodiscover	/Autodiscover/*	The Autodiscover service provides access to Exchange

		features for Microsoft Office Outlook 2007 clients that are connected to your Exchange messaging environment.

Return to top

ISA Server 2006 Features for Outlook Anywhere Client Access

The following table describes several of the benefits of using ISA Server 2006 to protect client access to your Exchange deployment using Outlook Anywhere.

ISA Server 2006 features for Outlook Anywhere

Feature	Description	More information
Exchange server locations are hidden	When you publish an application through ISA Server, you're protecting the server from direct external access because the name and IP address of the server can't be accessed by the user. The user accesses the ISA Server computer. This computer forwards the request to the server according to the conditions of the server publishing rule.	Publishing Exchange Server 2007 with ISA Server 2006
SSL Bridging and Inspection	SSL bridging protects against attacks that are hidden in SSL-encrypted connections. For SSL-enabled Web applications, after ISA Server receives the client's request, ISA Server decrypts it, inspects it, and ends the SSL connection with the client computer. The Web publishing rules determine how ISA Server communicates the request for the object to the published Web server. If the secure Web publishing rule is configured to forward the request by using secure HTTP (HTTPS), ISA Server initiates a new SSL connection with the published server. Because the ISA Server computer is now an SSL client, it requires the published Web server to respond with a server-side certificate.	Best Practices for Performance in ISA Server 2006

Return to top

ISA Server 2006 Deployment Options for Outlook Anywhere

Before you deploy ISA Server 2006 to help secure communication from Outlook Anywhere clients on the Internet to Exchange Client Access servers, you must verify that you've correctly configured your Exchange deployment to support Outlook Anywhere clients. You will then run the Exchange Publishing Rule wizard to provide Outlook Anywhere access to your Exchange deployment.

Install a Server Certificate for ISA Server 2006

To enable an encrypted channel by using SSL between the client computer and the ISA Server computer, you must install a server certificate on the ISA Server computer. This certificate should be issued by a public certification authority (CA) because it will be accessed by users on the Internet. If a private CA is used, the root CA certificate from the private CA must be installed on any computer that must create an encrypted channel (HTTPS) to the ISA Server computer.

For more information about how to install a server certificate on ISA Server 2006, see Publishing Exchange Server 2007 with ISA Server 2006.

Return to top

How to Deploy ISA Server 2006 for Outlook Anywhere

You can run the Exchange Publishing Rule wizard to provide Outlook Anywhere access to your Exchange deployment by following these steps:

1. **Create a server farm (optional)** When you have more than one Exchange Client Access server, you can use ISA Server to provide load balancing for these servers. The server farm properties determine the following:
   - Servers that are included in the farm
   - Connectivity verification method that ISA Server will use to verify that the servers are functioning
2. **Create a Web listener** When you create a Web publishing rule, you must specify a Web listener to use. The Web listener properties determine the following:
   - IP addresses and ports on the specified networks that the ISA Server computer uses to listen for Web requests (HTTP or HTTPS)
   - Server certificates to use with IP addresses
   - Authentication method to use
   - Number of concurrent connections that are allowed
   - Single sign-on (SSO) settings
3. **Create an Exchange Web client access publishing rule** When you publish an internal Exchange 2010 Client Access server through ISA Server 2006, you protect the Web server from direct external access because the name and IP address of the server can't be accessed by the user. The user accesses the ISA Server computer. The ISA Server computer forwards the request to the internal Web server according to the conditions of your Web server publishing rule. An Exchange Web client access publishing rule is a Web publishing rule that contains default settings appropriate to Exchange client access.

For more information about how to use the Exchange Publishing Rule wizard, see

Publishing Exchange Server 2007 with ISA Server 2006.

Return to top

1.6.2.8.1.3 Using ISA Server with Exchange ActiveSync

Using ISA Server with Exchange ActiveSync

Managing Client Access Servers > Managing External Client Access > Configuring External Client Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-12*

We recommend that you use Microsoft Internet Security and Acceleration (ISA) Server 2006 to enhance the security of all available client access methods in your Microsoft Exchange Server 2010 deployment. When you configure Microsoft Exchange ActiveSync client access with ISA Server 2006, communications between the Exchange ActiveSync clients and the Exchange server computer pass through an ISA Server computer to add an additional layer of Secure Sockets Layer (SSL) encryption.

Exchange ActiveSync enables information workers to access their Microsoft Exchange messaging data using a mobile device. For more information about Exchange ActiveSync, see the following topics:

- Understanding Exchange ActiveSync
- Managing Exchange ActiveSync

Benefits of Using ISA Server 2006 with Exchange ActiveSync

The following table describes several of the benefits of using ISA Server 2006 to protect client access through Outlook Anywhere to your Exchange deployment.

ISA Server 2006 features for Exchange ActiveSync

Feature	Description
Exchange server locations are hidden	When you publish an application through ISA Server, you are protecting the server from direct external access because the name and IP address of the server can't be viewed by the user. The user accesses the ISA Server computer. The ISA Server computer then forwards the request to the server according to the conditions of the server publishing rule.
SSL Bridging and Inspection	SSL bridging protects against attacks that are hidden in SSL-encrypted connections. For SSL-enabled Web applications, after ISA Server receives the client's request, ISA Server decrypts it, inspects it, and ends the SSL connection with the client computer. The Web publishing rules determine how ISA Server communicates the request for the

	object to the published Web server. If the secure Web publishing rule is configured to forward the request using Secure HTTP (HTTPS), ISA Server initiates a new SSL connection with the published server. Because the ISA Server computer is now an SSL client, it requires the published Web server to respond with a server-side certificate.

ISA Server 2006 Deployment Prerequisites for Exchange ActiveSync

When you deploy ISA Server 2006 to help secure communication from Exchange ActiveSync clients on the Internet to Exchange 2010 computers that have the Client Access server role installed, we recommend that you confirm the following:

- Forms based authentication isn't configured on the Exchange Client Access server. When ISA Server 2006 is being used to publish Exchange client access, we recommend forms-based authentication be configured only on the ISA Server computer.
- A server certificate is installed on the Exchange Client Access server. This certificate can be from an internal certification authority (CA) or a public CA.
- SSL is required on all Exchange Client Access virtual directories.

After you confirm these settings, you can configure ISA Server 2006 to provide Exchange ActiveSync access for your clients.

How to Deploy ISA Server 2006 for Exchange ActiveSync

To enable an encrypted channel between the client computer and the ISA Server computer, you first have to install a server certificate on the ISA Server computer. This certificate should be issued by a public CA because it will be accessed by users on the Internet. If a private CA is used, the root certificate from the private CA must be installed on any computer that requires a secure (HTTPS) connection to the ISA Server computer.

For more information about how to install a server certificate on ISA Server 2006, see Publishing Exchange Server 2007 with ISA Server 2006.

After a server certificate is installed on the ISA Server computer, you can run the New Exchange Publishing Rule Wizard. Running the New Exchange Publishing Rule Wizard to provide Exchange ActiveSync access involves the following steps:

1. **Create a server farm (optional)** When you have more than one Client Access server within your organization, you can use ISA Server to provide load balancing for these servers. The server farm properties determine the following:
   - The specific servers included in the farm.
   - The connectivity verification method that ISA Server will use to verify that the servers are functioning correctly.
2. **Create a Web listener** When you create a Web publishing rule, you must specify a Web listener. The Web listener properties determine the following:
   - The IP addresses and ports on the specified networks the ISA Server computer uses to listen for Web requests (HTTP or HTTPS).
   - Which server certificates to use with IP addresses.
   - The authentication method to use.

- The number of concurrent connections allowed.
- Single sign-on (SSO) settings.

3. **Create an Exchange Web client access publishing rule** When you publish an internal Exchange 2010 Client Access server through ISA Server 2006, you are protecting the Web server from direct external access because the name and IP address of the server can't be viewed by the user. The user accesses the ISA Server computer. The ISA Server computer then forwards the request to the internal Web server according to the conditions of your Web server publishing rule. An Exchange Web client access publishing rule is a Web publishing rule that contains default settings appropriate to Exchange client access.

For more information about how to use the New Exchange Publishing Rule Wizard, see Microsoft ISA Server 2006.

1.6.2.8.1.4 Using ISA Server with POP3 and IMAP4

Using ISA Server with POP3 and IMAP4

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

You can use Microsoft Internet Security and Acceleration (ISA) Server 2006 with POP3 and IMAP4. We recommend that you use ISA Server 2006 for all your client-to-server connections in Microsoft Exchange Server 2010. When you publish POP3 and IMAP4 client access with ISA Server 2006, communications from the POP3 or IMAP4 clients that are located on the Internet to the ISA Server computer and from the ISA Server computer to the Client Access server are encrypted by using Secure Sockets Layer (SSL).

ISA Server 2006 Features for POP3 and IMAP4 Access

The following table describes several benefits of using ISA Server 2006 to protect POP3 and IMAP4 client access to your Exchange deployment. The links in the "More information" column of the table also apply when you're using ISA Server 2006 with Exchange 2010.

ISA Server 2006 benefits for POP3 and IMAP4

Feature	Description	More information
Exchange server locations are hidden	When you publish an application through ISA Server, you're protecting the server from direct external access, because the name and IP address of the server can't be accessed by the user. The user accesses the ISA Server computer. This computer forwards the request to the Exchange server according to the conditions of the server	Publishing Exchange Server 2007 with ISA Server 2006

	publishing rule.	
SSL bridging and inspection	SSL bridging protects against attacks that are hidden in SSL-encrypted connections. For SSL-enabled Web applications, after ISA Server receives the client's request, ISA Server decrypts it, inspects it, and then ends the SSL connection with the client computer. The Web publishing rules determine how ISA Server communicates the request for the object to the published Web server. If the secure Web publishing rule is configured to forward the request by using secure HTTP (HTTPS), ISA Server initiates a new SSL connection with the published server. Because the ISA Server computer is now an SSL client, it requires the published Web server to respond with a server-side certificate.	Best Practices for Performance in ISA Server 2006

Install a Server Certificate for ISA Server 2006

To enable an encrypted channel using SSL between the client computer and the ISA Server computer, you must install a server certificate on the ISA Server computer. This certificate should be issued by a public certification authority (CA) because it will be accessed by users on the Internet. If a private CA is used, the root certificate from the private CA must be installed on any computer that has to create an encrypted channel (HTTPS) to the ISA Server computer.

For more information about how to install a server certificate on ISA Server 2006, see Publishing Exchange Server 2007 with ISA Server 2006. This information also applies to installing a server certificate on ISA Server 2006 when you're using Exchange 2010.

How to Deploy ISA Server 2006 for POP3 and IMAP4

You can run the Exchange Publishing Rule Wizard to provide POP3 and IMAP4 access to your Exchange deployment by following these steps:

1. **Create a server farm (optional)** When you have more than one Exchange Client Access server, you can use ISA Server to provide load balancing for these servers. The settings you configure allow you to specify the following:
   - The servers that are included in the server farm.
   - The connectivity verification method that ISA Server will use to confirm that the servers are functioning.

2. **Create a Web listener** When you create a Web publishing rule, you must specify a Web listener to use. The settings you configure allow you to specify the following:
   - IP addresses and ports on the specified networks that the ISA Server computer uses to listen for Web requests (HTTP or HTTPS).
   - Server certificates to use with IP addresses.
   - The authentication method to use.
   - The number of concurrent connections that are allowed.
   - Single sign-on settings.
3. **Create an Exchange Web client access publishing rule** When you create an Exchange Web client access publishing rule, you protect the Web server from direct external access because the Web server name and IP address are hidden from the user. The user accesses Exchange through the ISA Server computer. The ISA Server computer forwards the request to the internal Web server according to the conditions of your Web server publishing rule. An Exchange Web client access publishing rule is a Web publishing rule that contains default settings appropriate to Exchange Client Access.

For more information about how to use the New Exchange Publishing Rule Wizard, see Publishing Exchange Server 2007 with ISA Server 2006. This information also applies to publishing Exchange 2010 with ISA Server 2006.

1.6.2.8.1.5 Configure External Client Access Namespaces

Configure External Client Access Namespaces

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-05-19*

When a user has synchronized a mobile phone with their mailbox, the Manage Mobile Device wizard lets you view and manage the mobile phones for that user.

Looking for other management tasks related to Client Access namespaces? Check out Managing External Client Access.

Prerequisites

The Client Access server role has been installed.

What Do You Want to Do?

- Use the EMC to configure external Client Access namespaces
- Use the Shell to configure external Client Access namespaces

Use the EMC to configure external Client Access namespaces

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.

2. In the action pane, click **Configure External Client Access Domain** to open the **Configure External Client Access Domain** wizard.
   - This wizard helps you associate an external DNS address with one or more Client Access servers. The `ExternalURL` property for all services is configured when an external Client Access domain is specified.
3. On the **Configure External Client Access Domain** page, enter the domain name you'll use with your external Client Access servers.
4. Click **Add** to select the Client Access servers that will be associated with this *ExternalURL*.

5. Click **Configure** to complete the **Configure External Client Access Domain** wizard.

Use the Shell to configure external Client Access namespaces

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server settings" entry in the Client Access Permissions topic.

These examples configure the `ExternalURL` property for each Client Access method. Each of these configuration changes is necessary to duplicate the functionality of the **Configure External Client Access Namespace** wizard.

The following example configures the `ExternalURL` property for Exchange ActiveSync virtual directory.

```
Set-ActivesyncVirtualDirectory -Identity "CAS_Server_Name\Microsoft-Server-Active
```

The following example configures the `ExternalURL` property for the Outlook Web App virtual directory.

```
Set-OwaVirtualDirectory -Identity "CAS_Server_Name\OWA (Default Web Site)" -Exter
```

The following example configures the `ExternalURL` property for the Outlook Address Book virtual directory.

```
Set-OABVirtualDirectory -Identity "CAS_Server_name\oab (Default Web Site)" -Exter
```

The following example configures the `ExternalURL` property for the Exchange Web Services virtual directory.

```
Set-WebServicesVirtualDirectory -Identity "CAS_Server_Name\EWS (Default Web Site)
```

The following example configures the `ExternalURL` property for the Outlook Anywhere virtual directory.

```
Enable-OutlookAnywhere -Server CAS01 -ExternalHostname "mail.contoso.com" -Extern
```

For More Information

View or Configure Exchange ActiveSync Virtual Directory Properties

View or Configure Outlook Web App Virtual Directories

Understanding Client Access Server Namespaces

Understanding Client Access Server Publishing

1.6.2.9 Maximum Client Access Service Sessions Per User

Maximum Client Access Service Sessions Per User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-22*

For optimal performance, there is a maximum number of concurrent sessions that a Client Access server can support. Microsoft Exchange Server 2010 imposes limits on the number of concurrent service sessions per user. The limits are set in several different ways. For some client interactions, limits are set for the maximum number of concurrent threads per server or the maximum number of sessions per server. For other client interactions, the limits are set for the maximum number of user sessions per server. Limits are set to improve performance, to prevent users from being locked out of e-mail access, and to prevent service disruption.

Session Limits by Client Type

The following table lists the maximum number of service sessions that are allowed per user for the different client types and services in Exchange 2010.

Client type	Maximum user sessions per server
Exchange ActiveSync	16
Availability Service	16
Exchange Web Services	16
Exchange Management Console	16
RPC Client Access	32
Outlook Web App	16
POP3/IMAP4	16
Unified Messaging	16

1.6.2.10 Using Kerberos with a Client Access Server Array or a Load-Balancing Solution

Using Kerberos with a Client Access Server Array or a Load-Balancing Solution

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-07*

For Microsoft Exchange Server 2010 deployments that have more than one Client Access

server in an Active Directory site, the topology will often require a Client Access server array and a load-balancing solution to distribute traffic among all Client Access servers in the site. For more information about Client Access server arrays, see Understanding RPC Client Access. For more information about load balancing, see Understanding Load Balancing in Exchange 2010.

Using Kerberos Authentication

Typically, mail clients on domain-joined computers inside your network use NTLM authentication. In some circumstances, you might have to use Kerberos authentication. This should only be done if it's required, because Kerberos presents additional challenges in setup and implementation. For more information about Kerberos, see Kerberos Enhancements and Microsoft Kerberos.

Note:

Kerberos can only be used for domain-joined computers inside your network. This includes clients connected by a VPN. For connections outside the network, such as Outlook Anywhere, Kerberos isn't supported.

You may be required to use Kerberos authentication for your Exchange 2010 organization for the following reasons:

- Kerberos authentication is necessary for your local security policy.
- You're encountering or anticipating NTLM scalability issues, for example, when direct MAPI connectivity to the RPC Client Access service causes intermittent NTLM failures.
  In large-scale customer deployments, NTLM can cause bottlenecks on Client Access servers that can result in sporadic authentication failures. Services that use NTLM authentication are more sensitive to Active Directory latency issues. These lead to authentication failures when increases in the rate of Client Access server requests are encountered.

To configure Kerberos authentication, you must be familiar with Active Directory and the setup of Client Access server arrays. And you must have a working knowledge of Kerberos.

Problems with Kerberos and Load-Balanced Client Access Servers

When Client Access servers are load-balanced or are part of a Client Access server array, clients configured with NTLM authentication will connect without a problem. However, using Kerberos requires additional setup and was problematic prior to Exchange 2010 Service Pack 1 (SP1).

In a topology with a load balancer or a Client Access array, a client doesn't connect to an individual server by name, but rather by the array or load balancer name. This impedes Kerberos authentication unless you perform additional configuration steps.

When you use Kerberos, the first configuration step is to set up an array of specific Service Principal Names (SPNs) for the client access services. As soon as the array is set up, e-mail clients that are configured to use Negotiate authentication will try to perform Kerberos authentication. They'll obtain Kerberos service tickets in the context of the array and present those tickets to the Client Access server. However, on any particular Client Access server, Exchange services run in the context of either the local system or network service account and will try to authenticate the Kerberos service tickets in those contexts, rather than in the context of the array. This causes a context mismatch and results in a Kerberos authentication failure. Because of the enhanced security of Kerberos, clients configured to perform Negotiate authentication won't just fall back to NTLM

authentication, but will either default to using Outlook Anywhere, if available, or fail to authenticate and connect.

For Kerberos authentication to succeed, the Client Access server array member must use an alternate credential that's shared by all members of the array. The credential must also be associated with the array-specific SPNs. This shared credential may be either a computer account or a service account and must be known by every Client Access server within the array. Typically, organizations require that account passwords change periodically. This mandates an ongoing task of distributing and updating this shared credential to all Client Access servers. Before Exchange 2010 SP1, neither Windows Server 2008 nor Microsoft Exchange had a solution for this issue.

Note:

Although this discussion refers to a network load balancer and a Client Access server array, any network infrastructure or configuration that doesn't result in the client connecting directly to a specific Client Access server will have these same authentication issues. Other examples of this configuration include Client Access servers with DNS round-robin load balancing and Client Access servers with custom DNS records. The following solution is designed to simplify distribution of the alternate service account credential to members of a Client Access server array or Client Access servers behind a network load balancer. It's not designed to work with configurations where the Client Access servers aren't configured in a Client Access array.

The Solution

To resolve this problem, there must be a shared credential that can be used by all Client Access servers in the array or behind the load balancer. This credential is known as an *alternate service account credential* (ASA credential) and can be either a computer or a user service account. To distribute this alternate service account credential to all Client Access servers, a three-fold solution has been implemented in Exchange 2010 SP1.

The Client Access server service host has been extended to use a shared credential for Kerberos authentication. This service host extension monitors the local machine. When credentials are added or removed, the Kerberos authentication package on the local system and the network service context is updated. As soon as a credential is added to the authentication package, all client access services can use it for Kerberos authentication. The Client Access server will also be able to authenticate service requests addressed directly in addition to being able to use the shared credential. This extension, known as a *servicelet*, runs by default and requires no configuration or action to run.

The shared credential and password can be obtained and set using the Exchange Management Shell. This enables the credential to be set from a remote computer. The credential is set by storing the credential in the target computer's registry for consumption by the service host. You set the credential using the **Set-ClientAccessServer** cmdlet with the new *AlternateServiceAccountCredential* parameter. After the shared credential password has been set, the shared credential allows Client Access services to perform Kerberos authentication for Intranet connected clients. For more information about the **Set-ClientAccessServer** cmdlet, see Set-ClientAccessServer.

A management script has been created to help automate the distribution of the shared credential to all Client Access servers specified within the scope of the script. This script is the recommended way to use and maintain a shared credential for client Access server array Kerberos authentication. The script provides an automated way to use the **Set-ClientAccessServer** cmdlet to facilitate the following tasks:

- **Initial Setup** The ASA credential is set on all Client Access servers within an array or forest.
- **Password Rollover** A new password for the ASA credential is generated and rolled out to all Client Access servers in addition to updating Active Directory.
- **Adding one or more computers to a Client Access server array** The ASA

credential is copied from an existing server and distributed to other servers so they can perform Kerberos authentication with the current credential and password.

- **Ongoing maintenance** A scheduled task is created to regularly roll the password by using an unattended method.

For More Information

For more information about how to configure Kerberos authentication for load-balanced Client Access servers, see Configuring Kerberos Authentication for Load-Balanced Client Access Servers.

For more information about the RollAlternateServiceAccountCredential.ps1 script, see Using the RollAlternateserviceAccountPassword.ps1 Script in the Shell.

1.6.2.10.1 Configuring Kerberos Authentication for Load-Balanced Client Access Servers

Configuring Kerberos Authentication for Load-Balanced Client Access Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-07*

To use Kerberos authentication with a load-balanced array of Client Access servers, several configuration steps must be completed. For more information about how to use Kerberos with a Client Access server array or a load-balancing solution, see Using Kerberos with a Client Access Server Array or a Load-Balancing Solution.

Create the Alternate Service Account Credential in Active Directory

All computers within the Client Access server array must share the same service account. In addition, any Client Access servers that may be called on in a datacenter activation scenario must also share the same service account. In general, it's sufficient to have a single service account per forest. This account is referred to as the alternate service account credential (ASA credential).

Note:

If your deployment is complex and extends beyond the scenarios outlined below, has administrator delegation issues, or has multiple forest segments on different Exchange deployment schedules, you may have to create additional accounts. The **RollAlternateServiceAccountPasswordl**.ps1 script must be run separately for every account created.

Credential Type

You can create a computer account or a user account for the alternate service account. Because a computer account doesn’t allow interactive logon, it may have simpler security policies than a user account and therefore is the preferred solution for the ASA credential. If you create a computer account, the password doesn't actually expire, but we still recommend updating the password periodically. Local group policy can specify a maximum account age for computer accounts and there might be scripts scheduled to periodically delete computer accounts that do not meet current policies. Periodically updating the

password for computer accounts will ensure that your computer accounts aren't deleted for not meeting local policy. Your local security policy will determine when the password needs to be changed.

Credential Name

There are no particular requirements for the name of the ASA credential. You can use any name that conforms to your naming scheme.

Groups and Roles

The ASA credential doesn't need special security privileges. If you are deploying a computer account for the ASA credential this means that the account only needs to be a member of the Domain Computers security group. If you are deploying a user account for the ASA credential, this means that the account only needs to be a member of the Domain Users security group.

Password

The password you provide when you create the account will never actually be used. Instead, the script will reset the password. So when you create the account, you can use any password that conforms to your organization's password requirements.

Cross-Forest Scenarios

If you have a cross-forest or resource-forest deployment, and users are outside the Active Directory forest that contains Exchange, you must configure cross-forest trusts and routing name suffixes across forests. For more information, see Accessing Resources Across Forests and Routing Name Suffixes Across Forests.

Identifying the Service Principal Names That Should Be Associated with the Alternate Service Account Credential

After you create the alternate service account, you must determine the Exchange service principal names (SPNs) that will be associated with the ASA credentials. The list of Exchange SPNs may vary with your configuration, but should include at least the following.

- **http** Use this SPN for Exchange Web Services, Offline Address Book downloads, and the Autodiscover service.
- **exchangeMDB** Use this SPN for RPC Client Access.
- **exchangeRFR** Use this SPN for the Address Book service.
- **exchangeAB** Use this SPN for the Address Book service.

The SPN values must be configured to match the service name being used on the network load balancer, rather than on individual servers.

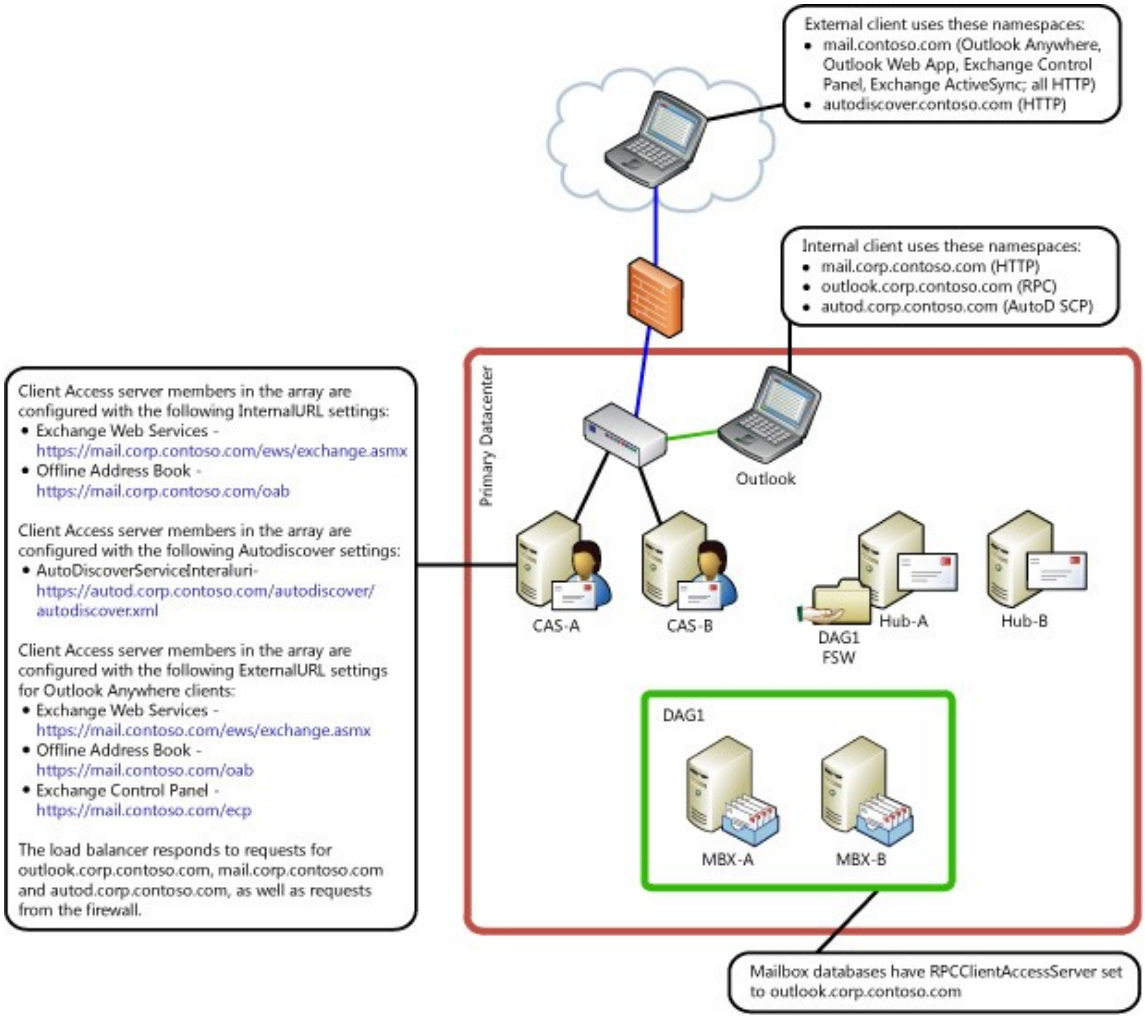
To help plan which SPN values you should deploy, consider the following conceptual scenarios:

1. Single Active Directory Site
2. Multiple Active Directory Sites
3. Multiple Active Directory Sites with DAG Site Resiliency

In each of these scenarios, it's assumed that load-balanced fully qualified domain names have been deployed for the Internal URLs, External URLs, and Autodiscover Internal URI used by the Client Access server members. For more information see Understanding Proxying and Redirection.

Single Active Directory Site

If you have a single Active Directory site, your environment may resemble the one in the following illustration.



Based on the fully qualified domain names that are used by the internal Outlook clients in the previous illustration, the following SPNs would need to be deployed on the ASA credential:

- http/mail.corp.contoso.com
- http/autod.corp.contoso.com
- exchangeMDB/outlook.corp.contoso.com
- exchangeRFR/outlook.corp.contoso.com
- exchangeAB/outlook.corp.contoso.com

External or Internet-based clients that use Outlook Anywhere won't use Kerberos authentication. Therefore, the fully qualified domain names that are used by these clients don't have to be added as SPNs to the ASA credential.

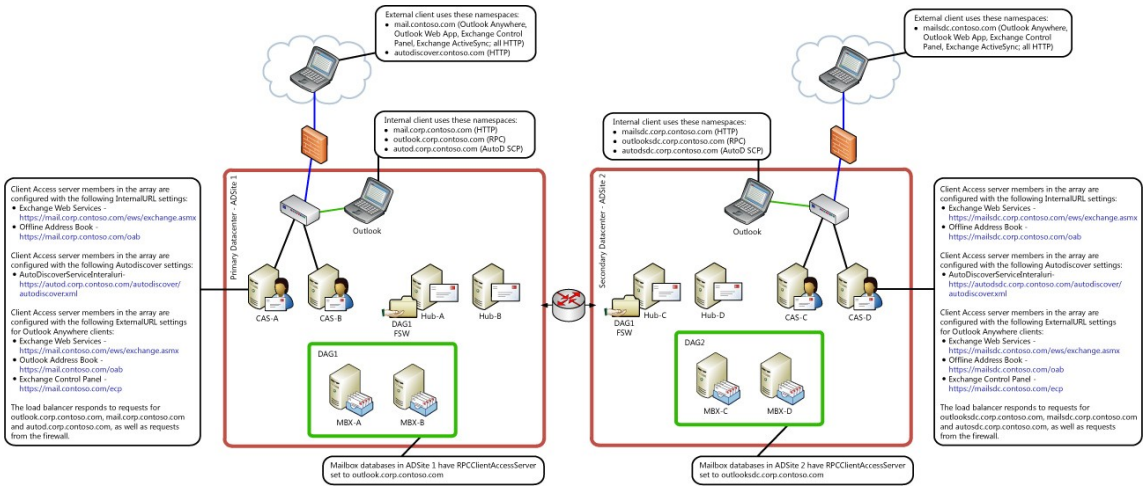
Important:

If you deploy a split DNS infrastructure, external and internal clients use the same fully qualified domain names and those names must be represented as SPNs on the ASA credential.

Multiple Active Directory Sites

If you have multiple Active Directory sites, your environment may resemble the one in the

following illustration.



Based on the fully qualified domain names that are used by the internal Outlook clients in the previous illustration, the following SPNs would have to be deployed on the ASA credential that's used for the Client Access server array with the Active Directory site ADSite1:

- http/mail.corp.contoso.com
- http/autod.corp.contoso.com
- exchangeMDB/outlook.corp.contoso.com
- exchangeRFR/outlook.corp.contoso.com
- exchangeAB/outlook.corp.contoso.com

Based on the fully qualified domain names that are used by the internal Outlook clients in the previous illustration, the following SPNs would need to be deployed on the ASA credential that's used for the Client Access server array within the Active Directory site ADSite2:

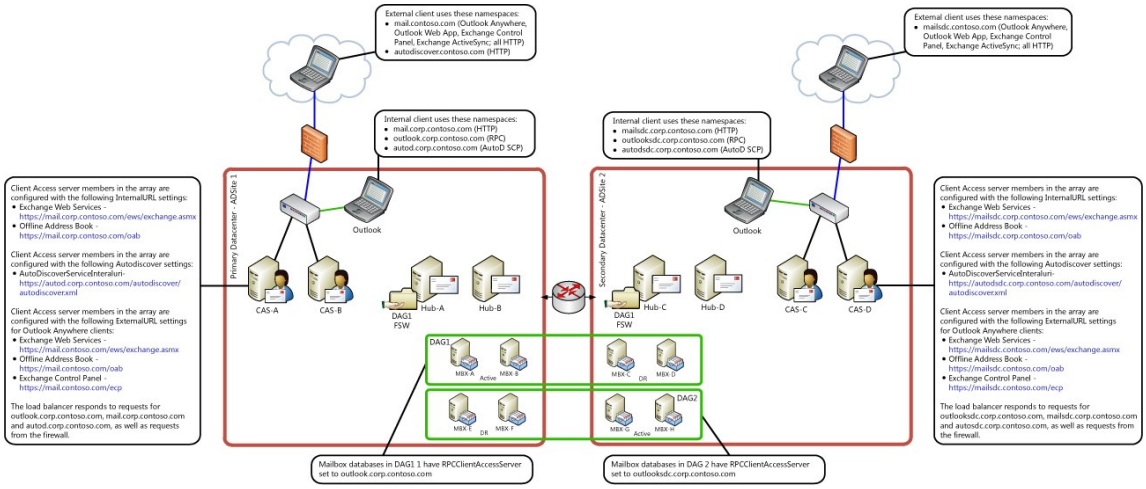
- http/mailsdc.corp.contoso.com
- http/autodsdc.corp.contoso.com
- exchangeMDB/outlooksdc.corp.contoso.com
- exchangeRFR/outlooksdc.corp.contoso.com
- exchangeAB/outlooksdc.corp.contoso.com

Note:

This example shows that you can use multiple ASA credentials for this particular scenario. However, you can use a single ASA credential for all Active Directory sites that host Client Access server arrays where you want to deploy Kerberos authentication.

Multiple Active Directory Sites with DAG Site Resiliency

If you have multiple Active Directory sites with DAG site resiliency, your environment may resemble the one in the following illustration.



Because this architecture includes a Database Availability Group (DAG) that's stretched across both Active Directory sites, you must deploy a single ASA credential for use by members of the Client Access server arrays in ADSite1 and ADSite2. If you don't use a single ASA credential, clients will have Kerberos authentication issues when you perform a datacenter switchover because the secondary datacenter Client Access server array members won't be able to decrypt the Kerberos session ticket. For more information about activating the secondary datacenter, see Datacenter Switchovers.

Based on the fully qualified domain names that are used by the internal Outlook clients in the previous illustration, the following SPNs would need to be deployed on the ASA credential that's in use for the Client Access server arrays in ADSite1 and ADSite2:

- http/mail.corp.contoso.com
- http/autod.corp.contoso.com
- exchangeMDB/outlook.corp.contoso.com
- exchangeRFR/outlook.corp.contoso.com
- exchangeAB/outlook.corp.contoso.com
- http/mailsdc.corp.contoso.com
- http/autodsdc.corp.contoso.com
- exchangeMDB/outlooksdc.corp.contoso.com
- exchangeRFR/outlooksdc.corp.contoso.com
- exchangeAB/outlooksdc.corp.contoso.com

Convert the Offline Address Book Virtual Directory to an Application

Out of the box, the Offline Address Book virtual directory isn't a Web application, so it isn't controlled by the Microsoft Exchange Service Host service. Therefore, Kerberos authentication requests to the Offline Address Book virtual directory can't be decrypted by the ASA credential.

To convert the Offline Address Book virtual directory to a Web application, run the **ConvertOABDir.ps1** script on each Client Access server member. The script will also create a new application pool for the Offline Address Book virtual directory. The script is located in the Exchange 2010 SP2 Scripts directory, or you can download the script here.

Deploying the Alternate Service Account Credential

After you've created the ASA credential, verify the account has replicated to all domain controllers within all Active Directory sites that contain the client Access servers that will use the ASA credential.

You can then run the AlternateServiceAccount credential script in the Exchange Management Shell. For more information, see Using the RollAlternateserviceAccountPassword.ps1 Script in the Shell. After the script has run, we recommend that you verify that all the targeted servers have been updated correctly.

Note:
The script is provided in English only.

For help troubleshooting script errors, see Troubleshooting the RollAlternateServiceAccountCredential.ps1 Script.

The following example output of the RollAlternateServiceAccountPassword.ps1 script uses a computer account that's created as the ASA credential. The account is named contoso/newSharedServiceAccountName. In the following example, the script applies the credential settings to each member of a Client Access server array called outlook.corp.contoso.com.

To run the script, use the following command.

```
RollAlternateServiceAccountPassword.ps1 -ToArrayMembers outlook.corp.contoso.com
```

You should receive the following output after you run the script. There's one prompt that asks you for approval to change the password.

```
========== Started at 08/02/2010 15:48:09 ==========Destination servers that will
```

You'll also see two Event IDs in your event logs. One event is for the start of the script and one is for successful completion. The following is an excerpt from the successful completion event.

```
Log Name:      ApplicationSource:        MSExchange Management ApplicationEvent I
```

Verifying the Deployment of the ASA Credential

In the Exchange Management Shell, run the following command to check the settings on the Client Access servers.

```
Get-ClientAccessServer -IncludeAlternateServiceAccountCredentialStatus | fl name,
```

The result of this command should look like the following.

```
Name                                  : CASAAlternateServiceAccountConfiguration :
```

If you've run the script several times and made changes, the Previous entry will show you when the last change was made.

```
Name                                  : NAE14CASAlternateServiceAccountConfigurati
```

Associating Service Principal Names with the Alternate Service Account Credential

Before you configure the SPNs, verify that the target SPNs aren't already configured on a different account in the forest. The ASA credential must be the only account in the forest with which these SPNs are associated. You can verify that no other account in the forest

has the SPNs associated with it by running the **setspn** command with the *–q* and *–f* parameters from the command line. The following example shows how to run this command. The command should return nothing. If it returns a value, another account is already associated with the SPN you're thinking of using.

Note:

Only Windows Server 2008 supports the duplicate-checking forest wide parameter *(-f)* in the **setspn** command.

```
Setspn -q -f exchangeMDB/outlook.corp.contoso.com
```

The following command provides an example of how to set the SPNs on the shared ASA credential. The setspn command with this syntax must be run once for every target SPN that you identify.

```
Setspn -S exchangeMDB/outlook.corp.contoso.com contoso\newSharedServiceAccountNam
```

When you've set the SPNs, verify that they've been added by using the following command.

```
Setspn -L contoso\newSharedServiceAccountName$
```

Validating Exchange Client Kerberos Authentication

After you've successfully configured Kerberos and deployed the RollAlternateServiceAccountPasswordI.ps1 script, verify that clients can authenticate successfully.

Verifying that the Microsoft Exchange Service Host Service is Running

The Microsoft Exchange Service Host service on the Client Access servers is responsible for managing the ASA credential. If this service isn't running, Kerberos authentication won't be possible. By default, the service is configured to automatically start when the computer is started. Ensure that you've installed Exchange Server 2010 SP1 Rollup 3 or a later version on all Client Access servers in your environment.

Validating Authentication from Outlook

To ensure that Outlook is able to connect to the Client Access servers with Kerberos authentication, follow these steps:

1. Confirm that Outlook is configured to point to the correct load-balanced Client Access server array.
2. Configure the e-mail account server security settings to use logon network security **Negotiate Authentication**. Or, you could configure the client to use **Kerberos Password Authentication**. However, if the SPNs are ever removed, the clients won't be able to authenticate until you change the authentication mechanism back to **Negotiate Authentication**.
3. Confirm that Outlook Anywhere isn't enabled for the client. If Outlook fails to authenticate by using Kerberos, it will try to fall back to Outlook Anywhere, so Outlook Anywhere should be disabled for this test.
4. Restart Outlook.
5. If your desktop computer is running Windows 7, you can run **klist.exe** to see which Kerberos tickets have been granted and are in use. If you're not running Windows 7, you can obtain klist.exe from the Windows Server 2003 Resource Kit.

Validating Using the Test-OutlookConnectivity Cmdlet

To test whether Kerberos is working, use the **Test-OutlookConnectivity** cmdlet. This is the best way to see if TCP connectivity can be established. By default, the cmdlet will use

Negotiate authentication for a TCP connection. So if Kerberos is configured, it will be used. The file klist.exe can be used to view the Kerberos tickets on the computer. This can be run from the Client Access server itself, as well as from an automated monitoring tool such as SCOM. When using the **Test-OutlookConnectivity** cmdlet, ensure that the Mailbox database has the **RPCClientAccessServer** property set to the Client Access server array name. Otherwise the cmdlet won't test the shared ASA credential functionality.

```
Test-OutlookConnectivity -Identity administrator -MailboxCredential $c -Protocol
```

To make sure that the connection is made using Kerberos, view klist.exe to see if there are Kerberos tickets associated with the new SPNs that were added.

Validating Kerberos from the Client Access Server

To confirm that Kerberos is working correctly from the Client Access server, you can examine the protocol logs to verify successful Kerberos connections. You can use these logs in addition to the other validations to confirm that Kerberos is being used.

- On the Client Access server, examine the Address Book protocol logs. These logs are typically located at the following path: C:\Program Files\Microsoft \Exchange server\v14\Logging\AddressBook Service.
- Examine the latest log file and look for the word Kerberos after the script has been run. If you see Kerberos traffic, a connection has been made successfully. The line in the log file should look something like the following.

```
2010-06-11T22:58:49.799Z,9,0,/o=First Organization/ou=Exchange Administ
```

If you see the word Kerberos, then the server is successfully creating Kerberos authenticated connections. For more information about the Address Book service log, see Understanding the Address Book Service.

Troubleshooting Authentication Failures

There are several common problems that may occur when you're configuring Kerberos authentication.

Outlook Clients Configured to use Kerberos Authentication Only Can't Connect

If your Outlook client that's configured to use only Kerberos authentication can't connect, follow these troubleshooting steps:

1. Configure Outlook to use NTLM authentication only, and then verify connectivity. If a connection can't be made, verify that the Client Access server array is available or that network connectivity is stable.
   If NTLM connectivity is successful, but Kerberos is not, verify that the SPNs aren't registered on any other account besides the alternate service account. Make sure that the Exchange SPNs are registered on the account used by the shared alternate service account by using the setSPN query command as described earlier in this topic.
2. Make sure that the password is coordinated between all Client Access servers and Active Directory. To do this, run the script in attended mode and have it generate a new password.
3. Make sure that the Microsoft Exchange Address Book service is running on your Client Access servers.
4. If authentication still isn't successful, make sure that the virtual directories for the services you want to access with Kerberos have Integrated Windows authentication enabled. You can use the Get-VirtualDirectory cmdlets to verify the authentication methods. For more information on virtual directories, see Understanding Outlook Web App Virtual Directories and Understanding Exchange Web Services Virtual Directories.

Autodiscover Service Failures

If you notice the following Autodiscover service failure, it's probably because the Autodiscover service request header contains a large Kerberos authentication ticket that caused the header size to exceed the limit configured by the Internet Information Services (IIS) server. The error will be similar to the following.

```
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 09 Mar 2010 18:06:18 GMT
Connection: close
Content-Length: 346
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/stri
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Request Too Long</h2>
<hr><p>HTTP Error 400. The size of the request headers is too long.</p>
</BODY></HTML>
```

To fix this error, increase the IIS header size limit. For more information, see IIS documentation.

Ongoing Maintenance of the ASA Credential

If your local password on the shared ASA credential must be refreshed periodically, see Using the RollAlternateserviceAccountPassword.ps1 Script in the Shell for instructions for setting up a scheduled task to perform regular password maintenance. Be sure to monitor the scheduled task to ensure timely password rollovers and prevent possible authentication outages.

Turning Kerberos Authentication Off

To revert your Client Access server array so that it doesn't use Kerberos, remove the SPNs from the shared service account. If the SPNs are removed, Kerberos authentication won't be attempted by your clients, and clients configured to use Negotiate authentication will use NTLM. Clients configured to use only Kerberos will be unable to connect. Once the SPNs are removed you should also delete the shared service account. You can use the maintenance script to clean out credentials from all Client Access server array members by using the *toEntireForest* parameter and using the -copy from server parameter to specify a server that does not have any Kerberos credentials. In addition, you should eventually restart all client computers to clear the Kerberos ticket cache.

1.6.2.10.2 Troubleshooting the RollAlternateServiceAccountCredential.ps1 Script

Troubleshooting the RollAlternateServiceAccountCredential.ps1 Script

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic provides solutions and information about common errors that may occur when you use the RollAlternateServiceAccountPassword.ps1 script.

One or more of the Client Access servers can't be updated with the password

Problem

When you use the parameters *ToEntireForest* or *ToArrayMembers* with the script, in some instances, one or more of the Client Access servers may not be updated.

Resolution

Verify the servers the script will target all required servers by using the **Get-ClientAccessArray** cmdlet, as shown in the following example.

```
Get-ClientAccessArray | fl members
```

If the server that's failing to update is a member of the Client Access array and is still not updating correctly, rerun Exchange Setup and add the Client Access server role to the server again. You can also specify individual servers to target using the parameter *ToSpecificServers*.

Some servers aren't responding to the script

Problem

In some circumstances, servers might fail to update because of transient errors such as a bad network connection.

Resolution

Verify that the servers in question have network and Active Directory connectivity, and then try the script again.

Some array members are out of service for an extended period of time

Problem

If a server is out of rotation for a longer period of time but is still a member of the array, as determined by the **Get-ClientAccessArray cmdlet**, the script functionality may be impaired when using the parameters *ToArrayMembers* and *ToEntireForest*. The same problem will occur if a server has had a permanent failure but hasn't been cleanly removed from your deployment.

Resolution

To resolve this issue, remove the server from your deployment using Exchange Setup or run the script in attended mode until the server can be removed.

If the server will only be down for a short time, and you don't want to permanently remove Exchange, you can adjust the script to run against specific servers using the

parameter *ToSpecificServers* so that only active servers are targeted. Or, you can remove the RPC Client Access service from the non-responsive server's Active Directory object by using the **Remove-ClientAccessArray** cmdlet, as shown in the following example.

```
Remove-RPCClientAccess -Server Server.Contoso.com
```

After the RPC Client Access service has been removed, the server won't be returned as an array member by Get-ClientAccessArray and the script won't target it. As soon as the server is functional again, you can re-add the RPC Client Access service by using the **New-RpcClientAccess** cmdlet. When the RPC Client Access service is re-added, be sure to restart the Microsoft Exchange Address Book service on the affected server.

Caution:

Before you remove the RPC Client Access service from a server, see the topic Remove-RpcClientAccess.

For More Information

For more information about how to use Kerberos authentication with a Client Access server array or a load-balancing solution, see the following topics:

- Using Kerberos with a Client Access Server Array or a Load-Balancing Solution
- Configuring Kerberos Authentication for Load-Balanced Client Access Servers
- Using the RollAlternateserviceAccountPassword.ps1 Script in the Shell

1.6.2.10.3 Using the RollAlternateserviceAccountPassw ord.ps1 Script in the Shell

Using the RollAlternateserviceAccountPassword.ps1 Script in the Shell

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the RollAlternateServiceAccountPassword.ps1 script in Exchange Server 2010 Service Pack 1 (SP1) to update an alternate service account credential (ASA credential) and distribute the update to specified Client Access servers.

Note:

The Exchange Management Shell doesn't load scripts automatically. You must precede all scripts with "**.**" For example, to run the RollAlternateServiceAccountPassword.ps1 script, type `.\RollAlternateServiceAccountPassword.ps1`.

Note:

This script is provided in English only.

For more information about how to use Kerberos authentication with a Client Access server array or load-balancing solution, see Using Kerberos with a Client Access Server Array or a Load-Balancing Solution and Configuring Kerberos Authentication for Load-Balanced Client Access Servers.

For more information about how to use and write scripts, see Scripting with the Exchange

Management Shell.

```
RollAlternateServiceAccountPassword.ps1 -Scope <Object> -Identity <Object> -
Source <Object> -
```

Detailed Description

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access Security" entry in the Client Access Permissions topic.

Technical Details of the Alternate Service Account Credential Script

This script facilitates setup and maintenance of the ASA credential. After you've created the ASA credential and set the appropriate Service Principle Names, you can use the script to distribute the credential to all targeted Client Access servers.

To use the script, you must identify which servers you want to target and which credential you want to use as your ASA credential.

Server Scope

You can choose to have the script target all the Client Access servers in the forest, all members of a particular Client Access server array, or specific servers. The available parameters are *ToEntireForest*, *ToArrayMembers*, and *ToSpecificServers*. If you target the script to specific servers or to members of a specific server array, the *Identity* parameter must be specified with the servers or server array names you want to target.

Credential Source

The script can copy the alternate service account password from an existing server. Or, you can specify the account you want to use and let the script generate a new password for the account. The available parameters are *GenerateNewPasswordFor* and *CopyFrom*. The *GenerateNewPasswordFor* parameter requires that you specify an account string in the following format: DOMAIN\Account Name. If you're using a computer account, you must append "$" at the end of the account name, for example CONTOSO\ClientServerAcct$. The *CopyFrom* parameter takes the name of an existing Client Access server as the credential source.

Generating a New Password for a Credential

The password is created by the script. No user input is required. The script will try to distribute the password to all target computers, and will then try to update the Active Directory account credential with the newly-generated password.

The newly-generated password is 73 characters long and will satisfy standard strong password requirements. If your password requirements differ, you may need to set the password manually and then copy it to the target servers.

To prevent service interruption, the script examines each Client Access server and maintains the current password in addition to adding the new password. After the script has run, the shared ASA credential will be able to use either of 2 passwords: the current password as stored in Active Directory or the new password that hasn't yet been set in Active Directory.

All passwords that are no longer valid, such as an expired password, will be removed from the destination servers. If the password in Active Directory can't be changed, perhaps because the password has expired, the script will attempt a password reset. This will require the account running the script to have permissions to reset either Active Directory computer account passwords or user account passwords, depending on whether your alternate service account is a computer account or a user account.

If the passwords aren't changed successfully for all target Client Access servers, updating

the Active Directory password can cause an authentication failure. If the script is run in unattended mode, it won't update the Active Directory password with the new password unless all target Client Access servers have been updated successfully. If the script is run in attended mode, you will be asked whether you want to update the password in Active Directory.

Creating a Scheduled Task to Automate Password Maintenance

If you want the script to create a scheduled task to maintain the password on an ongoing basis, use the *CreateScheduledTask* parameter. This parameter requires a string for the name of the task you want to create.

Note:
Run the script and verify that it works correctly in attended mode before you create the unattended scheduled task.

The script creates a .cmd file in the folder where the script is located. It then creates a task to run that .cmd file every three weeks. You can use Windows Task Scheduler to modify the scheduled task, for example, to set it to run more or less often. By default, the task will run as the currently logged-on user. In addition, the script will only run when the user is logged on to the computer. We recommend that you modify the scheduled task to run whether the user is logged on or not. You can also choose to run it under a different account, if that account has Active Directory permissions to reset passwords as well as the Exchange Enterprise Administrator role. When creating a scheduled task, the script will automatically run in unattended mode.

Tasks Out of Scope of the Script

The script won't manage the SPNs of the ASA credential or allow you to remove an alternate service account from a server. To remove an alternate service account from a server, use the **Set-ClientAccessServer** cmdlet. If you have to remove Kerberos authentication, see Using Kerberos with a Client Access Server Array or a Load-Balancing Solution.

Troubleshooting the Script

We recommend that you run the script and verify that it works correctly in attended mode before you create the unattended scheduled task. For troubleshooting information, see Troubleshooting the RollAlternateServiceAccountCredential.ps1 Script.

Validating the Script

The output of the script when you run it interactively with the -verbose flag should indicate what script operations were successful. To confirm that the Client Access servers were updated, you can verify the last modified time stamp on the ASA credential. The following example generates a list of Client Access servers and the last time the alternate service account was updated.

```
Get-ClientAccessServer -IncludeAlternateServiceAccountCredentialstatus |Fl Name,
```

You can also examine the event log on the computer on which the script is run. The event log entries for the script are in the Application Event log and are from the source *MSExchange Management Application*. The following table lists the events that are logged and what the events mean.

Script Event IDs and their explanations

Event	Explanation
14001	Start
14002	Success (information)

14003	Successful but with Warnings. The script encountered some issues but was able to overcome them, or user input confirmed they weren't necessary. If the script is running in interactive mode, read the script output for further warning details.
14004	Failed

If the script runs as a scheduled task, its results are logged to the Exchange server **Logging** folder in a subfolder called **RollAlternateServiceAccountPassword**.

You can use the log to confirm that the task has been running successfully.

Parameters

Parameter	Required	Description
ToEntireForest	Optional	The *ToEntireForest* parameter targets the script to all Client Access servers in the forest.
ToArrayMembers	Optional	The *ToArrayMembers* parameter targets the script to all members of a specific Client Access server array. **Note:** If you're using the *ToArrayMembers* parameter or the *ToSpecificServers* parameter, you must specify the server names or the server array names using the *Identity* parameter.
ToSpecificServers	Optional	The *ToSpecificServers* parameter targets the script to specific servers. **Note:** If you're using the *ToArrayMembers* parameter or the *ToSpecificServers* parameter, you must specify the server names or the server array names using the *Identity* parameter.
Identity	Required	The *Identity* parameter specifies name of the Client Access server array or the names of the specific servers that you're targeting.
GenerateNewPasswordFor<String>	Optional	The *GenerateNewPasswordFor* parameter specifies that the script should generate a new

		password for the ASA. The string value must be the ASA account in the following format: DOMAIN\Account Name. If you're using a computer account, you must append the $ character at the end of the account name.
CopyFrom<String>	Optional	The *CopyFrom* parameter specifies that the credential is copied from another Client Access server. The string value specified is the name of the Client Access server.
Mode	Optional	The *Mode* switch specifies whether the script runs in attended or unattended mode. Unattended mode doesn't prompt for user input and automatically chooses more conservative options, when necessary.
CreateScheduledTask<String>	Optional	The *CreateScheduledTask* parameter tells the script to create a scheduled task to perform the ASA credential update. The string value is the name of the scheduled task that will be created. **Note:** This script creates a .cmd file in the folder where the script is located. The scheduled task will run the .cmd file once every three weeks. You can edit the task directly in Windows Task Scheduler to change the frequency of the task.
WhatIf	Optional	The *WhatIf* switch instructs the command to simulate the actions that it would take on the object. By using the *WhatIf* switch, you can view what changes would occur without having to apply any of those changes. You don't have to specify a value with the *WhatIf* switch.
Confirm	Optional	The *Confirm* switch causes the command to pause processing and requires you to acknowledge what the command will do before processing continues. You

		don't have to specify a value with the *Confirm* switch.
Verbose	Optional	The *Verbose* parameter tells the script to perform verbose logging, so that additional information about the script's actions is written to the log file.
Debug	Optional	The *Debug* parameter tells the script to run in debugging mode. This parameter should be used to determine why the script fails.

Examples

Example 1

This example uses the script to push the credential to all Client Access servers in the forest for first-time setup.

```
.\RollAlternateserviceAccountPassword.ps1 -ToEntireForest -GenerateNewPasswordFor
```

Example 2

This example generates a new password for a user account ASA credential and distributes the password to all members of Client Access server arrays where the name matches *mailbox*.

```
.\RollAlternateserviceAccountPassword.ps1 -ToArrayMembers *mailbox* -GenerateNewP
```

Example 3

This example schedules a once-a-month automated password roll scheduled task called "Exchange-RollAsa". It will update the ASA credential for all Client Access servers in the entire forest with a new, script-generated password. The scheduled task is created, but the script is not run. When the scheduled task is run, the script runs in unattended mode.

```
.\RollAlternateServiceAccountPassword.ps1 -CreateScheduledTask "Exchange-RollAsa"
```

Example 4

This example updates the ASA credential for all Client Access servers in the Client Access server array named CAS01. It obtains the credential from the Active Directory computer account ServiceAc1 in the domain Contoso.

```
.\RollAlternateserviceAccountPassword.ps1 -ToArrayMembers "CAS01" -GenerateNewPas
```

Example 5

This example shows how you can use the script to distribute the ASA to a new computer or to a computer that's being put back into service either because you're increasing the size of your server array or because you're re-introducing array members after maintenance.

You must update the ASA credential before the Client Access server receives traffic. Copy the shared ASA credential from any Client Access server that's already configured correctly. For example, if Server A currently has a working ASA credential and you've just added Server B to the array, you can use the script to copy the credential (including the password) from Server A to Server B. This is useful if Server B was down or not yet a member of the array when the password was rolled the last time.

```
.\RollAlternateServiceAccountPassword.ps1 -CopyFrom ServerA -ToSpecificServers Se
```

1.6.2.11 Managing Client Access Server Virtual Directories

Managing Client Access Server Virtual Directories

Exchange Server 2010 > Client Access > Managing Client Access Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-18*

Enable or Disable SSL on Exchange Web Services Virtual Directories

Reset Client Access Virtual Directories

Configure ECP Virtual Directory Properties

1.6.2.11.1 Enable or Disable SSL on Exchange Web Services Virtual Directories

Enable or Disable SSL on Exchange Web Services Virtual Directories

Client Access > Managing Client Access Servers > Managing Client Access Server Virtual Directories >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Exchange Web Services virtual directories help you manage calendar sharing and other functionality that's useful for your end users and server applications. An Exchange Web Services virtual directory is created by default on each Exchange computer that's running the Client Access server role. SSL is enabled by default on Exchange Web Services virtual directories. For more information about Exchange Web Services virtual directories, see Understanding Exchange Web Services Virtual Directories.

Important:

SSL should be enabled for each Client Access server in your organization if you don't have an SSL offloading device and want to maintain secure communications between client and server. If you want to enable SSL offloading, you must disable SSL on each Client Access server in your organization for which you want to enable SSL offloading. If your Client Access servers are running Exchange Server 2010 Service Pack 1 (SP1) or a later version, you can disable or enable SSL on an Exchange Web Services virtual directory by making a configuration change in Internet Information Services (IIS) Manager. However, if you're running Exchange 2010 RTM, you must make a configuration change in IIS Manager and also in a configuration file that's located in the Exchange 2010 installation directory.

Looking for other management tasks related to Exchange Web Services virtual directories? Check out the Exchange Web Services virtual directory cmdlets referenced in the Client Access Cmdlets topic.

What Do You Want to Do?

- Disable SSL on an Exchange Web Services virtual directory on a Client Access server running Exchange 2010 SP1 or a later version
- Disable SSL on an Exchange Web Services virtual directory on a Client Access server running Exchange 2010 RTM
- Enable SSL on an Exchange Web Services virtual directory on a Client Access

Disable SSL on an Exchange Web Services virtual directory on a Client Access server running Exchange 2010 SP1 or a later version

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Web Services permissions" entry in the Client Access Permissions topic.

1. Open IIS Manager and turn off SSL on the Exchange Web Services virtual directory using the following steps:
   1.a. In the console tree, click the plus sign (+) next to each of the following folders to show the **EWS** node: **Server Name** > **Sites** > **Default Web Site**.
   1.b. In the console tree, select **EWS**.
   1.c. In the result pane, under **IIS**, double-click **SSL Settings**.
   1.d. Make sure the **Require SSL** check box is cleared.
2. Perform this procedure on each Client Access server in your organization.

Disable SSL on an Exchange Web Services virtual directory on a Client Access server running Exchange 2010 RTM

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Web Services permissions" entry in the Client Access Permissions topic.

1. Open IIS Manager and turn off SSL on the Exchange Web Services virtual directory using the following steps:
   1.a. In the console tree, click the plus sign (+) next to each of the following folders to show the **EWS** node: **Server Name** > **Sites** > **Default Web Site**.
   1.b. In the console tree, select **EWS**.
   1.c. In the result pane, under **IIS**, double-click **SSL Settings**.
   1.d. Make sure the **Require SSL** check box is cleared.
2. Edit the configuration file in the directory in which you installed Exchange 2010.

   Caution:
   Save a copy of the configuration file before you begin the procedure. That way, you can revert to the original file if you make any errors while you're modifying the file.

   2.a. Go to C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess \exchweb\ews, where C:\ is the directory in which you installed Exchange 2010.
   2.b. In Notepad or another .xml editing tool, open the web.config file.
   2.c. Change all occurrences of the term **httpsTransport** to **httpTransport**.
   2.d. Save changes to web.config.
3. Perform this procedure on each Client Access server in your organization.

Enable SSL on an Exchange Web Services

virtual directory on a Client Access server running Exchange 2010 SP1 or a later version

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Web Services permissions" entry in the Client Access Permissions topic.

1. Open IIS Manager and turn on SSL on the Exchange Web Services virtual directory using the following steps:
   1.a. In the console tree, click the plus sign (+) next to each of the following folders to show the **EWS** node: **Server Name** > **Sites** > **Default Web Site**.
   1.b. In the console tree select **EWS**.
   1.c. In the result pane, under **IIS**, double-click **SSL Settings**.
   1.d. Make sure the **Require SSL** check box is selected.
2. Perform this procedure on each Client Access server in your organization.

Enable SSL on an Exchange Web Services virtual directory on a Client Access server running Exchange 2010 RTM

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Web Services permissions" entry in the Client Access Permissions topic.

1. Open IIS Manager and turn on SSL on the Exchange Web Services virtual directory using the following steps:
   1.a. In the console tree, click the plus sign (+) next to each of the following folders to show the **EWS** node: **Server Name** > **Sites** > **Default Web Site**.
   1.b. In the console tree select **EWS**.
   1.c. In the result pane, under **IIS**, double-click **SSL Settings**.
   1.d. Make sure the **Require SSL** check box is selected.
2. Edit the configuration file in the directory to which you installed Exchange 2010.

   Caution:

   Save a copy of the configuration file before you begin the procedure. That way, you can revert to the original file if you make any errors while you're modifying the file.

   2.a. Go to the C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess \exchweb\ews, where C:\ is the directory in which you installed Exchange 2010.
   2.b. In Notepad or another .xml editing tool, open the web.config file.
   2.c. Change all occurrences of the term **httpTransport** to **httpsTransport**.
   2.d. Save changes to web.config file.
3. Perform this procedure on each Client Access server in your organization.

Reset Client Access Virtual Directories

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the Reset Client Access Virtual Directory wizard to reset a virtual directory on an Exchange Server 2010 Client Access server. When you reset a virtual directory, the virtual directory is removed and a new virtual directory with default settings is created.

Important:

Because a new virtual directory with default settings is created when you reset a virtual directory, you need to reconfigure a virtual directory after it's reset. By default, the settings for a virtual directory are copied to the Program Files/Microsoft/Exchange Server/V14 directory.

What Do You Want to Do?

- Use the EMC to reset a Client Access server virtual directory
- Use the Shell to a Client Access server virtual directory

Use the EMC to reset a Client Access server virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Reset Client Access virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the action pane, click **Reset Client Access Virtual Directory**.
3. On the **Introduction** page, next to **Virtual directory to be reset**, click **Browse**. Select the virtual directory you want to reset and click **Next**. By default, the following Client Access virtual directories are listed:
   - Autodiscover (Default Web Site)
   - ecp (Default Web Site)
   - EWS (Default Web Site)
   - Microsoft-Server-ActiveSync (Default Web Site)
   - OAB (Default Web Site)
   - owa (default Web Site)
4. After the directory you want to reset is added to the list under **Virtual directory to be reset**, click **Next**.
5. On the **Log Location** page, specify the path and file name for the log file, and click **Next**. The log file includes the settings that exist on the virtual directory you're about to reset. These settings may be helpful if you want to re-create a virtual directory with the same settings. By default, the log file is copied to the Documents folder on the Client Access server.
6. On the **Reset Client Access Virtual Directory** page, click **Reset**.
7. On the **Completion** page, click **Finish**.
8. Restart Internet Information Services (IIS). You can restart IIS by running **iisreset /noforce** from a command prompt window.

Use the Shell to reset a Client Access server virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Reset Client Access virtual directories" entry in the Client Access Permissions topic.

To reset a virtual directory, you must remove the virtual directory and then create a new one.

The cmdlets that you run differ depending on the virtual directory you want to reset.

For example, to reset the Outlook Web App virtual directory on the Client Access server Server01, you need to do the following:

1. Remove the virtual directory by running the following cmdlet.

```
Remove -OwaVirtualDirectory -Identity 'Server01\owa (Default Web Site)
```

2. Create the new virtual directory by running the following cmdlet.

```
New-OwaVirtualDirectory -InternalUrl 'https://<Server01><DomainName>/o
```

3. Restart IIS. You can restart IIS by running **iisreset /noforce** from a command prompt window.

By default, the log file is copied to the Documents folder on the Client Access server. The log file includes the settings that exist on the virtual directory you're resetting. These settings may be helpful if you want to re-create a virtual directory with the same settings.

For more information about syntax and parameters, see the cmdlets that are used to manage the virtual directory that you want to reset.

Virtual directory name	Cmdlet used to create the virtual directory	Cmdlet used to remove the virtual directory
Autodiscover (Default Web Site)	New-AutodiscoverVirtualDirectory	Remove-AutodiscoverVirtualDirectory
ecp (Default Web Site)	New-EcpVirtualDirectory	Remove-EcpVirtualDirectory
EWS (Default Web Site)	New-WebServicesVirtualDirectory	Remove-WebServicesVirtualDirectory
Microsoft-Server-ActiveSync (Default Web Site)	New-ActiveSyncVirtualDirectory	Remove-ActiveSyncVirtualDirectory
OAB (Default Web Site)	New-OABVirtualDirectory	Remove-OABVirtualDirectory
owa (default Web Site)	New-OwaVirtualDirectory	Remove-OwaVirtualDirectory

1.6.2.11.3 Configure ECP Virtual Directory Properties

Configure ECP Virtual Directory Properties

Client Access > Managing Client Access Servers > Managing Client Access Server Virtual Directories >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can view or configure the settings that apply to your Exchange Control Panel (ECP) virtual directory properties.

What Do You Want to Do?

- Use the EMC to configure ECP virtual directory properties
- Use the Shell to configure ECP virtual directory properties

Use the EMC to configure ECP virtual directory properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Control Panel (ECP) virtual directory settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access** > **Exchange Control Panel**.
2. In the work pane, select **ecp (Default Web site)**, and then, in the action pane, under **ecp (Default Web site)**, click **Properties**. The **ecp (Default Web site) Properties** page will open.
3. On the **General** tab, in the **Internal URL** box, verify that the internal URL is correct for your organization.
4. In the **External URL** box, verify that the external URL is correct for your organization. The external URL isn't configured by default.
5. On the **Authentication** tab, specify the method by which your POP3 users will sign in. ECP uses the same sign-in format as Outlook Web App. By default, **Use forms based authentication** is selected.
   - Select **Use one or more standard authentication methods**, and then select one of the following check boxes if you want to use:
     Integrated Windows authentication
     Digest authentication for Windows domain servers
     Basic authentication (password is sent in clear text)
   - Select **Use forms based authentication** if you want to use forms-based authentication. ECP uses the same sign-in format as Outlook Web App.

Note:
To configure SSL settings for this ECP virtual directory, use Internet Information Services (IIS).

Use the Shell to configure ECP virtual directory properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Control Panel (ECP) virtual directory settings" entry in the Client Access Permissions topic.

This example disables Basic authentication on the default ECP virtual directory on the server named Server01.

```
Set-EcpVirtualDirectory -Identity "Server01\ecp (default web site)" -Basicauthent
```

For more information about syntax and parameters, see Set-EcpVirtualDirectory.

1.6.2.12 Set Message Size Limits for Exchange Web Services

Set Message Size Limits for Exchange Web Services

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-01-20*

You can modify message size limits to increase or decrease the size of e-mail messages that clients may send or receive.

To configure message size limits, you modify the following parameters on the Send and Receive connectors on the Hub Transport servers:

- **maxReceiveSize**
- **maxSendSize**
- **maxMessageSize**

To view the Send and Receive limits for your Exchange organization, use the following cmdlet:

Get-TransportConfig |fl max*size

To view the Send and Receive limits for individual mailboxes, use the following cmdlets:

Get-Mailbox –id sender |fl max*size

Get-Mailbox –id recipient |fl max*size

To determine whether the sender and recipient have enough room left in their mailboxes, you can run the following Exchange Management Shell cmdlets:

Get-MailboxStatistics –id sender | fl StorageLimitStatus,TotalItemSize

Get-Mailbox sender | fl prohibit*quota

Get-Mailbox sender | foreach {Get-MailboxDatabase –id $_.mailboxdatabase | fl prohibit*quota}

Get-MailboxStatistics –id recipient | fl StorageLimitStatus,TotalItemSize

Get-Mailbox recipient | fl prohibit*quota

Get-Mailbox recipient| foreach {Get-MailboxDatabase –id $_.mailboxdatabase | fl prohibit*quota}

Additionally, you must configure both of the following parameters in the Exchange Web Services (EWS) Web.config file for clients that use Exchange Web Services such as Microsoft Entourage 2008 for Mac, Web Services Edition to submit e-mail messages to Exchange:

- **maxAllowedContentLength** – This setting is used by the Request filtering role service in Internet Information Services 7 (IIS) to protect the Web server from receiving requests that are too large.
  The default values for this parameter are:

  Exchange 2007= 30000000 bytes

  Exchange 2010= 35000000 bytes

Note:
A change to this setting requires a restart of the MSExchangeServicesAppPool application pool. You can verify or modify this setting in the following ways.

- **maxRequestLength** - ASP.NET uses the maxRequestLength setting to determine the maximum amount of data that the Web browser can submit to the Client Access server. This setting is configured initially by Exchange Setup as an entry in the Web.config file for the Exchange Web Services application in IIS.

  Default for Exchange 2007 = 13280 KB

  Default for Exchange 2010 = 2097151 KB

- **maxReceivedMessageSize** – This setting applies only to Microsoft Exchange Server 2010. It indicates the maximum message size that is accepted by EWS. This maximum message size is 35,000,000 bytes, which translates to 25 MB of Base64-encoded data.
  The default values for this parameter are:

  Exchange 2010 RTM = 13600000 Bytes

  Exchange 2010 SP1 = 35000000 Bytes

  Note:
  The values for this limit differ for an on-premise Exchange 2010 deployment.

- **connectionTimeout** - This setting is used to provide a connection time limit. Because this parameter affects traffic to the Web site, we do not recommend changing this value unless you receive HTTP 408 error messages. The recommended method for changing this value is to use the IIS Configuration editor. The Configuration Editor is part of the IIS Administration Pack.

Note:
The size of a message is determined by the size of the message body plus the size of any attached files. For Microsoft Exchange Server 2010 Service Pack 1 (SP1), the default message size restrictions are set to 35 million bytes. This accommodates approximately 25 MB of Base64-encoded data. For Microsoft Exchange Server 2010, the default message size restrictions are set to 13.6 million bytes. This accommodates approximately 10 MB of Base64-encoded data.

Note:
After you set the message size properties for Exchange Web Services, you must stop and then start the Default Web site.

For information about other management tasks that are related to setting up message size limits, see Understanding Message Size Limits.

Use a text editor to modify the Web.config file

To modify the Web.config file, follow these steps:

1. Start Windows Explorer, and then locate the Web.config file. By default, this file is located in the following directory:
   %ProgramFiles%\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews
2. Create a copy of the file as a backup.
3. Open the Web.config file by using a text editor, such as Notepad.
4. Search for the **maxAllowedContentLength** entry. By default, this entry appears as follows in Microsoft Exchange Server 2010 RTM:

<requestLimits maxAllowedContentLength="13600000" />

5. Change the value for **maxAllowedContentLength** to accommodate the message size that you want to allow. Because message attachments are Base64-encoded before they are transferred, the value must be set high enough to accommodate the desired message size together with the encoding overhead.
   For example, to allow messages of approximately 20 MB, perform the following calculation:
   20971520 bytes * 4/3 for Base64 encoding = 27962027 (rounded up)

   Note:
   In this formula, the fraction 4/3 represents a message that is approximately 33 percent larger than the original. However, message size increase may be much larger, depending on the type of attachment that is sent, the attachment size, whether the attachment is already compressed, and the messaging client from which the message is sent. In some cases, you may experience message size increases of 100 percent after encoding (that is, messages that are twice the size of the original messages).
6. Search for **maxReceivedMessageSize**. This entry is listed after the **EWSServiceBehavior** entries. By default, this entry appears as follows in Exchange 2010 RTM:
   <httpsTransport maxReceivedMessageSize="13600000" authenticationScheme="Anonymous" maxBufferSize="81920" transferMode="Streamed" />
7. Change the value for **maxReceivedMessageSize** to the same value as for **maxAllowedContentLength** to accommodate the desired message size together with the base64 encoding overhead.
8. Save the changes to the Web.config file, and then exit the text editor.
9. Stop and then start the default Web site for the settings to take effect.

   Important:
   You must configure at least the same message size limits on the appropriate transport servers to support the increased message size. For more information, see Understanding Message Size Limits.

1.6.3 Securing Client Access Servers

Securing Client Access Servers

Exchange Server 2010 > Client Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

This topic summarizes the security and authentication related options available for a computer running Microsoft Exchange Server 2010 that has the Client Access server role installed. The Client Access server role provides access to Outlook Web App, Microsoft Exchange ActiveSync, Outlook Anywhere, Post Office Protocol version 3 (POP3), and Internet Message Access Protocol version 4rev1 (IMAP4). In addition, it supports the Autodiscover service and the Availability service. Each of these protocols and services has unique security needs.

Managing Authentication

One of the most important security-related tasks you can perform for the Client Access server role is to configure an authentication method. The Client Access server role is installed with a default self-signed digital certificate. A digital certificate does two things:

- It authenticates that its holder is who or what the holder claims to be.
- It helps protect data exchanged online from theft or tampering.

Although the default, self-signed certificate is supported for Exchange ActiveSync and Outlook Web App, it isn't the most secure method of authentication. Also, it isn't supported for Outlook Anywhere. For additional security, consider configuring your Exchange 2010 Client Access server to use a trusted certificate from a third-party commercial certification authority (CA) or a trusted Windows public key infrastructure (PKI) CA. You can configure authentication separately for Exchange ActiveSync, Outlook Web App, Outlook Anywhere, POP3, and IMAP4.

For more information about how to configure authentication, see the following topic:

- Setting Up Standard Authentication Methods for Outlook Web App

Enhancing Secure Communications Between the Client Access Server and Other Servers

After you optimize the security of communications between clients and the Exchange 2010 Client Access server, you must optimize the security of the communications between the Exchange 2010 Client Access server and other servers in your organization. By default, HTTP, Exchange ActiveSync, POP3, and IMAP4 communication between the Client Access server and other servers, such as Exchange 2010 servers that have the Mailbox server role installed, domain controllers, and global catalog servers, is encrypted.

For More Information

For more information about how to manage security for the different components of your Client Access server, see the following topics:

- Understanding Security for Exchange ActiveSync
- Understanding Security for Outlook Web App
- Understanding Security for Outlook Anywhere
- Understanding Security for POP3 and IMAP4

1.6.3.1 Managing SSL for a Client Access Server

Managing SSL for a Client Access Server

Exchange Server 2010 > Client Access > Securing Client Access Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-05-18*

Understanding Digital Certificates and SSL

Obtain a Server Certificate from a Certification Authority

Install an SSL Certificate on a Client Access Server

Export an Exchange Certificate

Renew an Exchange Certificate

Configure SSL Certificates to Use Multiple Client Access Server Host Names

1.6.3.1.1 Obtain a Server Certificate from a Certification Authority

Obtain a Server Certificate from a Certification Authority

Client Access > Securing Client Access Servers > Managing SSL for a Client Access Server >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-03*

You can obtain a server certificate from a certification authority (CA). This is one step in the process to configure Secure Sockets Layer (SSL) or Transport Layer Security (TLS). You can obtain server certificates from a third-party CA. A third-party CA may require you to provide identification before a certificate can be issued. You can also issue your own server certificates by using an online CA, such as Microsoft Certificate Services.

Note:
Cryptography Next Generation (CNG) certificates are not supported in Microsoft Exchange Server 2010.

For more information about server certificates, see the Windows Server 2003 Internet Information Services (IIS) documentation.

Note:
Microsoft Exchange Server 2010 includes a default self-signed SSL certificate. You can replace this certificate with a third-party certificate from a CA. To do this, you must first delete the self-signed certificate. For more information about how to replace the self-signed certificate, see Install an SSL Certificate on a Client Access Server.

Looking for other management tasks related to SSL? Check out Managing SSL for a Client Access Server.

Prerequisites

Important:
As a security best practice, log on to your computer using an account that isn't in the Administrators group, and then use the **runas** command to run IIS Manager as an administrator. At a command prompt, type **runas /user:***Administrative_AccountName* **"mmc systemroot\system32\inetsrv\iis.msc"**.

Use the Shell to obtain a server certificate from a certification authority

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

The code example below outputs the certificate request in Base64 format to the command-line console. You must send the certificate request to a CA within the organization, a trusted CA outside the organization, or a commercial CA. You can do this

by pasting the certificate request output into an e-mail message or into the appropriate field on the certificate request Web page of the CA. You can also save the certificate request to a file using a text editor such as Notepad.

The certificate that results has the following attributes associated with it:

- Subject name: c=<ES>,o=<Woodgrove Bank>,cn=mail1.woodgrovebank.com
- Subject alternate names: woodgrovebank.com and example.com
- An exportable private key

```
New-ExchangeCertificate -GenerateRequest -SubjectName "c=US, o=Woodgrove Bank, cn
```

Use the procedures specified by your chosen CA to send the certificate request to the CA.

1.6.3.1.2 Install an SSL Certificate on a Client Access Server

Install an SSL Certificate on a Client Access Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to install a Secure Sockets Layer (SSL) certificate on a Microsoft Exchange Server 2010 Client Access server.

Looking for other management tasks related to SSL? Check out Managing SSL for a Client Access Server.

Prerequisites

You've previously requested a certificate from a certification authority by using the **New-ExchangeCertificate** cmdlet and then transmitted that request to a certification authority. The certification authority has returned a certificate file.

Use the Shell to install an SSL certificate on a Client Access server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access Server Security settings" entry in the Client Access Permissions topic.

This example imports an existing certificate and private key from the PKCS #12 file ExportedCert.pfx.

```
Import-ExchangeCertificate -FileData ([Byte[]]$(Get-Content -Path c:\certificates
```

For more information about syntax and parameters, see Import-ExchangeCertificate.

Configure SSL Certificates to Use Multiple Client Access Server Host Names

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to configure your Secure Sockets Layer (SSL) certificates to use multiple host names.

When you deploy your Microsoft Exchange Server 2010 Client Access servers, you must make sure that all your clients, such as Microsoft Office Outlook Web App and Office Outlook 2007, will be able to connect to the services by using an encrypted session without receiving an error message that states that the certificate isn't trusted.

By using the Shell, you can create a certificate request to include all the DNS host names of the Client Access servers. Then you can enable users to connect to the certificate for services, such as Outlook Anywhere, Autodiscover, POP3 and IMAP4, or Unified Messaging, that are listed in the alternate names attribute. For example, your users may be able to connect to your Exchange services by specifying the name as shown in the following examples:

- https://*CAS01*/owa
- https://*CAS01.FQDN.name*/owa
- https://*CASIntranetName*/owa
- https://autodiscover.*emaildomain*.com

Instead of having to require multiple certificates and maintain the configuration of multiple IP addresses and Internet Information Services (IIS) Web sites for each IP port and certificate combination, you can create a single certificate that enables clients to successfully connect to each host name by using SSL or Transport Layer Security (TLS).

You can create a single certificate by adding all the possible DNS name values to the certificate *Subject Alternative Name* property on the certificate request. A Windows–based Certificate Services certification authority should create a certificate for such a request.

Note:

Third-party or Internet-based certification authorities will issue certificates only for DNS names that you are authorized to use. Therefore, intranet DNS names probably won't be allowed.

To configure your SSL certificates to use multiple Client Access server host names, do the following:

1. Use the **New-ExchangeCertificate** cmdlet to create a certificate request file.
2. Send this file to a Windows Certificate Services certification authority and use the Web server template on the **Certification Authority** page. This will result in a .cer file that can be imported to the Client Access server.
3. Use the **Get-ExchangeCertificate** cmdlet to determine the thumbprint for your certificate.
4. After you've imported the certificate, you can assign it to IIS, IMAP4, and POP3 by using the **Enable-ExchangeCertificate** cmdlet.

Looking for other management tasks related to SSL? Check out Managing SSL for a Client Access Server.

Prerequisites

- You have logged on to your computer using an account that's not in the Administrators group, and then used the **runas** command to run IIS Manager as an administrator. This is a security best practice. To do this, at a command prompt, type **runas /user:***Administrative_AccountName* **"mmc systemroot \system32\inetsrv\iis.msc"**.
- You have read TLS Functionality and Related Terminology in Exchange 2010. This contains information about the many variables you must consider when you configure certificates for SSL or TLS services and how these variables can affect your overall configuration.

Use the Shell to create a certificate request file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

This example creates a text file that contains a certificate request in PKCS#10 format.

```
New-ExchangeCertificate -generaterequest -subjectname "dc=com,dc=contoso,o=Contos
```

Use the Shell to import a certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

This example imports a previously obtained certificate.

```
Import-ExchangeCertificate -path <certificate_file_name>.cer -friendlyname "Conto
```

Use the Shell to determine the thumbprint of your certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

This example determines the thumbprint of a certificate that matches the host name of CAS01.

```
Get-ExchangeCertificate -DomainName "CAS01"
```

Note:
This example will return multiple certificates if there are several certificates that match the host name you specified. Therefore, make sure that you select the thumbprint of the correct certificate for your request.

Use the Shell to assign the certificate to IIS, POP3, and IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

This example assigns the certificate to IIS, POP3, and IMAP4.

```
Enable-ExchangeCertificate -thumbprint <certificate-thumbprint> -services "IIS,PO
```

This example assigns the certificate to a server, which in turn assigns the certificate to all services that are running on the Exchange server.

```
Import-ExchangeCertificate -path <certificate file name> -friendlyname "Contoso C
```

For more information about syntax and parameters for the **Import-ExchangeCertificate**, **Enable-ExchangeCertificate**, **Get-ExchangeCertificate**, and **New-ExchangeCertificate** cmdlets, see Global Cmdlets.

1.6.3.1.4 Export an SSL Certificate

Export an SSL Certificate

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to export a Secure Sockets Layer (SSL) certificate. An SSL certificate is installed on a Microsoft Exchange Server 2010 Client Access server. The SSL certificate enables the Client Access server to encrypt communications with clients by using SSL technology. The SSL certificate installed on the Client Access server can be the default self-signed certificate, a certificate from a Windows public key infrastructure (PKI) certification authority (CA), or a certificate from a trusted commercial third-party CA.

You can export an existing certificate or a certificate request. To install a copy of the SSL certificate on a client computer or a mobile phone, the certificate must be exported by using the **Export-ExchangeCertificate** cmdlet.

Important:

Previous versions of Microsoft Exchange let you use Internet Information Services (IIS) to save a copy of the certificate. Although IIS will still let you save a copy of the certificate in Exchange 2010, we don't recommend that you do this. Use the **Export-ExchangeCertificate** cmdlet to generate a copy of the certificate for importing to another server, client computer, or mobile phone.

After you've exported the SSL certificate in the form of a PKCS #12 file, the file can then be imported by the following:

- Another Exchange 2010 server, by using the **Import-ExchangeCertificate** cmdlet
- A client computer, by using the Certificate Import wizard in the EMC
- A mobile phone, by using desktop ActiveSync

Note:

Not all mobile phones support installation of SSL certificates. For more information, see your mobile phone documentation.

Looking for other management tasks related to SSL? Check out Managing SSL for a Client Access Server.

Use the Shell to export an SSL certificate

The following command uses the **Export-ExchangeCertificate** cmdlet to export certificate data to the variable *$file*.

```
$file = Export-ExchangeCertificate -Thumbprint 5113ae0233a72fccb75b1d019862867533
```

For more information about syntax and parameters, see Export-ExchangeCertificate.

1.6.3.1.5 Export an Exchange Certificate

Export an Exchange Certificate

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Export Exchange Certificate Wizard to export an existing Exchange Secure Sockets Layer (SSL) certificate.

Prerequisites

The Client Access server role has been installed and at least one certificate is installed on your Client Access server.

What Do You Want to Do?

- Use the EMC to export an Exchange certificate
- Use the Shell to export an Exchange certificate

Use the EMC to export an Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

1. In the console tree, click **Server Configuration**.
2. Select the server that contains the certificate, and then select the certificate you want to export.
3. In the action pane, click **Export Exchange Certificate**.
4. On the **Export Exchange Certificate** page, select the certificate you want to export. The services that are checked are currently assigned to the certificate.
5. When you click **Export**, the **Progress Page** will confirm your selections and try to export the certificate.
6. The **Completion** page will display the status of the request together with the syntax of the Shell cmdlet needed to export the certificate.

Use the Shell to export an Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client

Access Permissions topic.

This example exports the Exchange certificate.

```
Export-ExchangeCertificate -Thumbprint 5113ae0233a72fccb75b1d0198628675333d010e -
```


1.6.3.1.6 Renew an Exchange Certificate

Renew an Exchange Certificate

Client Access > Securing Client Access Servers > Managing SSL for a Client Access Server >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-13*

You can use the Renew Exchange Certificate wizard to renew an existing Exchange Secure Sockets Layer (SSL) certificate.

Prerequisites

The Client Access server role has been installed and at least one certificate is installed on your Client Access server.

What Do You Want to Do?

- Use the EMC to renew an Exchange certificate
- Use the Shell to renew an Exchange certificate

Use the EMC to renew an Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

1. In the console tree, click **Server Configuration**.
2. Select the server that contains the certificate, and then select the certificate you want to renew.
3. In the action pane, click **Renew Exchange Certificate**.
4. On the **Renew Exchange Certificate** page, select the services you want to assign to the renewed certificate. The services that are checked are currently assigned to the certificate.
5. When you click **Assign**, the **Progress** page will confirm your selections and try to renew the certificate.
6. Click **Yes** to overwrite the existing certificate with the renewed certificate.
7. The **Completion** page will display the status of the request in addition to the syntax of the cmdlet needed to renew the certificate.

Use the Shell to renew an Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

This example renews the self-signed Exchange certificate by using its thumbprint to identify the certificate.

```
Get- ExchangeCertificate -Thumbprint 'AD19B141228C7CF98B5F78DCED978B7C45E15434' |
```

This example generates a request to renew a certificate issued by a certification authority.

```
Get- ExchangeCertificate -Thumbprint 'AD19B141228C7CF98B5F78DCED978B7C45E15434' |
```

For detailed syntax and parameter information, see **New-ExchangeCertificate**.

Note:

After you generate a certificate request, you must submit it to a certification authority, obtain a signed certificate and install the certificate on the same server. For details, see Obtain a Server Certificate from a Certification Authority and Install an SSL Certificate on a Client Access Server.

1.6.3.2 Managing Exchange ActiveSync Security

Managing Exchange ActiveSync Security

Exchange Server 2010 > Client Access > Securing Client Access Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-18*

Configure SSL for Exchange ActiveSync

Configure Authentication for Exchange ActiveSync

1.6.3.2.1 Configure SSL for Exchange ActiveSync

Configure SSL for Exchange ActiveSync

Client Access > Securing Client Access Servers > Managing Exchange ActiveSync Security >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-22*

You can configure Microsoft Exchange ActiveSync virtual directories to use Secure Sockets Layer (SSL). By default, when you install the Client Access server role on a computer that's running Microsoft Exchange Server 2010, an Exchange ActiveSync virtual directory is created on the default Internet Information Services (IIS) Web site on the Exchange server.

After you obtain an SSL certificate to use with the Client Access server on the default Web site or on the Web site where you host your Exchange ActiveSync virtual directory, you can configure the Web site to require SSL. You can enable SSL for all Web sites hosted by the Client Access server or enable SSL only for Exchange ActiveSync.

Configuring an Exchange ActiveSync virtual directory to use SSL is just one step in managing security for Exchange ActiveSync. For more information about how to manage security for Exchange ActiveSync, see Managing Exchange ActiveSync Security.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Use IIS Manager to configure SSL on the Exchange ActiveSync virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync server settings" entry in the Client Access Permissions topic.

If you are using IIS 7.0 or a later version, follow these steps:

1. In IIS Manager, select **Default Web site** or the Web site on which you are hosting your **Microsoft-Server-ActiveSync** virtual directory.
2. In the Web site **Home** pane, in the **IIS** area, double-click **SSL Settings**.
3. In **SSL Settings**, select the **Require SSL** check box. **Require 128-bit SSL** is optional. But if it is selected, this option provides greater security.

   Note:

   If you are using an SSL certificate that was created during Exchange Setup, an error message notifies you that the certificate is not a trusted certificate. Make sure that you trust the certification authority (CA) that issued the certificate or use an SSL certificate that is trusted by your CA.

4. Under **Client Certificates**, select **Ignore**.
5. In the action pane, click **Apply** to save your changes.

If you are using a version of IIS earlier than IIS 7, follow these steps:

1. In IIS Manager, select the **Default Web site** or the **Microsoft-Server-ActiveSync** virtual directory, and then click **Properties**.

   Note:

   If you want to configure SSL only for Exchange ActiveSync, select the **Microsoft-Server-ActiveSync** virtual directory under the Default Web site. Otherwise, you'll configure SSL for all virtual directories hosted on the Client Access server.

2. On the **Directory Security** tab, in **Secure Communications**, click **Edit**.
3. In **Secure Communications**, select **Require Secure Channel (SSL)**.
4. After you complete this procedure, your Exchange ActiveSync virtual directory on the Web site will be configured to use SSL. For more information about Exchange ActiveSync, see Managing Exchange ActiveSync Security.

1.6.3.2.2 Configure Authentication for Exchange ActiveSync

Configure Authentication for Exchange ActiveSync

Client Access > Securing Client Access Servers > Managing Exchange ActiveSync Security >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure Basic authentication for Microsoft Exchange ActiveSync. By default, when you install Microsoft Exchange Server 2010, Exchange ActiveSync is configured to use Basic authentication with Secure Sockets Layer (SSL) encryption. Other standard authentication methods include Digest authentication and Integrated Windows authentication. If you must return Exchange ActiveSync to Basic authentication, you can use the procedures in this topic.

Important:

If you configure Basic authentication for Exchange ActiveSync, we recommend that you require SSL for communications between mobile phones and Exchange ActiveSync. For more information about how to enable SSL, see Configure SSL for Exchange ActiveSync.

Looking for other management tasks related to Exchange ActiveSync? Check out Managing Exchange ActiveSync.

Use the EMC to configure Basic authentication for Exchange ActiveSync

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync Security settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the result pane, click the **Exchange ActiveSync** tab.
3. Select the **Microsoft-Server-ActiveSync** virtual directory.
4. In the action pane, under **Microsoft-Server-ActiveSync**, click **Properties**.
5. Click the **Authentication** tab.
6. Select the **Basic authentication (password is sent in clear text)** check box.
7. Click **Apply** to save your changes or click **OK** to save your changes and close the **Microsoft-Server-ActiveSync properties** dialog box.

Use the Shell to configure Basic authentication for Exchange ActiveSync

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange ActiveSync server settings" entry in the Client Access Permissions topic.

This example configures the Exchange ActiveSync virtual directory for basic authentication.

```
Set-ActiveSyncVirtualDirectory -Identity "ExchSrvr\Microsoft-Server-ActiveSync (D
```

For more information about syntax and parameters, see Set-ActiveSyncVirtualDirectory.

1.6.3.3 Managing Outlook Anywhere Security

Managing Outlook Anywhere Security

Exchange Server 2010 > Client Access > Securing Client Access Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

Configure SSL for Outlook Anywhere

Configure Authentication for Outlook Anywhere

Configure SSL Offloading for Outlook Anywhere

1.6.3.3.1 Configure SSL for Outlook Anywhere

Configure SSL for Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-31*

You can configure the /rpc virtual directory to use Secure Sockets Layer (SSL) for Outlook Anywhere. By default, when you install the Microsoft Exchange Server 2010 Client Access server role, a virtual directory named /rpc is created on the default Internet Information Services (IIS) Web site on the Exchange server.

Looking for other management tasks related to Outlook Anywhere? Check out Managing Outlook Anywhere.

Use IIS to configure SSL on the /rpc virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "SSL for Outlook Anywhere" entry in the Client Access Permissions topic.

If you are using IIS 7.0 or a later version, follow these steps:

1. In IIS Manager, select **Default Web site** or the Web site on which you're hosting your Outlook Web App virtual directories.
2. In the Web site **Home** pane, double-click **SSL Settings** in the **IIS** area.
3. In **SSL Settings**, select the **Require SSL** check box.

Note:
The **Require 128-bit SSL** option is not required. However, if selected, this option helps to provide increased security.

Note:
If you are using an SSL certificate that was created during Exchange Setup, an error message notifies you that the certificate is not a trusted certificate. Make sure that you trust the certification authority (CA) that issued the certificate, or use an SSL certificate that is trusted by your CA.

4. Under **Client Certificates**, select **Ignore**.
5. In the action pane, click **Apply** to save your changes.

If you are using an earlier version of IIS than IIS 7, follow these steps:

1. In IIS, select the **Default Web site** or the **rpc** virtual directory, and then click **Properties**.

Note:
If you want to configure SSL only for Outlook Anywhere, select the **rpc** virtual directory under the **Default Web site**. Otherwise, you'll configure SSL for all virtual directories that are hosted on the Client Access server.

2. On the **Directory Security** tab, in **Secure Communications**, click **Edit**.

3. In **Secure Communications**, select **Require Secure Channel (SSL)**.

After you complete this procedure, your /rpc virtual directory is configured to use SSL.

Other Tasks

After you configure SSL on the /rpc virtual directory, you may also want to:

- Configure SSL Offloading for Outlook Anywhere
- Configure Authentication for Outlook Anywhere

  For more information about CAS security, see Securing Client Access Servers

1.6.3.3.2 Configure Authentication for Outlook Anywhere

Configure Authentication for Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to configure authentication for Outlook Anywhere.

The first time that you run the Enable Outlook Anywhere wizard in the EMC, you can select the authentication method that you want to use for Microsoft Office Outlook 2007, Outlook 2010, or Outlook 2003 clients. However, if you want to configure authentication and you've already run the Enable Outlook Anywhere wizard, you can use the **Set-OutlookAnywhere** cmdlet in the Shell.

Note:

When you specify authentication for Outlook Anywhere, you set the authentication method that will be used by the Outlook client. This authentication method is automatically provided to the client by the Autodiscover service. This authentication method is separate from the authentication method on the /rpc virtual directory that's located on your Microsoft Exchange Server 2010 Client Access servers. By default, the /rpc virtual directory is enabled for Basic authentication, and the authentication method can't be modified.

To choose the correct authentication method, see Understanding Security for Outlook Anywhere.

Looking for other management tasks related to Outlook Anywhere? Check out Managing Outlook Anywhere.

Use the Shell to configure authentication for Outlook Anywhere

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Anywhere configuration (enable, disable, change, view)" entry in the Client Access Permissions topic.

This example enables Basic authentication for Outlook Anywhere.

```
Set-OutlookAnywhere -Name Server01 -ClientAuthenticationMethod Basic
```

This example enables NTLM authentication Outlook Anywhere.

```
Set-OutlookAnywhere -Name Server01 -ClientAuthenticationMethod NTLM
```

For more information about syntax and parameters, see Set-OutlookAnywhere.

Other Tasks

After you configure authentication for Outlook Anywhere, you may also want to:

- Configure SSL for Outlook Anywhere
- Configure SSL Offloading for Outlook Anywhere

1.6.3.3.3 Configure SSL Offloading for Outlook Anywhere

Configure SSL Offloading for Outlook Anywhere

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to configure SSL offloading for Outlook Anywhere.

The first time that you run the Enable Outlook Anywhere wizard, you can enable SSL offloading by selecting the check box next to **Allow secure channel (SSL) offloading**. However, if you want to enable SSL offloading and you've already run the Enable Outlook Anywhere wizard without selecting this option, you can use the Shell and the **Set-OutlookAnywhere** cmdlet to set up SSL offloading.

Looking for other management tasks related to Outlook Anywhere? Check out Managing Outlook Anywhere.

Use the EMC to enable SSL offloading for Outlook Anywhere

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "SSL offloading for Outlook Anywhere" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the action pane, click **Enable Outlook Anywhere**.
3. In the Enable Outlook Anywhere wizard, in the box under **External host name**, type the external host name for your organization.
4. Select an available external authentication method. You can select **Basic authentication** or **NTLM authentication**.
5. If you're using an SSL accelerator and you want to do SSL offloading, select the check box next to **Allow secure channel (SSL) offloading**.

Note:

Don't select this option unless you're sure that you have an SSL accelerator that can handle SSL offloading. If you don't have an SSL accelerator that can

handle SSL offloading and you select this option, Outlook Anywhere won't function correctly.

6. Click **Enable** to apply these settings and enable Outlook Anywhere.
7. Click **Finish** to close the Enable Outlook Anywhere wizard.

Use the Shell to configure SSL offloading for Outlook Anywhere

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "SSL offloading for Outlook Anywhere" entry in the Client Access Permissions topic.

This example turns on SSL offloading for the specified Client Access server.

```
Set-OutlookAnywhere -Identity Server01 -SSLOffloading $true
```

For more information about syntax and parameters, see Set-OutlookAnywhere.

Other Tasks

After you configure SSL offloading, you may also want to:

- Configure SSL for Outlook Anywhere
- Configure Authentication for Outlook Anywhere

1.6.3.4 Managing POP3 and IMAP4 Security

Managing POP3 and IMAP4 Security

Exchange Server 2010 > Client Access > Securing Client Access Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-07*

Configuring TLS and SSL for POP3 and IMAP4 Access

Configuring Authentication for POP3 and IMAP4

1.6.3.4.1 Configuring TLS and SSL for POP3 and IMAP4 Access

Configuring TLS and SSL for POP3 and IMAP4 Access

Client Access > Securing Client Access Servers > Managing POP3 and IMAP4 Security >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-08*

Transport Layer Security (TLS) and Secure Sockets Layer (SSL) can be used to secure connections between your users and your Microsoft Exchange Server 2010 computers. TLS and SSL are cryptographic protocols that provide security for communications over the

Internet. We strongly recommend that you use TLS and SSL to help secure communications between your POP3 and IMAP4 clients and the Exchange Server 2010 Client Access server.

You can use the Exchange Management Console and the Exchange Management Shell to configure TLS and SSL on the Exchange Server 2010 server that has the POP3 and IMAP4 services enabled.

Looking for more information about securing Client Access servers? See Securing Client Access Servers.

Configuring TLS and SSL

Before you configure TLS and SSL to help secure POP3 and IMAP4 access, make sure that you understand the process for configuring TLS and SSL for the Exchange 2010 Client Access server. For more information about how to help secure communications, see the following topics:

Securing Client Access Servers

Managing SSL for a Client Access Server

Install an SSL Certificate on a Client Access Server

Understanding TLS Certificates

Configuring TLS and SSL for POP3 and IMAP4

You can use either the EMC or the Shell to configure SSL or TLS for POP3 and IMAP4 on an Exchange 2010 Client Access server.

For more information about how to configure SSL and TLS for POP3 and IMAP4, see the following topics:

Configure POP3 to Use TLS or SSL

Configure IMAP4 to Use TLS or SSL

Configuring Ports for POP3 and IMAP4 When Using TLS and SSL

When you use TLS and SSL for POP3 and IMAP4 access, the Exchange 2010 Client Access server uses the ports listed in the following table to communicate with clients.

Ports for POP3 and IMAP4 access when using TLS and SSL

Protocol	Default port
IMAP4/SSL	993 (TCP)
IMAP4 with or without TLS	143 (TCP)
POP3/SSL	995 (TCP)
POP3 with or without TLS	110 (TCP)

By default, the values in this table are used for communicating with clients. You can specify other ports to use with POP3 and IMAP4 clients if you want to disable communication through the default ports. For more information about how to configure ports for Exchange 2010 POP3 and IMAP4 clients, read Configure IP Addresses and Ports for POP3 and IMAP4 Access.

Configure POP3 to Use TLS or SSL

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Exchange Management Console or the Exchange Management Shell to configure POP3 to use Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

Note:
After you've configured POP3 to use TLS or SSL, you must restart the POP3 service for your settings to take effect. For information about how to restart the POP3 service, see Start and Stop the POP3 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to configure POP3 to use TLS or SSL

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **POP3** and then, in the action pane, under **POP3**, click **Properties**.
4. On the **POP3 Properties** page, click the **Authentication** tab.
5. In the box under **X.509 certificate name**, enter the name of the certificate.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to configure POP3 to use TLS or SSL

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example configures the POP3 service to use TLS or SSL security.

```
Set-PopSettings -server Server01 -X509CertificateName CertificateName01
```

For more information about syntax and parameters, see Set-PopSettings.

Other Tasks

After you configure POP3 to use TLS or SSL, you may also want to:

- Enable or Disable POP3 Access for a User
- Configure IP Addresses and Ports for POP3 and IMAP4 Access

Configure IMAP4 to Use TLS or SSL

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure IMAP4 to use Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

Note:
After you've configured IMAP4 to use TLS or SSL, you must restart the IMAP4 service. For information about how to restart the IMAP4 service, see Start and Stop the IMAP4 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to configure IMAP4 to use TLS or SSL

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **IMAP4** and then, in the action pane, under **IMAP4**, click **Properties**.
4. On the **IMAP4 Properties** page, click the **Authentication** tab.
5. In the box under **X.509 certificate name**, enter the name of the certificate.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to configure IMAP4 to use TLS or SSL

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example configures the IMAP4 service to use TLS or SSL.

```
Set-ImapSettings -server Server01 -X509CertificateName CertificateName01
```

For more information about syntax and parameters, see Set-ImapSettings.

Other Tasks

After you configure IMAP4 to use TLS or SSL, you may also want to:

- Enable or Disable IMAP4 Access for a User
- Configure IP Addresses and Ports for POP3 and IMAP4 Access

Configuring Authentication for POP3 and IMAP4

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-01*

When you use POP3 and IMAP4 clients, you can set authentication options, such as the ability to use TLS encryption, and configure ports for communication with clients. To successfully use the POP3 or IMAP4 services on your Microsoft Exchange Server 2010 server, you need to configure authentication. You can do this using the Exchange Management Console or the Exchange Management Shell.

Before you configure authentication, make sure you understand the process for configuring Secure Sockets Layer (SSL) for the server that has the Client Access server role installed. For more information about how to help secure communications, read the following topics:

- Securing Client Access Servers
- Managing SSL for a Client Access Server
- Install an SSL Certificate on a Client Access Server

Authentication Options for POP3 and IMAP4

There are three authentication options that you can use with POP3 and IMAP4. These options are configured when you use the EMC or the **Set-PopSettings** and **Set-ImapSettings** cmdlets in the Shell. The default ports to use differ depending on the authentication setting that you're using.

The following table lists the different authentication methods that can be used with POP3 and IMAP4 and the default ports for each method.

Authentication options for POP3 and IMAP4

Authentication method	Value	Default port	Description
PlainTextLogin	1	110 (POP3) 995 (POP3 SSL) 143 (IMAP4) 993 (IMAP4 SSL)	TLS encryption is not required on port 110. User name and password are sent unencrypted unless the underlying connection is encrypted by using TLS or SSL. For IMAP4, this corresponds to using the "login" command to authenticate to the Exchange 2010 computer that has the Mailbox server role installed.

PlainTextAuthentication	2	110 (POP3) 995 (POP3 SSL) 143 (IMAP4) 993 (IMAP4 SSL)	TLS encryption is not required on port 110 and port 143. However, Basic authentication is permitted only on a port that uses TLS or SSL encryption. For IMAP4, this corresponds to using the "authenticate" command to authenticate to the Mailbox server.
SecureLogin	3	110 (POP3) 995 (POP3 SSL) 143 (IMAP4) 993 (IMAP4 SSL)	Connection on port 110 and port 143 must use TLS encryption before authenticating.

Note:
Integrated Windows authentication (NTLM) isn't supported for POP3 or IMAP4 connections in the RTM version of Exchange 2010. Support for NTLM authentication for POP3 and IMAP4 connections was brought back in Exchange 2010 SP1. For more information, see Discontinued Features from Exchange 2007 to Exchange 2010 RTM.

1.6.3.4.2.1 Configure Authentication for POP3

Configure Authentication for POP3

Securing Client Access Servers > Managing POP3 and IMAP4 Security > Configuring Authentication for POP3 and IMAP4 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the EMC and the Shell to configure the authentication options for POP3.

Note:
After you've configured authentication for POP3, you must restart the POP3 service. For information about how to restart the POP3 service, see Start and Stop the POP3 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to configure POP3 to use TLS or SSL

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **POP3** and then, in the action pane, under **POP3**, click **Properties**.
4. On the **POP3 Properties** page, click the **Authentication** tab.
5. Under **Logon Method**, select one of the following:
   5.a. **Plain text logon** (Basic authentication) No TLS connection is required for the client to authenticate to the server.
   5.b. **Plain text authentication logon** (Integrated Windows authentication) No TLS connection is required for the client to authenticate to the server.
   5.c. **Secure logon** A TLS connection is required for the client to authenticate to the server.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to configure authentication for POP3

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example allows Basic authentication on an unsecured port if you won't be using TLS encryption.

```
Set-PopSettings -LoginType PlainTextLogin
```

This example restricts Basic authentication to use only secured ports if you won't be using TLS encryption.

```
Set-PopSettings -LoginType PlainTextAuthentication
```

This example allows authentication after you use TLS encryption.

```
Set-PopSettings -LoginType SecureLogin
```

For more information about syntax and parameters, see Set-PopSettings.

Other Tasks

After you configure authentication for POP3, you may also want to:

- Configure Ports for POP3 Authentication
- Set Connection Limits for POP3

1.6.3.4.2.2 Configure Authentication for IMAP4

Configure Authentication for IMAP4

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to configure the authentication options for IMAP4.

Note:

After you've configured authentication for IMAP4, you must restart the IMAP4 service. For

information about how to restart the IMAP4 service, see Start and Stop the IMAP4 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to configure IMAP4 to use TLS or SSL

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **IMAP4** and then, in the action pane, under **IMAP4**, click **Properties**.
4. On the **IMAP4 Properties** page, click the **Authentication** tab.
5. Under **Logon Method**, select one of the following:
   - 5.a. **Plain text logon** (Basic authentication) No TLS connection is required for the client to authenticate to the server.
   - 5.b. **Plain text authentication logon** (Integrated Windows authentication) No TLS connection is required for the client to authenticate to the server.
   - 5.c. **Secure logon** A TLS connection is required for the client to authenticate to the server.
6. Click **Apply**, and then click **OK** to save your changes.

Use the Shell to configure authentication for IMAP4

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example allows Basic authentication on an unsecured port if you won't be using TLS encryption,

```
Set-ImapSettings -LoginType PlainTextLogin
```

This example restricts Basic authentication to use only secured ports if you won't be using TLS encryption.

```
Set-ImapSettings -LoginType PlainTextAuthentication
```

This example allows authentication after you use TLS encryption.

```
Set-ImapSettings -LoginType SecureLogin
```

For more information about syntax and parameters, see Set-ImapSettings.

Other Tasks

After you configure authentication for IMAP4, you may also want to:

- Configure Ports for IMAP4 Authentication
- Set Connection Limits for IMAP4

1.6.3.4.2.3 Configure Ports for POP3 Authentication

Configure Ports for POP3 Authentication

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to configure Exchange to use ports other than the default ports for POP3 authentication.

Note:

After you've configured ports for POP3 authentication, you must restart the POP3 service. For more information about how to restart the POP3 service, see Start and Stop the POP3 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to configure ports for POP3 authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **IMAP4** and then, in the action pane, under **POP3**, click **Properties**.
4. On the **Binding** tab, do one of the following:
   - To configure ports for TLS or unencrypted connections, under **TLS or Unencrypted Connections**, click **Edit**. Under **Port to Use**, in the box next to **Port**, enter a port number.
   - To configure ports for SSL connections, under **Secure Sockets Layer (SSL) Connections**, click **Edit**. Under **Port to Use**, in the box next to **Port**, enter a port number.
5. Click **OK** to save your changes.

Use the Shell to configure ports for POP3 authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example sets the port for unencrypted or TLS POP3 connections to a value other than the default port number.

```
Set-PopSettings -UnencryptedOrTLSBindings IPaddress:Port
```

This example sets the port for SSL POP3 connections to a value other than the default port number.

```
Set-PopSettings -SSLBindings IPaddress:Port
```

For more information about syntax and parameters, see Set-PopSettings.

Other Tasks

After you configure ports for POP3 authentication, you may also want to:

- Configure Ports for IMAP4 Authentication

1.6.3.4.2.4 Configure Ports for IMAP4 Authentication

Configure Ports for IMAP4 Authentication

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to configure Exchange to use ports other than the default ports for IMAP4 authentication.

Note:

After you've configured ports for IMAP4 authentication, you must restart the IMAP4 service. For information about how to restart the IMAP4 service, see Start and Stop the IMAP4 Service.

Looking for other management tasks related to setting up POP3 and IMAP4? Check out Managing POP3 and IMAP4.

Use the EMC to configure ports for IMAP4 authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration > Client Access**.
2. In the work pane, click the **POP3 and IMAP4** tab.
3. Select **IMAP4** and then, in the action pane, under **IMAP4**, click **Properties**.
4. On the **Binding** tab, do one of the following:
   - 4.a. To configure ports for TLS or unencrypted connections, under **TLS or Unencrypted Connections**, click **Edit**. Under **Port to Use**, in the box next to **Port**, enter a port number.
   - 4.b. To configure ports for SSL connections, under **Secure Sockets Layer (SSL) Connections**, click **Edit**. Under **Port to Use**, in the box next to **Port**, enter a port number.
5. Click **OK** to save your changes.

Use the Shell to configure ports for IMAP4

authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "POP3 and IMAP4" entry in the Client Access Permissions topic.

This example sets the port for unencrypted or TLS IMAP4 connections to a value other than the default port number.

```
Set-ImapSettings -UnencryptedOrTLSBindings IPaddress:Port
```

This example sets the port for SSL IMAP4 connections to a value other than the default port number.

```
Set-ImapSettings -SSLBindings IPaddress:Port
```

For more information about syntax and parameters, see Set-ImapSettings.

Other Tasks

After you configure ports for IMAP4 authentication, you may also want to:

- Configure Ports for POP3 Authentication

1.6.3.5 Managing Outlook Web App Security

Managing Outlook Web App Security

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-25*

This topic describes the authentication methods that you can use to help secure Outlook Web App on computers running Microsoft Exchange Server 2010 that have the Client Access server role installed.

Looking for management tasks related to securing client access? See Securing Client Access Servers.

Contents

Authentication Methods

You can configure the following types of authentication methods on an Exchange 2010 Client Access server:

- Standard
- Forms-based authentication

In addition, you can use the following types of authentication:

- Microsoft Internet Security and Acceleration (ISA) Server forms-based authentication
- Smart card and certificate authentication
- RSA SecurID authentication

Standard and Forms-Based Authentication

You can configure standard and forms-based authentication methods for Outlook Web App by using the Exchange Management Console or the Exchange Management Shell.

- **Standard authentication methods** Standard authentication methods include Integrated Windows authentication, Digest authentication, and Basic authentication. For more information about how to configure standard authentication methods, see Setting Up Standard Authentication Methods for Outlook Web App.
- **Forms-based authentication** Forms-based authentication creates a sign in page for Outlook Web App. Forms-based authentication uses cookies to store encrypted user sign in credentials and password information. For more information about forms-based authentication, see Setting Up Forms-Based Authentication for Outlook Web App.

If you configure multiple authentication methods, Internet Information Services (IIS) uses most restrictive method first. IIS then searches the list of available authentication protocols starting with the most restrictive until an authentication method that is supported by the client and the server is found.

The following table compares the standard and forms-based authentication methods using security level, handling of user sign-in credentials, and client requirements as the criteria.

Comparison of standard and forms-based authentication

Authentication method	Security level	How passwords are sent	Client requirements
Basic authentication	Low (unless Secure Sockets Layer (SSL) is enabled)	Base 64-encoded clear text	All browsers support Basic authentication.
Digest authentication	Medium	Hashed by using MD5.	Microsoft Internet Explorer 5 through Internet Explorer 8.
Integrated Windows authentication	Low (unless SSL is enabled)	Hashed when Integrated Windows authentication is used; Kerberos ticket when Kerberos is used. Integrated Windows authentication includes the Kerberos and NTLM authentication methods.	Internet Explorer 2.0 through Internet Explorer 8 for Integrated Windows authentication. Windows 2000 Server or Windows Server 2008 with Internet Explorer 5 through Internet Explorer 8 for Kerberos.
Forms-based authentication	High	Encrypts user authentication information and stores it in a cookie. Requires SSL to keep	Internet Explorer

		the cookie secure.	

Return to top

Other Authentication Methods

There are other authentication methods that you can use to help secure Outlook Web App. These methods include:

- **ISA Server forms-based authentication** Using ISA Server, you can securely publish Outlook Web App servers by using mail server publishing rules. ISA Server also lets you configure forms-based authentication and control e-mail attachment availability to help protect resources for your organization when they're accessed through Outlook Web App. For more information about how to use ISA Server as an advanced firewall solution, see the Internet Security and Acceleration Server Web site.
- **Smart card and certificate authentication** Certificates can reside either in the certificate store on a client computer or on a smart card. A certificate authentication method uses the Extensible Authentication Protocol (EAP) and Transport Layer Security (TLS) protocols. In EAP-TLS certificate authentication, the client and the server prove their identities to one another. For example, an Outlook Web App client on a user's computer presents its user certificate to the Client Access server, and the Client Access server presents its computer certificate to the Outlook Web App client computer. This provides mutual authentication. For more information about smart card and other certificate authentication methods, see Windows Server 2008 and Windows Server 2008 R2
- **RSA SecurID authentication** You can use the third-party product, RSA SecurID, to configure RSA SecurID authentication methods on the Client Access server. For more information about RSA SecurID, see http://www.rsasecurity.com.

1.6.3.5.1 Configure Outlook Web App Virtual Directories to Use SSL

Configure Outlook Web App Virtual Directories to Use SSL

Client Access > Securing Client Access Servers > Managing Outlook Web App Security >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Internet Information Services (IIS) Manager to configure Outlook Web App virtual directories to use Secure Sockets Layer (SSL). By default, when you install the Client Access server role, an Outlook Web App virtual directory named \owa is created in the default IIS Web site on the Exchange server. By default, this virtual directory and the default Web site are configured to require SSL.

If you want to use SSL to help secure additional Outlook Web App virtual directories or Web sites that you've created, you must do so manually. To configure a site to use SSL, you must obtain a certificate and configure the Web site or virtual directory to require SSL by using that certificate.

Looking for other management tasks related to security for Outlook Web App? Check out

Managing Outlook Web App Security.

Prerequisites

Identify the SSL certificate that you'll use. For more information about how to obtain and manage SSL certificates, see Managing SSL for a Client Access Server.

Use IIS Manager to configure SSL on Outlook Web App virtual directories

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "IIS Manager" entry in the Client Access Permissions topic.

1. In IIS Manager, select the **Default Web site** or the Web site where you're hosting your Outlook Web App virtual directories.
2. On the web site **Home**, double-click **SSL Settings**.
3. In **SSL Settings**, select **Require SSL**. **Require 128-bit SSL** is optional, but if checked it will provide greater security.

   Note:

   If you're using an SSL certificate that was created during Exchange Setup, an error message will appear to notify you that the certificate isn't a trusted certificate. Make sure that you trust the certification authority (CA) that issued the certificate or use an SSL certificate that's trusted by your CA.
4. Under **Client Certificates**, select **Ignore**.
5. In the action pane, click **Apply** to save your changes.

After you complete this procedure, all Outlook Web App virtual directories on the Web site for which you haven't explicitly disabled SSL will be configured to use SSL.

Other Tasks

After you configure SSL on Outlook Web App virtual directories, you may also want to review:

- Setting Up Forms-Based Authentication for Outlook Web App
- Outlook Web App and S/MIME

1.6.3.5.2 Setting Up Forms-Based Authentication for Outlook Web App

Setting Up Forms-Based Authentication for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-10*

Forms-based authentication enables a sign-in page for Exchange Server 2010 Outlook Web App that uses a cookie to store a user's encrypted sign-in credentials in the Internet browser. Tracking the use of this cookie enables the Exchange server to monitor the activity of Outlook Web App sessions on public and private computers. If a session is inactive for too long, the server blocks access until the user re-authenticates.

Contents

Using Cookies to Control Access

The first time that the user name and password are sent to the Client Access server to authenticate an Outlook Web App session, an encrypted cookie is created that's used to track user activity. When the user closes the Internet browser or clicks **Sign Out** to sign out of their Outlook Web App session, the cookie is cleared. The user name and password are sent to the Client Access server only for the initial user sign-in. After the initial sign-in is complete, only the cookie is used for authentication between the client computer and the Client Access server.

Setting the Value for Cookie Time-Out on Public Computers

By default, when a user selects the **This is a public or shared computer** option on the Outlook Web App sign-in page, the cookie on the computer expires automatically and the user is signed out when they haven't used Outlook Web App for 15 minutes.

Automatic time-out is valuable because it helps protect users' accounts from unauthorized access. To match the security requirements of your organization, you can configure the inactivity time-out values on the Exchange Client Access server.

Although automatic time-out greatly reduces the risk of unauthorized access, it doesn't eliminate the possibility that an unauthorized user might access an Outlook Web App account if a session is left running on a public computer. Therefore, make sure to warn users to take precautions to avoid risks. For example, tell them to sign out from Outlook Web App and close the Web browser when they've finished using Outlook Web App.

For more information about how to configure cookie time-out values for public computers, see Set the Forms-Based Authentication Public Computer Cookie Time-Out Value.

Setting the Value for Cookie Time-Out on Private Computers

When a user selects the **This is a private computer** option on the Outlook Web App sign-in page, the Exchange server allows a longer period of inactivity before automatically ending the Outlook Web App session. The default time-out value for private sign-in is eight hours. Because of the relationship between the recycle time of encryption keys and the time-out value configured on the server, the actual default time-out value for private sign-in can be between eight to twelve hours. For more information, see Understanding Encryption for User Sign-in from Public and Private Computers. The private computer cookie time-out option is intended to benefit Outlook Web App users who are using their own computer or a computer that's on a corporate network.

It's important to warn users about the risks associated with selecting the **This is a private computer** option. A user should select the private computer option only if they are the sole operator of the computer and the computer complies with the security policies for your organization.

For more information about how to configure cookie time-out values for private computers, see Set the Forms-Based Authentication Private Computer Cookie Time-Out

Value.

Return to top

Determining User Activity

After an Outlook Web App session has been inactive for a certain period of time, the Client Access server no longer has the decryption key to read the cookie and the user will be denied access until they authenticate again.

Exchange 2010 uses the following information to determine user activity:

- Interaction between the client computer and the Client Access server that's initiated by the user is considered activity. For example, if a user opens, sends, or saves an item; switches folders or modules; or updates the view or the Web browser window, Exchange 2010 considers this to be activity.

  Note:
  Interaction between the client computer and the server that's automatically generated by the Client Access server isn't considered activity. For example, new e-mail notifications and reminders that are generated by the Client Access server in an Outlook Web App session aren't considered activity.

- In Outlook Web App, any user interaction, including entering text in an e-mail message or meeting request, is considered activity. In the light version of Outlook Web App, any user activity other than entering text is considered activity.

Configuring the Sign-in Prompt Used by Forms-Based Authentication

Instead of a pop-up window, forms-based authentication creates a sign-in page for Outlook Web App. You can configure the sign-in prompt for forms-based authentication using the Exchange Management Console or the Exchange Management Shell. The configuration changes you make change only the text of the sign-in prompt. They don't change the format in which the user must sign in. For example, you can configure the forms-based authentication sign-in page to prompt users to provide their sign-in information in the format domain\user name. However, a user can also enter his or her user principal name (UPN) and the sign-in will be successful.

The following types of sign-in prompts can be used by forms-based authentication on the Outlook Web App sign-in page. Select the prompt that will be easiest for your users to understand and use.

- **Full Domain** The domain and user name of the user in the format domain \user name. For example, Contoso\Kweku.
- **Principal Name** The UPN. The UPN has two parts: the UPN prefix that's the user account name and the UPN suffix that's the DNS domain name. The prefix and the suffix are joined by the at (@) sign to make the complete UPN. For example, Kweku@contoso.com. Users can access Outlook Web App by entering their primary e-mail address or by entering their UPN.
- **User Name** The user name only. The domain name isn't included. For example, Kweku. This sign-in format will work only if the domain name has been configured.

  Note:
  If necessary, you can change the format the user must use to sign in to Outlook Web App by configuring Active Directory and Internet Information Services (IIS). Using Active Directory and IIS to set which user name formats users can enter to be authenticated is independent of the Outlook Web App

forms-based authentication prompt discussed earlier.

Return to top

Understanding Encryption for User Sign-in from Public and Private Computers

Encryption of user sign-in credentials for both public and private Outlook Web App sign-in types involves a set of six Hashed-based Message Authentication Codes (HMACs). HMACs are 160-bit keys that are generated on the Client Access server. HMACs improve sign-in security by combining hashing algorithms with cryptographic functions to encrypt user sign-in credentials. Encryption and decryption of a cookie are performed by the same Client Access server. Only the Client Access server that generated the authentication key has the key to decrypt that cookie.

When forms-based authentication is used, the Client Access server cycles through a set of three keys for each type of sign-in, public and private, at a set rate. This is known as the recycle time. The recycle time for a key is one-half of the time-out value for the sign-in. For example, when the time-out value for the public sign-in is set to 15 minutes, the public key recycle time is 7.5 minutes.

The six sign-in keys are created by the Client Access server when the Outlook Web App virtual directories are started. Three are used with public computer sign-ins, and three are used with private computer sign-ins. When a user signs in, the current key for their sign-in type is used to encrypt the user's authentication information into a cookie.

When the recycle time has passed, the Client Access server moves to the next key. After all three keys for a type of sign-in have been used, the Client Access server deletes the oldest key and creates a new one. The Client Access server always keeps three keys available for each sign-in type: the current key and the two most recent keys. The recycling of keys continues as long as Outlook Web App is running on the Client Access server. The same keys are used for all users.

Any cookie that has been encrypted by using an active key will be accepted. When a user activity request is received by the Client Access server, the cookie for that request is replaced with a new cookie that's been encrypted by using the newest key. A user session is timed out when the cookie associated with it is encrypted by an older key that's been discarded.

Because of the relationship between the recycle time of encryption keys and user time-out configured on the server, the actual time-out period for a user can be between the configured time-out and the configured time-out plus one-half of that value. For example, if the configured time-out is 30 minutes, the actual time-out for any user session may be between 30 minutes and 45 minutes.

The following table provides information about the cookie time-out and authentication key recycling time based on a user sign-in from a public or private computer.

Default cookie time-out and authentication key recycling time for each user sign-in type

Sign-in	Cookie time-out value	Recycle time for authentication key if you use the default time-out value
Public	One minute to 30 days. The default is 15 minutes.	7.5 minutes

Private	One minute to 30 days. The default is 8 hours.	4 hours

Note:
You can configure the cookie time-out value in minutes by using the registry. The recycle time of the authentication key is at least one-third, and not more than one-half, that of the cookie time-out value.

Return to top

Using SSL to Help Secure Outlook Web App

By default, Secure Sockets Layer (SSL) encryption is turned on when you install the Client Access server role. If SSL isn't used, the user name and password will be sent in clear text at initial sign-in. When SSL is used, it encrypts all communications between the client computer and the Client Access server and helps prevent sensitive information, such as user names, passwords, and e-mail messages, from being viewed by third parties.

Return to top

1.6.3.5.2.1 Configure Forms-Based Authentication for Outlook Web App

Configure Forms-Based Authentication for Outlook Web App

Securing Client Access Servers > Managing Outlook Web App Security > Setting Up Forms-Based Authentication for Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure forms-based authentication and the sign-in prompt that's used by forms-based authentication on an Outlook Web App virtual directory on a Client Access server.

Forms-based authentication gives you three options for the default sign-in format. These options change only the text on the Outlook Web App sign-in page. They don't cause a particular format to be required. The user can use any of the standard sign-in formats regardless of the text on the page.

- **FullDomain** This is the domain and user name of the user in the format domain\user name. For example, for a user named Kweku in the domain Contoso, the sign-in would be contoso\kweku.
- **PrincipalName** If user principal name (UPN) sign-in format is specified, the **User Name** field on the Outlook Web App sign-in page guides the user to enter their e-mail address. For example, kweku@contoso.com. Users can access Outlook Web App by entering their primary e-mail address or by entering their UPN.
- **UserName** This is the user name only and doesn't include the domain name. For example, Kweku. If you use the *UserName* sign-in prompt for forms-based authentication, you must also specify the *DefaultDomain* property. The *DefaultDomain* property determines the default domain to use when a user tries to access Outlook Web App. For example, if the default domain is Contoso, and a domain user named Kweku signs in to Outlook Web App, only Kweku must be entered as the user name. The server will use the default

domain Contoso. If the user isn't a member of the Contoso domain, the domain and user name must be entered.

Looking for other management tasks related to forms-based authentication? Check out Setting Up Forms-Based Authentication for Outlook Web App.

Use the EMC to configure forms-based authentication for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, select **Server Configuration**, select **Client Access**, select the server that hosts the Outlook Web App virtual directory, and then click the **Outlook Web App** tab.
2. In the work pane, select the virtual directory that you want to configure to use forms-based authentication, and then click **Properties**.
3. Click the **Authentication** tab.
4. Select **Use forms-based authentication**.
5. Select the sign-in format that you want to use.

Note:

You must restart Internet Information Services (IIS) by using the command `iisreset/noforce` for these changes to take effect.

Use the Shell to configure forms-based authentication for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example configures forms-based authentication on an Outlook Web App virtual directory in the default IIS Web site on the local Exchange server.

```
Set-owavirtualdirectory -identity "owa (default web site)" -FormsAuthentication:$
```

Use the Shell to configure the default sign-in method used by forms-based authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example configures a full domain sign-in format,

```
Set-owavirtualdirectory -identity "owa (default web site)" -LogonFormat FullDomai
```

This example configures a UPN sign-in format.

```
Set-owavirtualdirectory -identity "owa (default web site)" -LogonFormat Principal
```

This example configures a user name sign-in format and sets the default domain.

```
Set-owavirtualdirectory -identity "owa (default web site)" -LogonFormat UserName
```

Note:
You must restart IIS by using the command `iisreset/noforce` for these changes to take effect.

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

Other Tasks

After you configure forms-based authentication for Outlook Web App, you may also want to:

- Configure Outlook Web App Virtual Directories to Use SSL
- Set the Forms-Based Authentication Private Computer Cookie Time-Out Value
- Set the Forms-Based Authentication Public Computer Cookie Time-Out Value

1.6.3.5.2.2 Set the Forms-Based Authentication Public Computer Cookie Time-Out Value

Set the Forms-Based Authentication Public Computer Cookie Time-Out Value

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to configure the cookie time-out values for public computers by using forms-based authentication on an Outlook Web App virtual directory on a Microsoft Exchange Server 2010 Client Access server.

Caution:
Although automatic time-out reduces the risk of unauthorized access, it doesn't completely eliminate the possibility that an unauthorized user might access an Exchange mailbox if a session is left running on a public computer. Therefore, make sure to warn users to take precautions to avoid risks.

Looking for other management tasks related to forms-based authentication? Check out Setting Up Forms-Based Authentication for Outlook Web App.

Prerequisites

Note:
The Outlook Web App virtual directory must be configured to use forms-based authentication.

Caution:
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Use Registry Editor to set the cookie time-out values for public computers using forms-based authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Registry Editor" entry in the Client Access Permissions topic.

1. On the Client Access server, sign in by using the Exchange administrator account, and then start Registry Editor (regedit).
2. In Registry Editor, locate the following registry key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA**
3. On the **Edit** menu, point to **New**, and then click **DWORD Value**. In the details pane, name the new value **PublicTimeout**.
4. Right-click the **PublicTimeout** DWORD value, and then click **Modify**.
5. In **Edit DWORD Value**, under **Base**, click **Decimal**.
6. In the **Value Data** box, type a value in minutes between 1 and 43,200 for a maximum of 30 days. Click **OK**.

Note:

You must restart the Forms-Based Authentication service for the changes to take effect. On the Client Access server, go to **Start** > **Administrative Tools** > **Services**. In Services, right-click **Microsoft Exchange Forms-Based Authentication service**, and then click **Restart**.

Use the Shell to set the cookie time-out values for public computers using forms-based authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App mailbox policies" entry in the Client Access Permissions topic.

This example sets the public computer cookie time-out value.

```
set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\MSExchange OWA' -name P
```

Note:

You must restart the Forms-Based Authentication service for the changes to take effect. On the Client Access server, go to **Start** > **Administrative Tools** > **Services**. In Services, right-click **Microsoft Exchange Forms-Based Authentication service**, and then click **Restart**.

This example lets you view the public computer cookie time-out value.

```
get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\MSExchange OWA' -name P
```

Other Tasks

After you set the cookie time-out values for public computers using forms-based authentication, you may also want to:

- Configure Outlook Web App Virtual Directories to Use SSL

1.6.3.5.2.3 Set the Forms-Based Authentication Private Computer Cookie Time-Out Value

Set the Forms-Based Authentication Private Computer Cookie Time-Out Value

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can set the cookie time-out values for private computers by using forms-based authentication on an Outlook Web App virtual directory in Microsoft Exchange Server 2010. Private computers are also known as trusted computers.

Caution:

It's important that you warn users of the risks associated with selecting the **This is a private computer** option. A user should select **This is a private computer** only if the user is the sole operator of the computer and the computer complies with your organization's security policies.

Looking for other management tasks related to forms-based authentication? Check out Setting Up Forms-Based Authentication for Outlook Web App.

Prerequisites

The Outlook Web App virtual directory is configured to use forms-based authentication.

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Use Registry Editor to set the cookie time-out values for private computers using forms-based authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Registry Editor" entry in the Client Access Permissions topic.

1. On the Exchange Client Access server, sign in by using your Exchange administrator account, and then start Registry Editor (regedit).
2. In Registry Editor, locate the following registry key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA**
3. On the **Edit** menu, point to **New**, and then click **DWORD Value**. In the details pane, name the new value **PrivateTimeout**.
4. Right-click the **PrivateTimeout** DWORD value, and then click **Modify**.
5. In **Edit DWORD Value**, under **Base**, click **Decimal**.
6. In the **Value Data** box, type a value in minutes between 1 and 43,200 for a maximum of 30 days. Click **OK**.

Note:

You must restart the Forms-Based Authentication service for the changes to take effect. On the Client Access server, go to **Start** > **Administrative Tools** > **Services**. In Services, right-click **Microsoft Exchange Forms-Based Authentication service** and click **Restart**.

Use the Shell to set the cookie time-out values for private computers using forms-based authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example sets the private computer cookie time-out value.

```
set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\MSExchange OWA' -name P
```

Note:

You must restart the Forms-Based Authentication service for the changes to take effect. On the Client Access server, go to **Start** > **Administrative Tools** > **Services**. In Services, right-click **Microsoft Exchange Forms-Based Authentication service** and click **Restart**.

This example lets you view the private computer cookie time-out value.

```
get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\MSExchange OWA' -name P
```

Other Tasks

After you set the cookie time-out values for private computers using forms-based authentication, you may also want to:

- Configure Outlook Web App Virtual Directories to Use SSL

1.6.3.5.3 Setting Up Standard Authentication Methods for Outlook Web App

Setting Up Standard Authentication Methods for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Standard authentication methods can help secure Microsoft Exchange Server 2010 Client Access servers for Outlook Web App.

In Exchange 2010, Client Access servers support Integrated Windows authentication and HTTP 1.1 Digest authentication for Exchange 2010 virtual directories. Exchange 2010 virtual directories on a server that's running only the Client Access server role support only Basic and forms-based authentication.

Standard authentication methods include Basic authentication, Digest authentication, and Integrated Windows authentication.

Note:
By default, Exchange 2010 enables forms-based authentication.

Contents

Basic Authentication

Basic authentication is a simple authentication mechanism that's defined by the HTTP specification that encodes a user's sign-in name and password before the user's credentials are sent to the server.

Basic authentication doesn't support single sign-on. Windows Server 2008 authentication enables single sign-on to all network resources. With single sign-on, a user can sign in to the domain one time by using a single password or smart card and authenticate to any computer in the domain.

Basic authentication is supported by all Web browsers but isn't secure unless you require Secure Sockets Layer (SSL) encryption.

Digest Authentication

Digest authentication transmits passwords over the network as a hash value for additional security. Digest authentication can be used only in Windows Server 2008, Windows Server 2003, and Microsoft Windows 2000 Server domains for users who have an account that's stored in Active Directory. For more information about Digest authentication, see the Windows Server 2008 and Internet Information Services (IIS) Manager documentation.

Digest authentication is available only on Exchange 2010 virtual directories.

Important:
If you're using Digest or Basic authentication, when a user uses a kiosk, caching credentials can pose a security risk if the user can't close the browser and end the browser process between sessions. This risk occurs because a user's credentials remain in the cache when the next user accesses the kiosk. To enable Outlook Web App on a kiosk, make sure that the user can close the browser between sessions and end the browser processes. Otherwise, consider using a third-party product that incorporates two-factor authentication, in which the user must present a physical token together with a password to use Outlook Web App on the kiosk.

Integrated Windows Authentication

Integrated Windows authentication requires that users have a valid Windows Server 2008, Windows Server 2003, or Windows 2000 Server user account name and password to access information. Users signed in to the local network aren't prompted for their user names and passwords. Instead, the server negotiates with the Windows security packages that are installed on the client computer. This method enables the server to authenticate users without prompting them for sign-in information. The authentication credentials are protected, but all other communication will be sent in clear text unless SSL is used.

On an Exchange 2010 server on which only the Client Access server role is installed, Integrated Windows authentication can be used only with Exchange 2010 virtual directories. On a server that has both the Client Access and Mailbox roles installed, Integrated Windows authentication can be used with any virtual directory. For more information about Integrated Windows authentication, see the Windows Server 2008 documentation.

Note:
Integrated Windows authentication is supported only on computers that are running a Windows operating system and Internet Explorer. Integrated Windows authentication may work with other Web browsers if they've been configured to pass the user's sign-in credentials to the server that's requesting authentication.

1.6.3.5.3.1 Configure Integrated Windows Authentication

Configure Integrated Windows Authentication

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure Integrated Windows authentication for Outlook Web App in Microsoft Exchange Server 2010. Integrated Windows authentication enables the server to authenticate users who are signed in to the network without prompting them for their user name and password and without transmitting information that isn't encrypted over the network.

Note:
Integrated Windows authentication can be set only on Exchange 2010 virtual directories on an Exchange 2010 server that has only the Client Access server role installed. Integrated Windows authentication can be set on any Outlook Web App virtual directory on an Exchange 2010 server that has both the Client Access and Mailbox server roles installed.

Looking for other management tasks related to standard authentication for Outlook Web App? Check out Setting Up Standard Authentication Methods for Outlook Web App.

Use the EMC to configure Integrated Windows authentication for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, locate the virtual directory that you want to configure to use Integrated Windows authentication by using the information in step 2 or step 3.
2. Select **Server Configuration**, select **Client Access**, select the server hosting the Outlook Web App virtual directory, and then click the **Outlook Web App** tab.
3. In the work pane, select the virtual directory that you want to configure to use Integrated Windows authentication, and then click **Properties**.
4. Click the **Authentication** tab.

5. Select **Use one or more standard authentication methods**.
6. Select **Integrated Windows authentication**.
7. Click **OK**.

Use the Shell to configure Integrated Windows authentication for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example configures Integrated Windows authentication on the default Outlook Web App virtual directory in the default Internet Information Services (IIS) Web site on the local Exchange server.

```
Set-OwaVirtualDirectory -Identity "owa (Default Web Site)" -WindowsAuthentication
```

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

Other Tasks

After you configure Integrated Windows authentication for Outlook Web App, you may also want toConfigure Outlook Web App Virtual Directories to Use SSL.

1.6.3.5.3.2 Configure Basic Authentication

Configure Basic Authentication

Securing Client Access Servers > Managing Outlook Web App Security > Setting Up Standard Authentication Methods for Outlook Web App >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure Windows Basic authentication for Outlook Web App in Microsoft Exchange Server 2010. Basic authentication sends the user's sign-in name and password in clear text and shouldn't be used without using Secure Sockets Layer (SSL) encryption between the client computers and the computer that has the Client Access server role installed.

Looking for other management tasks related to standard authentication for Outlook Web App? Check out Setting Up Standard Authentication Methods for Outlook Web App.

Use the EMC to configure Basic authentication for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, locate the virtual directory that you want to configure to use Basic authentication by using the information in step 2 or step 3.

2. Select **Server Configuration**, select **Client Access**, select the server hosting the Outlook Web App virtual directory, and then click the **Outlook Web App** tab.
3. In the work pane, select the virtual directory that you want to configure to use Basic authentication, and then click **Properties**.
4. Click the **Authentication** tab.
5. Select **Use one or more standard authentication methods**.
6. Select **Basic authentication**.
7. Click **OK**.

Use the Shell to configure Basic authentication for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example configures Basic authentication on the default Outlook Web App virtual directory in the default Internet Information Services (IIS) Web site on the local Exchange server.

```
Set-OwaVirtualDirectory -Identity "owa (Default Web Site)" -BasicAuthentication <
```

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

Other Tasks

After you configure Basic authentication for Outlook Web App, you may also want to Configure Outlook Web App Virtual Directories to Use SSL.

1.6.3.5.3.3 Configure Digest Authentication

Configure Digest Authentication

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure Windows Digest authentication for Outlook Web App in Microsoft Exchange Server 2010. Digest authentication transmits passwords over the network as a hash value for additional security. Digest authentication isn't fully secure if the user is unable to close the browser and end the browser process between sessions. This problem may occur if the user is using Outlook Web App on a kiosk. If the browser can't be closed, the user's credentials remain in the cache where the next user may be able to access them.

Note:

Digest authentication can be set only on Exchange 2010 virtual directories.

Looking for other management tasks related to security for Outlook Web App? Check out Managing Outlook Web App Security.

Use the EMC to configure Digest authentication for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, locate the virtual directory that you want to configure to use Digest authentication by using the information in step 2 or step 3.
2. Select **Server Configuration**, select **Client Access**, select the server hosting the Outlook Web App virtual directory, and then click the **Outlook Web App** tab.
3. In the work pane, select the virtual directory that you want to configure to use Digest authentication, and then click **Properties**.
4. Click the **Authentication** tab.
5. Select **Use one or more standard authentication methods**.
6. Select **Digest authentication**.
7. Click **OK**.

Use the Shell to configure Digest authentication for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example configures Digest authentication on the default Outlook Web App virtual directory in the default Internet Information Services (IIS) Web site on the local Exchange server.

```
Set-OwaVirtualDirectory -Identity "owa (Default Web Site)" -DigestAuthentication
```

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

1.6.3.5.4 Outlook Web App and S/MIME

Outlook Web App and S/MIME

Client Access > Securing Client Access Servers > Managing Outlook Web App Security >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

S/MIME lets users encrypt outgoing messages and attachments so that only intended recipients who have a digital identification (ID), also known as a certificate, can read them. With S/MIME, users can digitally sign a message, which provides the recipients with a way to verify the identity of the sender and that the message hasn't been tampered with.

Contents

Supporting S/MIME

To support S/MIME in your Exchange organization, you must build a public key infrastructure (PKI).

A PKI is a system of digital certificates, certification authorities (CAs), and registration authorities (RAs) that verify and authenticate the validity of each party that is involved in an electronic transaction by using public key cryptography. When you implement a CA in an organization that uses Active Directory, you provide an infrastructure for certificate life-cycle management, renewal, trust management, and revocation. However, there is some additional cost involved in deploying servers and infrastructure to create and manage Microsoft Windows PKI-generated certificates.

Certificate Services is required to deploy a Windows PKI and can be installed through Add or Remove Programs in Control Panel. You can install Certificate Services on any server in the domain.

If you obtain certificates from a domain-joined Windows CA, you can use the CA to request or sign certificates to issue to the servers or computers on your network. This enables you to use a PKI that resembles a third-party certificate vendor, but is less expensive. Although these PKI certificates cannot be deployed publicly, as other types of certificates can be, when a PKI CA signs the requestor's certificate by using the private key, the requestor is verified. The public key of this CA is part of the certificate. A server that has this certificate in the trusted root certificate store can use that public key to decrypt the requestor's certificate and authenticate the requestor.

A PKI enables organizations to publish their own certificates. Clients can request and receive certificates from a PKI on the internal network. The PKI can renew or revoke certificates.

Requirements to Support S/MIME in Outlook Web App

S/MIME requires that users sign in to Outlook Web App using Microsoft Internet Explorer 7 or Internet Explorer 8. In addition to requiring Internet Explorer 7 or Internet Explorer 8, S/MIME also requires that Secure Sockets Layer (SSL) be used by the /owa virtual directory. S/MIME is not supported in Outlook Web App Light.

Using S/MIME in Outlook Web App

Users must have a digital ID and must install the S/MIME control for Outlook Web App before they can send encrypted and digitally-signed messages using Outlook Web App. They must also have a digital ID and the S/MIME control to read encrypted messages in Outlook Web App. The S/MIME control is necessary to verify the signature on a digitally-signed message.

The S/MIME control for Outlook Web App is installed on a user’s computer by using the SMIME tab in Options. After the user has received a digital ID and the S/MIME control has

been installed on their computer, they can use S/MIME to help secure e-mail mail messages.

Feature Additions and Limitations with S/MIME

When they use S/MIME, users gain additional features that are not otherwise available in Outlook Web App. These features include the ability to do the following:

- Attach messages to messages
- Paste images in messages
- Attach files by using a simpler UI and let users attach multiple files in a single operation.
- When they use S/MIME, users will encounter the following limitations:
- WebReady Document Viewing only works in clear-signed messages. It does not work in encrypted messages or in opaque-signed messages.
- When some content types are sent from Outlook as S/MIME messages, they cannot be displayed in Outlook Web App. Outlook Web App will display a banner in the message header when this happens.
- Most S/MIME features are not available when a user opens a folder in another mailbox or uses explicit sign-in to open another user's mailbox. The only S/MIME feature that is available in those cases is verification of digital signatures.

For More Information

Active Directory Certificate Services and Public Key Management

1.6.3.5.4.1 Enable or Disable S/MIME in Outlook Web App

Enable or Disable S/MIME in Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the EMC and the Shell to enable or disable use of Secure/Multipurpose Internet Mail Extensions (S/MIME) in Microsoft Office Outlook Web App. By default, S/MIME is enabled on the /owa virtual directory.

Looking for other management tasks related to security for Outlook Web App? Check out Managing Outlook Web App Security.

Use the EMC to enable or disable S/MIME in Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. At the top of the work pane, click the server that hosts the Outlook Web App

virtual directory.
3. In the work pane, select **owa (Default Web Site)**, and then, in the action pane, click **Properties**.
4. On the **owa (Default Web Site) Properties** page, click the **Segmentation** tab.
5. In the **Segmentation** window, find the **S/MIME** feature.
6. To enable or disable S/MIME, select **S/MIME**, and then click **Enable** or **Disable**.
7. Click **OK** to save your change, and then close the properties window.

Use the Shell to enable or disable S/MIME in Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Outlook Web App virtual directories" entry in the Client Access Permissions topic.

This example disables S/MIME on the Outlook Web App virtual directory named /owa in the default Internet Information Services (IIS) Web site on the local server.

```
Set-OWAVirtualDirectory -identity "owa (Default Web Site)" -SMimeEnabled $false
```

This example enables S/MIME.

```
Set-OWAVirtualDirectory -identity "owa (Default Web Site)" -SMimeEnabled $true
```

For information about syntax and parameters, see Set-OwaVirtualDirectory.

Note:
Availability of S/MIME in Outlook Web App can be controlled on a per-user basis by using the Set-CASMailbox cmdlet and the `OWASMimeEnabled` parameter.

Other Tasks

After you enable or disable S/MIME in Outlook Web App, you may also want to Manage S/MIME for Outlook Web App.

1.6.3.5.4.2 Manage S/MIME for Outlook Web App

Manage S/MIME for Outlook Web App

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can edit the registry on a Microsoft Exchange Server 2010 Client Access server so you can manage the behavior of Secure/Multipurpose Internet Mail Extensions (S/MIME) for Outlook Web App.

You can change the registry on an Exchange 2010 server that has the Client Access server role installed to control the behavior of S/MIME in Outlook Web App. These changes are made per server. If you have more than one Client Access server and need the same S/MIME behavior on all Client Access servers, you must make the same changes on each server. Changes to the S/MIME settings in the registry take effect immediately

and will affect Outlook Web App users the next time that they take any action that uses the S/MIME control. You do not have to force users to sign out or to restart any services.

Looking for other management tasks related to Outlook Web App security? Check out Managing Outlook Web App Security.

Prerequisites

If you're unfamiliar with managing public key infrastructures (PKIs) and certificates, we recommend that you start by reviewing the Active Directory Certificate Services and Public Key Management.

S/MIME Control Settings

The following tables list the names, possible values, defaults, and behavior of the registry settings that you can use to control the behavior of the S/MIME control in Outlook Web App.

Check CRL on Send

Exchange 2010 value name and type	CheckCRLOnSend (DWORD)
Exchange 2007 value name and type	CheckCRLOnSend (DWORD)
Exchange 2003 value name and type	CheckCRL (DWORD)
Values and defaults	1=True, 0=False (default)
Explanation	By default, if a certificate revocation list (CRL) distribution point in a sender's certificate chain cannot be accessed during revocation verification when sending signed or encrypted e-mail, Outlook Web App will not display a warning notifying the sender that the certificate cannot be verified. Instead, it allows the e-mail to be sent. When **CheckCRLonSend** is set to true, if a CRL distribution point in a sender's certificate chain cannot be accessed during revocation verification when sending signed or encrypted e-mail, Outlook Web App will indicate a failure and prevent the e-mail message from being sent.

Distribution List Expansion Timeout

Exchange 2010 value name and type	DLExpansionTimeout (DWORD)
Exchange 2007 value name and type	DLExpansionTimeout (DWORD)
Exchange 2003 value name and type	DLExpansionTimeout (DWORD)
Values and defaults	Distribution List Expansion Timeout represents the time that it will take, in milliseconds, before a request to expand a distribution list will time out. The default value is 60000 (60 seconds). The minimum

	value is 0. Setting **DLExpansionTimeout** to 0 disables the ability to send encrypted e-mail to distribution lists. The maximum value is 2147483647. When **DLExpansionTimeout** is set to the maximum value, there is no distribution list expansion time-out and Outlook Web App will wait until the distribution list is expanded, regardless of how long expansion takes.
Explanation	This attribute controls how long Outlook Web App will wait, in milliseconds, for a distribution list in Active Directory to expand when sending encrypted e-mail before the operation fails. When sending encrypted e-mail to a distribution list, Outlook Web App must expand the distribution list to retrieve the encryption certificate of each recipient for use in the encryption operation. The time this operation takes varies depending on the size of the distribution list and the performance of the underlying Active Directory infrastructure. While the distribution list is being expanded, the sender will receive no response from Outlook Web App. This attribute specifies how long Outlook Web App should wait for the full distribution list to be expanded. If the operation has not completed in the time specified by this value, the operation will fail and the mail will not be sent. The sender will be returned to the compose form, which will include an InfoBar that includes the following error message: The action could not be completed. Please try again. If the problem continues, contact technical support for your organization.

Use Secondary Proxies When Finding Certificates

Exchange 2010 value name and type	UseSecondaryProxiesWhenFindingCertificates (DWORD)
Exchange 2007 value name and type	UseSecondaryProxiesWhenFindingCertificates (DWORD)
Exchange 2003 value name and type	CertMatchingDoNotUseProxies (DWORD)
Values and defaults	1=True (default), 0=False
Explanation	Outlook Web App tries to find the correct certificate in Active Directory for a recipient when sending encrypted e-mail. The certificate subject or subject alternative name values can contain an SMTP address as one of its values. Because a recipient can have multiple SMTP proxy addresses in the directory, the subject or subject alternative

	name of the certificate may not match the primary SMTP address. Instead it may match one of the proxy addresses. If **UseSecondaryProxiesWhenFindingCertificates** is set to true, Outlook Web App will accept certificates that do not match the primary SMTP address of the recipient as valid. If **UseSecondaryProxiesWhenFindingCertificates** is set to false, Outlook Web App will accept as valid only certificates that match the primary SMTP address of the recipient.

CRL Connection Timeout

Exchange 2010 value name and type	CRLConnectionTimeout (DWORD)
Exchange 2007 value name and type	CRLConnectionTimeout (DWORD)
Exchange 2003 value name and type	RevocationURLRetrievalTimeout (DWORD)
Values and defaults	CRL Connection Timeout represents the time it will take, in milliseconds, before a CRL connection request will time out. The default value is 60000 (60 seconds). The minimum value is 5000 (5 seconds). A maximum value of 2147483647 can be specified. If **CRLConnectionTimeout** is set to the maximum value, the connection will not time out.
Explanation	CRL Connection Timeout specifies the time, in milliseconds, that Outlook Web App will wait while connecting to retrieve a single CRL as part of a certificate validation operation. Validating a certificate requires retrieving the certification authority's CRL from the CRL distribution point that is specified within the certificate. This operation must be performed for each certificate in the complete certificate chain. When multiple CRLs must be retrieved, this key will apply to each connection. For example, if three CRLs must be retrieved and **CRLConnectionTimeout** is set to 60 seconds, each CRL retrieval operation will have a time-out limit of 60 seconds. If the CRL is not retrieved before the time-out limit that is specified, the operation fails. If **CRLConnectionTimeout** is set to less than 5000, the default value (60000) will be used. If **CRLConnectionTimeout** is set to the maximum, 2147483647, the connection will not time out.

CRL Retrieval Timeout

Exchange 2010 value name and type	CRLRetrievalTimeout (DWORD)
Exchange 2007 value name and type	CRLRetrievalTimeout (DWORD)
Exchange 2003 value name and type	CertURLRetrievalTimeout (DWORD)
Values and defaults	CRL Retrieval Timeout specifies the time, in milliseconds, that Outlook Web App will wait while connecting to complete all of the CRL retrievals for a single message. The default value is 10000 (10 seconds). The minimum value is 0. The maximum value is 2147483647.
Explanation	This attribute resembles CRL Connection Timeout, however it specifies the time, in milliseconds, that Outlook Web App will wait to retrieve all CRLs when validating a certificate. If all CRLs are not retrieved before the time-out limit that is specified, the operation will fail. When you set this value, it is important to remember that, in a certificate validation operation, CRL Connection Timeout is applied to each CRL retrieval and to the overall operation of all CRL retrievals. For example, if three CRLs must be retrieved and **CRLConnectionTimeout** is set to 60 seconds, and **CRLRetrievalTimeout** is set to 120 seconds, each CRL retrieval operation will have a time-out of 60 seconds and the overall operation will have a time-out of 120 seconds. In this example, if any individual CRL retrieval takes more than 60 seconds, the operation will fail. Also, if all the CRL retrievals take more than 120 seconds, the operation will fail.

Disable CRL Check

Exchange 2010 value name and type	DisableCRLCheck (DWORD)
Exchange 2007 value name and type	DisableCRLCheck (DWORD)
Exchange 2003 value name and type	DisableCRLCheck (DWORD)
Values and defaults	1=True, 0=False (default)
Explanation	When set to true, **DisableCRLCheck** prevents CRLs from being checked while certificates are being validated. Disabling CRL checking can increase the time it takes to validate the signatures of signed e-mail. However, it will also show revoked e-mail signed with revoked certificates as valid instead of not valid.

Allow User Choice of Signing Certificate

Exchange 2010 value name and type	AllowUserChoiceOfSigningCertificate (DWORD)
Exchange 2007 value name and type	AllowUserChoiceOfSigningCertificate (DWORD)
Exchange 2003 value name and type	Not available. This was a new feature in Exchange 2007.
Values and defaults	1=True, 0=False (default)
Explanation	When set to true, **AllowUserChoiceOfSigningCertificate** lets users select which signing certificate to use to digitally sign e-mail when they use Outlook Web App with the S/MIME control. This is controlled only from the S/MIME options tab.

Always Sign

Exchange 2010 value name and type	AlwaysSign (DWORD)
Exchange 2007 value name and type	AlwaysSign (DWORD)
Exchange 2003 value name and type	AlwaysSign (DWORD)
Values and defaults	1=True, 0=False (default)
Explanation	When set to true, **AlwaysSign** will force users to digitally sign e-mail when they use Outlook Web App with the S/MIME control. Also, the Options page and the Message Options dialog box will show the "Send signed e-mail" option as selected.

Always Encrypt

Exchange 2010 value name and type	AlwaysEncrypt (DWORD)
Exchange 2007 value name and type	AlwaysEncrypt (DWORD)
Exchange 2003 value name and type	AlwaysEncrypt (DWORD)
Values and defaults	1=True, 0=False (default)
Explanation	When set to true, **AlwaysEncrypt** will force users to encrypt e-mail when they use Outlook Web App with the S/MIME control. Also, the Options page and the Message Options dialog box will display the "Send encrypted e-mail" option as selected.

Clear Sign

Exchange 2010 value name and type	ClearSign (DWORD)
Exchange 2007 value name and type	ClearSign (DWORD)
Exchange 2003 value name and type	ClearSign (DWORD)

Values and defaults	1=True (default), 0=False
Explanation	When set to true, **ClearSign** forces any digitally signed e-mail message that is sent from Outlook Web App to be clear-signed. The default setting for this attribute is true. Setting this value to false will cause Outlook Web App to use an opaque signature. Clear-signed e-mail messages are larger than opaque-signed signatures, but they can be opened and read with most e-mail clients, including clients that do not support S/MIME.

Include Certificate Chain Without Root Certificate

Exchange 2010 value name and type	IncludeCertificateChainWithoutRootCertificate (DWORD)
Exchange 2007 value name and type	IncludeCertificateChainWithoutRootCertificate (DWORD)
Exchange 2003 value name and type	SecurityFlags (value 0x001)
Values and defaults	1=True, 0=False (default)
Explanation	The default behavior of Outlook Web App is to include only the signing and encrypting certificates, not their corresponding certificate chains, when sending signed or encrypted e-mail. This option may be necessary for interoperating with other clients, or in environments where intermediate certification authorities (CAs) cannot be reached by using the **Authority Information Access** attribute or by having the intermediate CA trusted in the Computer account of the Exchange 2010 mailbox server. When **IncludeCertificateChainWithoutRootCertificate** is set to true, signed or encrypted e-mail will include the full certificate chain, except for the root certificate. This setting increases the size of signed and encrypted messages.

Include Certificate Chain and Root

Exchange 2010 value name and type	IncludeCertificateChainAndRootCertificate (DWORD)
Exchange 2007 value name and type	IncludeCertificateChainAndRootCertificate (DWORD)
Exchange 2003 value name and type	SecurityFlags (value 0x002)
Values and defaults	1=True, 0=False (default)
Explanation	Include Certificate Chain and Root resembles Include Certificate Chain Without

	Root Certificate, but, when it is set to true, it includes the root certificate and the full certificate chain. When set to true, **IncludeCertificateChainAndRootCertificate** increases the size of signed and encrypted messages more than **IncludeCertificateChainWithoutRootCertificate**.

Encrypt Temporary Buffers

Exchange 2010 value name and type	EncryptTemporaryBuffers (DWORD)
Exchange 2007 value name and type	EncryptTemporaryBuffers (DWORD)
Exchange 2003 value name and type	SecurityFlags (value 0x004)
Values and defaults	1=True (default), 0=False
Explanation	By default, all client-side temporary buffers that are used to store message data are encrypted by using an ephemeral key and the 3DES algorithm. This setting can be used to enable or disable encrypting the temporary buffers. Disabling encryption of the buffers can increase performance of the Outlook Web App client. However, it leaves information unencrypted in the buffer of the local system. Before you disable this feature, see your organization's security policy.

Signed E-Mail Certificate Inclusion

Exchange 2010 value name and type	SignedEmailCertificateInclusion (DWORD)
Exchange 2007 value name and type	SignedEmailCertificateInclusion (DWORD)
Exchange 2003 value name and type	SecurityFlags (value 0x008)
Values and defaults	1=True (default), 0=False
Explanation	By default Outlook Web App with the S/MIME control installed includes both signing and encrypting certificates with signed e-mail. When you disable this setting by setting **SignedEmailCertificateInclusion** to false, the size of messages that are sent from Outlook Web App with the S/MIME control will decrease. However, recipients will not have access to the sender's encryption certificate in the received message. They will have to obtain that certificate another way, either by retrieving it from a directory or obtaining it from the sender.

Bcc Encrypted E-Mail Forking

Exchange 2010 value name and type	BccEncryptedEmailForking (DWORD)
Exchange 2007 value name and type	BccEncryptedEmailForking (DWORD)
Exchange 2003 value name and type	SecurityFlags (values 0x040, 0x080)
Values and defaults	0=One encrypted message per Bcc recipient (default) 1=One single encrypted message for all Bcc recipients 2=One encrypted message without Bc forking
Explanation	By default, Outlook Web App will submit a separate encrypted message for each recipient on the Bcc line of an encrypted message. This option provides the most security for Bcc recipients of an encrypted message. By changing the value of **BccEncryptedEmailForking**, you can require Outlook Web App to create a single encrypted message for all Bcc recipients or one encrypted message without a separate message for each Bcc recipient.

Include S/MIME Capabilities in Message

Exchange 2010 value name and type	IncludeSMIMECapabilitiesInMessage (DWORD)
Exchange 2007 value name and type	IncludeSMIMECapabilitiesInMessage (DWORD)
Exchange 2003 value name and type	SecurityFlags (value 0x100)
Values and defaults	1=True, 0=False (default)
Explanation	When **IncludeSMIMECapabilitiesInMessage** is set to true, Outlook Web App will add attributes to outgoing signed and encrypted messages that indicate which encryption and signing algorithms and key lengths are supported. Enabling this attribute will increase the size of messages. However, enabling it can make it easier for some e-mail clients to interoperate with Outlook Web App.

Copy Recipient Headers

Exchange 2010 value name and type	CopyRecipientHeaders (DWORD)
Exchange 2007 value name and type	CopyRecipientHeaders (DWORD)
Exchange 2003 value name and type	SecurityFlags (value 0x200)
Values and defaults	1=True, 0=False (default)

Explanation	When it is set to true, **CopyRecipientHeaders** puts a copy of the From, To, and Cc recipient headers in the signed part of the message. This allows the recipient to verify that these headers were not tampered with while the message was in transit. Enabling this feature increases the message size.

Only Use Smart Card

Exchange 2010 value name and type	OnlyUseSmartCard (DWORD)
Exchange 2007 value name and type	OnlyUseSmartCard (DWORD)
Exchange 2003 value name and type	SmartCardOnly (DWORD)
Values and defaults	1=True, 0=False (default)
Explanation	When it is set to true, **OnlyUseSmartCard** forces the use of smart card-based certificates for signing and decryption when you use Outlook Web App together with the S/MIME control. Users cannot use certificates not on a smartcard.

Triple Wrap Encrypted Mail

Exchange 2010 value name and type	TripleWrapSignedEncryptedMail (DWORD)
Exchange 2007 value name and type	TripleWrapSignedEncryptedMail (DWORD)
Exchange 2003 value name and type	TripleWrap (DWORD)
Values and defaults	1=True (default), 0=False
Explanation	When **TripleWrapSignedEncryptedMail** is set to true, encrypted e-mail messages that are digitally signed are triple-wrapped. When a message is tripled-wrapped, the digitally-signed message is encrypted, and then the encrypted message is digitally signed. When set to false, the digitally signed message is only encrypted, there is no additional digital signing of the encrypted message. By default, this attribute is set to true. Triple-wrapped messages afford the most security for digitally-signed and encrypted e-mail under the S/MIME standard, but they are larger than messages that are not triple-wrapped.

Use Key Identifier

Exchange 2010 value name and type	UseKeyIdentifier (DWORD)
Exchange 2007 value name and type	UseKeyIdentifier (DWORD)
Exchange 2003 value name and type	UseKeyIdentifier (DWORD)

Values and defaults	1=True, 0=False (default)
Explanation	By default, when encrypting e-mail, Outlook Web App will encode the lockbox where the asymmetrically-encrypted token that is required to decrypt the rest of the message is stored. It encodes the lockbox by indicating the issuer and serial number of each recipient's certificate. This can then be used to locate the certificate and private key for decrypting the message. An alternative way to locate the certificate and private key for decrypting the message is to use a certificate's key identifier by setting **UseKeyIdentifier** to true. Because a key pair can be reused in new certificates, using the key identifier for encrypted e-mail enables users to keep only the most recent certificate and the associated private key, instead of all old certificates, which can only be matched by issuer and serial number. By default, because some e-mail clients do not support finding certificates with a key identifier, Outlook Web App uses the issuer and serial number of each recipient's certificate. However, enabling this feature can make it easier to manage encrypted messages by eliminating the need for users to keep old, expired certificates on their system.

S/MIME Encryption Algorithms

Exchange 2010 value name and type	EncryptionAlgorithms (Reg-SZ)
Exchange 2007 value name and type	EncryptionAlgorithms (Reg-SZ)
Exchange 2003 value name and type	EncryptionAlgorithms (Reg_SZ)
Values and defaults	This key is a semicolon-separated list that represents the symmetric encryption algorithms to use when encrypting messages when using Outlook Web App together with the S/MIME control. List format: {Well-known algorithm ID}[:key length to use]|[,Custom replacement algorithm OID]; {Well-known algorithm ID}[:key length to use]|[,Custom replacement algorithm OID]; … Supported algorithms and their ALG_IDs: • DES6601 • 3DES6603 • RC26602 • AES128660E • AES192660F • AES2566610

	Key length is only applicable to variable-key length algorithms when the key length is not encoded into the algorithm ID itself. RC2 is the only such algorithm in the previous list. Custom replacement algorithm OID You can supply your own algorithm by implementing it within a cryptographic service provider (CSP), assigning it a custom object ID, and specifying the OID by using the **EncryptionAlgorithms** key. An OID must be specified together with a well-known algorithm ID. Outlook Web App needs a well-known algorithm ID so that it can infer how the algorithm should be used. For example, to provide a custom replacement for the 3DES algorithm, you would specify the ALG_ID of 3DES (0x6603) and the custom OID of the replacement algorithm. The values of the registry key should be listed from the longest key length to the shortest because the order reflects priority of use. For example, to list 3DES, RC2-128, RC2-64, DES, RC2-56, and RC2-40, type the value in the following way: 6603;6602:128;6602:64;6601;6602:56;6602:40 If the registry key is present, algorithms that are specified in the key will always be used. If the key is not present, Outlook Web App will fall back to its default internal list. This list begins with AES256 in computers that are running Windows Vista and with 3DES in computers that are running Windows XP. The AES algorithms are only used if the user's computer supports them. AES is not supported on Windows XP and messages that are encrypted by using AES cannot be read on computers that are running Windows XP.
Explanation	Outlook Web App will try to use the strongest algorithm with the longest available key length on the user's computer. If the encryption algorithm or minimum key length is not available on the user's computer, Outlook Web App will not allow encryption.

S/MIME Default Signing Algorithm

Exchange 2010 value name and type	SigningAlgorithms (Reg_SZ)
Exchange 2007 value name and type	SigningAlgorithms (Reg_SZ)
Exchange 2003 value name and type	DefaultSigningAlgorithm (reg_SZ)
Values and defaults	The **SigningAlgorithms** key specifies the list of signing algorithms to use when signing messages using Outlook Web App with the S/MIME control installed. The following table enumerates the

	signing algorithms, their algorithm IDs, and the supported key lengths for each. Format: {Well-known algorithm ID} Well-known algorithm IDs, and key lengths • CALG_SHA_512800E • CALG_SHA_384800D • CALG_SHA_256800C • SHA10x8004 • MD50x8003 If the registry key is present, the algorithm that is specified in the key will always be used. If the key is not present, Outlook Web App will fall back to its internal default list. This list begins with SHA-1. Messages that are digitally signed by using CALG_SHA_256 cannot be verified on computers that are running Windows XP.
Explanation	This attribute specifies the digital signing algorithm to use when digitally signing messages by using Outlook Web App together with the S/MIME control.

Force S/MIME Client Upgrade

Exchange 2010 value name and type	ForceSMIMEClientUpgrade (DWORD)
Exchange 2007 value name and type	ForceSMIMEClientUpgrade (DWORD)
Exchange 2003 value name and type	Not available. This was a new feature in Exchange 2007.
Values and defaults	1=True (default), 0=False
Explanation	When **ForceSMIMEClientUpgrade** is set to true, if the client control version on the user's computer is older than the version on the server, the user must download and install the new control before they can continue to use any S/MIME Read or Compose forms. If this value is set to false, the user will receive a warning if the S/MIME control on their computer is older than the version on the server. However, they will be able to use S/MIME without updating the control.

Use Registry Editor to change the S/MIME control settings for Outlook Web App

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Registry Editor" entry in the Client Access Permissions topic.

Caution:
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

1. Start Registry Editor (regedit).
2. Locate the following registry subkey:
   HKLM\System\CurrentControlSet\Services\MSExchange OWA\SMIME
3. Find the key that you want to change.
4. Set the key to the value that's required by your organization.
5. If the key that you need doesn't exist, create a new DWORD with that name, and then set it to the value that's required by your organization.

1.6.3.6 Understanding Extended Protection for Authentication

Understanding Extended Protection for Authentication

Exchange Server 2010 > Client Access > Securing Client Access Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-30*

Extended Protection for Authentication is a feature that helps to protect credentials for network connections that are being authenticated using Integrated Windows authentication. Integrated Windows authentication uses the Negotiate, Kerberos, and NTLM authentication methods. We strongly recommend that you use Extended Protection for Authentication if you're using Integrated Windows authentication.

Exchange Server 2010 Service Pack 1 (SP1) supports Extended Protection for Authentication. However, by default, Extended Protection for Authentication isn't enabled on computers running Exchange 2010.

Contents

Requirements for Extended Protection for Authentication

To use this feature, both the client and the server must be running a Microsoft Windows operating system that includes the Extended Protection for Authentication security update.

Default installations of Windows 7 and Windows Server 2008 R2 operating systems include this security update. However, for client or server computers that are running other versions of Windows (for example Windows Vista or Windows Server 2008 SP2), you must install the update. For detailed information about the operating systems that are supported by default, see Microsoft Knowledge Base article 973811, Microsoft Security

Advisory: Extended protection for authentication.

Exchange 2010 Prerequisite Checking

Exchange 2010 Setup doesn't require that the Extended Protection for Authentication security update be installed before Setup can continue. Instead, when you set up Extended Protection for Authentication for the first time, you'll be prompted to install the security updates referenced in Microsoft Knowledge Base article 968389, Extended Protection for Authentication on your computer if they're not already installed.

For More Information

Microsoft Knowledge Base article 973811, Microsoft Security Advisory: Extended protection authentication for authentication

MSDN Library topic Integrated Windows Authentication with Extended Protection

1.6.4 Troubleshooting Reference for Client Access Servers

Troubleshooting Reference for Client Access Servers

Exchange Server 2010 > Client Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-09-24*

After you've installed the Client Access server role on a computer running Microsoft Exchange Server 2010, you may have to test the functionality of the server or solve problems related to client connectivity. The following information will help you troubleshoot common errors and test to ensure that your Client Access server is configured correctly. This topic will be updated on a regular basis.

Test Client Access Server Connectivity

The Microsoft Exchange Remote Connectivity Analyzer (ExRCA) can help you confirm that connectivity for your Exchange servers is configured correctly and to diagnose any connectivity issues. The Remote Connectivity Analyzer Web site offers tests for Microsoft Exchange ActiveSync, Exchange Web Services, Outlook, and Internet e-mail.

For more information, see Understanding the Remote Connectivity Analyzer.

Outlook Client Connectivity

The following links and information will help you troubleshoot Outlook client connectivity.

Cannot Open Mailbox in Outlook 2007

If you can't open a user's mailbox in Microsoft Office Outlook 2007, but you can open the mailbox in Microsoft Office Outlook Web App, verify the server information by running the following command:

```
Get-MailboxDatabase | fl RPCClientAccessServer
```

If the output of that command is the name of the Exchange 2010 Mailbox server, it's likely that the Client Access server role and the Mailbox server role were installed in the incorrect order. The value of the parameter *RPCClientAccessServer* is set to the Mailbox server instead of the Client Access server. To resolve this issue, run the following command:

```
Get-MailboxDatabase | Set-MailboxDatabase -RPCClientAccessServer <FQDN of the Cli
```

Cannot Open Mailbox in Outlook 2003 and Exchange 2010 RTM

If you're trying to access a mailbox on an Exchange 2010 Mailbox server with Office Outlook 2003, you might receive one of the following error messages:

- Cannot start Microsoft Office Outlook. Unable to open the Office window. The set of folders could not be opened.
- Unable to open your default e-mail folders. The information store could not be opened.

In Exchange 2010, the RPC endpoint is encrypted by default. However, Outlook 2003 doesn't enforce encrypted MAPI connections. When you upgrade your organization to Exchange 2010, your clients that are running Outlook 2007 or later versions will automatically be compatible with the change to RPC Client Access, because they support RPC encryption by default. However, Outlook 2003 doesn't use RPC encryption, and RPC Client Access requires it by default.

Note:

By default, Exchange 2010 Service Pack 1 (SP1) encryption on the RPC endpoint isn't enabled. Therefore, this error shouldn't occur.

To configure Outlook 2003 to use RPC encryption, follow these steps:

1. Click **Tools** > **E-Mail Accounts** > **View or Change an Existing Account**.
2. Select the account and click **More Settings**.
3. Click the **Security** tab.
4. Select the check box **Encrypt data between Microsoft Office Outlook and Microsoft Exchange Server**.
5. Click **OK**.

E-Mail Messages Take a Long Time to Load for Outlook 2003 Clients

UDP notification support was removed from Exchange 2010. As a result, Outlook 2003 can only use polling notifications in online mode. This will result in a slight delay in updates to item status (30 seconds on average with up to a one-minute delay) when changes are made to items in a mailbox accessed with Outlook 2003. There are two workarounds for this issue:

- Use Outlook 2003 in Cached Exchange Mode.
- Adjust the polling interval on the Client Access server. This will impact the performance of the Client Access server.

For more information about this issue, see E-mail messages take a long time to send and receive.

Event ID 106 is logged when you start the RPC Client Access service

If the Microsoft Exchange RPC Client Access service is started on an Exchange 2010 Mailbox server that doesn't have the Client Access server role installed, Event ID 106 is logged in the Application log. This error occurs because the performance counters of the RPC Client Access service aren't installed when the Mailbox server role is installed without the Client Access server role. To resolve this error, install the Client Access server role on the Exchange 2010 server.

DNS Change Prevents User from Signing In to Outlook Web App

When a user tries to sign in to Outlook Web App, he may receive the following error message:

- A server configuration change is temporarily preventing access to your account. Please close all Internet Explorer windows and try again in a few minutes. If the problem continues, contact your helpdesk.

This can happen when the DNS record of the Client Access server is modified and a user tries to sign in to Outlook Web App before the DNS cache in Internet Explorer is refreshed. This can be resolved by the user closing all browser windows to force Internet Explorer to update the DNS cache. See How Internet Explorer uses the cache for DNS host entries for information about the DNS cache in Internet Explorer.

To avoid this, create a second DNS entry for the Client Access server and use the **Set-OwaVirtualDirectory** cmdlet to configure the *FailbackUrl* parameter to match. The *FailbackUrl* parameter specifies the host name Outlook Web App uses to connect to the Client Access server after failback in a site resilience process and requires a separate DNS entry pointing to the original Client Access server's IP address. The *FailbackUrl* parameter must be different from the *ExternalUrl* parameter.

This example configures the *FailbackUrl* parameter.

```
Set-owavirtualdirectory -identity "owa (default web site)" -FailbackUrl "<failbac
```

For more information about syntax and parameters, see Set-OwaVirtualDirectory.

Troubleshoot Certificate Wizard errors

Exchange 2010 uses Microsoft Windows HTTP Services (WinHTTP) to manage all HTTP/HTTPS traffic. Because of this, Exchange 2010 does not use the proxy server settings that may be configured in the web browser. WinHTTP uses Web Proxy Auto-Discover Protocol (WPAD), and requires that a Proxy Access Control (PAC) file be specified through DHCP or DNS.

If the WinHTTP proxy settings are configured incorrectly, the following issues may occur:

1. After you import a valid third-party certificate to an Exchange 2010 CAS, the EMC may report the following status: The certificate status could not be determined because the revocation check failed
2. If you run the **Get-ExchangeCertificate** cmdlet in the Exchange Management Shell, you see the following status for the imported certificate: Status : RevocationCheckFailure

To resolve these issues, follow these steps:

1. To list the WinHTTP proxy settings, type the following command at a command prompt, and then press Enter: **netsh winhttp show proxy**. The response shows the current proxy information that is being used by Exchange. Typically, you receive a response that resembles the following:

   ```
   C:\>netsh winhttp show proxy
   Current WinHTTP proxy settings:
   Direct access (no proxy server)
   ```

2. If the correct server is not identified in the response, configure the proxy setting for WinHTTP by using the netsh command. Also, configure the server FQDN in the bypass-list so that the Exchange Management Shell and the Exchange Management Console can contact Remote PowerShell.
3. To do this, type the following command at a command prompt, and then

press Enter: **netsh winhttp set proxy proxy-server="http=<Proxy_Server_Name>" bypass-list="*.<Exchange_Server_Hostname_Domain>"**

Note:

Replace the *<Proxy_Server_Name>* placeholder by using the proxy server name. Also, replace the *<Exchange_Server_Hostname_Domain>* placeholder by using the second-level domain name and the first-level domain name of the Exchange Server (for example, *microsoft.com*)

4. Close and then open the Exchange Management Console. Check the status of the certificate. If the proxy settings are correct but the certificate status is still incorrect, run the following commands at a command prompt to clear the OCSP/CRL cache:
   certutil -urlcache ocsp delete
   certutil -urlcache crl delete
5. Restart the server, and then open the Exchange Management Console to check the status of the certificate.

1.6.5 Error and Event Reference for Client Access Servers

Error and Event Reference for Client Access Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-01*

Microsoft Exchange Server 2010 Client Access server components, features, and services generate Error events to let you effectively troubleshoot and monitor Client Access servers.

Event Viewer maintains logs about program, security, and system events on your computer. You can use Event Viewer to view and manage the event logs, to gather information about hardware and software problems, and to monitor Microsoft Windows security events. Although Event Viewer is an Windows operating system tool and not a Microsoft Exchange tool, Event Viewer is useful when you troubleshoot problems that affect Exchange. This topic describes the basic concepts related to Event Viewer.

This topic also describes the events that a Client Access server lists in Event Viewer, explains how to use events to monitor Client Access components, and describes the error messages that are generated by a Client Access server.

Address Book Service Errors and Events

The following events are generated by the Address Book service.

Event ID	Event Type	Description
1000	Success	Microsoft Exchange Address Book Service has started successfully.
1001	Success	Microsoft Exchange Address Book Service has stopped successfully.

1002	Error	Failed to register service principal name %1. Failed with error code %2.
1003	Error	Cannot start the service due to Win32 error %1 while removing unnecessary privileges.
1004	Error	An unexpected error occurred while starting the Microsoft Exchange Address Book service.
1005	Error	An unexpected error occurred while stopping the Microsoft Exchange Address Book service.
1007	Error	No RPC endpoints were enabled in the configuration file.
1008	Error	Unable to register the %1 RPC interface. Failed with the error code %2.
1009	Error	%1 was not present or invalid in the configuration file. Protocol logging has been disabled.

Other Client Access Errors and Events

The following additional Client Access errors and events are grouped according to the Client Access feature areas.

- ActiveSync Errors and Events
- Availability Service Errors and Events
- Autodiscover Errors and Events
- Certificate Deployment Errors and Events
- OWA Errors and Events
- RPCHTTPAutoConfig Errors and Events
- ServiceHost Errors and Events

1.6.5.1 ActiveSync Errors and Events

ActiveSync Errors and Events

Exchange Server 2010 > Client Access > Error and Event Reference for Client Access Servers >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-14*

Microsoft Exchange Server 2010 ActiveSync generates events in Event Viewer so that you

can troubleshoot and verify the performance of ActiveSync features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

ActiveSync Errors and Events

The following table provides a list of the ActiveSync events that you can use to troubleshoot and monitor ActiveSync.

ActiveSync events

Event ID	Category	Event type	Value or description
MSExchange ActiveSync 1023	Requests	Warning	Exchange ActiveSync tried to access a mailbox on Mailbox server "%1". It could not access the mailbox because the Mailbox server is offline
MSExchange ActiveSync 1018	Requests	Warning	A user tried to perform a full-text search of their mailbox from their mobile phone, but Content Indexing is not enabled on Mailbox server "%1". If you do not want Exchange ActiveSync users and other Exchange users to be able to search their mailbox data on the server, no user action is required. If you want Exchange ActiveSync users and other Exchange users to be able to search their mailbox data on the server, make sure that the Microsoft Exchange Search service is running on your Mailbox servers. In addition, make sure that you have enabled full-text search on the appropriate database on the Mailbox server.
MSExchange ActiveSync 1008	Requests	Warning	An exception occurred and was handled by

			Exchange ActiveSync. This may have been caused by an outdated or corrupted Exchange ActiveSync device partnership. This can occur if a user tries to modify the same item from multiple computers. If this is the case, Exchange ActiveSync will re-create the partnership with the device. Items will be updated at the next synchronization. URL=%1%2.
MSExchange ActiveSync 1034	Requests	Warning	The proxy request to %1 has timed out.
MSExchange ActiveSync 1038	Requests	Error	The account "%1" doesn't have the appropriate permissions to modify the Exchange ActiveSync service privileges. Please check the assigned permissions for the account running the Exchange ActiveSync ASP.NET process. Error code: "%2".
MSExchange ActiveSync 1022	Requests	Warning	The connection between the Client Access server and Mailbox server "%1" failed. If this event is logged infrequently or only during scheduled downtime for a Mailbox server, no user action is required. If this event occurs repeatedly, check network connectivity using PING or PingPath. Also, check connectivity using the Test-ActiveSyncConnectivity cmdlet. More information: %2
MSExchange ActiveSync 1010	Requests	Warning	Direct Push has detected that the

			configuration value for the maximum heartbeat interval is set to a value higher than the maximum allowed value of "%1" seconds. Therefore, the default maximum heartbeat interval of "%2" seconds and the default minimum heartbeat interval of "%3" seconds will be used until the next time that the computer is restarted. To avoid seeing this message in the future, use Internet Information Services (IIS) Manager to correct this configuration. Reset the value to the default, or use another acceptable value.
MSExchange ActiveSync 1009	Requests	Warning	Direct Push has detected that the configuration value for the minimum heartbeat interval is set to a value higher than the maximum heartbeat interval. Therefore, the default minimum heartbeat interval of "%1" seconds and the default maximum heartbeat interval of "%2" seconds will be used until the next time that the computer is restarted. To avoid seeing this message in the future, use Internet Information Services (IIS) Manager to correct these values. Reset the values to the default, or use other acceptable values.
MSExchange ActiveSync 1032	Requests	Warning	The connection to mailbox "%1" on

			Mailbox server "%2" failed. Examine the event log of Mailbox server "%2". More information%2
MSExchange ActiveSync 1036	Configuration	Error	The Client Access server cannot proxy the Exchange ActiveSync client request to the Exchange server %1. For this to work, Integrated Windows authentication must be configured on the Microsoft-Server-ActiveSync virtual directory on the Exchange server %1.
MSExchange ActiveSync 1015	Server	Error	Exchange ActiveSync experienced a transient error when it tried to access Active Directory information for user "%1". Exchange ActiveSync will try this operation again. If this event occurs infrequently, no user action is required. If this event occurs frequently, check network connectivity using PING or PingPath. You can also use the Test-ActiveSyncConnectivity cmdlet. More information: %2
MSExchange ActiveSync 1016	Server	Error	Exchange ActiveSync has encountered repeated failures when it tries to access data on Mailbox server [%1]. It will temporarily stop making requests to the Mailbox server for [%2] seconds to reduce load on that server. This delay may occur if the Mailbox server is overloaded. If this event is logged

			frequently, review the Application log on this server and the Mailbox server noted above for other events that could indicate the root cause of performance problems. Additional information:"%3".
MSExchange ActiveSync 1033	Configuration	Warning	The setting %1 in the Web.Config file was not valid. The previous value was %2 and has been changed to %3.
MSExchange ActiveSync 1035	Configuration	Warning	The proxy request has failed due to an invalid SSL certificate on %1.
MSExchange ActiveSync 1011	Configuration	Warning	Direct Push has detected that the configuration value for the minimum heartbeat interval is set to a value that is too low. Therefore, the default minimum heartbeat interval of "%1" seconds and the default maximum heartbeat interval of "%2" seconds will be used until the next time that the computer is restarted. To avoid seeing this message in the future, use Internet Information Services (IIS) Manager to correct this configuration. Reset the value to the default, or use another acceptable value.

1.6.5.2 Availability Service Errors and Events

Availability Service Errors and Events

Exchange Server 2010 > Client Access > Error and Event Reference for Client Access Servers >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 Availability generates events in Event Viewer so that you can troubleshoot and verify the performance of the Exchange Availability features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Exchange Availability Service Errors and Events

The following table provides a list of the Availability events that you can use to troubleshoot and monitor the Availability service.

Availability Service events

Event ID	Category	Event type	Logging	Value or description	Class
MSExchange Availability 4018	Availability Service	Error	LogAlways	Process %1: An exception occurred while attempting to locate a Client Access server to handle a request for e-mail address %2. The returned exception is %3.	Availability
MSExchange Availability 4001	Availability Service	Error	LogAlways	Process %1: %2 failed. Exception returned is %3. This event may occur when Availability Service cannot discover an Availability Service in the remote forest.	Availability
MSExchange Availability 4017	Availability Service	Error	LogAlways	Process %1: No Client Access server was found to handle a request for e-mail address %2. This may be due to a	Availability

				misconfigured topology.	
MSExchange Availability 4010	Availability Service Authentication	Error	LogAlways	Process %1: Request from %2 failed security checks.	Availability
MSExchange Availability 4003	Availability Service	Error	LogAlways	Process %1: %2 failed. The exception returned is % 3. The Availability service could not successfully retrieve Schedule+ free/busy data for one or more legacy Exchange mailboxes. To find the root cause of this error, increase the diagnostic logging level of the MSExchange Availability service.	Availability
MSExchange Availability 4006	Availability Service	Error	LogAlways	Process %1: Failed to initialize service, exception returned is % 2	Availability
MSExchange Availability 4002	Availability Service	Error	LogAlways	Process %1: %2 failed. Caller SIDs: % 3. The exception returned is % 4. Make sure that the Active Directory site/ forest that contain the user's mailbox has at least one local Exchange 2010 server running the	Availability

				Availability service. Turn up logging for the Availability service and test basic network connectivity.	
MSExchange Availability 4005	Availability Service	Warning	LogAlways	Process %1: Configuration information for the current forest could not be found in Active Directory. To find the root cause of this error, increase the diagnostic logging level of the MSExchange Availability service.	Availability
MSExchange Availability 4016	Availability Service	Error	LogAlways	Process %1: Unable to logon as network service context for proxying requests. Cross-site and cross-forests requests could fail because of this. Exception is %2.	Availability
MSExchange Availability 4012	Availability Service Configuration	Error	LogAlways	Process %1: Cross-forest proxy request to %2 could not be initiated due to invalid credentials. Specific error is: %3	Availability

1.6.5.3 Autodiscover Errors and Events

Autodiscover Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Autodiscover service events in Event Viewer so that you can troubleshoot and verify the performance of the Autodiscover features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Autodiscover Errors and Events

The following table provides a list of the UM auto attendant events that you can use to troubleshoot and monitor Unified Messaging.

Autodiscover events

Event ID	Category	Event type	Logging	Value or description	Class
MSExchange Autodiscover 1111	Core	Warning	LogAlways	Error "%1" while loading assembly "%2".%nStack Trace:%3. The event is logged when Autodiscover is unable to load an assembly because the assembly file does not have appropriate access permissions (executable and read permissions).	Autodiscover
MSExchange Autodiscover 1201	Provider	Warning	LogAlways	Time:%1, Id: %2, Error Response with the ErrCode:"%3", Message:"%4", DebugData:"%5" was generated for EMailAddress:	Autodiscover

				"%6", LegacyDN:"%7" by "%8".	
MSExchange Autodiscover 1112	Core	Warning	LogAlways	Error "%1" while loading assembly "%2".%nStack Trace:%3. The event is logged when Autodiscover is unable to find an assembly or DLL that Autodiscover is trying to reference.	Autodiscover
MSExchange Autodiscover 1108	Core	Warning	LogAlways	Error "%1" while loading assembly "%2".%nStack Trace:%3. The event is logged because the Microsoft Exchange Autodiscover service found the managed assembly or DLL it was referencing, but failed to load the assembly.	Autodiscover
MSExchange Autodiscover 2	Web	Error	LogAlways	Anonymous Request received from HostAddress:"%1", HostName:"%2". Invalid Autodiscover site configuration. To fix the problem remove Anonymous access.	Autodiscover
MSExchange Autodiscover 1	Web	Error	LogAlways	Unhandled Exception "%1"%nStack trace: %2	Autodiscover

MSExchange Autodiscover 1109	Core	Warning	LogAlways	Error "%1" while loading assembly "%2".%nStack Trace:%3. This event is logged when the loader that Autodiscover is using to load an assembly or DLL has failed because the loader may not be valid.	Autodiscover
MSExchange Autodiscover 101	Core	Error	LogAlways	No providers were found. The Autodiscover service won't be able to process any valid requests.	Autodiscover
MSExchange Autodiscover 1105	Core	Warning	LogAlways	Requested provider for Request Schema:"%1" and Response Schema:"%2" cannot be found.	Autodiscover
MSExchange Autodiscover 1110	Core	Warning	LogAlways	Error "%1" while loading assembly "%2".%nStack Trace:%3. The event is logged when the Autodiscover provider is unable to load the assembly it is referencing because the assembly or DLL could be in an invalid format.	Autodiscover
MSExchange Autodiscover 1106	Core	Warning	LogAlways	Error "%1" while loading the assembly "%2".%nStack	Autodiscover

				Trace:%3. This error may occur because the provider file is corrupt, is in an incorrect format, or has insufficient permissions.	
MSExchange Autodiscover 1113	Core	Warning	LogAlways	Provider "%1" has invalid attribute - "%2". The entry is not added to the table.	Autodiscover

1.6.5.4 Certificate Deployment Errors and Events

Certificate Deployment Errors and Events

Exchange Server 2010 > Client Access > Error and Event Reference for Client Access Servers >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Certificate Deployment events in Event Viewer so that you can troubleshoot and verify the Certificate Deployment features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Certificate Deployment Errors and Events

The following table provides a list of the Certificate Deployment events.

Event ID	Category	Event type	Value or description
MSExchange Certificate Deployment 2009	General	Warning	The federation certificate %1 will expire in less than 15 days. Renew the certificate soon to ensure proper functionality of federation trust services.

1.6.5.5 OWA Errors and Events

OWA Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-14*

Microsoft Exchange Server 2010 generates Outlook Web App events in Event Viewer so that you can troubleshoot and verify the OWA features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

MSExchange OWA Errors and Events

The following table provides a list of OWA errors and events.

Event ID	Category	Event type	Logging	Value or description	Class
MSExchange OWA 39	Proxy	Error	LogAlways	Client Access server "%1" tried to proxy Outlook Web App traffic to Client Access server "%2". This failed because "%2" didn't respond. Outlook Web App will try to proxy this traffic to Client Access server "%3" in the same Active Directory site.Additional information: %4.	OWA
MSExchange OWA 7	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.Invalid forms registry file %1 Line number = %2 Position = %3. You can't define a base experience when you choose to	OWA

				inherit from another forms registry. The base experience of the other forms registry is always used.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about troubleshooting the forms registry.	
MSExchange OWA 50	ADNotifications	Error	LogAlways	Settings change notifications couldn't be registered in Active Directory for virtual directory "%1" under web site "%2". Exception message:"%3".	OWA
MSExchange OWA 70	Transcoding	Error	LogAlways	The ACL of the temporary folder couldn't be set because the WebReady Document Viewing Manager doesn't have the permissions to set it. The value of the	OWA

				temporary folder is set by a registry key. If the registry key doesn't exist, the default Microsoft Windows temporary folder will be used. The registry key that controls the temporary folder is named HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet\Services \MSExchange OWA \WebReadyDocumentViewing \TempFolderLocation. For WebReady Document Viewing to function correctly, the Local System account must have full control permissions assigned to the temporary folder that you have configured.Exception message: "%1".	
MSExchange OWA 16	Configuration	Error	LogAlways	There's an error in your Outlook Web App configurationThe configuration for virtual directory "%1" couldn't be found. This	OWA

				can be fixed using the Get-, Set-, or New-OwaVirtualDirectory cmdlets. Make sure the VirtualDirectory property of the corresponding OwaVirtualDirectory object matches the name of this virtual directory.	
MSExchange OWA 5	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.Invalid forms registry file %1 Line number = %2 Position = %3. Expected element = %4.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about troubleshooting the forms registry.	OWA
MSExchange OWA 3	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.Forms registry %1 specifies %2 as the base experience, but %2 is not defined in the	OWA

				forms registry.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about how to troubleshoot the forms registry.	
MSExchange OWA 24	Themes	Error	LogAlways	Outlook Web App couldn't initialize.It couldn't parse file "%1" in theme folder "%2". The theme ID attribute "%3" wasn't found. Line %4, Position %5.	OWA
MSExchange OWA 37	Configuration	Error	LogAlways	The sign-in to Outlook Web App failed. The Active Directory profile for "%1" doesn't have a primary SMTP address.This may have happened because the user's account wasn't created using the Exchange Management Console or the Exchange command-line tools. The following	OWA

				Exchange Management Shell steps provide one way of correcting the most common cause of the problem. Get-User "%2" | Disable-Mailbox. Get-User "%3" | Enable-Mailbox At the prompt, enter the mailbox database name (normally "Mailbox Store").	
MSExchange OWA 46	Proxy	Error	LogAlways	Client Access server "%1", running Exchange version "%2", is proxying Outlook Web App traffic to Client Access server "%3", which runs Exchange version "%4". To ensure reliable interoperability, the proxying Client Access server needs to be running a newer version of Exchange than the Client Access server it is proxying to. If the proxying Client Access server is running a newer version of Exchange than the Client Access	OWA

				server it is proxying to, the proxying Client Access server needs to have an Outlook Web App resource folder (for example, "<Exchange Server installation path>) \ClientAccess \owa \8.0.498.0" that contains all the same versioned resource files as the Client Access server it is proxying to. If you will be running Outlook Web App proxying with mismatched server versions, you can manually copy this resource folder to the proxying Client Access server. After you copy this resource folder to the proxying Client Access server, you need to restart IIS before proxying will work.	
MSExchange OWA 42	Proxy	Error	LogAlways	Client Access server "%1" tried to proxy Outlook Web App traffic to Client Access server "%2". This failed	OWA

				because one of these configuration problems was encountered:1. "%2" has been set to use "http://" (not using SSL) instead of "https://" (using SSL). You can modify this by setting the InternalUrl parameter of the Outlook Web App virtual directory this proxy traffic is going to. You can set that parameter using the Set-OwaVirtualDirectory cmdlet in the Exchange Management Shell.2. The destination virtual directory returned an HTTP 403 error code. This usually means it's not configured to accept SSL access. You can change this configuration by using IIS Manager on the Client Access server "%2".If you don't want this proxy connection to use SSL, you need to set the registry key "AllowProxying	

				WithoutSSL" on this Client Access server and to set the InternalUrl and SSL settings for the Outlook Web App virtual directory this proxy traffic is going to accordingly.	
MSExchange OWA 47	Transcoding	Warning	LogAlways	A folder couldn't be created to cache the current Outlook Web App process. Other processes may be using the same directory. To fix this problem, stop the processes that are using the same directory, and then restart Outlook Web App. Exception message: "%1".	OWA
MSExchange OWA 10	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.Invalid forms registry file %1 Line number = %2 Position = %3. The value "%4" specified for the MinimumVersion element isn't a valid number.The forms registry is a critical component of Outlook Web App. If this	OWA

				error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about how to troubleshoot the forms registry.	
MSExchange OWA 38	Proxy	Error	LogAlways	Client Access server "%1" tried to proxy or redirect Outlook Web App traffic for mailbox "%2". This failed because one of the service discovery entries returned for the Client Access server to use for this mailbox is malformed. The service discovery URLs should be in the format "http [s]:// hostname [:port]/owa". The malformed entry is stored as "%3".	OWA
MSExchange OWA 40	Proxy	Error	LogAlways	Client Access server "%1" tried to proxy Outlook Web App traffic to Client Access server "%2". This failed because "%2" didn't respond.Additional information: %	OWA

				3.	
MSExchange OWA 71	Proxy	Error	LogAlways	Microsoft Exchange Client Access server %1 tried to proxy Outlook traffic to Client Access server %2. This failed because the authentication for the connection between the two Client Access servers failed. This may be due to one of these configuration problems: 1. The host name in %2 may not be registered as a Service Principal Name (SPN) with Kerberos on the target Client Access server. This usually happens because you used the IP address, instead of the host name, of the target Client Access server in the "internalURL" configuration for the Outlook Web App virtual directory on the target Client Access server. You can change the "internalURL" configuration for the target Client Access	OWA

				server using the "Set-OwaVirtualDirectory" task. If you don't want to change the "internalURL" configuration for the Outlook Web App virtual directory on the target Client Access server, you can also use the tool "setspn.exe" on the target Client Access server to register additional SPNs for which that Client Access server will accept Kerberos authentication. 2.The server hosting %2 may be configured not to allow Kerberos authentication. It might be set to use Integrated Windows authentication for the Outlook Web App virtual directory, but be configured to only use NTLM (not Kerberos) authentication for Integrated Windows authentication. If you suspect this may be the cause of the failure, see	

				the IIS documentation for additional troubleshooting steps.	
MSExchange OWA 28	SmallIcons	Error	LogAlways	Outlook Web App couldn't initialize.The small icon configuration file named %1 doesn't exist.The small icon configuration file is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about how to troubleshoot the small icon configuration file.	OWA
MSExchange OWA 57	Proxy	Warning	LogAlways	Outlook Web App isn't available for this mailbox. The Client Access server %1, running Exchange version %2, tried to find a Client Access server to proxy Outlook Web App traffic for mailbox %3. It couldn't find the Client Access server in the target Active	OWA

				Directory site.Additional information: %4. If the problem continues, contact your helpdesk.	
MSExchange OWA 21	Themes	Error	LogAlways	Outlook Web App couldn't initialize.File "%1" in theme folder "%2" couldn't be parsed. The attribute "%3" is empty. Line %4, Position %5.	OWA
MSExchange OWA 22	Themes	Error	LogAlways	Outlook Web App couldn't initialize.It couldn't parse file "%1" in theme folder "%2". The attribute "%3" exceeds the maximum length of %4 characters. Line %5, Position %6.	OWA
MSExchange OWA 4	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.More than one forms registry is named %1. Each registry name must be unique. Rename one of the forms registries.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web	OWA

				App. The Help and Support Center provides information about troubleshooting the forms registry.	
MSExchange OWA 19	Themes	Error	LogAlways	Outlook Web App couldn't initialize.File "%1" in theme folder "%2" wasn't parsed. The xml element "%3" is missing.	OWA
MSExchange OWA 1	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.The forms registry folder %1 doesn't exist.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about how to troubleshoot the forms registry.	OWA
MSExchange OWA 44	Proxy	Error	LogAlways	Client Access server "%1" tried to proxy Outlook Web App traffic to Client Access server "%2". This failed for user "%3" because this	OWA

				user is a member of too many groups. Outlook Web App limits group membership when proxying to "%4".	
MSExchange OWA 2	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.Forms registry %1 inherits forms registry %2, but forms registry %2 couldn't be found.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about troubleshooting the forms registry.	OWA
MSExchange OWA 31	Configuration	Error	LogAlways	The Address Book custom properties couldn't be parsed. RootElementNotFound in "%1" at line number = "%2". Make sure that this file contains "CustomProperties" as the root element. If this error isn't addressed,	OWA

				users won't be able to view the custom properties. The Help and Support Center provides information about how to troubleshoot this issue.	
MSExchange OWA 26	Themes	Error	LogAlways	Outlook Web App couldn't initialize.A base theme couldn't be found. The base theme must be in a folder with name = "%1".	OWA
MSExchange OWA 54	ADNotifications	Error	LogAlways	The Active Directory system configuration session couldn't be retrieved.Exception message:"%1".	OWA
MSExchange OWA 43	Proxy	Warning	LogAlways	Client Access server "%1" tried to proxy Outlook Web App traffic to Client Access server "%2". This failed because the Outlook Web App registry key "AllowInternalUntrustedCerts" is set to "0", but no certificate trusted by "%1" was available for the Secure Sockets Layer (SSL)	OWA

				encryption of the proxy connection.	
MSExchange OWA 30	Configuration	Error	LogAlways	There's an error in your Outlook Web App configuration.The authentication type on the /owa virtual directory is set to Anonymous. This check box must be cleared for Outlook Web App to function correctly.	OWA
MSExchange OWA 45	Proxy	Error	LogAlways	Client Access server "%1" tried to proxy Outlook Web App traffic to "%2". This failed because "%2" couldn't verify that the Active Directory account "%3" used to authenticate has the necessary access rights to send Outlook Web App proxy traffic.Additional information: %4.	OWA
MSExchange OWA 9	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.Invalid forms registry file %1 Line number = %2 Position = %3. Message = %4.The forms registry is a	OWA

				critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about troubleshooting the forms registry.	
MSExchange OWA 15	Configuration		LogAlways	There's an error in your Outlook Web App configurationThe character '%5' isn't valid for file extensions. It was found in character %4 of "%3" in element %2 of the %1 array in the Outlook Web App attachment policy for the %6 virtual directory. This can be corrected using the Exchange Management Console.	OWA
MSExchange OWA 53	ADNotifications	Error	LogAlways	The message classification settings couldn't be read from Active Directory for virtual directory "%1" under web site "%2".Exception	OWA

				message:"%3".	
MSExchange OWA 36	Configuration	Error	LogAlways	The Address Book custom properties couldn't be parsed. An invalid value was provided for the attribute "%1" and in the file "%2" at line number "%3". The values of these attributes can't be null or empty.	OWA
MSExchange OWA 41	Proxy	Error	LogAlways	The Client Access server "%1" attempted to proxy Outlook Web App traffic for mailbox "%2". This failed because no Client Access server with an Outlook Web App virtual directory configured for Kerberos authentication could be found in the Active Directory site of the mailbox. The simplest way to configure an Outlook Web App virtual directory for Kerberos authentication is to set it to use Integrated Windows authentication by using the Set-OwaVirtualDir	OWA

				ectory cmdlet in the Exchange Management Shell, or by using the Exchange Management Console. If you already have a Client Access server deployed in the target Active Directory site with an Outlook Web App virtual directory configured for Kerberos authentication, the proxying Client Access server may not be finding that target Client Access server because it does not have an internalUrl parameter configured. You can configure the internalUrl parameter for the Outlook Web App virtual directory on the Client Access server in the target Active Directory site by using the Set-OwaVirtualDirectory cmdlet.	
MSExchange OWA 11	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.Invalid forms registry file %1 Line number	OWA

				= %2 Position = %3. The value "%4" specified for the ApplicationElement element isn't one of the expected values.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about troubleshooting the forms registry.	
MSExchange OWA 59	Configuration	Warning	LogAlways	A corrupted calendar configuration was detected (user = %1), The configuration is being reset.	OWA
MSExchange OWA 29	Configuration	Error	LogAlways	There's an error in your configuration.The authentication type specified in the %1web.config file is incorrect. The correct authentication type is "Windows".	OWA
MSExchange OWA 48	Transcoding	Error	LogAlways	WebReady Document Viewing isn't registered. To	OWA

				fix this problem, reinstall Outlook Web App.	
MSExchange OWA 34	Configuration	Error	LogAlways	The Address Book custom properties couldn't be parsed. Invalid element found in "%1" at line number ="%2" position = "%3". The custom properties couldn't be parsed because an invalid element was encountered. The only element that can have attributes in the custom properties file is "customProperty". If this error isn't addressed, users won't be able to view the custom properties. The Help and Support Center provides information about how to troubleshoot this issue.	OWA
MSExchange OWA 49	Transcoding	Warning	LogAlways	WebReady Document Viewing can't be found. To fix this problem, reinstall Outlook Web App.	OWA

MSExchange OWA 33	Configuration	Error	LogAlways	The Address Book custom properties couldn't be parsed. "%1" attribute wasn't found in "%2" at line number = "%3". Having the "%1" as the "%4" attribute in the custom properties file is a requirement for Outlook Web App to parse it and display the values to users. If this error isn't addressed, users won't be able to view the custom properties. The Help and Support Center provides information about how to troubleshoot this issue.	OWA
MSExchange OWA 6	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.Invalid forms registry file %1 Line number = %2 Position = %3. Expected attribute = %4.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access	OWA

				Outlook Web App. The Help and Support Center provides information about troubleshooting the forms registry.	
MSExchange OWA 20	Themes	Warning	LogAlways	Outlook Web App couldn't initialize.File "%1" in theme folder "%2" wasn't parsed. More than one instance of the attribute "%3" was found. Line %4, Position %5.	OWA
MSExchange OWA 55	FormsRegistry	Error	LogAlways	Outlook Web App couldn't initialize.Invalid forms registry file %1 Line number = %2 Position = %3 The value "%4" specified for the IsRichClient attribute isn't a valid Boolean value. Change this property in the registry to contain True or False.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support	OWA

				Center provides information about how to troubleshoot the forms registry.	
MSExchange OWA 35	Configuration	Error	LogAlways	The Address Book custom properties couldn't be parsed. Invalid file "%1" Line number = %2 Position = %3 Message = "%4". A valid custom property file format is required for Outlook Web App to parse it and display the values to users. If this error isn't addressed, users won't be able to view the custom properties. The Help and Support Center provides information about troubleshooting this issue.	OWA
MSExchange OWA 65	ADNotifications	Error	LogAlways	An error occurred while the Outlook Web App configuration settings were being loaded. Virtual directory: "%1". Web site: "%2".Error message:"%3"	OWA
MSExchange	FormsRegistry	Error	LogAlways	Outlook Web	OWA

OWA 8				App couldn't initialize.Invalid forms registry file %1 Line number = %2 Position = %3. You must either define a base experience or a forms registry to inherit from.The forms registry is a critical component of Outlook Web App. If this error isn't addressed, users might not be able to access Outlook Web App. The Help and Support Center provides information about troubleshooting the forms registry.	
MSExchange OWA 18	Themes	Error	LogAlways	Outlook Web App couldn't initialize.Themes folder "%1" doesn't exist.	OWA
MSExchange OWA 52	ADNotifications	Error	LogAlways	The configuration settings couldn't be read from Active Directory for virtual directory "%1" under Web site "%2".Exception message:"%3".	OWA
MSExchange OWA 61	Configuration	Error	LogAlways	Outlook Web App has encountered	OWA

				an error. This can happen if the mailbox was created using Active Directory Users and Computers instead of the Exchange Management Console or the Exchange Management Shell, or if the version number of the user's mailbox object doesn't match the mailbox version that's configured on the Exchange 2003 server or on the computer running the Mailbox server role. To correct this error, run cmdlet Set-Mailbox -Identity <Mailbox Identity> -ApplyMandatoryProperties.	
MSExchange OWA 60	SmallIcons	Warning	LogAlways	Outlook Web App encountered an error during initialization.The values (%1) defined for the Alt attribute in the small icon configuration file aren't valid.	OWA
MSExchange OWA 25	Themes	Error	LogAlways	Outlook Web App couldn't initialize.It couldn't parse	OWA

				file "%1" in theme folder "%2". There was an error parsing the XML file. Line %3, Position %4.	

1.6.5.6 RPCHTTPAutoConfig Errors and Events

RPCHTTPAutoConfig Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-14*

Microsoft Exchange Server 2010 generates RPC Over Autonconfig events in Event Viewer so that you can troubleshoot and verify the RPC Over Autonconfig features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

RPC Over HTTP Autoconfig Errors and Events

The following table provides a list of RPC Over Autonconfig errors and events.

Event ID	Category	Event type	Value or description
MSExchangeRPCHTTPAutoconfig 2003	General	Error	The RPC over HTTP Proxy component is not installed or is not properly configured. Use the Windows Component Wizard to add the RPC over HTTP Proxy component to the Networking Services.
MSExchangeRPCHTTPAutoconfig 2008	General	Information	The RPC over HTTP Proxy component is currently disabled. This prevents Outlook Anywhere from being

			configured correctly. Enable the RPC over HTTP Proxy component by setting a registry key %1, value %2 to DWORD 1, or disable Outlook Anywhere.
MSExchangeRPCHTTPAutoconfig 3002	General	Warning	Exchange has added the string "ncacn_HTTP:6004" to the following registry key entry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\NSPI Interface Protocol Sequences. You must reboot the server before you can use it for Outlook Anywhere.
MSExchangeRPCHTTPAutoconfig 3003	General	Information	The Outlook Anywhere authentication settings have been updated.Old settings: %1New settings: %2
MSExchangeRPCHTTPAutoconfig 3008	General	Information	The Outlook Anywhere feature has been enabled. The Client Access server resource pool registry setting has been modified to reflect this change.New value: %2
MSExchangeRPCHTTPAutoconfig 3009	General	Information	A Client Access server has been added or removed. The Client Access server resource pool registry setting has been modified.Old value: %1New value: %2
MSExchangeRPCHTTPAutoconfig 3010	General	Information	The Outlook Anywhere feature is disabled. The Client Access server resource pool registry setting has been modified to reflect this state.Old value: %

			1New value: %2
MSExchangeRPCHTTPAutoconfig 3011	General	Information	The Outlook Anywhere feature has been enabled. The Client Access Array registry setting has been modified to reflect this change.New value: %2
MSExchangeRPCHTTPAutoconfig 3012	General	Information	A Client Access array has been added or removed. The Client Access array registry setting has been modified.Old value: %1New value: %2
MSExchangeRPCHTTPAutoconfig 3013	General	Information	The Outlook Anywhere feature is disabled. The Client Access Array registry setting has been modified to reflect this state.Old value: %1New value: %2
MSExchangeRPCHTTPAutoconfig 3015	General	Error	The RPC/HTTP Load Balancing service couldn't be started.
MSExchangeRPCHTTPAutoconfig 3016	General	Warning	The RPC/HTTP Load Balancing service isn't installed.
MSExchangeRPCHTTPAutoconfig 3017	General	Information	The RPC/HTTP Load Balancing service has been stopped.
MSExchangeRPCHTTPAutoconfig 3020	General	Information	A Global Catalog (GC) server has been added or removed. The %3 registry setting has been modified.Old value: %1New value: %2
MSExchangeRPCHTTPAutoconfig 3021	General	Information	The Outlook Anywhere feature is disabled. The %3 registry setting has been modified to reflect this state.Old value: %1New value: %2
MSExchangeRPCHTTPAutoconfig 3022	General	Error	The registry value %3 is the wrong Type.Expected Type:

			%1Found Type: %2This may prevent Outlook Anywhere settings from being updated.

1.6.5.7 ServiceHost Errors and Events

ServiceHost Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Microsoft Exchange Service Host service Certificate Deployment events in Event Viewer so that you can troubleshoot and verify the Microsoft Exchange Service Host features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Microsoft Exchange Service Host service Errors and Events

The following table provides a list of Microsoft Exchange Service Host service errors and events.

Event ID	Category	Event type	Value or description
MSExchangeServiceHost 2001	General	Information	Loading servicelet module %1.
MSExchangeServiceHost 2003	General	Information	Service starting.
MSExchangeServiceHost 2004	General	Information	Service started successfully.
MSExchangeServiceHost 2010	General	Information	Service stopped successfully.
MSExchangeServiceHost 2014	General	Information	The Mailbox server role is installed.
MSExchangeServiceHost 2016	General	Information	The Client Access server role is installed.
MSExchangeServiceHost 2017	General	Information	The Unified Messaging server role is installed.
MSExchangeServiceHost 2018	General	Information	The Hub Transport server role is

			installed.

1.7 Transport

Transport

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-10*

The component of Microsoft Exchange that is responsible for transferring messages is known as Transport. Two server roles are involved:

- **Edge Transport** The mail routing server that typically sits at the perimeter of the topology and routes mail between the Exchange organization and the Internet.
- **Hub Transport** The mail routing server that routes mail within the Exchange organization.

The following topics are gateways to information about Transport in Exchange Server 2010:

Understanding Transport

View a list of links to topics that provide detailed information about the transport features in Microsoft Exchange Server 2010, which will help you gain a better understanding of the Hub Transport and Edge Transport server roles.

Managing Transport Servers

View a list of links to topics that provide information about managing transport features in your organization.

Securing Transport Servers

View a list of links to topics that provide information about managing the security of your transport infrastructure.

Troubleshooting Reference for Transport Servers

View a list of links to topics that provide information about troubleshooting transport issues.

Performance Counter Reference for Transport Servers

Learn about various performance counters used by transport servers.

Error and Event Reference for Transport Servers

Learn about transport errors and events you may encounter.

1.7.1 Understanding Transport

Understanding Transport

Exchange Server 2010 > Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-09*

The component of Microsoft Exchange that is responsible for transferring messages is known as Transport. The following topics provide detailed information about the Transport features in Exchange Server 2010:

Overview of the Edge Transport Server Role

Overview of the Hub Transport Server Role

Understanding Accepted Domains

Understanding Address Rewriting

Understanding Anti-Spam and Antivirus Functionality

Understanding Approval Framework

Understanding Back Pressure

Understanding Content Conversion

Understanding Delivery Agents

Understanding DSNs and NDRs

Understanding DNS Query Failure Sensitivity

Understanding Domain Security

Understanding Edge Subscriptions

Understanding Edge Transport Server Cloned Configuration

Understanding the EdgeTransport.exe.Config File

Understanding Exchange 2010 Support for X.400 Authoritative Domains

Understanding Foreign Connectors

Understanding Group Metrics

Understanding Header Firewall

Understanding SMTP Failover and Load Balancing in Transport

Understanding Journaling

Understanding MailTips

Understanding Message Routing

Understanding Message Size Limits

Understanding Message Throttling

Understanding Moderated Transport

Understanding the Pickup and Replay Directories

Understanding Priority Queuing

Understanding Receive Connectors

Understanding Recipient Resolution

Understanding Remote Domains

Understanding Send Connectors

Understanding Shadow Redundancy

Understanding TLS Certificates

Understanding Transport Agents

Understanding Transport Database Configuration Options

Understanding Transport Logs

Understanding Transport Pipeline

Understanding Transport Policy and Compliance Agents

Understanding Transport Queues

Understanding Transport Rules

1.7.1.1 Overview of the Edge Transport Server Role

Overview of the Edge Transport Server Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2010, the Edge Transport server role is deployed in your organization's perimeter network. Designed to minimize the attack surface, the Edge Transport server handles all Internet-facing mail flow, which provides SMTP relay and smart host services for the Exchange organization. Additional layers of message protection and security are provided by a series of agents that run on the Edge Transport server and act on messages as they're processed by the message transport components. These agents support the features that provide protection against viruses and spam and apply transport rules to control message flow.

The computer that has the Edge Transport server role installed doesn't have access to Active Directory. All configuration and recipient information is stored in Active Directory Lightweight Directory Services (AD LDS). To perform recipient lookup tasks, the Edge Transport server requires data that resides in Active Directory. This data is synchronized to the Edge Transport server using EdgeSync. EdgeSync is a collection of processes that are run on a computer that has the Hub Transport server role installed to establish one-way replication of recipient and configuration information from Active Directory to the AD LDS instance on an Edge Transport server. The Microsoft Exchange EdgeSync service copies only the information that's required for the Edge Transport server to perform anti-spam configuration tasks and the information about the connector configuration that's

required to enable end-to-end mail flow. The Microsoft Exchange EdgeSync service performs scheduled updates so that the information in AD LDS remains current.

You can install more than one Edge Transport server in the perimeter network. Deploying more than one Edge Transport server provides redundancy and failover capabilities for your inbound message flow. You can load-balance SMTP traffic to your organization between Edge Transport servers by defining more than one mail exchange (MX) resource record with the same priority in the Domain Name System (DNS) database for your mail domain. You can achieve consistency in configuration between multiple Edge Transport servers by using cloned configuration scripts.

The message-processing scenarios that you can manage on the Edge Transport server role are described in the following sections.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Internet Mail Flow

Servers that run the Edge Transport server role accept messages that come into the Exchange 2010 organization from the Internet. After the messages are processed by the Edge Transport server, they are routed to Hub Transport servers inside the organization.

All messages that are sent to the Internet from the organization are routed to Edge Transport servers after the messages are processed by the Hub Transport server. You can configure the Edge Transport server to use DNS to resolve MX resource records for external SMTP domains, or you can configure the Edge Transport server to forward messages to a smart host for DNS resolution.

For more information about mail flow, see Understanding Transport Pipeline.

Anti-Spam and Antivirus Protection

In Exchange 2010, the anti-spam and antivirus features provide services to block viruses and spam, or unsolicited commercial e-mail, at the network perimeter. Most viruses use spam-like tactics to gain access to your organization and to entice users to open an e-mail message. If you can filter out most of your spam, you're also more likely to capture viruses before they enter your organization.

Spammers use a variety of techniques to send spam into your organization. Servers that run the Edge Transport server role help prevent users in your organization from receiving spam by providing a collection of agents that work together to provide different layers of spam filtering and protection. Establishing tarpitting intervals on connectors makes e-mail harvesting attempts ineffective.

For more information about the anti-spam and antivirus features in Exchange 2010, see Understanding Anti-Spam and Antivirus Functionality.

Edge Transport Rules

Edge Transport rules are used to control the flow of messages that are sent to or received from the Internet. The Edge Transport rules help protect corporate network resources and data by applying an action to messages that meet specified conditions. These rules are configured for each server. Edge Transport rule conditions are based on data, such as specific words or text patterns in the message subject, body, header, or From address, the spam confidence level (SCL), or attachment type. Actions determine how the message is processed when a specified condition is true. Possible actions include

quarantine of a message, dropping or rejecting a message, appending additional recipients, or logging an event. Optional exceptions exempt particular messages from having an action applied.

For more information about the Edge Transport rules, see Understanding Transport Rules.

Address Rewriting

You use address rewriting to present a consistent appearance to external recipients of messages from your Exchange 2010 organization. You configure the Address Rewriting agent on the Edge Transport server role to enable the modification of the SMTP addresses on inbound and outbound messages. Address rewriting is especially useful when a newly merged organization that has several domains wants to present a consistent appearance of e-mail addresses to external recipients.

For more information about address rewriting, see Understanding Address Rewriting.

1.7.1.2 Overview of the Hub Transport Server Role

Overview of the Hub Transport Server Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Deployed inside your Active Directory forest, the Hub Transport server role handles all mail flow inside the organization, applies transport rules, applies journaling policies, and delivers messages to a recipient's mailbox. Messages that are sent to the Internet are relayed by the Hub Transport server to the Edge Transport server role that's deployed in the perimeter network. Messages that are received from the Internet are processed by the Edge Transport server before they're relayed to the Hub Transport server. If you don't have an Edge Transport server, you can configure the Hub Transport server to relay Internet messages directly or utilize a third-party smart host. You can also install and configure the Edge Transport server agents on the Hub Transport server to provide anti-spam and antivirus protection inside the organization, although this isn't recommended.

You can install the Hub Transport server role on the same hardware with any other internal server role or on a server that's dedicated to the Hub Transport server role. You must deploy a Hub Transport server role in each Active Directory site that contains a Mailbox server role. Deploying more than one Hub Transport server per site provides redundancy. When you install more than one Hub Transport server in an Active Directory site, the connections are distributed.

The message-processing scenarios that you can manage on the Hub Transport server role are described in the following sections.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Internal Mail Flow

The Hub Transport server role processes all messages that are sent inside the Microsoft Exchange Server 2010 organization before the messages are delivered to a recipient's Inbox or are routed to users outside the organization. There are no exceptions to this behavior; messages are always passed through a server that runs the Hub Transport

server role.

Messages are submitted to the Hub Transport server in three ways: through SMTP submission, from the Pickup directory, or when a user inside the organization sends a message, which is picked up from the user's Outbox by the *store driver*. The store driver is a software component of the Hub Transport server that delivers inbound messages to *Exchange stores*, the databases that contain public folder and mailbox stores.

When messages are submitted to the Hub Transport server, they're processed by the categorizer. The *categorizer* is a component of Exchange transport that processes all inbound messages and determines what to do with the messages based on information about the intended recipients. In Exchange 2010, the Hub Transport server uses the categorizer to expand distribution lists and to identify alternative recipients and forwarding addresses. After the categorizer retrieves full information about the recipients, it uses that information to apply policies, route the messages, and perform content conversion. Messages are then delivered locally by the store driver to a recipient's mailbox, or they're delivered remotely by using SMTP to send messages to another transport server. Messages that are sent by users in your organization are picked up from the sender's Outbox by the store driver and are put in the Submission queue on a server that runs the Hub Transport server role. For more information, see Understanding Transport Pipeline.

Messaging Policy and Compliance Features

With a collection of transport agents, you can configure rules and settings that are applied as messages enter and leave the mail flow components. You can create messaging policy and rule settings that are designed to meet different regulations and that can easily be changed to adapt to your organization's requirements. The transport-based messaging policy and compliance features include server-based rules that you configure to enforce your organization's compliance scenarios and the Journaling agent that acts to enforce message retention. For more information, see Planning for Compliance.

Anti-Spam and Antivirus Protection

Exchange 2010 provides anti-spam and antivirus protection for messages. Although these features are designed for use in the perimeter network on the Edge Transport server role, the Edge Transport agents can also be configured on the Hub Transport server. By default, these agents aren't enabled on the Hub Transport server role. To use the anti-spam features on the Hub Transport server, you must register the agents in a configuration file and enable the features that you want to use by running a provided Exchange Management Shell script. You install and enable the antivirus agent in a separate operation. For more information, see Understanding Anti-Spam and Antivirus Functionality.

1.7.1.3 Understanding Accepted Domains

Understanding Accepted Domains

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-23*

An accepted domain is any SMTP namespace for which a Microsoft Exchange organization sends or receives e-mail. Accepted domains include those domains for which the Exchange organization is authoritative. An Exchange organization is authoritative when it handles mail delivery for recipients in the accepted domain. Accepted domains also include domains for which the Exchange organization receives mail and then relays it to an e-mail server that's outside the Active Directory forest for delivery to the recipient.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Configuring Accepted Domains

Accepted domains are configured as global settings for the Exchange organization and on computers that have the Edge Transport server role installed. You must configure every domain for which your Hub Transport servers relay or deliver messages as an accepted domain in your organization. The Edge Transport server requires that all domains for which it accepts and relays messages are configured as accepted domains.

We recommend that you create and manage all accepted domains inside the organization and synchronize that information to the Edge Transport server by creating an Edge Subscription. When you subscribe the Edge Transport server to the Microsoft Exchange Server 2010 organization, all accepted domains that are configured in the organizational settings for the Hub Transport server role are replicated to the Edge Transport server during EdgeSync synchronization. To modify the accepted domain configuration on an Edge Transport server that's subscribed to the Exchange 2010 organization, you must make the change on the Hub Transport server.

There are three types of accepted domains: authoritative, internal relay, and external relay. These accepted domain types are described in the following sections.

Return to top

Authoritative Domains

An organization may have more than one SMTP domain. The set of e-mail domains for an organization are the authoritative domains. In Exchange 2010, an accepted domain is considered authoritative when the Exchange organization hosts mailboxes for recipients in this SMTP domain. The Edge Transport servers should always accept e-mail that's addressed to any of the organization's authoritative domains.

By default, when the first Hub Transport server role is installed, one accepted domain is configured as authoritative for the Exchange organization. The default accepted domain is the fully qualified domain name (FQDN) for your forest root domain. Frequently, the internal domain name differs from the external domain name. For example, your internal domain name may be Contoso.local, although your external domain name is Contoso.com. The Domain Name System (DNS) mail exchange (MX) resource record for your organization

references Contoso.com. Contoso.com is the SMTP namespace that you assign to users when you create an e-mail address policy. You must create an accepted domain to match your external domain name.

By default, no accepted domains are configured on the Edge Transport server role.

Return to top

Relay Domains

When e-mail is received from the Internet by an Edge Transport server and the recipient of the message isn't part of an authoritative domain, the sending server tries to relay through the Exchange server. When a server acts as a relay server that has no restrictions, it can put a large burden on Internet-connected servers. Administrators can prevent this open relay scenario by rejecting all e-mail that isn't addressed to a recipient in the organization's authoritative domains. However, there are scenarios where an organization wants to let partners or subsidiaries relay e-mail through the Exchange servers. In Exchange 2010, you can configure accepted domains as relay domains. Your organization receives the e-mail messages and then relays the messages to another e-mail server.

You can configure a relay domain as an internal relay domain or as an external relay domain. These two relay domain types are described in the following sections.

Internal Relay Domain

When you configure an internal relay domain, some or all of the recipients in this domain don't have mailboxes in this Exchange organization. Mail from the Internet is relayed for this domain through Hub Transport servers in this Exchange organization. This configuration is used in the scenarios that are described in this section.

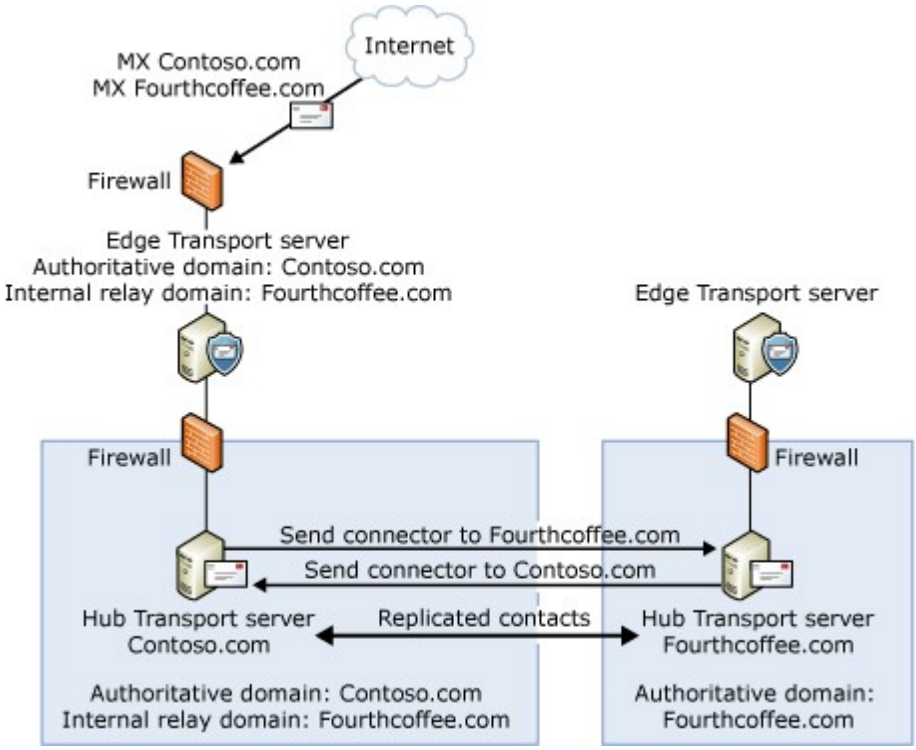
An organization may have to share the same SMTP address space between two or more different e-mail systems. For example, you may have to share the SMTP address space between Microsoft Exchange and a third-party e-mail system, or between Exchange environments that are configured in different Active Directory forests. In these scenarios, users in each e-mail system have the same domain suffix as part of their e-mail addresses.

To support these scenarios, you must create an accepted domain that's configured as an internal relay domain. You must also add a Send connector that's sourced on a Hub Transport server and configured to send e-mail to the shared address space. If an accepted domain is configured as authoritative and a recipient isn't found in Active Directory, a non-delivery report (NDR) is returned to the sender. The accepted domain that's configured as an internal relay domain first tries to deliver to a recipient in the Exchange organization. If the recipient isn't found, the message is routed to the Send connector that has the closest address space match.

If an organization contains more than one forest and has configured global address list (GAL) synchronization, the SMTP domain for one forest may be configured as an internal relay domain in a second forest. Messages from the Internet that are addressed to recipients in internal relay domains are received and processed by the Edge Transport server and then relayed to the Hub Transport servers in the same organization. The receiving Hub Transport servers then route the messages to the Hub Transport servers in the recipient forest. You configure the SMTP domain as an internal relay domain to make sure that e-mail that's addressed to that domain is accepted by the Exchange organization. The connector configuration of your organization determines how messages are routed.

In the following figure, Fourthcoffee.com is configured as an internal relay domain for the

Exchange 2010 organization in the Contoso.com forest. The MX resource records for Fourthcoffee.com reference a public IP address for the Contoso.com organization. A forest trust exists between Fourthcoffee.com and Contoso.com, and GAL synchronization is configured. The Contoso.com Edge Transport server accepts messages for the Fourthcoffee.com SMTP domain from the Internet and then relays those messages to the Hub Transport servers in the Contoso.com Exchange organization. The messages are then routed to the Hub Transport servers in the Fourthcoffee.com Exchange organization. A cross-forest Send connector is configured for routing messages from Contoso.com to Fourthcoffee.com. Messages that are sent from Fourthcoffee.com to external recipients are routed to the Hub Transport servers in the Contoso.com forest. A second cross-forest Send connector is configured for routing messages from Fourthcoffee.com to Contoso.com. When the Hub Transport servers in Contoso.com receive messages from the internal relay domain Fourthcoffee.com, they deliver messages for recipients in authoritative domains and relay messages for Internet recipients to the Edge Transport server for delivery.



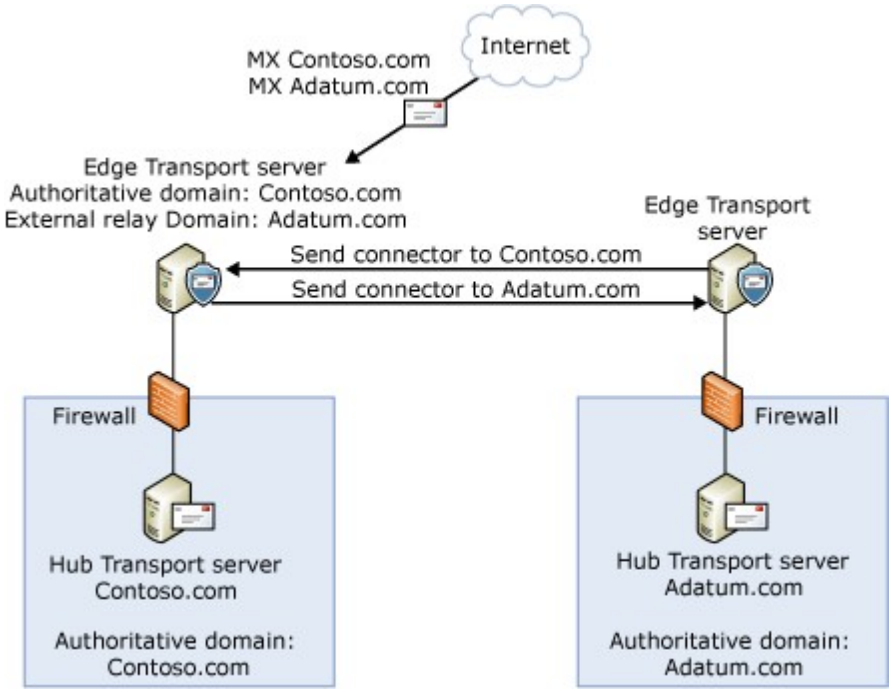
External Relay Domain

When you configure an external relay domain, messages are relayed to an e-mail server that's outside the Exchange organization and outside the organization's network perimeter. The messages are relayed by the Edge Transport server.

In this scenario, the MX resource record for the external relay domain references a public IP address for the Exchange 2010 organization that's relaying messages. The Edge Transport server receives the messages for recipients in the external relay domain and then routes the messages to the e-mail system for the external relay domain. A Send connector from the Edge Transport server to the external relay domain is required in this scenario. The external relay domain may also use your organization's Edge Transport server as a smart host for outgoing mail.

In the following figure, Adatum.com is configured as an external relay domain for the Exchange 2010 organization in the Contoso.com forest. The MX resource record for Adatum.com references a public IP address for the Contoso.com organization. The

Contoso.com Edge Transport server accepts messages for the Adatum.com SMTP domain from the Internet and then relays those messages to the e-mail servers in the Adatum.com organization. Adatum.com also uses the Contoso.com Edge Transport server as a smart host for routing outgoing messages. Messages that are sent from Adatum.com to external recipients are routed to the Edge Transport servers in the Contoso.com organization. When the Edge Transport servers in Contoso.com receive messages from Adatum.com, they deliver messages for recipients in authoritative domains and internal relay domains to the Hub Transport servers and route messages to the Internet.



Return to top

Accepted Domains and E-Mail Address Policies

You must configure an accepted domain before that SMTP address space can be used in an e-mail address policy. When you create an accepted domain, you can use a wildcard character (*) in the address space to indicate that all subdomains of the SMTP address space are also accepted by the Exchange organization. For example, to configure Contoso.com and all its subdomains as accepted domains, enter *.Contoso.com as the SMTP address space. The accepted domain entries are automatically available for use in an e-mail address policy.

If you delete an accepted domain that's used in an e-mail address policy, the policy is no longer valid, and recipients with e-mail addresses in that SMTP domain will be unable to send or receive e-mail.

Return to top

1.7.1.4 Understanding Address Rewriting

Understanding Address Rewriting

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-18*

In Microsoft Exchange Server 2010, address rewriting enables you to modify the addresses of senders and recipients on messages that enter and leave your Exchange 2010 organization.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Why Use Address Rewriting?

You use address rewriting to present a consistent appearance to external recipients of messages from your Exchange 2010 organization. Address rewriting can be valuable to organizations that use third-party vendors to provide e-mail support and services. Customers and partners expect e-mail messages to come from the organization, not a third-party vendor. Similarly, after a merger or acquisition, an organization might want all e-mail messages to appear to come from the single new organization. The address rewriting feature frees organizations to structure their businesses by business requirements instead of by technical requirements or limitations.

You can also use address rewriting to enable appropriate routing of inbound messages from outside your Exchange 2010 organization to internal recipients. Address rewriting enables replies to messages that were rewritten to be correctly routed to the original sender of the rewritten message.

You configure Address Rewriting agents on the Receive connector and Send connector on a computer that has the Edge Transport server role installed.

Return to top

Address Rewriting Scenarios

The following scenarios are examples of how address rewriting can benefit organizations:

- **Group consolidation** Some organizations segment their internal businesses into separate domains that are based on business or technical requirements. However, this configuration can cause e-mail messages to appear as if they come from separate groups or even separate organizations. This appearance might not be desirable to the organization.
  The following example shows how an organization, Contoso, Ltd., could hide its subdomains:
  - Outbound messages from the Northamerica.contoso.com, Europe.contoso.com, and Asia.contoso.com domains are rewritten to appear as if they all originate from a single Contoso.com domain. All messages are rewritten as they pass through Edge Transport servers that provide SMTP connectivity between the whole organization and the Internet.
  - Inbound messages to the Contoso.com domain are passed on by the Edge Transport server to the Hub Transport server role, which then determines the correct recipient. For example, messages to chris@contoso.com are sent to an internal Hub Transport server, which then determines the correct mailbox to send the message to by using the proxy address that's configured on the recipient's e-mail account.
- **Mergers and acquisitions** When organizations merge or are acquired, their technology infrastructure must be modified to match new business and technical requirements. An acquired company may continue to run as a separate business unit, but the e-mail administrator can use address rewriting to make the two organizations appear as if they're one integrated organization.
  The following example shows how Contoso, Ltd. could hide the e-mail domain of the newly acquired company, Fourth Coffee:
  - Contoso, Ltd. wants all outbound messages from Fourth Coffee's Exchange organization to appear as if they originate from Contoso.com. All messages from both organizations are sent through the Edge Transport servers at Contoso, Ltd., where e-mail messages are rewritten from *someone*@fourthcoffee.com to *someone*@contoso.com.
  - Inbound messages to adam@contoso.com are rewritten and routed to his adam@fourthcoffee.com e-mail account. Incoming messages that use his old adam@fourthcoffee.com domain are also accepted, because the domain still exists. Inbound replies to e-mail messages that were rewritten are handled by the Edge Transport servers at Contoso, Ltd., where the Address Rewriting agent rewrites the recipient address so that replies are correctly routed to the appropriate Fourthcoffee.com e-mail address. Replies to e-mail messages that were sent before the merger to Fourthcoffee.com e-mail addresses are routed directly to Fourth Coffee's e-mail servers.
- **Partners** Many organizations use external partners to provide services for their customers, other partners, or the organization itself. To avoid confusion, the organization might replace the e-mail domain of the partner organization with its own e-mail domain.
  The following example shows how Contoso, Ltd. could hide a partner's e-mail domain:
  - Contoso, Ltd. provides support for the larger Wingtip Toys organization. Wingtip Toys wants a unified experience for its customers and requires all messages that originate from support personnel at Contoso, Ltd. to appear as if they were sent from Wingtip Toys. All outbound messages that relate to Wingtip Toys are sent through their Edge Transport servers, and all Contoso.com addresses are rewritten to appear as Wingtiptoys.com addresses.
  - Inbound messages for support@wingtiptoys.com are accepted by Wingtip Toy's Edge Transport servers, rewritten, and then routed to the

support@contoso.com e-mail address.

> **Caution:**
> So that inbound e-mail is appropriately mapped and routed, you must make sure that the user name part of the address is unique across all e-mail organizations that may be affected by address rewriting.

Return to top

SMTP Message Headers

Address Rewriting agents rewrite e-mail addresses by rewriting the SMTP headers on e-mail messages that are sent and received by an Edge Transport server. Address Rewriting agents typically rewrite outbound messages because the organization wants to hide the internal domains and subdomains as effectively as possible and present a single external domain to the Internet. Address Rewriting agents typically rewrite inbound messages to route those messages to their intended recipients. For these reasons, Address Rewriting agents rewrite several SMTP header fields on outbound e-mail messages. Address Rewriting agents rewrite only one SMTP header field on inbound e-mail messages. The following table shows which SMTP header fields are rewritten on outbound and inbound messages.

SMTP header fields rewritten on outbound and inbound messages

SMTP header field	Outbound	Inbound
Envelope From (MAIL FROM)	Rewritten	Not rewritten
Envelope To (RCPT TO)	Not rewritten	Rewritten
Body To	Rewritten	Not rewritten
Body Cc	Rewritten	Not rewritten
Body From	Rewritten	Not rewritten
Body Sender	Rewritten	Not rewritten
Body Reply-To	Rewritten	Not rewritten
Body Return-Receipt-To	Rewritten	Not rewritten
Body Disposition-Notification-To	Rewritten	Not rewritten
Body Resent-From	Rewritten	Not rewritten
Body Resent-Sender	Rewritten	Not rewritten

Return to top

What Address Rewriting Agents Don't Rewrite

Address Rewriting agents don't rewrite several SMTP header fields, because address rewriting would break SMTP functionality. For example, changing these SMTP headers could affect message loop detection, invalidate the signature, or make a rights-protected

message unreadable. The following SMTP header fields aren't modified by the Address Rewriting agents:

- **Return-Path**
- **Received**
- **Message-ID**
- **X-MS-TNEF-Correlator**
- **Content-Type Boundary=string**
- **Headers located inside MIME body parts**

Address Rewriting agents also don't rewrite header fields within e-mail messages that contain domains for which the Hub Transport server isn't authoritative. Rewriting such domains causes an uncontrollable form of message relay.

Address Rewriting agents also don't modify the header fields of messages that are embedded in another message. Senders and recipients expect embedded messages to remain intact and be delivered without modification, as long as the messages don't trigger transport rules that are implemented between the sender and recipient.

Return to top

Considerations for Use of Outbound-Only Address Rewriting

When an e-mail message is outbound from the Exchange 2010 organization, outbound-only address rewriting involves modification of the sender SMTP address only. The Address Rewriting agent is configured only on the Send connector on the Edge Transport server. The following list shows the conditions that are required to configure an outbound-only Address Rewriting agent:

- The resulting addresses must be unique across the organization. For example, if the unique e-mail addresses ed@sales.contoso.com and ed@research.contoso.com are included in a rule to rewrite all addresses to contoso.com, the Address Rewriting agent will rewrite both addresses to ed@contoso.com and will cause a conflict.
- A proxy address must be configured on each mailbox that matches the rewritten e-mail address. This enables those mailboxes to receive replies to e-mail messages in which headers are rewritten.
- When you use wildcard characters, there must be a period between the wildcard character and the domain name.
- You can use wildcard characters only in the internal domain.
- No characters can be in front of the wildcard character.
- Outbound-only address rewriting can't affect the user name or display name part of the address.
- Only literal strings are supported.

Return to top

Considerations for Bidirectional Address Rewriting

Bidirectional address rewriting modifies the sender SMTP address on e-mail messages that are leaving the Exchange organization and the recipient SMTP address on e-mail messages that are entering the Exchange organization. To do this, you configure the Address Rewriting agent on both the Send connector and Receive connector on the Edge Transport server.

The following list shows the conditions that are required when you create a bidirectional Address Rewriting agent:

- You can't use wildcard characters.
- You must use full SMTP addresses when you configure a bidirectional address rewriting rule. For example, the internal address is chris@contoso.com, and the external address is support@contoso.com.
- Only literal strings are supported.
- The address must be unique across the organization. For example, if an e-mail address, bob@contoso.com, already exists, mapping robert@fourthcoffee.com to bob@contoso.com will cause replies to messages from bob@contoso.com to be delivered to the wrong person.

Return to top

Considerations for Rewriting Addresses in Multiple Domains

Before you create an address rewrite entry that rewrites multiple domains, you must prepare your subdomains. Also, before you perform the procedure for creating an address rewrite entry for multiple subdomains that's described in Create an Address Rewrite Entry, you must understand the requirements for rewriting e-mail addresses in multiple domains to a single domain, and the appropriate preconfiguration for the affected mailboxes and contacts.

Important Considerations

When you flatten internal subdomains into a single external domain, you must consider the following factors, which apply only when multiple subdomains are being rewritten:

- **Unique aliases are required** All e-mail aliases, the part of the e-mail address to the left of the at (@) sign, must be unique across all subdomains. For example, if there is a joe@sales.contoso.com, there can't be a joe@marketing.contoso.com.
- **Proxy addresses are required** A proxy address that matches the e-mail address that's produced by the Address Rewriting agent must be configured on every e-mail account that's in the subdomains that are rewritten. For example, if joe@sales.contoso.com is rewritten to joe@contoso.com, the e-mail address joe@contoso.com must be added as a proxy address to Joe's mailbox.
- **Contacts may be required** If you're rewriting e-mail from a non-Exchange 2010 e-mail system, you must create Active Directory mail-enabled contacts for each e-mail address in the non-Exchange 2010 e-mail address that's being rewritten. This mail-enabled contact must contain the original e-mail address and the rewritten e-mail address. For example, if joe@unix.contoso.com is rewritten to joe@contoso.com, you must create a mail-enabled contact in Active Directory with joe@unix.contoso.com as the target SMTP address and joe@contoso.com as the proxy SMTP address.

These factors are important because rewriting addresses in multiple subdomains causes a many-to-one relationship between internal subdomains and the externally visible domain. Because of this many-to-one relationship, the Address Rewriting agent can't determine which subdomain contains the correct recipient when a message that's addressed to the externally visible domain is received.

Important:

Make sure that every e-mail alias that exists across all subdomains is unique. Exchange 2010 doesn't check to verify that every e-mail alias that can be rewritten to a single domain is unique.

Removing Conflicting E-Mail Addresses

To create an address rewrite entry that rewrites multiple subdomains, you must first make sure that all e-mail aliases are unique across all your subdomains. For example, consider the following configuration:

The following users are in the subdomains sales.contoso.com, marketing.contoso.com and research.contoso.com:

- maria@sales.contoso.com
- chris@sales.contoso.com
- david@marketing.contoso.com
- brian@marketing.contoso.com
- chris@research.contoso.com
- adam@research.contoso.com

Each subdomain has two users, and each user has a unique e-mail address. However, you want to rewrite the subdomains sales.contoso.com, marketing.contoso.com, and research.contoso.com into a single domain that's called contoso.com. The following table shows each original e-mail address and its corresponding rewritten e-mail address.

Original e-mail addresses and corresponding rewritten e-mail addresses

Original e-mail address	Rewritten e-mail address
maria@sales.contoso.com	maria@contoso.com
chris@sales.contoso.com	chris@contoso.com
david@marketing.contoso.com	david@contoso.com
brian@marketing.contoso.com	brian@contoso.com
chris@research.contoso.com	chris@contoso.com
adam@research.contoso.com	adam@contoso.com

When the e-mail addresses in each subdomain are rewritten, a conflict occurs between chris@sales.contoso.com and chris@research.contoso.com. Therefore, both e-mail addresses are rewritten to chris@contoso.com. To resolve this situation, you must change the e-mail address of one of the recipient mailboxes to an address that doesn't conflict with the e-mail address in any other subdomain.

Applying Proxy Addresses to Recipient Mailboxes

For internal recipient mailboxes to receive replies to addresses that have been rewritten, you must configure those recipient mailboxes by using a proxy address that matches the rewritten external address.

For example, if a mailbox exists for adam@research.contoso.com, and the rewritten external address is adam@contoso.com, the mailbox must be configured by using a proxy address that's set to adam@contoso.com.

Return to top

Prioritization of Address Rewriting Entries

The rule that best matches the internal and external domain pair is applied. The following prioritization is the exact order of address rewriting entries from highest priority to lowest priority:

1. **Individual e-mail addresses** An example is mapping john@contoso.com to

support@contoso.com.

2. **Specific domain or subdomain mapping** An example is mapping Contoso.com to Northwindtraders.com or Sales.contoso.com to Contoso.com.
3. **Domain flattening** An example is flattening *.contoso.com into Contoso.com. For example, the following two rules are configured on the Edge Transport server:

```
*.contoso.com maps to Contoso.com
Japan.sales.contoso.com maps to contoso.jp
```

If masato@japan.sales.contoso.com sends an e-mail message, the address is rewritten as masato@contoso.jp, because that rule most closely matches the sender's internal domain, even though the *.contoso.com rule is present.

Return to top

Digitally Signed, Encrypted, and Rights-Protected Messages

Address rewriting shouldn't affect most signed, encrypted, or rights-protected messages. If address rewriting were to invalidate a signature, make an encrypted or rights-protected message unreadable, or otherwise change the security status of such messages in any way, address rewriting isn't applied.

Addresses and information in the following message sections can be rewritten, because information in these sections isn't part of message signing, encryption, or rights protection:

- SMTP envelope fields
- Top-level message body headers

Addresses and information in the following message sections isn't rewritten because information in these sections is part of message signing, encryption, or rights protection:

- Headers located inside MIME body parts that may be signed
- The boundary string parameter of the MIME content type

Return to top

1.7.1.5 Understanding Anti-Spam and Antivirus Functionality

Understanding Anti-Spam and Antivirus Functionality

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-18*

Spammers, or malicious senders, use a variety of techniques to send spam into your organization. No single tool or process can eliminate all spam. Microsoft Exchange Server 2010 builds on the foundation of Exchange Server 2007 to provide a layered, multipronged, and multifaceted approach to reducing spam and viruses. Exchange 2010 includes a variety of anti-spam and antivirus features that are designed to work cumulatively to reduce the spam that enters your organization.

You can reduce the incidences of virus outbreaks and attacks by malicious software, which is also referred to as *malware*, in your organization if you reduce the overall volume of spam that enters your organization. When you eliminate the bulk of the spam at the

computer that has the Edge Transport server role installed, you save processing resources, bandwidth, and storage when the messages are scanned for viruses and other malware further along the mail flow path.

The layered approach to reducing spam refers to the configuration of several anti-spam and antivirus features that filter inbound messages in a specific order. Each feature filters for a specific characteristic or set of related characteristics on the inbound message.

The following sections provide brief descriptions of each default anti-spam and antivirus feature.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Anti-Spam and Antivirus Filters

The anti-spam and antivirus filters are applied in a specific order. For more information, see Understanding Anti-Spam and Antivirus Mail Flow. The following order applies:

1. **Connection filtering** Connection filtering inspects the IP address of the remote server that's trying to send messages to determine what action, if any, to take on an inbound message. The remote IP address is available to the Connection Filter agent as a byproduct of the underlying TCP/IP connection that's required for the SMTP session. Connection filtering uses a variety of IP Block lists, IP Allow lists, as well as IP Block List provider services or IP Allow List provider services to determine whether the connection from the specific IP should be blocked or allowed in the organization.
2. **Sender filtering** Sender filtering compares the sender on the MAIL FROM: SMTP command to an administrator-defined list of senders or sender domains who are prohibited from sending messages to the organization to determine what action, if any, to take on an inbound message.
3. **Recipient filtering** Recipient filtering compares the message recipients on the RCPT TO: SMTP command to an administrator-defined Recipient Block list. If a match is found, the message isn't permitted to enter the organization. The recipient filter also compares recipients on inbound messages to the local recipient directory to determine whether the message is addressed to valid recipients. When a message isn't addressed to valid recipients, the message can be rejected at the organization's network perimeter.
4. **Sender ID** Sender ID relies on the IP address of the sending server and the Purported Responsible Address (PRA) of the sender to determine whether the sender is spoofed or not. PRA is calculated based on the following message headers:
   - Resent-Sender:
   - Resent-From:
   - Sender:
   - From:

For more information about the PRA, see Understanding Sender ID and RFC 4407.

5. **Content filtering** Content filtering uses Microsoft SmartScreen technology to assess the contents of a message. Intelligent Message Filter is the underlying technology of Exchange content filtering. Intelligent Message Filter is based on patented machine-learning technology from Microsoft Research. During its development, Intelligent Message Filter learned distinguishing characteristics of legitimate e-mail messages and spam. Regular updates with Microsoft Exchange Anti-spam Update service ensure that the most up-to-date information is always included when the Intelligent Message Filter runs. Based on the characteristics of millions of messages, Intelligent Message Filter recognizes indicators of both legitimate messages and spam messages. Intelligent Message Filter can accurately assess the probability that an inbound e-mail message is either a legitimate message or spam.
   Spam quarantine is a feature of the Content Filter agent that reduces the risk of losing legitimate messages that are incorrectly classified as spam. Spam quarantine provides a temporary storage location for messages that are identified as spam and that shouldn't be delivered to a user mailbox inside the organization.
   Content filtering also acts on the safelist aggregation feature. Safelist aggregation collects data from the anti-spam safe lists that Microsoft Outlook and Outlook Web App users configure and makes this data available to the Content Filter agent on the computer that has the Edge Transport server role installed in Exchange 2010.
   When an Exchange administrator enables and correctly configures safelist aggregation, the Content Filter agent passes safe e-mail messages to the enterprise mailbox without additional processing. E-mail messages that Outlook users receive from contacts or that those users have added to their Outlook Safe Senders List or have trusted are identified by the Content Filter agent as safe. The result is that messages that are identified as safe aren't classified as spam and unintentionally filtered out of the messaging system.
6. **Sender reputation** Sender reputation relies on persisted data about the IP address of the sending server to determine what action, if any, to take on an inbound message. The Protocol Analysis agent is the underlying agent that implements the sender reputation functionality. A sender reputation level (SRL) is calculated from several sender characteristics that are derived from message analysis and external tests.
   Senders whose SRL exceeds a configurable threshold will be temporarily blocked. All their future connections are rejected for up to 48 hours.
   In addition to the locally calculated IP reputation, Exchange 2010 also takes advantage of IP reputation anti-spam updates, available via Microsoft Update, which provide sender reputation information about IP addresses that are known to send spam.
7. **Attachment filtering** Attachment filtering filters messages based on attachment file name, file name extension, or file MIME content type. You can configure attachment filtering to block a message and its attachment, to strip the attachment and allow the message to pass through, or to silently delete the message and its attachment.
8. **Microsoft Forefront Protection 2010 for Exchange Server** Forefront Protection 2010 for Exchange Server (FPE) is an antivirus software package that's tightly integrated with Exchange 2010 and offers antivirus protection for the Exchange environment. The antivirus protection that's provided by FPE is language independent. However, the setup, administration of the product, and end-user notifications are available in 11 server languages. For more information, see Microsoft Forefront Protection 2010 for Exchange Server.
9. **Outlook junk e-mail filtering** The Outlook junk e-mail filter uses state-of-the-art technology to evaluate whether a message should be treated as a junk e-mail message based on several factors, such as the time that the message was sent, the content and structure of the message, and the

metadata collected by the Exchange Server anti-spam filters. Messages caught by the filter are moved to a special Junk E-mail folder, where the recipient can access them later.

Return to top

Anti-Spam Stamps

Anti-spam stamps help you diagnose spam-related problems by applying diagnostic metadata, or stamps, such as sender-specific information, puzzle validation results, and content filtering results, to messages as they pass through the anti-spam features that filter inbound messages from the Internet. These stamps are visible to the end-user mail client and encode sender-specific information, the version of the spam filter definition file, Outlook puzzle validation results, and content filtering results.

Return to top

Microsoft Update for Anti-Spam Services

Exchange 2010 offers additional services to help keep anti-spam components up to date, taking advantage of the proven Microsoft Update infrastructure.

Microsoft Exchange 2010 Standard Anti-spam Filter Updates offer anti-spam updates every two weeks via Microsoft Update.

The Forefront Security for Exchange Server Anti-spam Update service is a premium service that updates the content filter daily via Microsoft Update. In addition, the premium service includes the spam signature and IP Reputation Service updates that are available on an as-needed basis, up to several times a day. Spam signature updates identify the most recent spam campaigns. IP Reputation Service updates provide sender reputation information about IP addresses that are known to send spam.

Note:

To use the premium service, you must have the Exchange Enterprise client access license (CAL).

Return to top

Using Exchange Hosted Services

Spam filtering is enhanced by or is also available as a service from Microsoft Exchange Hosted Services.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

Return to top

Strategy for Anti-Spam Approach

Your strategy for how to configure the anti-spam features and establish the aggressiveness of your anti-spam agent settings requires that you plan and calculate carefully. If you set all anti-spam filters to their most aggressive levels and configure all anti-spam features to reject all suspicious messages, you're more likely to reject messages that aren't spam. On the other hand, if you don't set the anti-spam filters at a sufficiently aggressive level and don't set the spam confidence level (SCL) threshold low enough, you probably won't see a reduction in the spam that enters your organization.

It's a best practice to reject a message when Exchange detects a bad message through the Connection Filter agent, Recipient Filter agent, or Sender Filter agent. This approach is better than quarantining such messages or assigning metadata, such as anti-spam stamps, to such messages. The Connection Filter agent and Recipient Filter agent automatically block messages that are identified by the respective filters. The Sender Filter agent is configurable.

This best practice is recommended because the SCL that underlies connection filtering, recipient filtering, or sender filtering is relatively high. For example, with sender filtering, where the administrator has configured specific senders to block, there's no reason to assign the sender filtering data to such messages and to continue to process them. In most organizations, blocked messages should be rejected. (If you didn't want the messages rejected, you wouldn't have put them on the Blocked Senders List.)

The same logic applies to real-time block list services and recipient filtering, although the underlying confidence isn't as high as the IP Block list. You should be aware that the further along the mail flow path a message travels, the greater the probability of false positives, because the anti-spam features are evaluating more variables. Therefore, you may find that if you configure the first several anti-spam features in the anti-spam chain more aggressively, you can reduce the bulk of your spam. As a result, you'll save processing, bandwidth, and disk resources so that you can process more ambiguous messages.

Ultimately, you must plan to monitor the overall effectiveness of the anti-spam features. If you monitor carefully, you can continue to adjust the anti-spam features to work well together for your environment. With this approach, you should plan on a fairly non-aggressive configuration of the anti-spam features when you start. This approach lets you minimize the number of false positives. As you monitor and adjust the anti-spam features, you can become more aggressive about the type of spam and spam attacks that your organization experiences.

Return to top

1.7.1.5.1 Understanding Anti-Spam and Antivirus Mail Flow

Understanding Anti-Spam and Antivirus Mail Flow

Transport > Understanding Transport > Understanding Anti-Spam and Antivirus Functionality >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-07*

When an external user sends e-mail messages to a server running Microsoft Exchange

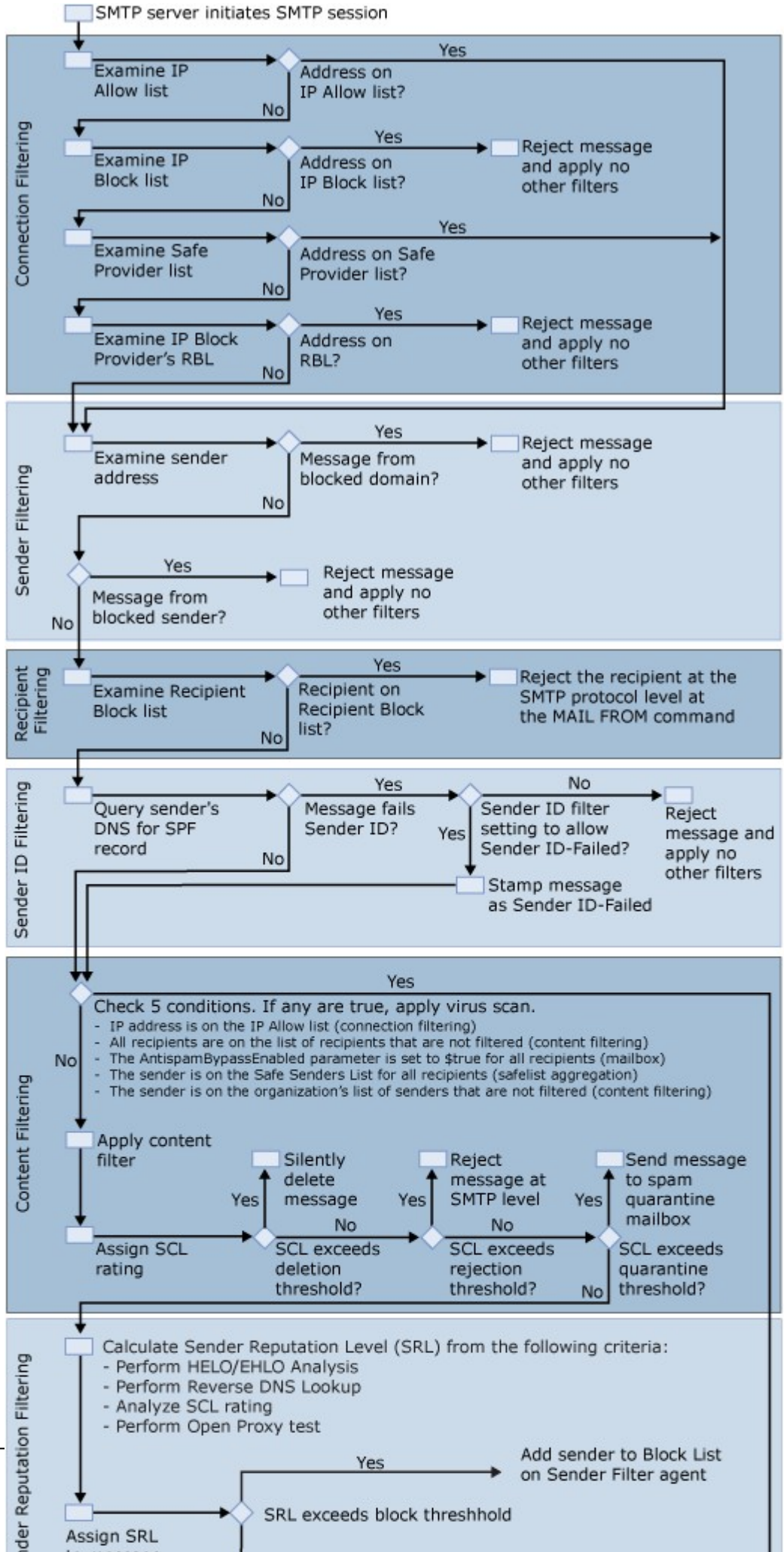
that runs the anti-spam features, the anti-spam features cumulatively evaluate characteristics of inbound messages and either filter out messages suspected to be spam or assign messages a rating based on the probability that the message is spam. This rating is stored with the message as a message property called the *spam confidence level (SCL) rating*. This rating is persisted with the message when the message is sent to other Exchange servers.

The following figure shows the order in which the default anti-spam features and Microsoft Forefront Protection for Exchange Server filter inbound messages from the Internet. By default, the anti-spam and antivirus features are arranged in this order with the filters that use the least resources filtering first, and then the filters that use the greatest resources filtering last.

Note:

The following figures and explanations assume that the Microsoft Exchange Server 2010 Edge Transport server is the first SMTP server to accept inbound messages. In some organizations, the Edge Transport server may be deployed behind a third-party SMTP server. When the Exchange 2010 Edge Transport server is deployed behind a third-party SMTP gateway server, the Exchange 2010 Edge Transport server requires additional configuration. Specifically, you must make sure that all SMTP gateway servers are listed in the **InternalSMTPServer** property of the **TransportConfig** object. For more information, see Set-TransportConfig.

For more information about additional Exchange anti-spam and antivirus features, see Microsoft Forefront Protection 2010 for Exchange Server.


SMTP server initiates SMTP session
Connection Filtering
Examine IP Allow list
Address on IP Allow list?
Yes
No
Examine IP Block list
Address on IP Block list?
Reject message and apply no other filters
Examine Safe Provider list
Address on Safe Provider list?
Examine IP Block Provider's RBL
Address on RBL?
Sender Filtering
Examine sender address
Message from blocked domain?
Message from blocked sender?
Recipient Filtering
Examine Recipient Block list
Recipient on Recipient Block list?
Reject the recipient at the SMTP protocol level at the MAIL FROM command
Sender ID Filtering
Query sender's DNS for SPF record
Message fails Sender ID?
Sender ID filter setting to allow Sender ID-Failed?
Reject message and apply no other filters
Stamp message as Sender ID-Failed
Content Filtering
Check 5 conditions. If any are true, apply virus scan.
- IP address is on the IP Allow list (connection filtering)
- All recipients are on the list of recipients that are not filtered (content filtering)
- The AntispamBypassEnabled parameter is set to $true for all recipients (mailbox)
- The sender is on the Safe Senders List for all recipients (safelist aggregation)
- The sender is on the organization's list of senders that are not filtered (content filtering)
Apply content filter
Assign SCL rating
Silently delete message
SCL exceeds deletion threshold?
Reject message at SMTP level
SCL exceeds rejection threshold?
Send message to spam quarantine mailbox
SCL exceeds quarantine threshold?
Sender Reputation Filtering
Calculate Sender Reputation Level (SRL) from the following criteria:
- Perform HELO/EHLO Analysis
- Perform Reverse DNS Lookup
- Analyze SCL rating
- Perform Open Proxy test
Assign SRL
SRL exceeds block threshhold
Add sender to Block List on Sender Filter agent

As shown in the preceding figure, when an SMTP server connects to Exchange 2010 and initiates an SMTP session, filters are applied in the following order when the Edge Transport server is Internet-facing:

- Connection filtering
- Sender filtering
- Recipient filtering
- Sender ID filtering
- Content filtering
- Sender reputation filtering
- Attachment filtering
- Antivirus scanning
- Outlook junk e-mail filtering

Note:

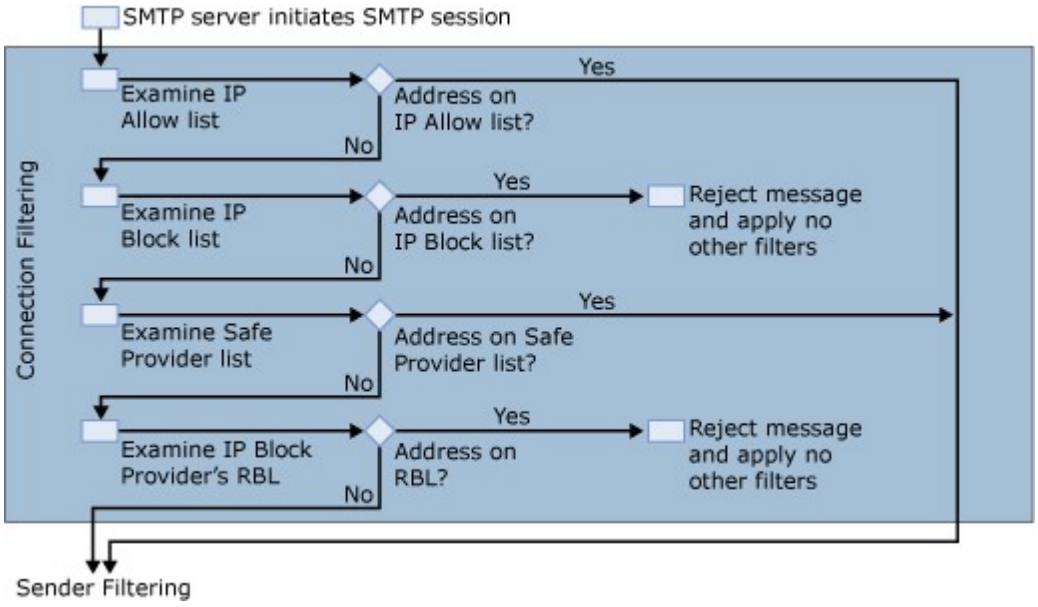
Connection filtering gathers information during two different events. In the first event, connection filtering gathers IP address information from the connection (shown in the preceding figure). In the second event, connection filtering gathers information when the Sender Filter agent parses the message headers to determine the first external IP address (shown in the figure in "Sender Filtering" later in this topic). Agents may monitor multiple events. The preceding figure shows a high-level view of the approximate order in which agents are applied, when all agents are enabled, for the purposes of illustrating message flow. For more information about specific events and which agents monitor which events, see Understanding Transport Agents.

Looking for management tasks related to anti-spam and antivirus functionality? See Managing Anti-Spam and Antivirus Features.

Contents

Connection Filtering

During the SMTP session, Exchange 2010 applies connection filtering by using the criteria shown in the following figure.



The following process applies:

1. The Connection Filter agent examines the administrator-defined IP Allow list. If the IP address of the sending server is on the administrator-defined IP Allow list, the message is then processed by sender filtering.
2. The Connection Filter agent examines the local IP Block list. If the IP address of the sending server is found on the local IP Block list, the message is automatically rejected, and no other filters are applied.
3. The Connection Filter agent examines the list of allowed IP addresses from any IP Allow List providers that you have. If the IP address of the sending server is on the list of allowed IP addresses from the IP Allow List providers, the message is then processed by sender filtering.
4. The Connection Filter agent examines the real-time block lists of any IP Block List providers that you've configured. If the sending server's IP address is found on a real-time block list, the message is rejected, and no other filters are applied.

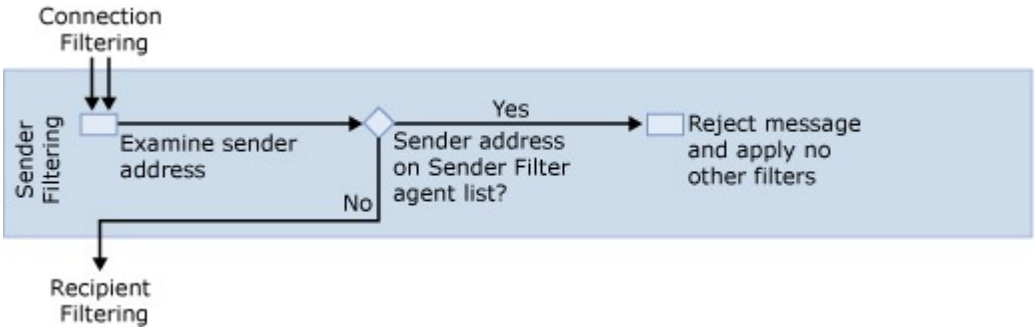
For more information, see Understanding Connection Filtering.

Note:
If the Connection Filter agent is deployed on a computer behind another server that faces the Internet, other filters, such as sender filtering and recipient filtering, are invoked before the Connection Filter agent.

Return to top

Sender Filtering

After connection filtering has been applied, Exchange 2010 examines the sender e-mail address against the list of blocked senders that you configure in sender filtering as shown in the following figure.



The Sender Filter agent then checks the sender's e-mail address contained in the From header fields in the message envelope and the message header. If either From header field matches the address in the Blocked Sender list, Exchange 2010 rejects the message at the protocol level, and no other filters are applied.

Note:
Even if recipients in your organization have put senders on their Microsoft Outlook Safe Senders List, sender filtering on the Edge Transport server will override the recipient's Outlook setting and reject the messages.

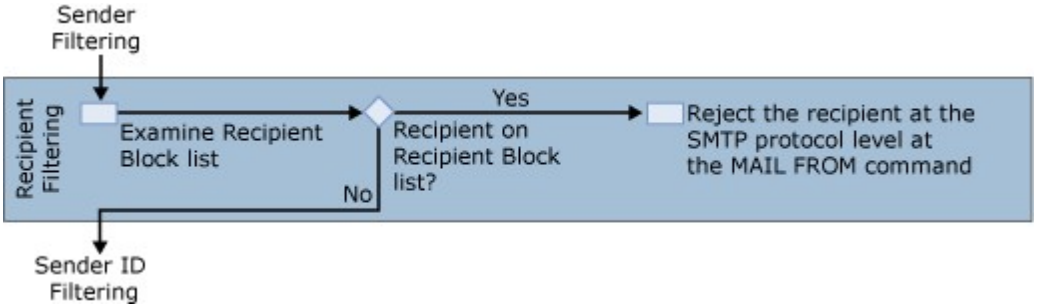
For more information about sender filtering, see Understanding Sender Filtering.

For more information about message envelopes and message headers, see Understanding the Pickup and Replay Directories.

Return to top

Recipient Filtering

If sender filtering doesn't reject the message, Exchange runs connection filtering again. Exchange then applies the Recipient Filter agent as shown in the following figure.



The Recipient Filter agent examines the recipient against the Recipient Block list that you configure in the Recipient Filter agent settings. If the intended recipient matches an e-mail address on your Recipient Block list, Exchange 2010 rejects the message for that particular recipient. In addition, the Recipient Filter agent checks whether the recipient is present in the organization. If the recipient isn't present in the organization, Exchange rejects the message for that particular recipient.

If multiple recipients are listed on the message and all the recipients aren't on the Recipient Block list, the message will continue to process. Otherwise, if the message is bound for only a single blocked recipient, no other filters are applied.

When a message with blocked recipients is processed, the set of blocked recipients are removed from the message, and the message continues into the organization. Protocol-

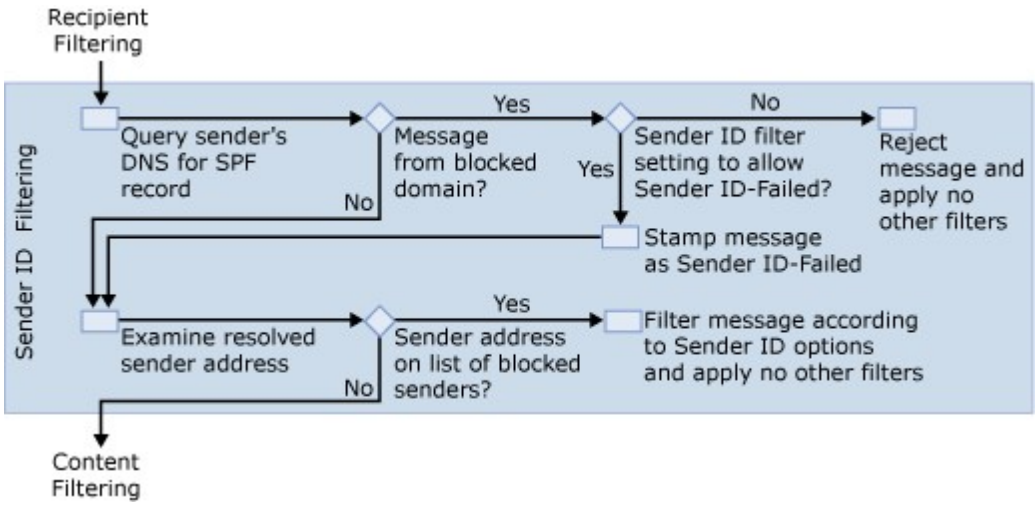
level SMTP rejection responses are sent to the sender for each blocked recipient. The Sender Reputation agent monitors the **OnReject** event to calculate sender reputation level (SRL).

For more information, see Understanding Recipient Filtering.

Return to top

Sender ID Filtering

If the message still contains valid recipients after recipient filtering has been applied, Exchange 2010 runs the Sender ID agent as shown in the following figure.



First, the Sender ID agent determines the Purported Responsible Address (PRA) of the message using the algorithm described in RFC 4407. This step is required to accurately identify the message sender. The PRA is an SMTP address, such as kim@contoso.com. The Sender ID agent then performs a Domain Name System (DNS) lookup against the domain part of the PRA. If that domain has published a sender policy framework (SPF) record, the agent uses the SPF record to evaluate the message according to the specification for RFC 4408. The result of the evaluation is stamped on the message in the anti-spam stamp. If that domain doesn't have a published SPF record, the Sender ID agent stamps a Sender ID result of "None" on the message. For more information about the types of stamps used for Sender ID filtering, see Understanding Anti-Spam Stamps.

If the sender's DNS is from a blocked domain or a blocked address, the following actions may be taken depending on your configuration of Sender ID actions:

- **Reject message** If the Sender ID action is set to **Reject Message**, Exchange rejects the message and sends an SMTP error response to the sending server. The SMTP error response is a 5*xx* level protocol response with text that corresponds to the Sender ID status.
- **Delete message** If the Sender ID action is set to **Delete Message**, Exchange deletes the message without informing the sending server of the deletion. The computer that has the Edge Transport server role installed sends a fake "OK" SMTP command to the sending server, and then deletes the message. Because the sending server assumes that the message was sent, the sending server won't retry sending the message in the same session.
- **Stamp message with Sender ID result and continue processing** Exchange stamps the message with the Sender ID result and continues processing the message. This metadata is evaluated by the Content Filter agent when an SCL is calculated. Additionally, sender reputation uses the message metadata

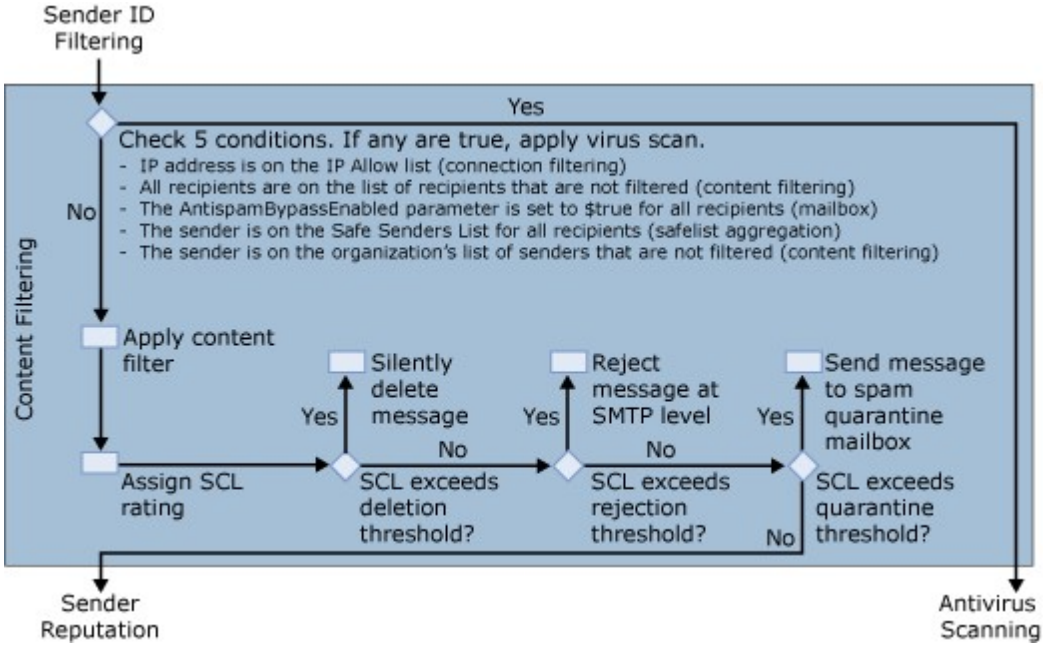
when it calculates an SRL for the sender of the message.

For more information, see Understanding Sender ID.

Return to top

Content Filtering

Before Exchange content filtering calls the Exchange Intelligent Message Filter, it applies sender filtering again. The Exchange server then applies the Content Filter agent as shown in the following figure.



The Content Filter agent checks the following conditions in the message. If any of the conditions are true, the message bypasses content filtering and attachment filtering. These messages then go to antivirus scanning for processing. The following conditions are checked:

- The sender's IP address is on the IP Allow list for connection filtering.
- All recipients are on the exceptions list for content filtering.
- The *AntiSpamBypassEnabled* parameter is set to `$True` on all the recipients' mailboxes.
- All the recipients have added this sender to their Outlook Safe Senders List, which is updated to the Edge Transport server by using safelist aggregation.
- The sender is a trusted partner and on the organization's list of senders that aren't filtered.

In addition to the conditions listed, if the SMTP session has been authenticated as a trusted partner, and if the administrator has granted the Bypass Anti-Spam (Ms-Exch-Bypass-Anti-Spam) permission to partners, the anti-spam agents will be disabled for messages during that session. The Bypass Anti-Spam permission isn't granted to partners by default and must be assigned by an administrator.

If a message doesn't meet any of the conditions described, content filtering is applied. Content filtering assigns an SCL rating to the message. Based on the SCL rating, one of the following actions occurs:

- If the SCL rating on the message is equal to or greater than the SCL delete

threshold, and the SCL delete threshold is enabled, the Content Filter agent deletes the message. There is no protocol-level communication that tells the sending system or sender that the message was deleted. If the SCL rating is lower than the SCL delete threshold value, the Content Filter agent doesn't delete the message. Instead, the Content Filter agent compares the SCL value to the SCL reject threshold.

- If the SCL rating on the message is equal to or greater than the SCL reject threshold, and the SCL reject threshold is enabled, the Content Filter agent rejects the message and sends a rejection response to the sending system. You can customize the rejection response. In some cases, a non-delivery report (NDR) is sent to the original sender of the message. If the SCL rating is lower than the SCL reject threshold value, the Content Filter agent doesn't reject the message. Instead, the Content Filter agent compares the SCL value to the SCL quarantine threshold.
- If the SCL rating on the message is equal to or greater than the SCL quarantine threshold, and the SCL quarantine threshold is enabled, the Content Filter agent sends the message to the spam quarantine mailbox. For more information about how to manage the spam quarantine mailbox, see Understanding Content Filtering. The message then continues to attachment filtering.

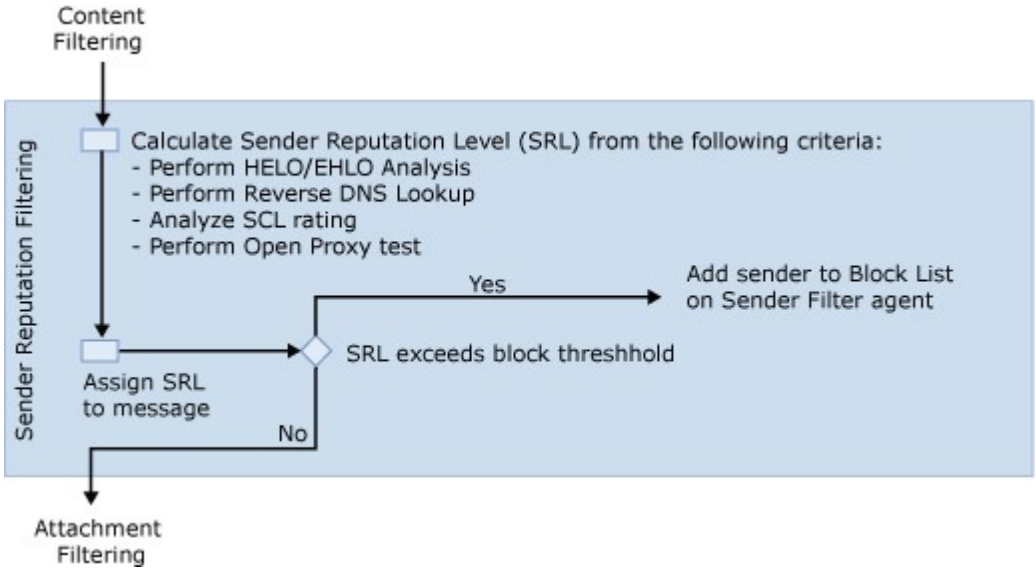
For more information, see the following topics:

- Configure Safelist Aggregation
- Understanding Content Filtering

Return to top

Sender Reputation Filtering

After content filtering has been applied, Exchange applies sender reputation filtering as shown in the following figure.



Sender reputation weighs each of the following message statistics and calculates an SRL for each sender:

- HELO/EHLO analysis
- Reverse DNS lookup
- Analysis of SCL ratings on messages from a specific sender
- Sender open proxy test

The SRL is a number from 0 through 9 that predicts the probability that a specific sender is a spammer or otherwise malicious user. A value of 0 indicates that the sender isn't likely to be a spammer; a value of 9 indicates that the sender is likely to be a spammer.

You can configure an SRL block threshold from 0 through 9 by which sender reputation issues a request to the Sender Filter agent to block the sender from sending a message into the organization. When a sender is blocked, the sender is added to the Blocked Senders list for a configurable period. How blocked messages are handled depends on the configuration of the Sender Filter agent. The following actions are the options for handling blocked messages:

- Reject
- Delete and archive
- Accept and mark as a blocked sender

If a sender is included in the IP Block list or Microsoft IP Reputation Service, the Sender Reputation agent issues an immediate request to the Sender Filter agent to block the sender. To take advantage of this functionality, you must enable and configure the Microsoft Exchange Anti-spam Update Service.

By default, the Edge Transport server sets a rating of 0 for senders that haven't been analyzed. After a sender has sent 20 or more messages, sender reputation calculates an SRL that's based on the statistics listed earlier.

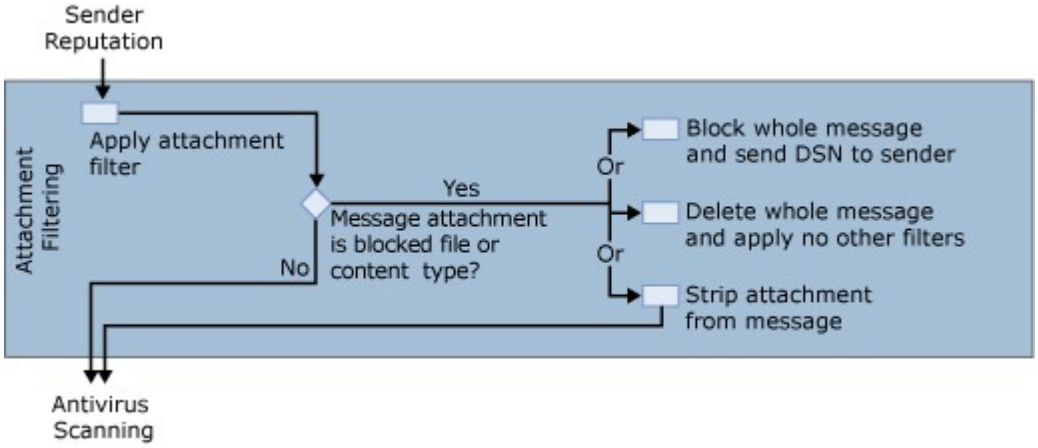
For more information, see the following topics:

- Understanding Sender Reputation
- Configure Sender Reputation Properties

Return to top

Attachment Filtering

After sender reputation filtering has been applied, Exchange applies attachment filtering as shown in the following figure.



You can configure attachment filtering to block attachments based on their MIME content type, file name, or file name extension. If attachment filtering detects a content type or file name that has been blocked, one of the following actions will occur based on your attachment filtering settings:

- **Reject** If the action setting is set to **Reject**, both the e-mail message and attachment are prevented from being delivered to the recipient and the system generates a delivery status notification (DSN) failure message to the

sender. You can customize your rejection response.

- **Silent Delete** If the action setting is set to **Silent Delete**, both the e-mail message and attachment are prevented from being delivered to the recipient. A notification that the e-mail message and attachment were blocked isn't returned to the sender.
- **Strip** If the action setting is set to **Strip**, the attachment is stripped from the e-mail message. This value allows the message and other attachments that don't match an entry on the attachment block list to be delivered to the recipient. A notification that the attachment was blocked is added to the recipient's e-mail message.

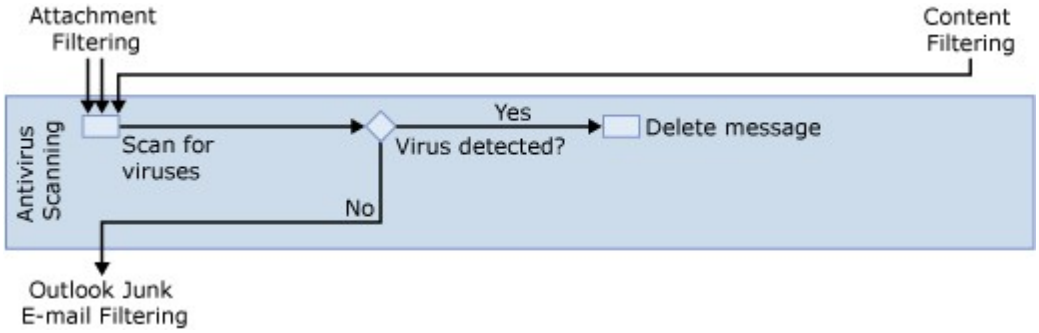
If the message wasn't rejected or deleted, or attachment filtering didn't detect blocked attachment types, the message is then scanned for viruses.

For more information, see Configure Attachment Filtering.

Return to top

Antivirus Scanning

After attachment filtering has been applied, or if the recipients were bypassed in content filtering, Forefront Protection for Exchange Server antivirus scanning is applied as shown in the following figure.



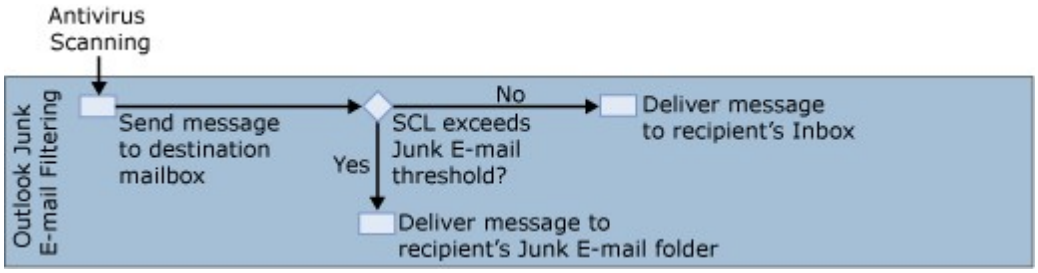
Forefront Protection for Exchange Server is an antivirus software package that's tightly integrated with Exchange 2010 and offers additional antivirus protection for your Exchange environment. When Forefront Protection for Exchange Server detects messages that seem to contain a virus, the system deletes the message, generates a notification message, and sends the notification to the recipient’s mailbox.

For more information, see Microsoft Forefront Protection 2010 for Exchange Server.

Return to top

Outlook Junk E-Mail Filtering

After all the filters are applied and the message has been scanned for viruses, the message is sent to the intended recipient's mailbox and junk e-mail filtering is applied as shown in the following figure.



If the SCL rating for the message is equal to or greater than the SCL Junk E-mail folder threshold, and the SCL Junk E-mail folder threshold is enabled, the Mailbox server puts the message in the Outlook user's Junk E-mail folder. If the SCL value for a message is lower than the values for the SCL delete, reject, quarantine, and Junk E-mail folder thresholds, the Mailbox server puts the message in the user's Inbox. For more information about the SCL thresholds, see Understanding Spam Confidence Level Threshold.

Return to top

1.7.1.5.2 Understanding Anti-Spam Stamps

Understanding Anti-Spam Stamps

Transport > Understanding Transport > Understanding Anti-Spam and Antivirus Functionality >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-28*

In Microsoft Exchange Server 2010, anti-spam stamps help you diagnose spam-related problems by applying diagnostic metadata, or stamps, such as sender-specific information, puzzle validation results, and content filtering results, to messages as they pass through the anti-spam features that filter inbound messages from the Internet. There are three anti-spam stamps: the phishing confidence level stamp, the spam confidence level stamp, and the Sender ID stamp.

This topic explains how to view anti-spam stamps and describes the contents of the anti-spam report.

You can use anti-spam stamps as diagnostic tools to determine what actions to take on false-positives and on suspected spam messages that individuals receive in their mailboxes.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Viewing Anti-Spam Stamps

You can view anti-spam stamps by using Microsoft Office Outlook 2007. For more information about how to view anti-spam stamps, see View Anti-Spam Stamps in Outlook 2010 and Outlook 2007.

Understanding the Anti-Spam Report

The anti-spam report is a summary report of the anti-spam filter results that have been applied to an e-mail message. The Content Filter agent applies this stamp to the message

envelope in the form of an X-header as follows.

```
X-MS-Exchange-Organization-Antispam-Report: DV:<DATVersion>;CW:CustomList;PCL:Phi
```

The following table describes the filter information that can appear in an anti-spam report.

Note:
The anti-spam report only displays information from the filters that were applied to the specific message. An anti-spam report doesn't usually contain all the information listed in the following table. For example, you may receive the following anti-spam report: `DV:3.1.3924.1409;SID:SenderIDStatus Fail;PCL:PhishingLevel SUSPICIOUS;CW:CustomList;PP:Presolved;TIME:TimeBasedFeatures`.

Filter information in an anti-spam report

Stamp	Description
SID	The Sender ID (SID) stamp is based on the sender policy framework (SPF) that authorizes the use of domains in e-mail. The SPF is displayed in the message envelope as `Received-SPF`. The Sender ID evaluation process generates a Sender ID status for the message. This status can be returned as one of the following values: • **Pass** Both the IP address and Purported Responsible Address (PRA) passed the Sender ID verification check. • **Neutral** Published Sender ID data is explicitly inconclusive. • **Soft fail** The IP address for the PRA may be in the not permitted set. • **Fail** The IP Address is not permitted; no PRA is found in the incoming mail or the sending domain does not exist. • **None** No published SPF data exists in the sender's DNS. • **TempError** A temporary DNS failure occurred, such as an unavailable DNS server. • **PermError** The DNS record is invalid, such as an error in the record format. The Sender ID stamp is displayed as an X-Header in the message envelope as follows: `X-MS-Exchange-Organization-SenderIdResult:<status>` For more information about Sender ID, see Understanding Sender ID.
DV	The DAT version (DV) stamp indicates the version of the spam definition file that was used when scanning the message.
SA	The signature action (SA) stamp indicates that the message was either recovered or deleted because of a signature that was found in the message.
SV	The signature DAT version (SV) stamp indicates the version of the signature file that was used when scanning the message.
PCL	The phishing confidence level (PCL) stamp displays the rating of the message based on its content and is applied when the message is processed by the Content Filter agent. This status can be returned as one of the following values: • **Neutral** The message's content isn't likely to be phishing. • **Suspicious** The message's content is likely to be phishing. The PCL value can range from 1 through 8. A PCL rating from 1 through 3 returns a status of `Neutral`. This means that the message's content

	isn't likely to be phishing. A PCL rating from 4 through 8 returns a status of `Suspicious`. This means that the message is likely to be phishing. The values are used to determine what action Outlook takes on messages. Outlook uses the PCL stamp to block the content of suspicious messages. The PCL stamp is displayed as an X-header in the message envelope as follows: `X-MS-Exchange-Organization-PCL:<status>`
SCL	The spam confidence level (SCL) stamp of the message displays the rating of the message based on its content. The Content Filter agent uses Microsoft SmartScreen technology to assess the contents of a message and to assign an SCL rating to each message. The SCL value is from 0 through 9, where 0 is considered less likely to be spam, and 9 is considered more likely to be spam. The actions that Exchange and Outlook take depend on your SCL threshold settings. The SCL stamp is displayed as an X-header in the message envelope as follows: `X-MS-Exchange-Organization-SCL:<status>` For more information about SCL thresholds and actions, see Understanding Spam Confidence Level Threshold.
CW	The custom weight (CW) stamp of a message indicates that the message contains an unapproved word or phrase and that the SCL value, or weight, of that unapproved word or phrase was applied to the final SCL score: • Unapproved phrases, or Block phrases, have maximum weight and change the SCL score to 9. • Approved words or phrases, or Allow phrases, have minimum weight and change the SCL score to 0. For more information about how to add approved and unapproved words or phrases to the Content Filtering agent, see Configure Content Filtering Properties.
PP	The presolved puzzle (PP) stamp indicates that if a sender's message contains a valid, solved computational postmark, based on Outlook E-mail Postmark validation functionality, it's unlikely that the sender is a malicious sender. In this case, the Content Filter agent would reduce the SCL rating. The Content Filter agent doesn't change the SCL rating if the E-mail Postmark validation feature is enabled and either of the following conditions is true: • An inbound message doesn't contain a computational postmark header. • The computational postmark header isn't valid. For more information about the postmark validation feature, see Configure Content Filtering Properties.

TIME:TimeBasedFeatures	The TIME stamp indicates that there was a significant time delay between the time that the message was sent and the time that the message was received. The TIME stamp is used to determine the final SCL rating for the message.
MIME:MIMECompliance	The MIME stamp indicates that the e-mail message isn't MIME compliant.
P100:PhishingBlock	The P100 stamp indicates that the message contains a URL that's present in a phishing definition file.
IPOnAllowList	The IPOnAllowList stamp indicates that the sender's IP address is on the IP Allow list. For more information about the IP Allow list, see Understanding Connection Filtering.
MessageSecurityAntispamBypass	The MessageSecurityAntispamBypass stamp indicates that the message wasn't filtered for content and that the sender has been granted permission to bypass the anti-spam filters.
SenderBypassed	The SenderBypassed stamp indicates that the Content Filter agent doesn't process any content filtering for messages that are received from this sender. For more information, see Configure Content Filtering Properties.
AllRecipientsBypassed	The AllRecipientsBypassed stamp indicates that one of the following conditions was met for all recipients listed in the message: • The *AntispamBypassedEnabled* parameter on the recipient's mailbox is set to `$true`. This is a per-recipient setting that can only be set by an administrator. For more information about this setting, see Set-Mailbox. • The message sender is in the recipient's Outlook Safe Senders List. For more information about the Safe Senders List, see Configure Safelist Aggregation. • The Content Filter agent doesn't process any content filtering for messages that are sent to this recipient. For more information about recipient exceptions, see Configure Content Filtering Properties.

1.7.1.5.3 Understanding Anti-Spam Updates

Understanding Anti-Spam Updates

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-06*

Microsoft Exchange Server 2010 includes many anti-spam features that depend on downloaded data to determine whether a message can be delivered with confidence that it isn't spam. The following data must be kept up-to-date for the anti-spam features to operate optimally:

- **Content filter updates** These updates contain data about phishing Web sites, Microsoft SmartScreen spam heuristics, and other Intelligent Message Filter updates. Content filter updates generally contain about 6 MB of data that's useful for longer periods of time than other anti-spam update data.
- **Microsoft IP Reputation Service data** The Microsoft IP Reputation Service is an IP Block list service offered exclusively to Exchange 2010 customers. Administrators can decide to implement and use the Microsoft IP Reputation

Service in addition to other real-time block list services.

- **Spam signature data** Spam signatures identify the latest spam campaigns. The spam is hashed into a message digest, or *spam signature*. This data is used by content filtering to assign a higher spam confidence level (SCL) to known spam. The spam signature files are small. A collection of spam signatures is only a few KB. The spam signatures are also time sensitive. Therefore, they're updated more frequently than other anti-spam data sets.

Anti-spam updates contain data only. They don't contain updated binaries or libraries. Anti-spam updates don't require mail flow interruption or service restarts.

Updates with Microsoft Update

By default, anti-spam updates aren't automatic. Instead, the administrator must visit Microsoft Update to download and install the content filter updates. The content filter update data is updated and available for download every two weeks.

Manual updates from Microsoft Update don't include the Microsoft IP Reputation Service or spam signature data. The Microsoft IP Reputation Service and spam signature data is only available when you use the anti-spam features of Microsoft Forefront Protection 2010 for Exchange Server (FPE).

Updates with Forefront Protection 2010 for Exchange Server

Microsoft Forefront Protection 2010 for Exchange Server (FPE) integrates multiple scan engines into a comprehensive, layered solution that helps you protect your Microsoft Exchange server messaging environment from malware, spam, and inappropriate content. FPE prevents the spread of malicious content by scanning all messages in real time with minimal impact on Exchange server performance or message delivery time.

You can enable FPE anti-spam technology in both the Exchange Edge Transport and Exchange Hub Transport roles. However, the Edge Transport role is the preferred location for anti-spam filtering. The technology includes a series of agents that are registered with Exchange and are invoked at specific points in the SMTP pipeline. FPE can also be integrated with Forefront Online Protection for Exchange (FOPE) to provide an additional layer of filtering for your messaging environment.

When you deploy FPE, the anti-spam features that are built in to Exchange are disabled. To learn more about how the FPE anti-spam solution works, see Using Antispam Filtering.

To learn more about how anti-spam updates work when you're using FPE, see Configuring and scheduling updates.

1.7.1.5.4 Understanding Attachment Filtering

Understanding Attachment Filtering

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

In Microsoft Exchange Server 2010, you can use attachment filtering to apply filters at the server level to control the attachments that users receive. Attachment filtering is

increasingly important in today's environment, where many attachments contain harmful viruses or inappropriate material that may cause significant damage to the user's computer or to the organization as a whole by damaging important documentation or releasing sensitive information to the public.

Note:

As a best practice, don't remove attachments from digitally signed, encrypted, or rights-protected e-mail messages. If you remove attachments from such messages, you invalidate the digitally signed messages and make encrypted and rights-protected messages unreadable.

Looking for management tasks related to anti-spam and antivirus functionality? See Managing Anti-Spam and Antivirus Features.

Types of Attachment Filtering in Exchange 2010

You can use the following types of attachment filtering to control attachments that enter or leave your organization:

- **Filtering based on file name or file name extension** You can filter attachments by specifying the exact file name or file name extension to be filtered. An example of an exact file name filter is BadFilename.exe. An example of a file name extension filter is *.exe.
- **Filtering based on file MIME content type** You can also filter attachments by specifying the MIME content type to be filtered. MIME content types indicate what the attachment is, whether it is a JPEG image, an executable file, a Microsoft Office Excel file, or some other file type. E-mail attachments are encoded in e-mail messages as ASCII text. E-mail servers and clients use the information about MIME content type to decode the ASCII text information in an e-mail message and convert it into a usable binary file familiar to the user. Content types are expressed as `type/subtype`. For example, the JPEG image content type is expressed as `image/jpeg`.
  To view a complete list of all file name extensions and content types that attachment filtering can filter on, run the following command.

```
Get-AttachmentFilterEntry | FL
```

If an attachment matches one of these filtering criteria, you can configure one of the following actions to be performed on the attachment:

- **Block whole message and attachment** An attachment that matches an attachment filter together with its whole e-mail message can be blocked from entering the messaging system. If an attachment and e-mail message are blocked, the sender receives a delivery status notification (DSN) message that states that the message contains an unacceptable attachment file name.
- **Strip attachment but allow message through** An attachment that matches an attachment filter can be removed whereas the e-mail message and any other attachments that don't match the filter are allowed through. If an attachment is stripped, it's replaced with a text file that explains why the attachment was removed. This action is the default setting.
- **Silently delete message and attachment** An attachment that matches an attachment filter together with its whole e-mail message can be blocked from entering the messaging system. If an attachment and e-mail message are blocked, neither the sender nor the recipient receives notification.

Caution:

You can't retrieve e-mail messages and attachments that are blocked or

attachments that are stripped. When you configure attachment filters, make sure that you carefully examine all possible file name matches and verify that legitimate attachments won't be affected by the filter.

- **RejectResponse** This parameter specifies the string response included in the non-delivery report (NDR) message if an e-mail message that has a filtered e-mail attachment is returned to the sender.

For more information, see Configure Attachment Filtering.

File Filtering by Using Forefront Protection for Exchange Server

The file filtering functionality provided by Microsoft Forefront Protection 2010 for Exchange Server includes advanced features that are unavailable in the default Attachment Filter agent included with Exchange 2010 Standard Edition.

For example, container files, which are files that contain other files, can be scanned for offending file types. Forefront Protection for Exchange Server filtering can scan the following container files and act upon embedded files:

- PKZip (.zip)
- GNU Zip (.gzip)
- Self-extracting compressed file archives (.zip)
- Compressed files (.zip)
- Java archive (.jar)
- TNEF (winmail.dat)
- Structured storage (.doc, .xls, .ppt, and others)
- MIME (.eml)
- SMIME (.eml)
- UUEncode (.uue)
- UNIX tape archive (.tar)
- RAR archive (.rar)
- MACBinary (.bin)

Note:

The default Attachment Filter agent included with Exchange 2010 Standard Edition detects file types even if they have been renamed. Attachment filtering also makes sure that compressed files with a .zip or .lzh file name extension don't contain blocked attachments by performing a file name extension match against the files in the compressed files. Forefront Protection for Exchange Server file filtering has the additional capability of determining if a blocked attachment has been renamed within a container file.

You can also filter files by file size. Additionally, you can configure Forefront Security for Exchange Server to quarantine filtered files or to send e-mail notifications based on file filter matches.

For more information, see Microsoft Forefront Protection 2010 for Exchange Server.

Understanding Connection Filtering

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-22*

The Connection Filter agent is an anti-spam agent enabled on computers running Microsoft Exchange Server 2010 that have the Edge Transport server role installed. The Connection Filter agent relies on the IP address of the remote server that's trying to connect, to determine what action, if any, to take on an inbound message. The remote IP address is available to the Connection Filter agent as a by-product of the underlying TCP/IP connection required for the SMTP session. Because the Connection Filter agent must evaluate the IP address of the remote server that's sending the message to be effective, the Connection Filter agent is typically enabled on the Internet-facing Edge Transport server. However, you may also perform additional configuration to run the Connection Filter agent deeper in the inbound message path.

When you configure anti-spam agents on an Edge Transport server, the agents act on messages cumulatively to reduce the number of unsolicited messages that enter the organization. To reduce redundancy and improve overall system performance and efficiency, you must understand the order in which the agents evaluate inbound messages. Understanding the order in which the filters evaluate inbound messages will help you optimize your configuration of the Edge Transport servers. For more information about how to plan and deploy the anti-spam agents, see Understanding Anti-Spam and Antivirus Functionality.

When you enable the Connection Filter agent, the Connection Filter agent is the first anti-spam agent to run when an inbound message is evaluated.

When an inbound message is submitted to an Edge Transport server on which the Connection Filter agent is enabled, the source IP address of the SMTP connection is checked against IP Allow lists and IP Block lists. If the source IP address is listed on an IP Allow list, the message is sent to the destination without additional processing by other anti-spam agents. If the source IP address is listed on an IP Block list, the SMTP connection is dropped after all RCPT TO headers in the message are processed.

Note:

The timing of when a specific connection is dropped may depend on other anti-spam configurations. For example, you can specify which recipients always receive e-mail messages, even if the source IP address is blocked. Additionally, you may have configured other agents that rely on content from the DATA command to be parsed. The Connection Filter agent always drops blocked connections according to the overall anti-spam configuration.

If the source IP address isn't listed on any IP Allow list or IP Block list, the message continues to flow through other anti-spam agents if other anti-spam agents are configured.

Looking for management tasks related to anti-spam and antivirus functionality? See Managing Anti-Spam and Antivirus Features.

Contents

Testing IP Block List and IP Allow List Functionality

IP Allow Lists and IP Block Lists

The Connection Filter agent compares the IP address of the server sending a message to any of the following data stores of IP addresses:

- Administrator-defined IP Allow lists and IP Block lists
- IP Block List providers
- IP Allow List providers

For more information about IP Block List providers, see "IP Block List Providers" later in this topic.

You must configure at least one of these data stores of IP addresses for the Connection Filter agent to be operational. If the data stores of IP addresses don't contain the IP addresses on the IP Allow lists or IP Block lists, or if you don't have any IP Block List providers or IP Allow List providers configured, you should disable the Connection Filter agent.

Administrator-Defined IP Allow Lists and IP Block Lists

Administrators of Edge Transport servers maintain administrator-defined lists of IP addresses. You can enter and delete the IP addresses that you want to allow or block by using the Exchange Management Console (EMC) or the Exchange Management Shell. You can add IP addresses individually, by IP address range, or by IP address and subnet mask.

When you add an IP address or IP address range, you must specify the IP address or IP address range as an IP Block list address or an IP Allow list address. Additionally, you can specify an expiration time for each IP Block list entry that you create. When you set the expiration time, the expiration time specifies how long the IP Block list entry is active. When the expiration time duration is reached, the IP Block list entry is disabled.

By using administrator-defined IP Allow lists and IP Block lists, you can configure connection filtering to support the following scenarios:

- To exempt IP addresses from the IP Block lists of IP Block List providers
  You may have to exempt IP addresses from the IP Block lists of IP Block List providers when legitimate senders are unintentionally put on an IP Block List provider's IP Block list. For example, legitimate senders could be unintentionally put on an IP Block list when an SMTP server was unintentionally configured to act as an open relay. In this scenario, the sender will probably try to correct the misconfiguration and remove the IP address from the IP Block List provider's IP Block list.
  For more information about IP Block List providers, see "IP Block List Providers" later in this topic.
- To deny access from IP addresses that are a source of unsolicited e-mail messages but aren't found on an IP Block List provider's IP Block lists
  Sometimes, you may receive a large quantity of unsolicited messages from a source that wasn't yet identified by a *real-time block list* service to which you subscribe.

IP Block List Providers

IP Block List provider services can help you reduce the number of unsolicited e-mail messages that enter your organization.

Note:

IP Block List provider services are frequently referred to as real-time block list services or

RBL services. The EMC refers to real-time block list services as IP Block List provider services. The terms real-time block list services, RBL services, and IP Block List provider services are equivalent.

IP Block List provider services compile lists of IP addresses from which spam has originated in the past. Additionally, some IP Block List providers provide lists of IP addresses for which SMTP is configured for open relay. There are also IP Block List provider services that provide lists of IP addresses that support dial-up access. Internet service providers (ISPs) that provide dial-up access services to their clients assign dynamic IP addresses for each dial-up session. Some ISPs block SMTP traffic from dial-up accounts. These ISPs and the attendant dial-up IP ranges aren't typically added to IP Block lists. However, some ISPs allow clients to send SMTP traffic from dial-up accounts. Malicious users take advantage of ISPs that allow SMTP traffic to send spam on dynamically assigned IP addresses. When the IP address is put on an IP Block list, the malicious users start another dial-up session and receive a new IP address. Frequently, a single IP Block List provider can provide a list of IP addresses that covers all these spam threats.

You can configure multiple IP Block List provider configurations by using the EMC or the Shell. Each service requires a separate IP Block List provider configuration in the EMC or the Shell.

When you configure the Connection Filter agent to use an IP Block List provider, the Connection Filter agent queries the IP Block List provider service to determine whether a match exists with the connecting IP addresses before the message is accepted into the organization.

Before the Connection Filter agent contacts the IP Block List provider to verify an IP address, the IP address is first compared to the administrator-defined IP Allow list and IP Block list. If the IP address doesn't exist on either the administrator-defined IP Allow list or IP Block list, the Connection Filter agent queries the IP Block List provider services according to the priority rating assigned to each provider. If the IP address appears on the IP Block list of an IP Block List provider, the Edge Transport server waits for and parses the RCPT TO header, responds to the sending system with an SMTP 550 error, and closes the connection. If the IP address doesn't appear on the IP Block lists of any one of the IP Block List providers, the next agent in the anti-spam chain processes the connection. For more information about the order in which the default anti-spam and antivirus agents filter inbound messages from the Internet, see Understanding Anti-Spam and Antivirus Functionality.

When you use the Connection Filter agent, it's a best practice to use one or more IP Block List providers to manage access into your organization. The use of an administrator-defined block list to maintain your own IP Block list is time-consuming and may be impossible from a human resource perspective in most organizations. Therefore, we recommend the use of an external IP Block List provider service, whose sole purpose is to maintain IP Block lists.

However, there may be some disadvantages to using an IP Block List provider. Because the Connection Filter agent must query an external entity for each unknown IP address, outages or delays at the IP Block List provider service can cause delays in the processing of messages on the Edge Transport server. In extreme cases, such outages or delays could cause a mail-flow bottleneck on the Edge Transport server.

The other disadvantage of using an external IP Block List provider service is that legitimate senders are sometimes added to the IP Block lists of IP Block List providers by mistake. For example, legitimate senders can be added to the IP Block lists maintained by IP Block List providers as the result of an SMTP misconfiguration, where the SMTP server was unintentionally configured to act as an open relay.

For each IP Block List provider service that you configure, you can customize the SMTP 550

error returned to the sender when the sender IP address is matched to an IP Block List provider service and is subsequently blocked by the Connection Filter agent. It's a best practice to customize the SMTP 550 error to identify the IP Block List provider service that identifies the sender as a blocked IP address. This best practice enables legitimate senders to contact the IP Block List provider service so that they can be removed from the IP Block List provider service's IP Block list.

Different IP Block List provider services may return different codes when the IP address of a remote server sending a message matches an IP address on an IP Block List provider service's IP Block list. Most IP Block List provider services return one of the following data types: bitmask or absolute value. Within these data types, there may be multiple values that indicate the type of list that the submitted IP address is on.

Bitmask Example

This section shows an example of the status codes returned by most Block List providers. For details about the status codes that the provider returns, see the documentation from the specific provider.

For bitmask data types, the IP Block List provider service returns a status code of 127.0.0.*x*, where the integer *x* is any one of the values listed in the following table.

Values and status codes for bitmask data types

Value	Status code
1	The IP address is on an IP Block list.
2	The SMTP server is configured to act as an open relay.
4	The IP address supports a dial-up IP address.

For absolute value types, the IP Block List provider service returns explicit responses based on the cause of the block of the IP address. The following table shows some examples of absolute values and the explicit responses.

Values and status codes for absolute value data types

Value	Explicit response
127.0.0.2	The IP address is a direct spam source.
127.0.0.4	The IP address is a bulk mailer.
127.0.0.5	The remote server sending the message is known to support multistage open relays.

IP Allow List Providers

You can also manage inbound messages by using IP Allow List provider services that provide IP Allow lists. IP Allow lists are sometimes referred to as IP safe lists or white lists elsewhere in the software industry. IP Allow List providers maintain lists of IP addresses that are definitively known not to be associated with any spam activity. When an IP Allow List provider returns an IP Allow match, which indicates that the sender's IP address is more likely to be a reputable or safe sender, the Connection Filter agent relays the message to the next agent in the anti-spam chain.

Return to top

Configuring Connection Filtering for Edge Transport Servers That Aren't the First SMTP Entry Point

In some organizations, the Edge Transport server role is installed on computers that don't process SMTP requests directly on the Internet. In this scenario, the Edge Transport server is behind another front-end SMTP server that processes inbound messages directly from the Internet. In this scenario, the Connection Filter agent must be able to extract the correct originating IP address from the message. To extract and evaluate the originating IP address, the Connection Filter agent must parse the Received headers from the message and compare those headers to the known SMTP server in the perimeter network.

When an RFC-compliant SMTP server receives a message, the server updates the message's Received header with the domain name and IP address of the sender. Therefore, for each SMTP server between the originating sender and the Edge Transport server, the SMTP server adds an additional Received header entry.

When you configure your perimeter network to support Exchange 2010, you must specify all the IP addresses for the SMTP servers in your perimeter network. The IP address data is replicated to Edge Transport servers by EdgeSync. When messages are received by the computer that runs the Connection Filter agent, the IP address in the Received header that doesn't match an SMTP server IP address in your perimeter network is assumed to be the originating IP address.

You must specify all internal SMTP servers on the transport configuration object in the Active Directory forest before you run connection filtering. Specify the internal SMTP servers by using the *InternalSMTPServers* parameter on the Set-TransportConfig cmdlet.

Return to top

Testing IP Block List and IP Allow List Functionality

After you configure an IP Block List provider service or IP Allow List provider service, you can test to make sure that connection filtering is configured correctly for the particular service. Most IP Block List provider services or IP Allow List provider services provide test IP addresses that you can use to test their services. When you run a test against an IP Block List provider service or an IP Allow List provider service, the Connection Filter agent issues a Domain Name System (DNS) query based on the real-time block list IP address that should respond with a specific response. For more information about how to test IP addresses against an IP Block List provider service or an IP Allow List provider service, see Test-IPAllowListProvider and Test-IPBlockListProvider.

Return to top

1.7.1.5.6 Understanding Content Filtering

Understanding Content Filtering

Transport > Understanding Transport > Understanding Anti-Spam and Antivirus Functionality >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

The Content Filter agent evaluates inbound e-mail messages and assesses the probability that an inbound message is legitimate or spam. Unlike many other filtering technologies, the Content Filter agent uses characteristics from a statistically significant sample of e-mail messages. The inclusion of legitimate messages in this sample reduces the chance of mistakes. Because the Content Filter agent recognizes characteristics of legitimate messages and spam, its accuracy is increased. Updates to the Content Filter agent are available periodically through Microsoft Update.

Contents

Using the Content Filter Agent

The Content Filter agent is one of several anti-spam agents. When you configure anti-spam agents on a computer that has the Edge Transport server role installed, the agents act on messages cumulatively to reduce the amount of spam that enters the organization. For more information about how to plan and deploy anti-spam agents, see Understanding Anti-Spam and Antivirus Functionality.

The Content Filter agent assigns a spam confidence level (SCL) rating to each message. The SCL rating is a number between 0 and 9. A higher SCL rating indicates that a message is more likely to be spam.

You can configure the Content Filter agent to take the following actions on messages according to their SCL rating:

- Delete message
- Reject message
- Quarantine message

For example, you may determine that messages that have an SCL rating of 7 or higher must be deleted, messages that have an SCL rating of 6 must be rejected, and messages that have an SCL rating of 5 must be quarantined.

You can adjust the SCL threshold behavior by assigning different SCL ratings to each of these actions. For more information about how to adjust the SCL threshold to suit your organization's requirements and about per-recipient SCL thresholds, see Understanding Spam Confidence Level Threshold.

Note:

Messages that are over 11 MB aren't scanned by the Intelligent Message Filter. Instead, they pass through the Content Filter without being scanned. However, the default maximum message size limit configured on Exchange 2010 Receive connectors is 10 MB. Therefore, the 11 MB threshold for the Intelligent Message Filter isn't a practical concern in the default Exchange configuration.

Allow Phrases and Block Phrases

You can customize how the Content Filter agent assigns SCL values by configuring custom words. Custom words are individual words or phrases that the Content Filter agent uses to apply appropriate filter processing. You configure approved words or phrases with Allow phrases and unapproved words or phrases with Block phrases. When the Content

Filter agent detects a preconfigured Allow phrase in an inbound message, the Content Filter agent automatically assigns an SCL value of 0 to the message. Alternatively, when the Content Filter agent detects a configured Block phrase in an inbound message, the Content Filter agent assigns an SCL rating of 9.

You can enter custom words or phrases in any combination of uppercase and lowercase letters. However, when the Content Filter agent evaluates message content, it ignores case. The maximum number of custom words or phrases that can be created is 800.

Outlook E-mail Postmark Validation

The Content Filter agent also includes Microsoft Office Outlook E-mail Postmark validation, a computational proof that Outlook applies to outgoing messages to help recipient messaging systems distinguish legitimate e-mail from junk e-mail. This feature helps reduce the chance of false positives. In the context of spam filtering, a *false positive* exists when a spam filter incorrectly identifies a message from a legitimate sender as spam. When Outlook E-mail Postmark validation is enabled, the Content Filter agent parses the inbound message for a computational postmark header. The presence of a valid, solved computational postmark header in the message indicates that the client computer that generated the message solved the computational postmark.

Computers don't require significant processing time to solve individual computational postmarks. However, processing postmarks for many messages may be prohibitive to a malicious sender. Anyone who sends millions of spam messages is unlikely to invest the processing power that is required to solve computational postmarks for all outbound spam. If a sender's e-mail contains a valid, solved computational postmark, it's unlikely that the sender is a malicious sender. In this case, the Content Filter agent would lower the SCL rating. If the postmark validation feature is enabled and an inbound message either doesn't contain a computational postmark header or the computational postmark header isn't valid, the Content Filter agent would not change the SCL rating.

Bypassing the Recipient, Sender, and Sender Domain

In some organizations, all e-mail to certain aliases must be accepted. This scenario can introduce problems if your organization is in an industry that manages significant volumes of spam.

For example, a company named Woodgrove Bank has an alias named customerloans@woodgrovebank.com that provides e-mail-based support to external loan customers. The Exchange administrators configure the Content Filter agent to set Block phrases that filter out words or phrases that are typically used in spam that is sent by unscrupulous loan agencies. To prevent potentially legitimate messages from being rejected, the administrators set exceptions to content filtering by entering a list of SMTP e-mail recipient addresses in the Content Filter agent configuration.

You can also specify senders and sender domains that you do not want the Content Filter agent to block.

Safelist Aggregation

In Exchange 2010, the Content Filter agent on the Edge Transport server uses the Outlook Safe Senders Lists, Blocked Sender List, Safe Recipients Lists, and trusted contacts from Outlook to optimize spam filtering. *Safelist aggregation* is a set of anti-spam functionality that is shared across Outlook and Exchange 2010. As its name suggests, this functionality collects data from the anti-spam safe lists that Outlook users configure and makes this data available to the anti-spam agents on the Edge Transport server. E-mail messages that Outlook users receive from contacts that those users have added to their Outlook Safe Recipients List, Safe Senders List, or trusted contacts list are identified by the Content Filter agent as safe. The Sender Filter agent also performs per-recipient sender filtering using the Blocked Senders list that users configure. For more information, see Understanding Safelist Aggregation.

Configuring the Content Filter Agent

You configure the Content Filter agent by using the Exchange Management Console or the Exchange Management Shell.

Important:

Configuration changes that you make to the Content Filter agent by using the Exchange Management Console or the Exchange Management Shell are only made to the local computer that has the Edge Transport server role installed. If you have multiple instances of the Edge Transport server role running in your organization, you must make Content Filter configuration changes to each computer.

For more information about how to configure content filtering, see Configure Content Filtering Properties.

Using SCL Value Stamped by the Content Filter Agent in Edge Transport Rules

In Exchange 2010, transport rules that run on Edge Transport servers are applied to messages by the Edge Rule agent on the `OnEndOfData` SMTP transport event. One of the transport rule conditions available on Edge Transport servers is the **with a spam confidence (SCL) rating that is greater than or equal to limit** transport rule condition. By using this transport rule condition, you can apply a transport rule action to a message based on the SCL value stamped on the message. The Content Filter agent stamps an SCL value on the message based on an analysis of the message content and is used to determine whether the message is spam. The Content Filter agent also runs on the `OnEndOfData` SMTP transport event.

Note:

Although the Content Filter agent also runs on other events, the SCL value is stamped on the message by the instance of the Content Filter agent registered on the `OnEndOfData` SMTP transport event.

Because both the Edge Rule agent and the Content Filter agent run on the `OnEndOfData` SMTP transport event, the priority value applied to each transport agent is used to determine which transport agent runs first. By default, the Edge Rule agent runs before the Content Filter agent to reduce the cost of processing messages that may be blocked by the Edge Rule agent. However, because the Edge Rule agent runs before the Content Filter agent and therefore the SCL value has not yet been stamped on the message, you can't use the **with a spam confidence (SCL) rating that is greater than or equal to limit** transport rule condition in the default configuration.

For details about how to configure the Content Filter agent to run before the Edge Rule agent on the `OnEndOfData` SMTP transport event, see Make the SCL Value Available to Edge Transport Rules. This enables the Content Filter agent to stamp an SCL value on a message that can then be read by the **with a spam confidence (SCL) rating that is greater than or equal to limit** transport rule condition.

For more information about transport agents and transport agent priority, see Understanding Transport Agents.

If you configure the Content Filter agent with a higher priority value than the Edge Rule agent, the Edge Transport server may incur additional processing costs because all the messages that are received by the Edge Transport server will be evaluated by the Content Filter agent. This is true even if the message is later rejected by a transport rule that is configured on the Edge Rule agent. Also, you will no longer be able to configure a

transport rule on the Edge Transport server to stamp a message that has an SCL value of –1. This value indicates to the Content Filter agent that the message should not be evaluated.

Forefront Protection 2010 for Exchange Server

Microsoft Forefront Protection 2010 for Exchange Server (FPE) integrates multiple scan engines into a comprehensive, layered solution that helps you protect your Microsoft Exchange server messaging environment from malware, spam, and inappropriate content. FPE prevents the spread of malicious content by scanning all messages in real time with minimal impact on Exchange server performance or message delivery time.

You can enable FPE anti-spam technology in both the Exchange Edge Transport and Exchange Hub Transport roles. However, the Edge Transport role is the preferred location for anti-spam filtering. The technology includes a series of agents that are registered with Exchange and are invoked at specific points in the SMTP pipeline. FPE can also be integrated with Forefront Online Protection for Exchange (FOPE) to provide an additional layer of filtering for your messaging environment.

When you deploy FPE, the anti-spam features that are built in to Exchange are disabled. To learn more about how the FPE anti-spam solution works, see Using Antispam Filtering.

1.7.1.5.7 Understanding Recipient Filtering

Understanding Recipient Filtering

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-30*

The Recipient Filter agent is an anti-spam agent enabled on computers running Microsoft Exchange Server 2010 that have the Edge Transport server role installed. The Recipient Filter agent relies on the RCPT TO SMTP header to determine what action, if any, to take on an inbound message.

When you configure anti-spam agents on an Edge Transport server, the agents act on messages cumulatively to reduce the number of unsolicited messages that enter the organization. For more information about how to plan and deploy anti-spam agents, see Understanding Anti-Spam and Antivirus Functionality.

The Recipient Filter agent blocks messages according to the characteristics of the intended recipient in the organization. The Recipient Filter agent can help you prevent the acceptance of messages in the following scenarios:

- **Nonexistent recipients** You can prevent delivery to recipients that aren't in the organization's address book. For example, you may want to stop delivery to frequently misused account names, such as administrator@contoso.com or support@contoso.com.
- **Restricted distribution lists** You can prevent delivery of Internet mail to distribution lists that should be used only by internal users.
- **Mailboxes that should never receive messages from the Internet** You can prevent delivery of Internet mail to a specific mailbox or alias that's typically used inside the organization, such as Helpdesk.

The Recipient Filter agent acts on recipients stored in one or both of the following data sources:

- **Recipient Block list** An administrator-defined list of recipients for which inbound messages from the Internet should never be accepted.
- **Recipient Lookup** Verification that the recipient is in the organization. Recipient Lookup requires access to Active Directory information provided by EdgeSync to Active Directory Lightweight Directory Services (AD LDS).

For more information about Recipient Block lists and Recipient Lookup functionality, see "Recipient Data Sources" later in this topic.

When you enable the Recipient Filter agent, one of the following actions is taken on inbound messages according to the characteristics of the recipients. These recipients are indicated by the RCPT TO header.

- If the inbound message contains a recipient that is on the Recipient Block list, the Edge Transport server sends a "550 5.1.1 User unknown" SMTP session error to the sending server.
- If the inbound message contains a recipient that doesn't match any recipients in Recipient Lookup, the Edge Transport server sends a "550 5.1.1 User unknown" SMTP session error to the sending server.
- If the recipient isn't on the Recipient Block list and the recipient is in Recipient Lookup, the Edge Transport server sends a "250 2.1.5 Recipient OK" SMTP response to the sending server, and the next anti-spam agent in the chain processes the message.

Looking for management tasks related to anti-spam and antivirus functionality? See Managing Anti-Spam and Antivirus Features.

Contents

Configuring AD LDS for Recipient Lookup

One of the most effective ways to reduce spam is to validate recipients before accepting inbound messages from the Internet. Therefore, it's a good idea to configure the AD LDS instance that runs on the Edge Transport server to synchronize with Active Directory. By default, AD LDS is installed and configured on the Edge Transport server. However, you must configure AD LDS to communicate with an Active Directory domain-joined global catalog server. Most of the time, you must also configure your firewall to enable specific ports to communicate with AD LDS. For more information, see Understanding Edge Subscriptions.

After you configure AD LDS to replicate a Recipient Block list from Active Directory, you must then enable blocking of messages sent to recipients who aren't present in the Exchange organization. You enable message blocking on the **Blocked Recipients** tab of the **Recipient Filtering Properties** page in the Exchange Management Console (EMC). You can also enable message blocking by using the Set-RecipientFilterConfig cmdlet in the Exchange Management Shell. For more information, see Set-RecipientFilterConfig.

Return to top

Recipient Data Sources

As mentioned earlier, the Recipient Filter agent references two data sources when it compares recipients on inbound messages: the Recipient Block list and Recipient Lookup.

Recipient Block List

The Recipient Block list is maintained by the Edge Transport server administrators. The Recipient Block list data is stored in the Edge Transport server instance of AD LDS. You must enter blocked recipients on each Edge Transport server computer.

You can enter the recipients that you want the Recipient Filter agent to block in the EMC on the **Blocked Recipients** tab of the **Recipient Filtering Properties** page. You use the **Set-RecipientFilterConfig** cmdlet in the Shell to enter recipients. For more information about how to configure the Recipient Filter agent, see Configure Recipient Filtering Properties.

Recipient Lookup

One benefit of the Recipient Filter agent is the ability to verify that the recipients on an inbound message are in your organization before Exchange 2010 transmits the message into your organization. The ability to verify recipients in your organization relies on a recipient data source available to the Edge Transport server. Because the Edge Transport server isn't an Active Directory domain-joined computer and could be segregated from the organization by a firewall, you must configure a Recipient Lookup data source for the Edge Transport server to use.

The Edge Transport server role uses AD LDS for configuration and data storage. For more information, see Understanding Edge Subscriptions.

Return to top

Tarpitting Functionality

Recipient Lookup functionality enables the sending server to determine whether an e-mail address is valid or invalid. As mentioned earlier, when the recipient of an inbound message is a known recipient, the Edge Transport server sends back a "250 2.1.5 Recipient OK" SMTP response to the sending server. This functionality provides an ideal environment for a directory harvest attack.

A *directory harvest attack* is an attempt to collect valid e-mail addresses from a particular organization so that the e-mail addresses can be added to a spam database. Because all spam income relies on trying to make people open e-mail messages, addresses known to be active are a commodity that malicious users, or *spammers*, pay for. Because the SMTP protocol provides feedback for known senders and unknown senders, a spammer can write an automated program that uses common names or dictionary terms to construct e-mail addresses to a specific domain. The program collects all e-mail addresses that return a "250 2.1.5 Recipient OK" SMTP response and discards all e-mail addresses that return a "550 5.1.1 User unknown" SMTP session error. The spammer can then sell the valid e-mail addresses or use them as recipients for unsolicited messages.

To combat directory harvest attacks, Exchange 2010 includes tarpitting functionality. *Tarpitting* is the practice of artificially delaying server responses for specific SMTP communication patterns that indicate high volumes of spam or other unwelcome messages. The intent of tarpitting is to slow down the communication process for such e-mail traffic so that the cost of sending spam increases for the person or organization sending the spam. Tarpitting makes directory harvest attacks too costly to automate

efficiently.

If tarpitting isn't configured, Exchange Server immediately returns a "550 5.1.1 User unknown" SMTP session error to the sender when a recipient isn't located in Recipient Lookup. Alternatively, if tarpitting is configured, SMTP waits a specified number of seconds before it returns the "550 5.1.1 User unknown" error. This pause in the SMTP session makes automating a directory harvest attack more difficult and less cost-effective for the spammer. By default, tarpitting is configured for 5 seconds on Receive connectors.

To configure the time before SMTP returns the "550 5.1.1 User unknown" error, use the EMC or the Shell to set the *TarpitInterval* value on the Receive connector. For more information about how to administer and configure Receive connectors, see Understanding Receive Connectors.

Return to top

Configuring the Tarpitting Interval

As explained in Understanding Recipient Filtering, you can configure the Receive connectors that process inbound messages from the Internet to slow down the SMTP response. Make sure that you enable tarpitting functionality on the Receive connectors, especially if you have enabled the Recipient Lookup feature of recipient filtering. If you don't enable tarpitting, and you have enabled the Recipient Lookup feature, you are exposing your organization to a directory harvest attack. A directory harvest attack will likely cause more spam.

When you specify a tarpitting interval time on a Receive connector, tarpitting is enabled. The default value is 5 seconds. We recommend that you start with a value of 5 (seconds). Use caution if you decide to change this value. An overly long interval could disrupt ordinary mail flow, whereas an overly brief interval may not be as effective in thwarting a directory harvest attack. If you change the tarpitting interval value, do so in small increments.

If you are running a version of Exchange Server earlier than Microsoft Exchange Server 2010 Service Pack 2 (SP2), you can set the tarpitting interval on the **Security** tab of the Receive connector property pages in the EMC, or you can use the Set-ReceiveConnector cmdlet in the Exchange Management Shell. For more information about how to use the EMC to configure the tarpitting interval, see Configure Receive Connector Properties.

If you are running Exchange Server 2010 SP2, or a later version, you set the tarpitting interval by using the Set-ReceiveConnector cmdlet in the Exchange Management Shell.

Return to top

Multiple Namespaces

Some organizations accept e-mail messages for multiple domains. For example, one organization may accept messages for both the Contoso.com and the Woodgrovebank.com domains. Sometimes organizations are authoritative for all the domains for which they accept messages. In the context of SMTP, the organization is authoritative for a domain if the organization hosts and manages the mailboxes for that domain. This relationship extends to the Edge Transport server. An Edge Transport server may accept messages for multiple domains, but it may not be authoritative for all the domains. For example, an Edge Transport server can be configured to be authoritative for all recipients in the Contoso.com domain, but the Edge Transport server still accepts and forwards messages for the Woodgrovebank.com domain.

When you enable the Recipient Filter agent, the Recipient Filter agent performs recipient lookups only for the domains specified as authoritative in the transport server

configuration. If an Edge Transport server accepts and forwards messages on behalf of another domain, but the Edge Transport server isn't configured as authoritative, the Recipient Filter agent doesn't perform a recipient lookup. However, if a recipient that's not authoritative is specified in the Recipient Block list, the recipient will still be blocked.

Return to top

1.7.1.5.8 Understanding Safelist Aggregation

Understanding Safelist Aggregation

Transport > Understanding Transport > Understanding Anti-Spam and Antivirus Functionality >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-29*

In Microsoft Exchange Server 2010, *safelist aggregation* refers to anti-spam functionality shared across Microsoft Outlook and Exchange. This functionality collects data from the anti-spam Safe Recipients Lists, Safe Senders Lists, Blocked Senders Lists, and contact data that Outlook users configure, and makes this data available to the anti-spam agents on the computer that has the Edge Transport server role installed. Safelist aggregation can help reduce the instances of false-positives in anti-spam filtering performed by the Edge Transport server.

When you enable and correctly configure safelist aggregation, the Content Filter agent passes safe e-mail messages to the enterprise mailbox without additional processing. E-mail messages that Outlook users receive from contacts that those users have added to their Outlook Safe Recipients List or Safe Senders List or have trusted are identified by the Content Filter agent as safe. An Outlook *contact* is a person, inside or outside the user's organization, about whom the user can save several types of information, such as e-mail and street addresses, telephone and fax numbers, and Web page URLs.

In Exchange 2010, the safelist aggregation process also replicates a per-recipient Blocked Senders List to the Edge Transport server. This allows the Sender Filtering agent on the Edge Transport server to block incoming messages from those senders.

Safelist aggregation can help reduce the instances of false-positives in anti-spam filtering performed by the Edge Transport server. A *false-positive* is a positive test or filter result in a subject or body of data that doesn't possess the attribute for which the filter or test is being conducted. In the context of spam filtering, a false-positive occurs when a spam filter incorrectly identifies a message from a legitimate sender as spam.

For organizations that filter hundreds of thousands of messages from the Internet every day, even a small percentage of false-positives means that users might not receive many messages identified incorrectly as spam, which were quarantined or deleted.

Safelist aggregation is likely the most effective way to reduce false-positives. In Office Outlook 2007, users can create *Safe Senders Lists*. Safe Senders Lists specify a list of domain names and e-mail addresses from which the Outlook user wants to receive messages. By default, e-mail addresses in Outlook Contacts and in the Exchange Server global address list are included in this list. By default, Outlook adds all external contacts to which the user sends mail to the Safe Senders List.

Contents

Information Stored in the Outlook User's Safelist Collection

A *safelist collection* is the combined data from the user's Safe Senders List, Safe Recipients List, Blocked Senders List, and external contacts. This data is stored in Outlook and in the Exchange mailbox.

The following types of information are stored in an Outlook user's safelist collection:

- **Safe senders and safe recipients** The From message header indicates a sender. The To field of the e-mail message indicates a recipient. Safe senders and safe recipients are represented by full SMTP addresses, such as masato@contoso.com. Outlook users can add senders and recipients to their safe lists.
- **Blocked senders** Just like safe senders, users can block unwanted senders by adding them to their Blocked Senders Lists.
- **Safe domain** The domain is the part of an SMTP address that follows the @ symbol. For example, contoso.com is the domain in the masato@contoso.com address. Outlook users can add sending domains to their safe lists.

  Important:

  Exchange provides functionality that allows you to specify whether to include the safe domain data for the anti-spam agents on the Edge Transport server by using the **Update-SafeList** cmdlet. In most cases, we don't recommend that you include domains because users may include the domains of large Internet service providers (ISP), which could unintentionally provide addresses that may be used or spoofed by spammers. By default, Exchange doesn't include the domains during safelist aggregation.

- **External contacts** Two types of external contacts can be included in the safelist aggregation. The first type of external contact includes contacts to whom Outlook users have sent mail. This class of contact is added to the Safe Senders List only if an Outlook user selects the corresponding option in the Junk E-mail settings in Outlook 2007.
  The second type of external contact includes the users' Outlook contacts. Users can add or import these contacts into Outlook. This class of contact is added to the Safe Senders List only if an Outlook user selects the corresponding option in the Junk E-mail Filter settings in Outlook 2010 or Outlook 2007.

Return to top

How Exchange Uses the Safelist Collection

The safelist collection is stored on the user's Mailbox server. A user can have up to 1,024 unique entries in a safelist collection. Exchange 2010 has a mailbox assistant, called the Junk E-mail Options mailbox assistant, which monitors changes to the safelist collection for your mailboxes. It then replicates these changes to Active Directory, where the safelist collection is stored on each user object. When the safelist collection is stored on the user object in Active Directory, the safelist collection is aggregated with the anti-spam functionality of Exchange 2010 and is optimized for minimized storage and replication. The Microsoft Exchange EdgeSync service replicates the safelist collection to the Active

Directory Lightweight Directory Services (AD LDS) instance on the Edge Transport server. The Edge Transport servers use the safelist collection data during content filtering.

Important:

Although the safe recipient data is stored in Outlook and can be aggregated into the safelist collection on the AD LDS instance on the Edge Transport server, the content filtering functionality doesn't act on safe recipient data.

Return to top

Hashing of Safelist Collection Entries

Safelist collection entries are hashed (SHA-256) one way before they are stored as array sets across three user object attributes, **msExchSafeSenderHash**, **msExchSafeRecipientHash**, and **msExchBlockedSendersHash**, as a binary large object. When data is hashed, an output of fixed length is produced, and the output is likely to be unique. For hashing of safelist collection entries, a 4-byte hash is produced. When a message is received from the Internet, Exchange hashes the sender address and compares it to the hashes stored on behalf of the Outlook user to whom the message was sent. If the sender matches the safe senders hash, the message bypasses content filtering. If the sender matches the blocked senders hash, the message is blocked.

One-way hashing of safelist collection entries performs the following important functions:

- **Minimizes storage and replication space** Most of the time, hashing reduces the size of the data hashed. Therefore, saving and transmitting a hashed version of a safelist collection entry conserves storage space and replication time. For example, a user who has 200 entries in his or her safelist collection would create about 800 bytes of hashed data stored and replicated in Active Directory.
- **Renders user safelist collections unusable by malicious users** Because one-way hash values are impossible to reverse-engineer into the original SMTP address or domain, the safelist collections don't yield usable e-mail addresses for malicious users who might compromise an Edge Transport server.

Return to top

Enabling Safelist Aggregation

Safelist aggregation is enabled by default in Exchange 2010. Unlike in Exchange Server 2007, you don't need to manually run the **Update-SafeList** cmdlet to hash and write the safelist collection data to Active Directory. In Exchange 2010, this is accomplished behind the scenes by the Junk E-mail Options mailbox assistant.

You can still manually run safelist aggregation by using the **UpdateSafelist** cmdlet. The **Update-SafeList** cmdlet reads the safelist collection from the user's mailbox, hashes each entry, sorts the entries for easy search, and then converts the hash to a binary attribute. Finally, the **Update-SafeList** cmdlet compares the binary attribute that was created to any value stored on the attribute. If the two values are identical, the **Update-SafeList** cmdlet doesn't update the user attribute value with the safelist aggregation data. If the two attribute values are different, the **Update-SafeList** cmdlet updates the safelist aggregation value.

To make the safelist aggregation data in Active Directory available to Edge Transport servers in the perimeter network, you must install and configure the Microsoft Exchange EdgeSync service so that the safelist aggregation data is replicated to AD LDS.

Return to top

Options available in the msexchangemailboxassistants.exe.config file

To activate the options to include safe domains, or to change the maximum values for the default settings, you must change the msexchangemailboxassistants.exe.config file. Specifically, the following settings and values can be changed in the **appsettings** section of the msexchangemailboxassistants.exe.config file:

Setting	Value
IncludeSafeDomains	The value for this setting can be True or False.
UpdateInterval	By default, the value for this setting is 15 minutes. This setting can have a value from 15 minutes through 1 day.
TestUpdateInterval	TestUpdateInterval is used in test environments. This setting can have a value from 10 seconds through 1 hour.
MaxSafeSenders	3*1024
MaxSafeRecipients	2*1024
MaxBlockedSenders	By default, the value for this setting is 500. The maximum value is 1000.

For example, the settings in the **appsettings** section of the msexchangemailboxassistants.exe.config file may be as follows:

```
<configuration>
  <runtime>
    <gcConcurrent enabled="false" />
    <generatePublisherEvidence enabled="false" />
  </runtime>
  <appSettings>
        <add key="IncludeSafeDomains" value="true" />
</appSettings>
</configuration>
```

Return to top

1.7.1.5.9 Understanding Sender Filtering

Understanding Sender Filtering

Transport > Understanding Transport > Understanding Anti-Spam and Antivirus Functionality >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-17*

The Sender Filter agent is an anti-spam filter that's enabled on computers that have the

Microsoft Exchange Server 2010 Edge Transport server role installed. The Sender Filter agent relies on the MAIL FROM: SMTP header to determine what action, if any, to take on an inbound e-mail message.

When you configure anti-spam filters on an Edge Transport server, the filters act on messages cumulatively to reduce the number of unsolicited messages that enter the enterprise. For more information about how to plan and deploy the anti-spam features, see Understanding Anti-Spam and Antivirus Functionality.

The Sender Filter agent acts on messages from specific senders outside the organization. Administrators of Edge Transport servers maintain a list of senders who are blocked from sending messages to the organization. As an administrator, you can block single senders (kim@contoso.com), whole domains (*.contoso.com), or domains and all subdomains (*.contoso.com). You can also configure what action the Sender Filter agent should take when a message that has a blocked sender is found. You can configure the following actions:

- The Sender Filter agent rejects the SMTP request with a "554 5.1.0 Sender Denied" SMTP session error and closes the connection.
- The Sender Filter agent accepts the message and updates the message to indicate that the message came from a blocked sender. Because the message came from a blocked sender and it's marked as such, the Content Filter agent will use this information when it calculates the spam confidence level (SCL).

You can use the Exchange Management Console (EMC) or the Exchange Management Shell to designate blocked senders and to define how the Sender Filter agent should act on messages from blocked senders. For more information about how to configure the Sender Filter agent, see Configure Sender Filtering Properties.

Important:

The MAIL FROM: SMTP headers can be spoofed. Therefore, you shouldn't rely on the Sender Filter agent only. Use the Sender Filter agent and the Sender ID agent together. The Sender ID agent uses the originating IP address of the sending server to try to verify that the domain in the MAIL FROM: SMTP header matches the domain that's registered. For more information about the Sender ID agent, see Understanding Sender ID.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Using the Sender Filter Agent to Block Messages

By default, sender filtering is enabled on the computer that has the Edge Transport server role installed for inbound messages that come from the Internet but aren't authenticated. These messages are handled as external messages. You can disable the Sender Filter agent in individual computer configurations by using the EMC or the Shell. For more information, see Enable or Disable Sender Filtering.

When you enable the Sender Filter agent on a computer, the Sender Filter agent filters all messages that come through all Receive connectors on that computer. As noted earlier in this topic, only messages that come from external sources are filtered. *External sources* are defined as non-authenticated sources. These are considered anonymous Internet sources.

For more information about how to configure Receive connectors and how message source categories are determined, see Understanding Receive Connectors.

As a best practice, you shouldn't filter e-mail messages from trusted partners or from inside your organization. When you run anti-spam filters, there's always a chance that the

filters will detect false positives. You should enable anti-spam agents to run only on messages from potentially untrusted and unknown sources. This will reduce the chance that anti-spam filters will mishandle legitimate messages. You can enable and disable the Sender Filter agent to run on messages from any source by using the Shell. For more information, see Set-SenderFilterConfig.

You can configure the Sender Filter agent to block inbound messages that don't specify a sender and domain in the MAIL FROM: SMTP header. You can use this feature to prevent non-delivery report (NDR) attacks on the Exchange server. Most legitimate SMTP messages come from SMTP servers that provide a sender and domain in the MAIL FROM: SMTP command.

Specifying the Block Action

After you've specified blocked senders and domains, you must specify how you want the Sender Filter agent to act on messages from blocked senders and domains. We recommend that you reject the messages. When you use the Sender Filter agent on which all blocked e-mail addresses and domains are specified by the Edge Transport server administrator, the chance of false positives is relatively less than when you use other anti-spam agents. For example, the Content Filter agent is an anti-spam agent that relies on many different variables to determine whether a message is spam.

There are only two scenarios in which legitimate messages may be rejected by the Sender Filter agent:

- If you mistype an e-mail address or domain name, the wrong sender may be blocked.
- If a domain name is reregistered to a legitimate company after you add the domain to your Blocked Senders list, you will unintentionally block legitimate messages.

In either of these cases, it may still make sense to reject the messages.

1.7.1.5.10 Understanding Sender ID

Understanding Sender ID

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-27*

The Sender ID agent is an anti-spam agent that's enabled on computers that have the Microsoft Exchange Server 2010 Edge Transport server role installed. The Sender ID agent relies on the RECEIVED SMTP header and a query to the sending system's DNS service to determine what action, if any, to take on an inbound message.

When you configure anti-spam agents on an Edge Transport server, the agents act on messages cumulatively to reduce the number of unsolicited e-mail messages that enter the organization. For more information about how to plan and deploy the anti-spam agents, see Understanding Anti-Spam and Antivirus Functionality.

Sender ID is intended to combat the impersonation of a sender and a domain, a practice that's frequently called *spoofing*. A *spoofed mail* is an e-mail message that has a sending address that was modified to appear as if it originates from a sender other than the actual sender of the message.

Spoofed mails typically contain a From: address that purports to be from a certain organization. In the past, it was relatively easy to spoof the From: address, in both the SMTP session, such as the MAIL FROM: header, and in the RFC 822 message data, such as From: "Masato Kawai" masato@contoso.com, because the headers weren't validated.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Using Sender ID to Combat Spoofing

In Exchange 2010, Sender ID makes spoofing more difficult. When you enable Sender ID, each message contains a Sender ID status in the metadata of the message. When an e-mail message is received, the Edge Transport server queries the sender's DNS server to verify that the IP address from which the message was received is authorized to send messages for the domain that's specified in the message headers. The IP address of the authorized sending server is referred to as the purported responsible address (PRA).

Domain administrators publish sender policy framework (SPF) records on their DNS servers. SPF records identify authorized outbound e-mail servers. If an SPF record is configured on the sender's DNS server, the Edge Transport server parses the SPF record and determines whether the IP address from which the message was received is authorized to send e-mail on behalf of the domain that's specified in the message. For more information about what an SPF record contains and how to create an SPF record, see Sender ID.

The Edge Transport server updates the message metadata with the Sender ID status based on the SPF record. After the Edge Transport server updates the message metadata, the Edge Transport server delivers the message as it ordinarily would.

Sender ID Status Values

The Sender ID evaluation process generates a Sender ID status for the message. The Sender ID status is used to evaluate the spam confidence level (SCL) rating for the message. This status can be set to one of the following values:

- **Pass** Both the IP address and Purported Responsible Address (PRA) passed the Sender ID verification check.
- **Neutral** Published Sender ID data is explicitly inconclusive.
- **Soft fail** The IP address for the PRA may be in the not permitted set.
- **Fail** The IP Address is not permitted; no PRA is found in the incoming mail or the sending domain does not exist.
- **None** No published SPF data exists in the sender's DNS.
- **TempError** A temporary DNS failure occurred, such as an unavailable DNS server.
- **PermError** The DNS record is invalid, such as an error in the record format.

The Sender ID status is added to the message metadata and is later converted to a MAPI property. The junk e-mail filter in Microsoft Office Outlook uses the MAPI property during the generation of the SCL value.

Outlook neither displays the Sender ID status nor necessarily flags a message as junk at certain Sender ID values. Outlook uses the Sender ID status value only during the calculation of the SCL value.

Besides the seven scenarios that generate the Sender ID statuses, the Sender ID evaluation process may reveal instances where the From: IP address is missing. If the From: IP address is missing, the Sender ID status can't be set. If the Sender ID status can't be set, Exchange continues to process the message without including a Sender ID status on the message. The message isn't discarded or rejected. In this scenario, Sender ID status isn't set, and an application event is logged.

For more information about how the Sender ID status is displayed in messages, see Understanding Anti-Spam Stamps.

Sender ID Options for Handling Spoofed Mail and Unreachable DNS Servers

You can also define how the Edge Transport server handles messages that are identified as spoofed mail and how the Edge Transport server handles messages when a DNS server can't be reached. The options for how the Edge Transport server handles spoofed mail and unreachable DNS servers include the following actions:

- **Stamp the status** This option is the default action. All inbound messages to your organization have the Sender ID status included in the metadata of the message.
- **Reject** This option rejects the message and sends an SMTP error response to the sending server. The SMTP error response is a 5*xx* level protocol response with text that corresponds to the Sender ID status.
- **Delete** This option deletes the message without informing the sending system of the deletion. In fact, the Edge Transport server sends a fake OK SMTP command to the sending server and then deletes the message. Because the sending server assumes the message was sent, it doesn't retry sending the message in the same session.

For more information about how to configure the Sender ID agent, see Configure Sender ID Properties.

Return to top

Updating Your Organization's Internet-Facing DNS to Support Sender ID

The effectiveness of Sender ID depends on specific DNS data. The more organizations that update their Internet-facing DNS servers by using an SPF record, the more effectively Sender ID identifies spoofed e-mail messages.

To support the Sender ID infrastructure, you must update your Internet-facing DNS data by creating an SPF record and hosting the SPF record on your public DNS servers. For more information about how to create and deploy SPF records, see Sender ID.

Return to top

Specifying Recipients and Sender Domains to Exclude From Sender ID

Filtering

You may want to exclude specific recipients and sender domains from Sender ID filtering. To do this, specify the recipients and sender domains in the Exchange Management Shell. You can't specify the recipients and sender domains in the Exchange Management Console.

For more information about how to set recipient and sender domain exclusions for Sender ID, see Set-SenderIdConfig.

Return to top

1.7.1.5.11 Understanding Sender Reputation

Understanding Sender Reputation

Transport > Understanding Transport > Understanding Anti-Spam and Antivirus Functionality >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-07*

Sender reputation is anti-spam functionality that's enabled on computers that have the Microsoft Exchange Server 2010 Edge Transport server role installed to block messages according to many characteristics of the sender. Sender reputation relies on persisted data about the sender to determine what action, if any, to take on an inbound message.

When you configure anti-spam agents on an Edge Transport server, the agents act on messages cumulatively to reduce the number of unsolicited messages that enter the organization. For more information about how to plan and deploy the anti-spam agents, see Understanding Anti-Spam and Antivirus Functionality.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Calculation of the Sender Reputation Level

A sender reputation level (SRL) is calculated from the following statistics:

- **HELO/EHLO analysis** The HELO and EHLO SMTP commands are intended to provide the domain name, such as Contoso.com, or IP address of the sending SMTP server to the receiving SMTP server. Malicious users, or *spammers*, frequently forge the HELO/EHLO statement in various ways. For example, they

type an IP address that doesn't match the IP address from which the connection originated. Spammers also put domains that are known to be locally supported at the receiving server in the HELO statement in an attempt to appear as if the domains are in the organization. In other cases, spammers change the domain that's passed in the HELO statement. The typical behavior of a legitimate user may be to use a different, but relatively constant, set of domains in their HELO statements.

Therefore, analysis of the HELO/EHLO statement on a per-sender basis may indicate that the sender is likely to be a spammer. For example, a sender that provides many different unique HELO/EHLO statements in a specific time period is more likely to be a spammer. Senders who consistently provide an IP address in the HELO statement that doesn't match the originating IP address as determined by the Connection Filter agent are also more likely to be spammers, as are remote senders who consistently provide a local domain name, which is in the same organization as the Edge Transport server, in the HELO statement.

- **Reverse DNS lookup** Sender reputation also verifies that the originating IP address from which the sender transmitted the message matches the registered domain name that the sender submits in the HELO or EHLO SMTP command.

  Sender reputation performs a reverse DNS query by submitting the originating IP address to DNS. The result that's returned by DNS is the domain name that's registered by using the domain naming authority for that IP address. Sender reputation compares the domain name that's returned by DNS to the domain name that the sender submitted in the HELO/EHLO SMTP command. If the domain names don't match, the sender is likely to be a spammer, and the overall SRL rating for the sender is adjusted upward.

  The Sender ID agent performs a similar task, but the success of the Sender ID agent relies on legitimate senders to update their DNS infrastructure to identify all the e-mail-sending SMTP servers in their organization. By performing a reverse DNS lookup, you can help identify potential spammers.
- **Analysis of SCL ratings on messages from a particular sender** When the Content Filter agent processes a message, it assigns a spam confidence level (SCL) rating to the message. The SCL rating is a number from 0 through 9. A higher SCL rating indicates that a message is more likely to be spam. Data about each sender and the SCL ratings that their messages yield is persisted for analysis by sender reputation. Sender reputation calculates statistics about a sender according to the ratio between all messages from that sender that had a low SCL rating in the past and all messages from that sender that had a high SCL rating in the past. Additionally, the number of messages that have a high SCL rating that the sender has sent in the last day is applied to the overall SRL.
- **Sender open proxy test** An *open proxy* is a proxy server that accepts connection requests from anyone anywhere and forwards the traffic as if it originated from the local hosts. Proxy servers relay TCP traffic through firewall hosts to provide user applications transparent access across the firewall. Because proxy protocols are lightweight and independent of user application protocols, proxies can be used by many different services. Proxies can also be used to share a single Internet connection by multiple hosts. Proxies are usually set up so that only trusted hosts inside the firewall can cross through the proxies.

  Open proxies can exist because of either of the following conditions:
  - Unintentional misconfiguration.
  - Malicious Trojan horse programs. A *Trojan horse* program is a program that masquerades as another common program in an attempt to receive information.

  Frequently with insufficient logging, open proxies provide an ideal way for malicious users to hide their true identities and launch denial of service attacks (DoS) or send spam. As more proxy servers are configured to be open by default, open proxies have become more common. Additionally, malicious users

can use multiple open proxies together to hide the sender's originating IP address.
When sender reputation performs an open proxy test, it does so by formatting an SMTP request in an attempt to connect back to the Edge Transport server from the open proxy. If an SMTP request is received from the proxy, sender reputation verifies that the proxy is an open proxy and updates the open proxy test statistic for that sender.

Sender reputation weighs each of these statistics and calculates an SRL for each sender. The SRL is a number from 0 through 9 that predicts the probability that a specific sender is a spammer or otherwise malicious user. A value of 0 indicates that the sender isn't likely to be a spammer; a value of 9 indicates that the sender is likely to be a spammer.

You can configure a block threshold from 0 through 9 at which sender reputation issues a request to the Sender Filter agent, and, therefore, blocks the sender from sending a message into the organization. When a sender is blocked, the sender is added to the Blocked Senders list for a configurable period. How blocked messages are handled depends on the configuration of the Sender Filter agent. The following actions are the options for handling blocked messages:

- Reject
- Delete and archive
- Accept and mark as a blocked sender

If a sender is included in the IP Block list or Microsoft IP Reputation Service, sender reputation issues an immediate request to the Sender Filter agent to block the sender. To take advantage of this functionality, you must enable and configure the Microsoft Exchange Anti-spam Update Service.

By default, the Edge Transport server sets a rating of 0 for senders that haven't been analyzed. After a sender has sent 20 or more messages, sender reputation calculates an SRL that's based on the statistics listed earlier in this topic.

Return to top

Use of the SRL

Sender reputation acts on messages during two phases of the SMTP session:

- **At the MAIL FROM: SMTP command** Sender reputation acts on a message only if the message was blocked or otherwise acted on by the Connection Filter agent, Sender Filter agent, Recipient Filter agent, or Sender ID agent. In this case, sender reputation retrieves the sender's current SRL rating from the sender profile that's persisted about that sender in the Edge Transport server database. After this rating is retrieved and evaluated, the Edge Transport server configuration dictates the behavior that occurs at a particular connection according to the block threshold.
- **After the "end of data" SMTP command** The end of data transfer (**_EOD**) SMTP command is given when all the actual message data is sent. At this point in the SMTP session, many of the anti-spam agents have processed the message. As a by-product of anti-spam processing, the statistics that sender reputation relies on are updated. Therefore, sender reputation has the data to calculate or recalculate an SRL rating for the sender.

For more information, see Configure Sender Reputation Properties.

Return to top

Enabling and Configuring the Detection of

Open Proxy Servers

Sender reputation evaluates several sender characteristics to calculate an SRL. Among the characteristics that sender reputation evaluates are the results of a test for open proxy servers. Frequently, spammers route messages through open proxy servers on the Internet. By routing spam through open proxy servers, spammers can send messages that appear to originate from a different server than their own.

When sender reputation calculates an SRL, sender reputation tries to connect to the sender's originating IP address by using a variety of common proxy protocols, such as SOCKS4, SOCKS5, HTTP, Telnet, Cisco, and Wingate. Sender reputation formats a protocol-specific request in an attempt to connect back to the Edge Transport server from the open proxy server by using an SMTP request. If an SMTP request is received from the proxy server, sender reputation verifies that the proxy server is an open proxy server and adjusts the SRL rating according to this result. By default, detection of open proxy servers is enabled on sender reputation.

For more information about how to enable detection of open proxy servers, see Configure Sender Reputation Properties.

For more information about how to configure detection of open proxy servers, see Configure Outbound Access for Detection of Open Proxy Servers for Sender Reputation.

Return to top

Setting the SRL Block Threshold

The SRL is a number from 0 through 9 that predicts the probability that a specific sender is a spammer or otherwise malicious user. You must set a threshold for sender blocking by SRL. This SRL block threshold defines the SRL value that must be exceeded for sender reputation to block a sender. By default, the SRL is set at 7. You should monitor the effectiveness of the agent at the default level. You may find that you can adjust the value to meet the needs of your organization. If you set other anti-spam agents aggressively, you may be able to set a higher SRL threshold for sender reputation than you would if the other anti-spam agents weren't set aggressively. For more information about how to adjust anti-spam configurations so that they work together to reduce spam, see Understanding Anti-Spam and Antivirus Functionality.

If the SRL block threshold is exceeded for a particular sender, sender reputation adds the sender to the IP Block list on the Connection Filter agent. Sometimes, spammers send batches of spam from a single sender. In this scenario, if sender reputation calculates an SRL that exceeds the SRL block threshold, the sender is added to the Sender Block List for a configurable duration of time. The default duration is 24 hours. After 24 hours, the sender is removed from the Sender Block List and can send messages again.

When a sender is added to the IP Block list, sender reputation deletes the profile for the sender. Sender reputation deletes the profile because the blocked sender's existing profile indicates that the sender's SRL exceeds the SRL block threshold. This would cause the blocked sender to be added to the IP Block list again as soon as the duration for sender blocking ends.

For more information, see Configure Sender Reputation Properties.

Return to top

Understanding Spam Confidence Level Threshold

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-10*

In Microsoft Exchange Server 2010, you can define specific actions according to spam confidence level (SCL) thresholds. For example, you can define different thresholds for rejecting, deleting, or quarantining messages on a server that has the Edge Transport server role installed.

The combination of this SCL threshold configuration on the Edge Transport server and the SCL Junk E-mail folder configuration on the user mailbox helps you implement a more comprehensive and precise anti-spam strategy. This more precise and detailed SCL threshold adjustment functionality in Exchange 2010 can help you reduce the overall cost of deploying and maintaining an anti-spam solution across your Exchange organization.

The SCL threshold configuration is used by the Content Filter agent, one of the default anti-spam agents included with Exchange 2010. The Content Filter agent uses Microsoft SmartScreen technology to assess the contents of a message and to assign an SCL rating to each message.

The Content Filter agent performs this function late in the anti-spam cycle, after other anti-spam agents have processed any inbound messages. Many of the other anti-spam agents that process inbound messages before they're processed by the Content Filter agent are deterministic in how they act on a message. For example, the Connection Filter agent rejects any message sent from an IP address on a real-time block list. The Sender Filter agent and Recipient Filter agent process messages in a similarly deterministic manner.

In Exchange 2010, these deterministic anti-spam agents process messages first and therefore greatly reduce the number of messages that must be processed by the Content Filter agent. For more information about the order in which anti-spam agents process messages, see Understanding Anti-Spam and Antivirus Mail Flow.

Because content filtering isn't an exact, deterministic process, the ability to adjust the action that the Content Filter agent performs on different SCL values is important. By carefully adjusting the SCL threshold configuration, you can minimize the following:

- Size of the spam quarantine storage
- Number of legitimate e-mail messages mistakenly quarantined
- Number of legitimate e-mail messages that reach the Microsoft Outlook user's Junk E-mail folder
- Number of offensive spam e-mail messages that reach the Outlook user's Inbox or Junk E-mail folder
- Number of spam e-mail messages that reach the Outlook user's Inbox

Looking for management tasks related to anti-spam and antivirus functionality? See Managing Anti-Spam and Antivirus Features.

SCL Threshold Actions in Exchange 2010

In Exchange 2010, by adjusting SCL threshold actions, you can escalate the content filtering action taken on messages that have a greater risk of being spam. To understand this functionality, it's helpful to understand the different SCL threshold actions and how they're implemented:

- **SCL delete threshold** When the SCL value for a specific message is equal to

or higher than the SCL delete threshold, the Content Filter agent deletes the message. There's no protocol-level communication that tells the sending system or sender that the message was deleted. If the SCL value for a message is lower than the SCL delete threshold value, the Content Filter agent doesn't delete the message. Instead, the Content Filter agent compares the SCL value to the SCL reject threshold.

- **SCL reject threshold** When the SCL value for a specific message is equal to or higher than the SCL reject threshold, the Content Filter agent deletes the message and sends a rejection response to the sending system. You can customize the rejection response. In some cases, a non-delivery report (NDR) is sent to the original sender of the message. If the SCL value for a message is lower than the SCL delete and SCL reject threshold values, the Content Filter agent doesn't delete or reject the message. Instead, the Content Filter agent compares the SCL value to the SCL quarantine threshold.
- **SCL quarantine threshold** When the SCL value for a specific message is equal to or higher than the SCL quarantine threshold, the Content Filter agent sends the message to a quarantine mailbox. E-mail administrators must periodically review the quarantine mailbox. If the SCL value for a message is lower than the SCL delete, reject, and quarantine threshold values, the Content Filter agent doesn't delete, reject, or quarantine the message. Instead, the Content Filter agent sends the message to the appropriate Mailbox server, where the per-recipient SCL Junk E-mail folder threshold value of the message is evaluated.
- **SCL Junk E-mail folder threshold** If the SCL value for a specific message exceeds the SCL Junk E-mail folder threshold, the Mailbox server puts the message in the Outlook user's Junk E-mail folder. If the SCL value for a message is lower than the SCL delete, reject, quarantine, and Junk E-mail folder threshold values, the Mailbox server puts the message in the user's Inbox.

For example, if you set the SCL delete threshold to 8, the SCL reject threshold to 7, the SCL quarantine threshold to 6, and the SCL Junk E-mail folder threshold to 5, all e-mail with an SCL of 5 or lower will be delivered to the user's Inbox.

As you plan and deploy your strategy for adjusting the SCL threshold, it's important to understand that the Content Filter agent and the SCL Junk E-mail folder process the SCL threshold value differently. The Content Filter agent takes action on the SCL threshold value that you configure. The SCL Junk E-mail folder takes action on the SCL threshold value that you configure plus 1. For example, if you configure the Delete action to an SCL of 4 on the Content Filter agent, all messages with an SCL of 4 or greater are deleted. However, if you configure the Delete action to an SCL of 4 on the SCL Junk E-mail folder, all messages with an SCL of 5 or greater are deleted.

To configure the SCL Junk E-mail folder threshold on individual user mailboxes, you must use the Set-Mailbox cmdlet in the Exchange Management Shell. You can configure the SCL delete, reject, and quarantine thresholds in two locations:

- **On the content filter configuration (per-transport server SCL configuration)** We recommend that you set the organization-wide SCL thresholds on the content filter configuration on the Edge Transport server. If you run anti-spam agents on the Hub Transport server, set the organization-wide SCL thresholds on the Hub Transport server. By applying the same SCL thresholds across all transport servers, you can establish a consistent baseline level of SCL functionality across the organization. Over time, as you analyze the spam functionality and metrics provided by the anti-spam logging and reporting features, you can make additional adjustments to these SCL threshold configurations as needed.
- **On user mailboxes (per-recipient SCL configuration)** You can use the **Set-Mailbox** cmdlet to set per-recipient SCL delete, reject, and quarantine thresholds on individual user mailboxes. As mentioned earlier in this topic, you set the SCL Junk E-mail folder threshold on individual user mailboxes by using

the **Set-Mailbox** cmdlet. The per-recipient SCL delete, reject, and quarantine thresholds are stored in Active Directory and are replicated to the Edge Transport servers by the Microsoft Exchange EdgeSync service. The per-recipient SCL threshold configurations are used by the Content Filter agent even if you've set per-transport server SCL configurations. Therefore, if you've set per-recipient SCL thresholds, the Content Filter agent uses the per-recipient SCL thresholds for specific users instead of the SCL configuration on the Content Filter agent.

Note:

Per-recipient SCL thresholds are not enforced on mail received through distribution groups. These types of messages are rejected at the Transport server before the per-recipient threshold settings are applied. Additionally, if you're using Microsoft Forefront Protection 2010 for Exchange Server, any per-recipient SCL threshold settings replicated to the Edge Transport servers by the Microsoft Exchange EdgeSync service will take precedence over the Forefront anti-spam settings.

For more information about how to use the **Set-Mailbox** cmdlet, see Set-Mailbox.

Best Practice for Setting Up and Adjusting SCL Thresholds

We recommend that you set up and adjust the SCL thresholds as follows:

1. Enable the SCL delete, reject, and quarantine thresholds on the content filter configuration on each Edge Transport server.
   We recommend that you enable SCL thresholds at an organization level and that you use the default values for these SCL thresholds. The default values were set by the Exchange Server team according to real-world data from the Microsoft IT messaging department and from Exchange 2010 early adopter feedback. The default values are optimized for large, global enterprise deployments.
   If needed, you can also configure the SCL delete, reject, and quarantine thresholds on a per-recipient configuration to bypass the SCL thresholds configured at the organization level. For more information about how to set the SCL thresholds on the content filter configurations, see Configure Content Filtering Properties.
2. Monitor spam reports and logs closely for the first week after you enable the SCL thresholds.
   You can use several built-in scripts located in the %ExchangeInstallPath%\Scripts folder, such as get-AntispamSCLHistogram.ps1, for gathering filtering result data. If the data indicates that you must make immediate adjustments, reconfigure the SCL thresholds. Otherwise, collect data and analyze the spam reporting to determine whether adjustments are required.

1.7.1.5.13 Understanding Spam Quarantine

Understanding Spam Quarantine

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Many organizations are bound by legal or regulatory requirements to preserve or deliver all legitimate e-mail messages. In Microsoft Exchange Server 2010, spam quarantine is a feature of the Content Filter agent that reduces the risk of losing legitimate messages. Spam quarantine provides a temporary storage location for messages identified as spam that shouldn't be delivered to a user mailbox inside the organization.

Messages identified by the Content Filter agent as spam are wrapped in a non-delivery report (NDR) and delivered to a spam quarantine mailbox inside the organization. You can manage messages delivered to the spam quarantine mailbox and take appropriate actions. For example, you can delete messages or let messages flagged as false positives in anti-spam filtering be routed to their intended recipients. In addition, you can configure the spam quarantine mailbox to automatically delete messages after a designated time period.

For more information about how the anti-spam agents filter inbound messages and the order in which the agents are applied, see Understanding Anti-Spam and Antivirus Functionality.

Looking for management tasks related to anti-spam and antivirus functionality? See Managing Anti-Spam and Antivirus Features.

Contents

Spam Confidence Level

When an external user sends e-mail messages to a server running Exchange that runs the anti-spam features, the anti-spam features cumulatively evaluate characteristics of the messages and act as follows:

- Those messages suspected to be spam are filtered out.
- A rating is assigned to messages based on the probability that a message is spam. This rating is stored with the message as a message property called the spam confidence level (SCL) rating.

Spam quarantine uses the SCL rating to determine whether mail has a high probability of being spam. The SCL rating is a numeric value from 0 through 9, where 0 is considered less likely to be spam, and 9 is considered most likely to be spam.

You can configure mail that has a certain SCL rating to be deleted, rejected, or quarantined. The rating that triggers any of these actions is referred to as the *SCL quarantine threshold*. Within content filtering, you can configure the Content Filter agent to base its actions on the SCL quarantine threshold. For example, you can set the following conditions:

- SCL delete threshold is set to 8.
- SCL reject threshold is set to 7.
- SCL quarantine threshold is set to 6.
- SCL Junk E-mail folder threshold is set to 5.

Based on the preceding SCL thresholds, all e-mail with an SCL of 6 will be delivered to the spam quarantine mailbox.

For more information, see Configure Content Filtering Properties.

Return to top

Spam Quarantine

When messages are received by the Edge Transport server and all default anti-spam filters are enabled, the anti-spam agents apply their filters. Then the content filter is applied as follows:

- If the SCL rating is greater than or equal to the SCL quarantine threshold but less than either the SCL delete threshold or SCL reject threshold, the message goes to the spam quarantine mailbox.
- If the SCL rating is lower than the spam quarantine threshold, it's delivered to the recipient's Inbox.

The message administrator uses Microsoft Office Outlook 2007 to monitor the spam quarantine mailbox for false positives. If a false positive is found, the administrator can send the message to the recipient's mailbox.

The message administrator can review the anti-spam stamps if either of the following conditions is true:

- Too many false positives are filtered into the spam quarantine mailbox.
- Not enough spam is being rejected or deleted.

For more information, see Understanding Anti-Spam Stamps.

You can then adjust the SCL settings to more accurately filter the spam coming into the organization. For more information, see Understanding Spam Confidence Level Threshold.

To use spam quarantine, you must follow these steps:

1. Enable content filtering.
2. Create a spam quarantine mailbox.
3. Specify the spam quarantine mailbox.
4. Configure the SCL quarantine threshold.
5. Manage the spam quarantine mailbox.
6. Adjust the SCL quarantine threshold as needed.

Enabling Content Filtering

You must enable content filtering before you can apply spam quarantine. By default, the Content Filter agent filters all external messages that come through all Receive connectors on the computer on which the Content Filter feature is enabled.

Important:

Configuration changes that you make to the Content Filter agent by using the Exchange Management Console or the Exchange Management Shell are made only to the local computer that has the Edge Transport server role installed. If multiple instances of the Edge Transport server role are running in your organization, you must apply sender reputation configuration changes to each computer.

For more information, see Enable or Disable Content Filtering.

Creating a Spam Quarantine Mailbox

You must create a spam quarantine mailbox before you can enable the feature. To set up a spam quarantine mailbox, you must follow these steps:

- **Create a dedicated Exchange database** We recommend that you create a dedicated database for the spam quarantine mailbox. The spam quarantine mailbox should have a large database, because if the storage quota limit is reached, messages will be lost. For more information, see Create a Mailbox Database.
- **Create an Active Directory user** We recommend that you create a separate

Active Directory user for the spam quarantine mailbox. You may apply different recipient policies, such as messaging records management and mailbox size, and delegation rights, according to your organization's compliance policies and needs.

- **Create a user mailbox** You must create a mailbox that you can use as the spam quarantine mailbox with an appropriate messaging records management policy that includes mailbox size and the number of days that messages will be saved before they are deleted. For more information, see Messaging Records Management.

  Note:
  If a quarantined message is rejected because of a storage quota, the message will be lost. Exchange doesn't generate NDRs for quarantined messages because the quarantined messages are wrapped as NDRs.

  For more information, see Create a Mailbox.
- **Set up the Outlook account profile** You must configure management or delegation of the Outlook account to meet the needs of your organization. In addition, to help with the account management, we recommend that you configure the Outlook profile to expose the original Sender[#0x0069001E], Recipient[#0x0E04001E], and Bcc[#0x0E02001E] fields in the Message view. For more information, see Release Quarantined Messages from the Spam Quarantine Mailbox.

Specifying the Spam Quarantine Mailbox

After you set up the spam quarantine mailbox, you must specify the spam quarantine mailbox in the content filter configuration. You use the **Set-ContentFilterConfig** cmdlet in the Shell to specify a spam quarantine mailbox. The *QuarantineMailbox* parameter uses the SMTP address of the spam quarantine mailbox.

Important:
You must specify the spam quarantine mailbox on all servers that have the Edge Transport server role installed in Active Directory where user mailboxes are located. To specify the spam quarantine mailbox in Active Directory, run the **Set-ContentFilterConfig** cmdlet on a Hub Transport server. You don't have to have content filtering enabled on the Hub Transport server to specify a spam quarantine mailbox in Active Directory.

For more information, see Specify a Spam Quarantine Mailbox.

Configuring the SCL Quarantine Threshold

The SCL quarantine threshold is the value at which a particular message identified as potential spam is delivered to the spam quarantine mailbox. You can set the SCL quarantine threshold to a value from 0 through 9, where 0 is considered less likely to be spam, and 9 is considered most likely to be spam.

For more information about how to adjust SCL thresholds to suit your organization's requirements and how to adjust per-recipient SCL thresholds, see Configure Content Filtering Properties.

Managing the Spam Quarantine Mailbox

When you manage your spam quarantine mailbox, follow these guidelines:

- Release items that have been sent to the spam quarantine mailbox by using the Send Again feature in Outlook to resend the original message. For more information, see Release Quarantined Messages from the Spam Quarantine Mailbox.
- Monitor the spam quarantine mailbox so that the size of the spam quarantine mailbox remains in an acceptable range. The volume of e-mail messages can change because of a larger set of recipients, the natural trend of larger messages, or the threshold on the SCL quarantine action.
- Monitor the spam quarantine mailbox for false positives. If your spam quarantine mailbox includes many false positives, adjust your SCL quarantine

threshold as described in "Adjusting the SCL Quarantine Threshold" later in this topic. For more information about how to determine why false positives are being delivered to the spam quarantine mailbox, see Understanding Anti-Spam Stamps.

- Use the same Outlook profile to recover quarantined messages from the spam quarantine mailbox. Applying permissions to a different Outlook profile to recover messages isn't supported. You can't use a different Outlook profile to recover or release messages from the spam quarantine mailbox.

Important:

NDRs identified as spam are deleted, even if their SCL rating indicates that they should be quarantined. NDRs aren't delivered to the spam quarantine mailbox. To track such messages, use the agent log or the message tracking log. For more information, see Get-AgentLog and Search Message Tracking Logs.

Adjusting the SCL Quarantine Threshold

After you configure the SCL quarantine threshold, periodically monitor the settings and adjust them based on your organization's needs. For example, if too many false positives are filtered into the spam quarantine mailbox, raise the SCL quarantine threshold to a larger number. For more information about how to adjust the SCL quarantine threshold, see Understanding Spam Confidence Level Threshold.

Return to top

Exchange Hosted Services

Spam filtering and quarantine functionality are enhanced by services available from Microsoft Exchange Hosted Services.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

Return to top

1.7.1.5.14 Using Edge Transport Rules to Manage Viruses

Using Edge Transport Rules to Manage Viruses

Transport > Understanding Transport > Understanding Anti-Spam and Antivirus Functionality >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Edge Rules agent and transport rules in Microsoft Exchange Server 2010 to help protect your organization from viruses.

New viruses threaten organizations every day. To minimize the damage caused by viruses, antivirus vendors and administrators must respond to virus threats as soon as possible. Despite a quick response, there will be a gap between the time that a virus threat appears and the time that a solution becomes available. This gap, when a virus threat remains unknown and unresolved, is called a *zero-day virus threat*.

At the same time, viruses that have been circulating on the Internet for many years also continue to pose a significant threat to organizations. Although the majority of these viruses can be identified by antivirus scanners, antivirus scanners may be taken offline by mistake, updated with out-of-date definitions, or experience other problems that make them unavailable.

The transport rules that run on computers that have the Edge Transport server role installed are designed to help you manage and control zero-day virus threats and preexisting or ongoing virus threats.

For more information about transport rules, see the following topics:

- Overview of Transport Rules
- Understanding How Transport Rules Are Applied

Looking for management tasks related to anti-spam and antivirus functionality? See Managing Anti-Spam and Antivirus Features.

Managing Virus Threats

Most viruses contain unique characteristics that identify them as a virus, such as a specific e-mail address in the From message header field, a specific subject, or an attachment. You can configure transport rules to identify potentially harmful messages by these unique characteristics and perform a specific action on them. Available actions include sending the message to a quarantine mailbox, deleting it completely, or adding a warning to the subject.

Identifying Virus Threats

It's important to maximize the number of infected messages that you identify in your perimeter network on Edge Transport servers to reduce the cost of processing the messages after they have entered the Exchange organization. If you can identify an infected message on Edge Transport servers and either reject or delete it, you don't incur the cost of storing the message on your internal servers or the cost of scanning the message for viruses.

When you create a transport rule to identify virus threats, you should examine the reports published about the virus and look for unique characteristics that identify the virus and that could be used in a transport rule. The following list describes some unique characteristics that a virus may contain:

- Limited number of strings in the subject or message body
- Specific e-mail address in either the From header field or To header field
- Specific message header field that has a specific value

Important:

Although you may be able to identify unique characteristics about a particular virus, you must make sure that these characteristics don't match any content that may exist in legitimate messages.

For more information about the types of message content that can be examined by transport rules on an Edge Transport server, see Transport Rule Predicates.

Controlling Virus Threats with Transport Rules

After you have identified the unique characteristics of a virus, you can create a transport rule to perform actions on it. The actions that you perform on specific messages depend

on your organization's policies.

Caution:

If you decide to drop an SMTP connection, delete a message, or reject a message, you can't retrieve it. If you want to prevent the message from being delivered, but don't want to delete it, configure the rule to deliver the message to a quarantine mailbox.

For more information about the actions available on transport rules on an Edge Transport server, see Transport Rule Actions.

For more information about how to manage and configure transport rules used to identify and perform actions on messages that may be infected with viruses, see the following topics:

- Create a Transport Rule
- View a Transport Rule
- Modify a Transport Rule
- Remove a Transport Rule
- Configure a Disclaimer

The following topics provide additional information that will help you manage and enhance transport rules:

- Transport Rule Predicates
- Transport Rule Actions
- Regular Expressions in Transport Rules

Using Exchange Hosted Services

Transport messaging policies are enhanced by services available from Microsoft Exchange Hosted Services.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

1.7.1.6 Understanding Approval Framework

Understanding Approval Framework

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-18*

Approval Framework

Microsoft Exchange uses the *approval framework* for simple decision-making about e-mail messages. For each workflow, the approval framework uses a special mailbox called the *arbitration mailbox*, which is used to store the original message and the decision state during the approval process.

The following workflow is followed by any application that uses the approval framework:

1. The user starts a new workflow process using the workflow application.
2. The workflow application sends an initiation message to the arbitration mailbox.
3. Exchange stores the message in the arbitration mailbox and sends approval requests to the specified decision makers.
4. The specified decision makers either approve or reject the approval request.
5. Exchange marks the decision on the original message that is stored in the arbitration mailbox.
6. The workflow application monitors the arbitration mailbox and acts on the decisions that are marked on the original message.

In Exchange Server 2010, the approval framework is used for the following:

- **Moderated recipients** For more information, see Understanding Moderated Transport.
- **Joining and departing distribution groups** For more information, see step 7 in Configure Distribution Group Properties.

1.7.1.7 Understanding Back Pressure

Understanding Back Pressure

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-02-02*

Back pressure is a system resource monitoring feature of the Microsoft Exchange Transport service that exists on Microsoft Exchange Server 2010 Hub Transport and Edge Transport servers. Exchange transport can detect when vital resources, such as available hard disk space and memory, are under pressure, and take action in an attempt to prevent service unavailability.

Back pressure prevents the system resources from being completely overwhelmed, and Exchange tries to deliver the existing messages. When utilization of the system resource returns to a normal level, the Exchange server gradually resumes normal operation.

In Exchange Server 2007, when a Hub Transport or Edge Transport server is under resource pressure, it rejects incoming connections. In Exchange 2010, incoming connections are accepted, but incoming messages over those connections are either accepted at a slower rate or are rejected. When an SMTP host attempts to make a connection to a Hub Transport or Edge Transport server that's in back pressure, the connection will succeed but when the host issues the MAIL FROM command to submit a message, depending on the resource that's under pressure, Exchange either delays the acknowledgement to the MAIL FROM command or rejects it.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Resources Monitored

The following system resources are monitored as part of the back pressure feature:

- Free space on the hard disk that stores the message queue database.
- Free space on the hard disk that stores the message queue database transaction logs.
- The number of uncommitted message queue database transactions that exist in memory.
- The memory that's used by the EdgeTransport.exe process.
- The memory that's used by all other processes.

For each monitored system resource on a Hub Transport server or Edge Transport server, the following three levels of resource utilization are applied:

- **Normal** The resource isn't overused. The server accepts new connections and messages.
- **Medium** The resource is slightly overused. Back pressure is applied to the server in a limited manner. Mail from senders in the authoritative domain can flow. However, depending on the specific resource under pressure, the server uses tarpitting to delay server response or rejects incoming MAIL FROM commands from other sources.
- **High** The resource is severely overused. Full back pressure is applied. All message flow stops, and the server rejects all new incoming MAIL FROM commands.

The following sections explain how Exchange handles the situation when a specific resource is under pressure.

Free Hard Disk Space for the Message Queue Database

By default, the message queue database is stored at C:\Program Files\Microsoft \Exchange Server\V14\TransportRoles\data\Queue. Exchange monitors the hard disk space utilization for this location. The high level of hard disk space utilization is calculated by using the following formula:

100 * (*hard disk size* - *fixed constant*) / *hard disk size*

The value of *fixed constant* is 500 megabytes (MB).

The results of this formula are expressed as a percentage of the total hard disk space that's being used. The results of the formula are always rounded down to the nearest integer. By default, the medium level of hard disk utilization is 2 percent less than the high level. By default, the normal level of hard disk utilization is 4 percent less than the high level.

For more information about the message queue database, see Understanding Transport Queues.

Free Hard Disk Space for the Message Queue Database Transaction Logs

By default, the message queue database transaction logs are stored at C:\Program Files \Microsoft\ExchangeServer\V14\TransportRoles\data\Queue. Exchange monitors the hard disk space utilization for this location. The EdgeTransport.exe.config file contains a *DatabaseCheckPointDepthMax* parameter that has a default value of 512 MB. This parameter controls the total allowed size of all uncommitted transaction logs that exist on the hard disk. This parameter is used in the formula that calculates hard disk utilization.

Note:

The value of the *DatabaseCheckPointDepthMax* parameter applies to all transport-related Extensible Storage Engine (ESE) databases that exist on the Hub Transport server or Edge Transport server. This would include the message queue database and the IP filter database.

By default, the high level of hard disk utilization is calculated by using the following formula:

100 * (*hard disk size* - Max(5 GB, 3**DatabaseCheckPointDepthMax*)) / *hard disk size*

The results of the formula are always rounded down to the nearest integer. By default, the medium level of hard disk utilization is 2 percent less than the high level. The normal level of hard disk utilization is 4 percent less than the high level.

For more information about the message queue database, see Understanding Transport Queues.

Number of Uncommitted Message Queue Database Transactions in Memory

A list of changes that are made to the message queue database is kept in memory until those changes can be committed to a transaction log. Then the list is committed to the message queue database itself. These outstanding message queue database transactions that are kept in memory are known as *version buckets*. The number of version buckets may increase to unacceptably high levels because of an unexpectedly high volume of incoming messages, spam attacks, problems with the message queue database integrity, or hard disk performance.

When Exchange starts receiving messages, these messages are grouped together in batches and then prepared as version buckets. If an incoming message has a large attachment, it can be separated into multiple batches. These batches that are being processed are known as *batch points*. The number of outstanding batch points can exceed the set thresholds, especially when there's an unexpectedly high volume of incoming messages with large attachments.

When version buckets or batch points are under pressure, the Exchange 2010 transport server will start throttling incoming connections by delaying acknowledgement to incoming messages. Exchange will reduce the rate of inbound message flow by tarpitting, which introduces a delay to the MAIL FROM commands. If the resource pressure condition continues, Exchange will gradually increase the tarpitting delay. After the resource utilization returns to normal, Exchange will gradually start reducing the acknowledgement delay and ease into normal operation. By default, Exchange will start delaying message acknowledgements 10 seconds when under resource pressure. If the resources continue to be under pressure, the delay is increased in 5-second increments up to 55 seconds.

Exchange 2010 keeps a history of version bucket and batch point resource utilization. If the resource utilization doesn't go down to normal level for a specific number of polling intervals, known as the history depth, Exchange will stop the tarpitting delay and start rejecting incoming messages until the resource utilization goes back to normal. By default, the history depths for version buckets and batch points are in 10 and 300 polling intervals respectively.

Memory Used by the EdgeTransport.exe Process

By default, the high level of memory utilization by the EdgeTransport.exe process is calculated by using the following formula:

75 percent of the total physical memory or 1 terabyte, whichever is less

This calculation doesn't include virtual memory that's available on the hard disk in the paging file, or the memory that's used by other processes. The results of this formula are expressed as a percentage of the total memory that's used by the EdgeTransport.exe process. The results of the formula are always rounded down to the nearest integer.

By default, the medium level of memory utilization by the EdgeTransport.exe file is calculated as 73 percent of the total physical memory or 2 percent less than the value of the high level, whichever is less. By default, the normal level of memory utilization by the EdgeTransport.exe file is calculated as 71 percent of the total physical memory or 4 percent less than the value of the high level, whichever is less.

If the memory utilization of the EdgeTransport.exe process is higher than the specified normal level, *garbage collection* is forced. Garbage collection is a process that checks for unused objects that exist in memory, and reclaims the memory that's used by those unused objects.

Exchange 2010 keeps a history of the memory utilization of the EdgeTransport.exe process. If the utilization doesn't go down to normal level for a specific number of polling intervals, known as the history depth, Exchange will start rejecting incoming messages until the resource utilization goes back to normal. By default, the history depth for EdgeTransport.exe memory utilization is 30 polling intervals.

Memory Used by All Processes

By default, the high level of memory utilization by all processes is 94 percent of total physical memory. This value doesn't include virtual memory that's available on the hard disk in the paging file.

When the specified memory utilization level is reached, *message dehydration* occurs. Message dehydration is the act of removing unnecessary elements of queued messages that are cached in memory. Complete messages are cached in memory for enhanced performance. Removal of the MIME content of queued messages from memory reduces the memory that's used at the expense of higher latency because the messages are read directly from the message queue database. By default, message dehydration is enabled.

Return to top

Actions Taken by Exchange Transport When Under Resource Pressure

The following table summarizes the actions taken by Exchange transport when a specific resource is under pressure.

Back pressure actions taken by Hub Transport and Edge Transport servers when responding to resource pressure

Resource under pressure	Utilization level	Actions taken
Hard disk space for message queue database	Medium	• Reject incoming messages from non-Exchange servers • Reject message submissions from Pickup and Replay directories

Hard disk space for message queue database	High	• Reject incoming messages from other Exchange servers • Reject message submissions from the store driver on Mailbox servers (Hub Transport server only) • Reject incoming messages from non-Exchange servers • Reject message submissions from Pickup and Replay directories
Hard disk space for message queue database transaction logs	Medium	• Reject incoming messages from non-Exchange servers • Reject message submissions from Pickup and Replay directories
Hard disk space for message queue database transaction logs	High	• Reject incoming messages from other Exchange servers • Reject message submissions from the store driver on Mailbox servers (Hub Transport server only) • Reject incoming messages from non-Exchange servers • Reject message submissions from Pickup and Replay directories

Version buckets	Medium	• Introduce or increment the tarpitting delay to incoming messages. If normal level isn't reached for the entire version bucket history depth, take the following actions:
		  • Reject incoming messages from non-Exchange servers
		  • Reject message submissions from Pickup and Replay directories

Version buckets	High	• Introduce or increment the tarpitting delay to incoming messages. If normal level isn't reached for the entire version bucket history depth, take the following actions:
		  • Reject incoming messages from other Exchange servers
		  • Reject message submissions from the store driver on Mailbox servers (Hub Transport server only)
		  • Reject incoming messages

		from non-Exchange servers • Reject message submissions from Pickup and Replay directories
Batch point	Medium	• Introduce or increment the tarpitting delay to incoming messages. If normal level isn't reached for the entire batch point history depth, take the following actions: • Reject incoming messages from non-Exchange servers • Reject message submissions from Pickup and Replay directories
Batch point	High	• Introduce or increment the tarpitting delay to incoming messages. If normal level isn't reached for the entire batch point history depth, take the following actions: • Reject incoming messages from other Exchange servers • Reject message submissions from the store driver on Mailbox servers (Hub Transport server only) • Reject incoming messages from non-Exchange servers • Reject message submissions from Pickup and Replay directories
Memory used by EdgeTransport.exe process	Medium	• Reject incoming messages from non-Exchange servers • Reject message submissions from Pickup and Replay directories • Force garbage collection
Memory used by EdgeTransport.exe process	High	• Reject incoming messages from other Exchange servers • Reject message submissions from the store driver on Mailbox servers (Hub Transport server only) • Reject incoming messages from non-Exchange servers • Reject message submissions from Pickup and Replay directories
Memory used by all processes	Medium	• Reject incoming messages from non-Exchange servers • Reject message submissions

		from Pickup and Replay directories • Force garbage collection
Memory used by all processes	High	• Reject incoming messages from other Exchange servers • Reject message submissions from the store driver on Mailbox servers (Hub Transport server only) • Reject incoming messages from non-Exchange servers • Reject message submissions from Pickup and Replay directories • Flush enhanced Domain Name System (DNS) cache from memory • Start message dehydration

Return to top

Back Pressure Configuration Options in the EdgeTransport.exe.config File

All configuration options for back pressure are available in the EdgeTransport.exe.config application configuration file. For more information about the EdgeTransport.exe.config file, see Understanding the EdgeTransport.exe.Config File.

Caution:

These settings are listed as a reference only. We strongly discourage any modifications to the back pressure settings in the EdgeTransport.exe.config file. Modifications to the back pressure settings may result in poor performance or data loss. We recommend that you investigate and correct the root cause of any back pressure events that you may encounter.

Back pressure configuration options

Parameter name	Default value
EnableResourceMonitoring	TRUE
ResourceMonitoringInterval	00:00:02
PercentageDatabaseDiskSpaceUsedHighThreshold	0. This value indicates that the default formula will be used.
PercentageDatabaseDiskSpaceUsedMediumThreshold	0. This value indicates that the actual value is 2 percent less than the value of *PercentageDatabaseDiskSpaceUsedHighThreshold*.
PercentageDatabaseDiskSpaceUsedNormalThreshold	0. This value indicates that the actual value is 2 percent less than the value of *PercentageDatabaseDiskSpaceUsedMediumThreshold*.
PercentageDatabaseLoggingDiskSpaceUsedHighThreshold	0. This value indicates that the default formula will be used.

PercentageDatabaseLoggingDiskSpaceUsedMediumThreshold	0. This value indicates that the actual value is 2 percent less than the value of *PercentageDatabaseLoggingDiskSpaceUsedHighThreshold*.
PercentageDatabaseLoggingDiskSpaceUsedNormalThreshold	0. This value indicates that the actual value is 2 percent less than the value of *PercentageDatabaseLoggingDiskSpaceUsedMediumThreshold*.
PercentagePrivateBytesUsedHighThreshold	0. This value indicates that the default calculation will be used.
PercentagePrivateBytesUsedMediumThreshold	0. This value indicates that the actual value is 2 percent less than the value of *PercentagePrivateBytesUsedHighThreshold*.
PercentagePrivateBytesUsedNormalThreshold	0. This value indicates that the actual value is 2 percent less than the value of *PercentagePrivateBytesUsedMediumThreshold*.
VersionBucketsHighThreshold	200
VersionBucketsMediumThreshold	120
VersionBucketsNormalThreshold	80
VersionBucketsHistoryDepth	10
BatchPointHighThreshold	4000
BatchPointMediumThreshold	2000
BatchPointNormalThreshold	1000
BatchPointHistoryDepth	300
BatchPointUseCostForPressure	TRUE
BatchPointBatchSize	40
BatchPointBatchTimeout	00:00:00.100
BatchPointItemExpiryInterval	00:05:00
SMTPBaseThrottlingDelayInterval	00:00:00
SMTPMaxThrottlingDelayInterval	00:00:55
SMTPStepThrottlingDelayInterval	00:00:05
SMTPStartThrottlingDelayInterval	00:00:10
PercentagePhysicalMemoryUsedLimit	94
DehydrateMessagesUnderMemoryPressure	TRUE
PrivateBytesHistoryDepth	30

Return to top

Back Pressure Logging Information

The following list describes the event log entries that are generated by specific back pressure events in Exchange 2010:

- **Event log entry for an increase in any resource utilization level**
  Event Type: Error
  Event Source: MSExchangeTransport
  Event Category: Resource Manager
  Event ID: 15004
  Description: Resource pressure increased from *Previous Utilization Level* to *Current Utilization Level*.
- **Event log entry for a decrease in any resource utilization level**
  Event Type: Information
  Event Source: MSExchangeTransport
  Event Category: Resource Manager
  Event ID: 15005
  Description: Resource pressure decreased from *Previous Utilization Level* to *Current Utilization Level*.
- **Event log entry for critically low available disk space**
  Event Type: Error
  Event Source: MSExchangeTransport
  Event Category: Resource Manager
  Event ID: 15006
  Description: The Microsoft Exchange Transport service is rejecting messages because available disk space is below the configured threshold. Administrative action may be required to free disk space for the service to continue operations.
- **Event log entry for critically low available memory**
  Event Type: Error
  Event Source: MSExchangeTransport
  Event Category: Resource Manager
  Event ID: 15007
  Description: The Microsoft Exchange Transport service is rejecting message submissions because the service continues to consume more memory than the configured threshold. This may require that this service be restarted to continue normal operation.

Return to top

1.7.1.8 Understanding Content Conversion

Understanding Content Conversion

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-07*

Content conversion is the process of correctly formatting a message for each recipient. The decision to perform content conversion on a message depends on the destination and format of the message being processed. Messages sent to recipients inside the Microsoft Exchange Server organization don't require any content conversion. Only messages sent to external recipients may require content conversion.

In an Exchange Server 2010 organization, content conversion is handled by the categorizer on a server that has the Hub Transport server role installed. Categorization on each message happens after a newly arrived message is put in the Submission queue. In addition to recipient resolution and routing resolution, content conversion is performed on the message before the message is put in a delivery queue. If a single message

contains multiple recipients, content conversion determines the appropriate encoding for each message recipient. On an Edge Transport server, an abbreviated categorization occurs, which doesn't involve content conversion.

Contents

Looking for management tasks related to content conversion? See Managing Transport Servers.

Understanding the Structure of E-mail Messages

To better understand content conversion, you must understand the structure of e-mail messages. An SMTP message is based on plain 7-bit US-ASCII text to compose and send e-mail messages. A standard SMTP message consists of the following elements:

- **Message envelope** The message envelope is defined in RFC 2821. The message envelope contains information required to transmit and deliver the message. Recipients never see the message envelope, because it's generated by the message transmission process and isn't actually part of the message contents.
- **Message contents** The message contents are defined in RFC 2822. The message contents consist of the following elements:
  - **Message header** The message header is a collection of header fields. Header fields consist of a field name, followed by a colon (:) character, followed by a field body, and ended by a carriage return/line feed (CR/LF) character combination.

    A field name must be composed of printable US-ASCII text characters except the colon (:) character. Specifically, ASCII characters that have values from 33 through 57 and 59 through 126 are permitted.

    A field body may be composed of any US-ASCII characters, except for the carriage return (CR) character and the line feed (LF) character. However, a field body may contain the CR/LF character combination when used in *header folding*. Header folding is the separation of a single header field body into multiple lines as described in section 2.2.3 of RFC 2822. Other field body syntax requirements are described in sections 3 and 4 of RFC 2822.
  - **Message body** The message body is a collection of lines of US-ASCII text characters that appears after the message header. The message header and the message body are separated by a blank line that ends with the CR/LF character combination. The message body is optional. Any line of text in the message body must be less than 998 characters. The CR and LF characters can only appear together to indicate the end of a line.

When SMTP messages contain elements that aren't plain US-ASCII text, the message must be encoded to preserve those elements. The MIME standard defines a method of encoding content in messages that isn't text. MIME allows for text in other character sets, attachments without text, multipart message bodies, and header fields in other character

sets. MIME is defined in RFC 2045, RFC 2046, RFC 2047, RFC 2048, and RFC 2077. MIME defines a collection of header fields that specifies additional message attributes. The following table describes some important MIME header fields.

Important MIME header fields

Header field name	Default value	Description
MIME-Version	1.0	This header field is the first MIME header field that appears in a MIME-formatted message. This header field appears after the other standard RFC 2822 header fields, but before any other MIME header fields. MIME-aware e-mail clients use this header field to identify a MIME-encoded message. When this header field is absent, MIME-aware e-mail clients identify the message as plain text.
Content-Type	text/plain	This header field identifies the media type of the message content as described in RFC 2046. A media type consists of a type, a subtype, and one or more optional parameters, such as a *charset*= parameter that defines the MIME character encoding. Types that begin with "x-" aren't standard. Subtypes that begin with "vnd." are vendor-specific. The Internet Assigned Numbers Authority (IANA) maintains a list of registered media types. For more information, see MIME Media Types. The *multipart* media type allows for multiple message parts in the same message by using sections defined by different media types. Some Content-Type field values include text/plain, text/html, multipart/mixed, and multipart/alternative.
Content-Transfer-Encoding	7bit	This header field can describe the following information about a message: • The encoding algorithm used to transform any non-US-ASCII text or binary data that exists in the message body. • An indicator that describes the current condition of the message body. There can be multiple values of the Content-Transfer-Encoding header field in a MIME message. When the Content-Transfer-Encoding header field appears in the message header, it applies to the whole body of the message. When the Content-Transfer-Encoding header field appears in one of the parts of a

		multipart message, it applies only to that part of the message. When an encoding algorithm is applied to the message body data, the message body data is transformed into plain US-ASCII text. This transformation allows the message to travel through older SMTP messaging servers that only support messages in US-ASCII text. The values of the Content-Transfer-Encoding header field that indicate an encoding algorithm was used on the message body are as follows: • **Quoted-printable** This encoding algorithm uses printable US-ASCII characters to encode the message body data. If the original message text is mostly US-ASCII text, Quoted-printable encoding gives somewhat readable and compact results. All printable US-ASCII text characters except the equal sign (=) character can be represented without encoding. • **Base64** This encoding algorithm is based primarily on the privacy-enhanced mail (PEM) standard defined in RFC 1421. Base64 encoding uses the 64-character alphabet encoding algorithm and output padding characters defined by PEM to encode the message body data. A Base64 encoded message is typically 33 percent larger than the original message. Base64 encoding creates a predictable increase in message size and is optimal for binary data and non-US-ASCII text. Typically, you won't see multiple encoding algorithms used in the same message. When no encoding algorithm has been used on the message body, the Content-Transfer-Encoding header field merely identifies the current condition of the message body data. The

		following values of the Content-Transfer-Encoding header field indicate that no encoding algorithms were used on the message body:
		• **7bit** This value indicates that the message body data is already in the RFC 2822 format. Specifically, this means that the following conditions must be true:
		  • All lines of text must be less than 998 characters long.
		  • All characters must be US-ASCII text that have character values from 1 through 127.
		  • The CR and LF characters can only be used together to indicate the end of a line of text.
		The whole message body may be 7bit, or part of the message body in a multipart message may be 7bit. If the multipart message contains other parts that have any binary data or non-US-ASCII text, that part of the message must be encoded using the Quoted-printable or Base64 encoding algorithms.
		Messages that have 7bit bodies can travel between SMTP messaging servers by using the standard DATA command.
		• **8bit** This value indicates that the message body data contains non-US-ASCII characters. Specifically, this means that the following conditions must be true:
		  • All lines of text must be less than 998 characters long.
		  • One or more characters in the message body have values larger than 127.
		  • The CR and LF characters can only be used together to indicate the end of a line of text.
		The whole message body may be 8bit, or part of the message body in a multipart message may be 8bit. If the

		multipart message contains other parts that have binary data, that part of the message must be encoded using the Quoted-printable or Base64 encoding algorithms. Messages that have 8bit bodies can only travel between SMTP messaging servers that support the 8BITMIME SMTP extension as defined in RFC 1652, such as servers running Exchange 2010, Exchange Server 2007, Exchange Server 2003, or Exchange 2000 Server. Specifically, this means that the following conditions must be true: • The 8BITMIME keyword must be advertised in the server's EHLO response. • Messages are still transferred by using the SMTP standard DATA command. However, the BODY=8BITMIME parameter must be added to the end of the MAIL FROM command. • **Binary** This value indicates that the message body contains non-US-ASCII text or binary data. Specifically, this means that the following conditions are true: • Any sequence of characters is allowed. • There is no line length limitation. • Binary message elements don't require encoding. Messages that have Binary bodies can only travel between SMTP messaging servers that support the BINARYMIME SMTP extension as defined in RFC 3030, such as servers running Exchange 2010, Exchange 2007, Exchange 2003, or Exchange 2000. Specifically, this means that the following conditions must be true: • The BINARYMIME keyword

		must be advertised in the server's EHLO response. • The BINARYMIME SMTP extension can only be used with the CHUNKING SMTP extension. *Chunking* enables large message bodies to be sent in multiple, smaller chunks. Chunking is also defined in RFC 3030. The CHUNKING keyword must also be advertised in the server's EHLO response. • Messages are transferred using the BDAT command instead of the standard DATA command. • The *BODY=BINARYMIME* parameter must be added to the end of the MAIL FROM command when the message has a message body. The values 7bit, 8bit, and Binary never exist together in the same multipart message. The values are mutually exclusive. The Quoted-printable or Base64 values may appear in a 7bit or 8bit multipart message body, but never in a Binary message body. If a multipart message body contains different parts composed of 7bit and 8bit content, the whole message is classified as 8bit. If a multipart message body contains different parts composed of 7bit, 8bit, and Binary content, the whole message is classified as Binary.
Content-Disposition	Attachment	This header field instructs a MIME-enabled e-mail client on how it should display an attached file, and is described in RFC 2183. The values of this field may be Inline or Attachment. When the value of this field is Inline, the attachment is displayed in the message body. When the value of this field is Attachment, the attached file appears as a regular attachment separate from the message body. Other parameters are available when the value is Attachment, such as Filename, Creation-date, and Size.

Exchange 2010 and Outlook Message

Formats

The following list describes the basic message formats available in Exchange 2010 and Microsoft Outlook:

- **Plain text** A plain text message uses only US-ASCII text as described in RFC 2822. The message can't contain different fonts or other text formatting. The following two formats can be used for a plain text message:
  - The message headers and the message body are composed of US-ASCII text. Attachments must be encoded by using *Uuencode*. Uuencode represents Unix-to-Unix encoding and defines an encoding algorithm to store binary attachments in the body of an e-mail message by using US-ASCII text characters.
  - The message is MIME-encoded with a Content-Type value of text/plain, and a Content-Transfer-Encoding value of 7bit for the text parts of a multipart message. Any message attachments are encoded by using Quoted-printable or Base64 encoding. By default, when you compose and send a plain text message in Outlook, the message is MIME-encoded with a Content-Type value of text/plain.
- **HTML** An HTML message supports text formatting, background images, tables, bullet points, and other graphical elements. By definition, an HTML-formatted message must be MIME-encoded to preserve these formatting elements.
- **Rich text format (RTF)** RTF supports text formatting and other graphical elements. RTF is synonymous with the Transport Neutral Encapsulation Format (TNEF). TNEF and RTF can be used interchangeably.
  Only Outlook and a few other MAPI e-mail clients understand RTF messages. MAPI is a Microsoft-developed messaging architecture that enables multiple applications to interact with different messaging systems across a variety of hardware platforms. MAPI is built on the Component Object Model (COM) architecture. Outlook uses MAPI to communicate with mailboxes on a computer running Exchange 2010 that has the Mailbox server role installed.
  The rich text message format is completely different from the rich text document format available in Microsoft Word.
- **TNEF** TNEF is a Microsoft-specific format for encapsulating MAPI message properties. A TNEF message contains a plain text version of the message and an attachment that packages the original formatted version of the message. Typically, this attachment is named Winmail.dat. The Winmail.dat attachment includes the following information:
  - Original formatted version of the message, including, for example, fonts, text sizes, and text colors
  - OLE objects, including, for example, embedded pictures or embedded Microsoft Office documents
  - Special Outlook features, including, for example, custom forms, voting buttons, or meeting requests
  - Regular message attachments that were in the original message

  The resulting plain text message can be represented in the following formats:
  - RFC 2822-compliant message composed of only US-ASCII text with a Winmail.dat attachment encoded in Uuencode
  - Multipart MIME-encoded message that has a Winmail.dat attachment

  A MAPI-compliant e-mail client that fully understands TNEF, such as Outlook, processes the Winmail.dat attachment and displays the original message content without ever displaying the Winmail.dat attachment. An e-mail client that doesn't understand TNEF may present a TNEF message in any of the following ways:
  - The plain text version of the message is displayed, and the message contains an attachment named Winmail.dat, Win.dat, or some other generic name such as Att*nnnnn*.dat or Att*nnnnn*.eml where the *nnnnn* placeholder represents a random number.

- The plain text version of the message is displayed. The TNEF attachment is ignored or removed. The result is a plain text message.
- Messaging servers that understand TNEF can be configured to remove TNEF attachments from incoming messages. The result is a plain text message. Moreover, some e-mail clients such as Microsoft Outlook Express may not understand TNEF, but recognize and ignore TNEF attachments. The result is a plain text message.

There are third-party utilities that can help convert Winmail.dat attachments. TNEF is understood by Exchange 2010, Exchange 2007, Exchange 2003, Exchange 2000, and Exchange Server version 5.5. TNEF messages are transferred between SMTP messaging servers by using the standard DATA command verb. TNEF is automatically used by Exchange based on the following situations:

- **Exchange 2003** If the Exchange organization is in mixed mode, TNEF is used for messages transferred between Exchange servers in different routing groups.
- **Exchange 2000** TNEF is used for messages transferred between Exchange servers in different routing groups.

- **Summary Transport Neutral Encapsulation Format (STNEF)** STNEF is equivalent to TNEF. However, STNEF messages are encoded differently than TNEF messages. Specifically, STNEF messages are always MIME-encoded and always have a Content-Transfer-Encoding value of Binary. Therefore, there's no plain text representation of the message, and there's no distinct Winmail.dat attachment contained in the body of the message. The whole message is represented by using only binary data. Messages that have a Content-Transfer-Encoding value of Binary can only be transferred between SMTP messaging servers that support and advertise the BINARYMIME and CHUNKING SMTP extensions as defined in RFC 3030. The messages are always transferred between SMTP messaging by using the BDAT command, instead of the standard DATA command.
  STNEF is understood by Exchange 2010, Exchange 2007, Exchange 2003, and Exchange 2000. STNEF is automatically used by Exchange if the following conditions are true:
  - **Exchange 2010** STNEF is used for all messages transferred between Exchange servers in the organization.
  - **Exchange 2007** STNEF is used for all messages transferred between Exchange servers in the organization.
  - **Exchange 2003** If the Exchange organization is in native mode, STNEF is used for all messages transferred between Exchange servers in the organization.
  - **Exchange 2000** STNEF is used for messages transferred between Exchange servers in the same routing group. An unsupported hotfix also enables Exchange 2000 to use STNEF for messages transferred between Exchange servers in different routing groups.

  Exchange never sends STNEF messages to external recipients. Only TNEF messages can be sent to recipients outside the Exchange organization.

Elements of Content Conversion

Content conversion is the act of correctly formatting a message for each external recipient. This conversion is performed by the categorizer on a Hub Transport server.

The content conversion options that you can set in an Exchange organization can be described in the following categories:

- **TNEF conversion options** These conversion options specify whether TNEF should be preserved or removed from messages that leave the Exchange organization.
- **Message encoding options** These options specify message encoding options, such as MIME and non-MIME character sets, message encoding, and

attachment formats.

These conversion and encoding options are independent of one another. For example, whether TNEF messages can leave the Exchange organization isn't related to the MIME encoding settings or plain text encoding settings of those messages.

You can specify the content conversion at various levels of the Exchange organization as described in the following list:

- **Remote domain settings** Remote domains define the settings for outgoing message transfers between the Exchange 2010 organization and domains outside the Active Directory forest. Even if you don't create remote domain entries for specific domains, there's a predefined remote domain named Default that applies to all remote address spaces (*).
- **Mail user and mail contact settings** Mail users resemble mail contacts—both have external e-mail addresses and contain information about people outside the Exchange organization. The main difference is mail users have security contexts that can be used to log on to the Active Directory domain and access resources to which they have been granted permission.
- **Outlook settings** In Outlook, you can set the message formatting and encoding options described in the following list:
  - **Message format** You can set the default message format for all messages. You can override the default message format as you compose a specific message.
  - **Internet message format** You can control whether TNEF messages are sent to remote recipients or whether they are first converted to a more compatible format. You can also specify various message encoding options for messages sent to remote recipients. These settings don't apply to messages sent to recipients in the Exchange organization.
  - **Internet recipient message format** You can control whether TNEF messages are sent to specific recipients or whether they are first converted to a more compatible format. You can set the conversion options for specific contacts in your Contacts folder, and you can override the conversion options for a specific recipient in the To, Cc, or Bcc fields as you compose a message. These conversion options aren't available for recipients in the Exchange organization.
  - **Internet recipient message encoding options** You can control the MIME or plain text encoding options for specific contacts in your Contacts folder, and you can override the conversion options for a specific recipient in the To, Cc, or Bcc fields as you compose a message. These conversion options aren't available for recipients in the Exchange organization.
  - **International options** You can control the character sets used in messages.

TNEF Conversion Options

You can specify the TNEF conversion options at the following levels:

- Remote domain settings
- Mail user and mail contact settings
- Outlook settings, including:
  - Message format
  - Internet message format
  - Internet recipient message format

For detailed information, see TNEF Conversion Options.

Message Encoding Options

You can specify the message options at the following levels:

- Remote domain settings
- Mail user and mail contact settings
- Outlook settings, including:

- Message format
- Internet message
- Internet recipient message format
- Message character set encoding options

For detailed information, see Message Encoding Options.

Content Conversion Performed by the Store Driver

The store driver also performs content conversion. The store driver exists on Hub Transport servers to transport messages between mailboxes on Mailbox servers and the Submission queue. Specifically, the store driver transports messages from the sender's Outbox to the Submission queue on the Hub Transport server, and the store driver transports the messages from the Submission queue on the Hub Transport server to the recipient's Inbox. The store driver converts all outgoing messages from MAPI and converts all incoming messages to MAPI. Content conversion tracing captures these store driver conversion failures.

For more information, see Content Conversion Tracing.

1.7.1.8.1 TNEF Conversion Options

TNEF Conversion Options

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The content conversion options that you can set in an Exchange organization can be described in the following categories:

- **TNEF conversion options** These conversion options specify whether Transport Neutral Encapsulation Format (TNEF) should be preserved or removed from messages that leave the Exchange organization.
- **Message encoding options** These options, such as MIME and non-MIME character sets, specify message encoding and attachment formats.

This topic describes the TNEF conversion options that you can specify at the following levels:

- Remote domain settings
- Mail user and mail contact settings
- Microsoft Outlook settings
  - Message format
  - Internet message format
  - Internet recipient message format

TNEF Conversion Options for Messages Sent to Remote Domains

When you configure TNEF conversion options for a remote domain, those TNEF conversion options are applied to all messages sent to that domain. For remote domains in your organization, you have the following configuration options for TNEF conversion:

- **TNEF use enabled** TNEF is used for all messages sent to the remote domain.
- **TNEF use disabled** TNEF is never used for any messages sent to the remote domain.
- **Unspecified** TNEF messages aren't specifically allowed or prevented for recipients in the remote domain. Whether TNEF messages are sent to recipients in the remote domain depends on the specific setting on the mail contact or mail user, or the setting specified by the sender in Outlook. This is the default setting.

In Microsoft Exchange 2010, you can set the TNEF conversion options for messages sent to a remote domain in the Exchange Management Shell or on the **Remote Domains** tab in the Exchange Management Console (EMC). For more information about configuring TNEF options for a remote domain, see the following topics:

- Configure Remote Domain Properties
- Set-RemoteDomain

TNEF Conversion Options for Messages Sent to Mail Users and Mail Contacts

When you configure TNEF conversion options for a mail contact or a mail user, those TNEF conversion options are applied to all messages sent to that specific recipient. For mail contacts and mail users in your organization, you have the following configuration options for TNEF conversion:

- **Always** TNEF is used for all messages sent to the recipient.
- **Never** TNEF is never used for any messages sent to the recipient.
- **Use default settings** TNEF messages aren't specifically allowed or prevented for the mail user or mail contact. Whether TNEF messages are sent to the recipient depends on the specific setting for the corresponding remote domain or the setting specified by the sender in Outlook. This is the default setting.

Note:

In both the EMC and the Shell, the TNEF conversion settings are referred to as **MAPI rich text format**.

You can set the TNEF conversion options for messages sent to mail users and mail contacts in the Shell or in the **Recipient Configuration** node in the EMC. For more information about configuring TNEF options for these recipient types, see the following topics:

- Configure Mail Contact Properties
- Configure Mail User Properties
- Set-MailContact
- Set-MailUser

TNEF Conversion Options for Messages Available in Outlook

Senders can control the default TNEF message conversion options for TNEF messages sent to all recipients outside the Exchange organization. These options are called *Internet message format* options. The options only apply to remote recipients, and not to recipients in the Exchange organization.

Note:

The following options define how messages containing Outlook rich text are handled when sent to external recipients. If the message format you're using is HTML or plain text, these settings don’t apply.

You have the following TNEF conversion options in Outlook:

- **Convert to HTML format** This is the default option. Any TNEF messages sent to remote recipients are converted to HTML. Any formatting in the message should closely resemble the original message. MIME-encoded HTML messages are supported by many, but not all, e-mail clients.
- **Convert to Plain Text format** Any TNEF messages sent to remote recipients are converted to plain text. Any formatting in the message is lost.
- **Send using Outlook Rich Text Format** Any TNEF messages sent to remote recipients remain TNEF messages.

These options can be configured in Outlook by navigating to **Tools > Options > Mail Format**, and then clicking **Internet Format**.

Senders can also control the default TNEF message conversion options for TNEF messages sent to specific recipients outside the Exchange organization. These options are called *Internet recipient message format* options. The options only apply to remote recipients stored in your Contacts folder, and not to recipients in the Exchange organization. You have the following TNEF conversion options for remote recipients in your Contacts folder:

- **Let Outlook decide the best sending format** This is the default setting. This setting forces Outlook to use the TNEF conversion option that's specified by the default Internet format. The possible values are **Convert to HTML format**, **Convert to Plain Text format**, or **Send using Outlook Rich Text Format**. Therefore, the TNEF message may be left as TNEF, converted to HTML, or converted to plain text. If you want to make sure that the TNEF message remains TNEF for this recipient, you should change this setting from **Let Outlook decide the best sending forma**t to **Send using Outlook Rich Text format**.
- **Send Plain Text only** Any TNEF messages sent to the recipient are converted to plain text. Any formatting in the message is lost.
- **Send using Outlook Rich Text format** Any TNEF messages sent to remote recipients remain TNEF messages.

These options can be configured for a contact in Outlook by opening that contact and then double-clicking the **E-mail** field and selecting **Internet format**.

Order of Precedence for TNEF Conversion Options

Exchange 2010 uses the order of precedence as described in the following list to determine the TNEF conversion options for outgoing messages sent to recipients outside the Exchange organization:

1. Outlook settings
2. Mail user or mail contact settings
3. Remote domain settings

The list specifies the order of precedence from lowest to highest. A setting made at a higher level overrides a setting made at a lower level.

Exchange never sends Summary Transport Neutral Encoding Format (STNEF) messages to external recipients. Only TNEF messages can be sent to recipients outside the Exchange organization.

1.7.1.8.2 Message Encoding Options

Message Encoding Options

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The content conversion options that you can set in an Exchange organization can be described in the following categories:

- **TNEF conversion options** These conversion options specify whether Transport Neutral Encapsulation Format (TNEF) should be preserved or removed from messages that leave the Exchange organization.
- **Message encoding options** These options specify message encoding options, such as MIME and non-MIME character sets, message encoding, and attachment formats.

This topic describes message encoding options that you can specify at the following levels:

- Remote domain settings
- Mail user and mail contact settings
- Microsoft Outlook settings
  - Message format
  - Internet message format
  - Internet recipient message format
  - Message character set encoding options

Message Encoding Options for Messages Sent to Remote Domains

When you configure message encoding options for a remote domain, the specific settings are applied for all messages sent to that domain. For remote domains in your organization, you have the following configuration options for message encoding:

- **Content type** You can specify the content type for MIME messages sent to the recipients in the remote domain. You can use of the following settings:
  - **MimeHtmlText** All messages are converted to MIME messages that use HTML formatting, unless the original message is a text message. If the original message is a text message, the outgoing message will be a MIME message that uses text formatting. This is the default setting.
  - **MimeText** All messages are converted to MIME messages that use text formatting.
  - **MimeHtml** All messages are converted to MIME messages that use HTML formatting.

  Note:
  You can only configure this setting using the Exchange Management Shell.
- **Line wrap size** You can specify the maximum number of characters that can exist on a single line of text in the body of the e-mail message. Older e-mail client applications may prefer 78 characters per line.
- **MIME character set** The character set that you specify will only be used for MIME messages that don't have their own character set specified. Setting this parameter won't overwrite character sets that are already specified in the outgoing mail. For a list of valid character set names, see Supported Character Sets for Remote Domain Configuration.
- **Non-MIME character set** This parameter is used if either of the following conditions are true:

- Incoming messages from a remote domain are missing the value of the *charset*= parameter in the MIME Content-Type: header field.
- Outgoing messages to a remote domain are missing the value of the MIME character set.

For a list of valid character set names, see Supported Character Sets for Remote Domain Configuration.

In Microsoft Exchange Server 2010, you can set the message encoding options for recipients in remote domains in the Shell or on the **Remote Domains** tab in the Exchange Management Console (EMC). For more information, see the following topics:

- Configure Remote Domain Properties
- Set-RemoteDomain

Message Encoding Options for Mail Users and Mail Contacts

When you configure message encoding options for a mail contact or a mail user, that option is applied to all messages sent to that specific recipient. For mail contacts and mail users in your organization, you have the following configuration options for message encoding:

- **UsePreferMessageFormat** This parameter specifies whether the message format settings configured for the mail contact override the global settings configured for the remote domain. If you disable this setting, Exchange ignores other message encoding options for this recipient and the message encoding is determined by the configuration of the remote domain or the settings configured by the message sender.
- **MessageFormat** This parameter specifies the message format. You can either specify Text or Mime as the message format. The value of this setting is dependent on the *MessageBodyFormat* parameter. If the message body format is Html or TextAndHtml, you must set this parameter to Mime.
- **MessageBodyFormat** This parameter specifies the message body format. You can specify Text, Html, or TextAndHtml. The value of this setting is dependent on the *MessageFormat* parameter. If the message format is Text, you must also set this parameter to Text.
- **MacAttachmentFormat** This parameter specifies the Apple Macintosh operating system attachment format for messages. You can specify BinHex, UuEncode, AppleSingle, or AppleDouble. The value of this setting is dependent on the *MessageFormat* parameter. If the message format is set to Text, you must set this parameter to either BinHex or UuEncode. If the message format is set to Mime, you must set this parameter to BinHex, AppleSingle or AppleDouble.

You must use the Shell to set the message encoding options for mail users and mail contacts. For more information, see the following topics:

- Enable-MailContact
- New-MailContact
- Set-MailContact
- Enable-MailUser
- New-MailUser
- Set-MailUser

Message Encoding Options Available in Outlook

As a sender, you can specify message encoding options in Outlook at any of the following stages:

- By configuring the default message format to be either plain text or HTML.
- By setting the message format as you're composing it to either plain text or HTML using the **Format** area in the **Options** tab.
- By configuring the message encoding options for messages that are sent to all recipients outside the Exchange organization. These options are called *Internet message format* options. The options only apply to remote recipients, and not to recipients in the Exchange organization. These options can be configured in Outlook by navigating to the **Tools > Options > Mail Format**, and clicking **Internet Format**.
- By configuring the message encoding options for messages that are sent to specific recipients outside the Exchange organization. These options are called *Internet recipient message format* options. The options only apply to remote recipients in your Contacts folder, and not to recipients in the Exchange organization. These options can be configured for a contact in Outlook by opening that contact and then double-clicking the **E-mail** field and selecting **Send Options**.

By default, Outlook uses automatic character set message encoding by scanning the whole text of the outgoing message to determine the appropriate encoding to use for the message. This setting applies to messages that you send to Internet recipients and recipients in the Exchange organization. However, you can bypass this and specify a preferred encoding for outgoing messages. These options can be configured in Outlook by navigating to **Tools > Options > Mail Format**, and clicking **International Options.**

Order of Precedence for Message Encoding Options

Exchange 2010 uses the order of precedence as described in the following list to determine the message encoding options for outgoing messages sent to recipients outside the Exchange organization:

1. Remote domain settings
2. Outlook settings
3. Mail user or mail contact settings

The list specifies the order of precedence from lowest to highest. A setting made at a higher level may override a setting made at a lower level.

The following table describes the order of precedence from lowest priority to highest priority for message character set encoding options.

Order of precedence from lowest priority to highest priority for message character set encoding options

Source	Parameter	Values
Set-RemoteDomain	*CharacterSet*	Specified
Set-RemoteDomain	*NonMimeCharacterSet*	Specified
Outlook setting	Message character set encoding	• Auto-select • Specified

The value of the *NonMimeCharacterSet* parameter from the **Set-RemoteDomain** cmdlet is used to assign a character set to the following types of messages:

- Outgoing messages to a configured remote domain that don't contain a specified character set
- Incoming messages from a configured remote domain that don't contain a specified character set

The value of the Windows ANSI code page for the Hub Transport server is used to assign a character set to the following types of messages:

- Internal messages that don't contain a specified character set
- Internal messages that contain a specified character set, but don't contain a specified server code page

If a message contains a specified but invalid character set, the Hub Transport server tries to replace the invalid character set with a valid character set.

The following table describes the order of precedence from lowest priority to highest priority for plain text message encoding options.

Order of precedence from lowest priority to highest priority for plain text message encoding options

Source	Parameter	Values
Set-RemoteDomain	*LineWrapSize*	• From 0 through 132 • unlimited
Outlook settings	Message format	Plain text
Outlook settings	Internet message format	Plain text options: • Encode attachments in UuEncode format when you send a plain text message • Automatically wrap text at *nn* characters
Outlook settings	Internet recipient message format	Plain text format: • Encode attachments in UuEncode attachment format • Use BinHex Mac attachment format
Set-MailUser **Set-MailContact**	*UsePreferMessageFormat*	• `$true` • `$false` If the value is `$false` or if the recipient isn't defined as a mail user or mail contact in the Exchange organization, the mail user or mail contact settings are ignored.
Set-MailUser **Set-MailContact**	*MessageFormat*	Text
Set-MailUser **Set-MailContact**	*MessageBodyFormat*	Text
Set-MailUser **Set-MailContact**	*MacAttachmentFormat*	• BinHex • UuEncode

The following table describes the order of precedence from lowest priority to highest priority for MIME message encoding options.

Order of precedence from lowest priority to highest priority for MIME

message encoding options

Source	Parameter	Values
Set-RemoteDomain	*ContentType*	• `MimeHtmlText` • `MimeText` • `MimeHtml`
Outlook settings	Message format	• Plain text • HTML
Outlook settings	Internet recipient message format	MIME message format • Plain text • Include both plain text and HTML • HTML

Set-MailUser
 	
Set-MailContact
	UsePreferMessageFormat	`$true`
		
		`$false`
		
		If the value is `$false` or if the recipient isn't defined as a mail user or mail contact in the Exchange organization, the mail user or mail contact settings are ignored.

Set-MailUser **Set-MailContact**	*MessageFormat*	• Text • Mime
Set-MailUser **Set-MailContact**	*MessageBodyFormat*	• `Text` • `Html` • `TextAndHtml`
Set-MailUser **Set-MailContact**	*MacAttachmentFormat*	• BinHex • AppleSingle • AppleDouble

1.7.1.8.3 Content Conversion Tracing

Content Conversion Tracing

Transport > Understanding Transport > Understanding Content Conversion >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-06*

Content conversion tracing captures failures in the content conversion that's performed by the store driver on inbound and outbound messages on a computer running Microsoft Exchange Server 2010 that has the Hub Transport server role installed.

The categorizer on a Hub Transport server is responsible for the content conversion of all messages sent to external recipients. However, the store driver on a Hub Transport server is responsible for the content conversion of messages sent to and from mailbox recipients. Specifically, the store driver must convert outbound messages from mailbox users from MAPI to MIME. The store driver must also convert inbound messages for mailbox users from MIME to MAPI. Content conversion tracing is responsible for capturing these MAPI conversion failures. Content conversion tracing doesn't capture any content conversion failures that the categorizer encounters as it converts messages sent to

external recipients.

Contents

Configuring Content Conversion Tracing

Content conversion tracing is controlled by the following parameters in the **Set-TransportServer** cmdlet in the Exchange Management Shell:

- *ContentConversionTracingEnabled* This parameter enables or disables content conversion. Valid values for this parameter are `$True` and `$False`. The default value is `$False`. If the Exchange organization contains multiple Hub Transport servers, you must enable content conversion tracing on each Hub Transport server responsible for delivery of messages to Mailbox servers.
- *PipelineTracingPath* Although this parameter is associated with pipeline tracing, it also specifies the root location of the content conversion tracing files. By default, the value of the *PipelineTracingPath* parameter is C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\PipelineTracing. The path must be local to the Exchange 2010 computer.

Content conversion creates a folder named ContentConversionTracing inside the path specified by the *PipelineTracingPath* parameter. Inside the ContentConversionTracing folder, content conversion creates two subfolders: InboundFailures and OutboundFailures. The InboundFailures folder contains the information from inbound message content conversion failures. The OutboundFailures folder contains the information from outbound message content conversion failures.

The maximum size for all the files in the InboundFailures folder is 128 megabytes (MB). The maximum size for all the files in the OutboundFailures folder is 128 MB. The content conversion tracing directories don't use circular logging to remove old files, depending on the age or size of the files. As soon as the maximum size for a folder is reached, content conversion tracing stops writing information to the folder. If you want to make sure that the maximum folder size limits aren't exceeded, you can create a scheduled task that periodically moves the content conversion tracing files to a different location.

The permissions required on the folders and subfolders used in content conversion tracing are as follows:

- Administrators: Full Control
- Network Service: Full Control
- System: Full Control

Caution:

Content conversion tracing copies the complete contents of e-mail messages. To avoid unwanted exposure of confidential information, you must set appropriate security permissions on the location of the content conversion tracing files.

Return to top

How Content Conversion Tracing Works

When the content conversion of an inbound message fails, a delivery status notification (DSN) that has the status code 5.6.0 is sent to the message sender. If content conversion tracing is enabled, the failure information is recorded at the time that the 5.6.0 DSN message is generated. Each content conversion error generates two separate files.

A content conversion error that occurs when an inbound message is converted from MIME to MAPI generates the following two files in the InboundFailures folder:

- **<GUID>.eml** This file contains the failed message in text format.
- **<GUID>.txt** This file contains the exception description, conversion results, conversion options, and message size limits imposed on all messages by the store driver.

A content conversion error that occurs when an outbound message is converted from MAPI to MIME generates the following two files in the OutboundFailures folder:

- **<GUID>.msg** This file contains the failed message in the Microsoft Outlook message format.
- **<GUID>.txt** This file contains the exception description, conversion results, conversion options, and message size limits imposed on all messages by the store driver.

The placeholder *<GUID>* is the same in both file names. Each content conversion error generates a different GUID that's used in the file names of the corresponding message and text files. An example of a GUID that's used in the file names is `038b930e-61fd-4bfd-b9b4-0374c18b73f7`.

Return to top

Considerations for Content Conversion Tracing

You can leave content conversion tracing enabled for proactive monitoring. Or, you can enable content conversion tracing to troubleshoot a specific failure event. You can usually reproduce inbound content conversion failures by asking the recipient of the 5.6.0 DSN message to resend the original message.

Inbound content conversion failures are the most common. Some of the reasons for inbound content conversion errors include the following:

- **Violations of message size limits** These message size limits are imposed by the store driver to help prevent denial of service attacks (DoS). These message limits are listed in the *<GUID>*.txt file. These message limits include the following:
  - **MaxMimeTextHeaderLength** This limit specifies the maximum number of text characters that can be used in a MIME header. The value is 2000.
  - **MaxMimeSubjectLength** This limit specifies the maximum number of text characters that can be used in the subject line. The value is 255.
  - **MSize** This limit specifies the maximum message size. The value is 2147483647 bytes.
  - **MaxMimeRecipients** This limit specifies the total number of recipients allowed in the To, Cc, and Bcc fields. The value is 12288.
  - **MaxRecipientPropertyLength** This limit specifies the maximum number of text characters that can be used in a recipient description. The value is 1000.
  - **MaxBodyPartsTotal** This limit specifies the maximum number of message parts that can be used in a MIME multipart message. The value is 250.
  - **MaxEmbeddedMessageDepth** This limit specifies the maximum number of forwarded messages that can exist in a message. The value is 30.

  For more information about configurable message size limits used in Hub

Transport servers or Edge Transport servers, see Understanding Message Size Limits.

- **Failure to convert an inbound iCalendar message to a meeting request** RFC 2445 defines iCalendar as a standard for calendar data exchange. Specific causes of the conversion failure include the following:
  - Incorrect use of iCalendar by the sending agent.
  - Constructs of iCalendar that can't be supported by the Outlook or Exchange calendar schema.

  Conversion failures of iCalendar don't result in the sender receiving a 5.6.0 DSN message. Instead, the message is delivered with an attached .ics file that contains the iCalendar message body.
- **Failures caused by badly formatted MIME messages** Unsolicited commercial e-mail or spam messages may have formatting errors in the message header, such as unmatched quotation marks in recipient descriptions. A much smaller number of failures caused by badly formatted MIME messages are considered bugs.

Outbound content conversion failures are much less common than inbound failures. When outbound failures occur, they are usually caused by Exchange code bugs or corrupted message content.

Return to top

1.7.1.9 Understanding Delivery Agents

Understanding Delivery Agents

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-17*

Delivery agents are responsible for delivering messages addressed to foreign systems that don't use the SMTP protocol. Each delivery agent works with a Delivery Agent connector. When a message is routed to a Delivery Agent connector, the associated delivery agent performs the content conversion and message delivery. Delivery agents are a significant improvement over Foreign connectors in handling non-SMTP messages in your Exchange organization.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Delivery Agents

A delivery agent is a custom agent that can:

- Establish a connection to the foreign system for message delivery.

- Retrieve messages from the remote delivery queues on Hub Transport servers.
- Deliver messages to the foreign system.
- Provide acknowledgement for each successful message delivery.

While the Foreign connector architecture remains in Microsoft Exchange Server 2010, we recommend using delivery agents for routing messages to non-SMTP systems whenever possible. Delivery agents provide the following benefits:

- They allow queue management of messages routed to foreign systems using the familiar queue management tools.
- Because the messages no longer need to be written to and read from the file system, message delivery performance is improved.
- They provide access to message properties with rich events for agent developers.
- Development time for a delivery agent is faster than implementing a Foreign connector because the delivery agent can use the message representation and management features of Exchange.
- You can now be sure that the messages are delivered to the foreign system as opposed to just being written to the Drop directory.
- The usage of Delivery Agent connectors allows service level agreement (SLA) analysis because it's now possible to track the latency of message delivery to the foreign system.

Return to top

Adding Delivery Agents to Your Organization

To use a delivery agent in your organization, you have to complete the following:

- Acquire the delivery agent. Typically, delivery agents are written by third parties. Exchange 2010 comes with only one Delivery Agent connector by default: the Text Messaging Delivery Agent connector.
- Install the delivery agent on your Hub Transport servers that will act as source servers for the Delivery Agent connectors.
- Create a Delivery Agent connector for the specific protocol.

When all of these steps are completed, messages to the foreign systems will be routed through the Delivery Agent connectors and processed by the delivery agent.

Delivery Agent Connectors

Don't confuse the Delivery Agent connectors with the actual delivery agents. Delivery Agent connectors are configured to make routing decisions. The Delivery Agent connectors handle queuing messages to be processed by the delivery agents; much like Send connectors or Routing Group connectors are used for SMTP delivery.

Delivery Agent connectors ensure that the messages destined to the foreign system are inserted into the appropriate queues on the Hub Transport servers that are used for delivering messages to the foreign systems. After the messages are queued, Connection Manager invokes the delivery agent to handle the actual delivery of the message to the foreign system.

Return to top

Events Used by Delivery Agents

Delivery agents act on the following events raised by the Connection Manager

component:

- **OnOpenConnection** This event is raised when there are messages in the queue to be delivered to the foreign system. It notifies the delivery agent to initiate a connection to the foreign system.
- **OnDeliverMailItem** This event notifies the delivery agent to retrieve the next item from the queue.
- **OnCloseConnection** This event is raised when there are no more messages in the queue to be delivered to the foreign system. It notifies the delivery agent to close the connection to the foreign system.

In a typical delivery scenario, the following interaction between Connection Manager and the delivery agent takes place:

1. Connection Manager detects messages queued for delivery to the foreign system.
2. Connection Manager invokes the delivery agent using the **OnOpenConnection** event.
3. The delivery agent establishes a connection with the foreign system. After the connection is established, it notifies Connection Manager using the **RegisterConnection** method.
4. Connection Manager raises the **OnDeliverMailItem** event.
5. The delivery agent retrieves the message from the queue and delivers it to the foreign system. After delivery is complete, it provides acknowledgement to Connection Manager.
6. If there are additional messages in the queue, steps 4 and 5 are repeated until all messages are delivered.
7. Connection Manager raises the **OnCloseConnection** event.
8. The delivery agent closes the connection with the foreign system and notifies Connection Manager using the **UnRegisterConnection** method.

Retry Situations

The following are the situations where messages or the entire Delivery Agent connector queue would end up in the Retry state:

- After Connection Manager raises the **OnOpenConnection** event, if no delivery agents respond with the **RegisterConnection** method, the entire queue for that Delivery Agent connector is put into retry.
- If the delivery agent doesn't provide an acknowledgement for a specific message, that message is put into retry.

Return to top

1.7.1.10 Understanding DSNs and NDRs

Understanding DSNs and NDRs

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-05-20*

This topic describes how to read and interpret non-delivery report (NDR) delivery status notification (DSN) messages in Microsoft Exchange Server 2010.

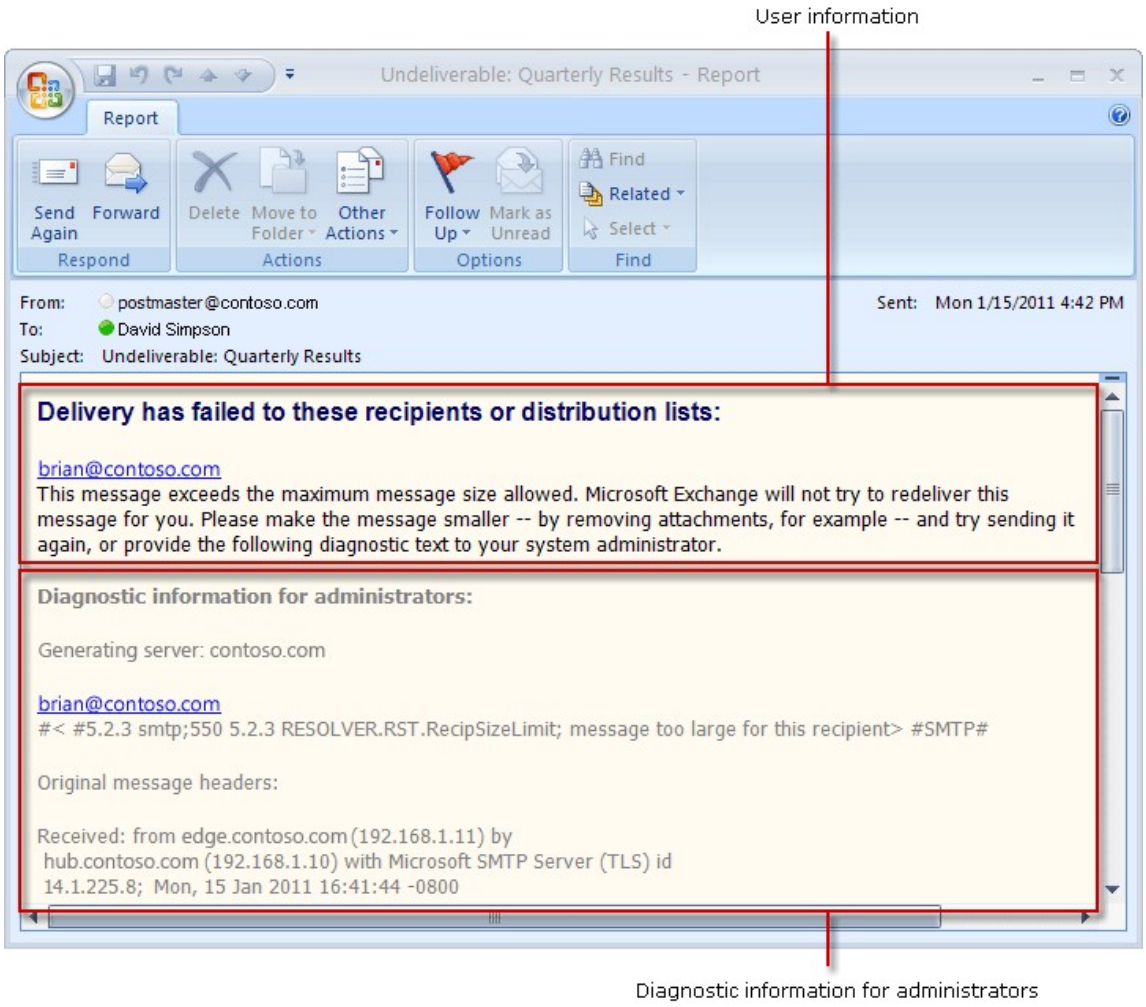
NDR Sections

In Exchange 2010, NDRs have been designed to make them easier to read and understand by both end-users and administrators. Information that is displayed in an NDR

is separated into the following two areas:

- A user information section
- A **Diagnostic information for administrators** section

The information in each section is targeted to the readers of that section. The user information section appears first and contains feedback to help the user understand in nontechnical terms why the delivery of the message failed. The **Diagnostic information for administrators** section provides deeper technical information such as the original message headers, to help e-mail administrators troubleshoot a delivery issue that may exist. The following figure shows the user information section and **Diagnostic information for administrators** section of an NDR.



User Information Section

The user information section of an NDR generated by Exchange 2010 contains information that you want to communicate to an end-user who has sent a message that is later returned with an NDR. The text that is displayed in this section is inserted by the Exchange server that generated the NDR.

The text in the user information section is designed to help the end-user determine why the message was rejected and how to resend the message successfully if the message should be resent. When applicable, the fully qualified domain name (FQDN) of the server that rejected the message is included in the user information section. If delivery fails to more than one recipient, the e-mail address of each recipient is listed and the reason for the failure is included in the space below the recipient's e-mail address.

You can modify the text in the user information section by using the **New-SystemMessage** cmdlet. By creating a custom message, you can provide specific information to end-users, such as a telephone number to use to contact the helpdesk department or a hyperlink to use to obtain self-service support. For more information about how to customize the text that is displayed in the user information section, Create a Custom DSN Message.

Diagnostic Information for Administrators

The **Diagnostic information for administrators** section contains more detailed information about the specific error that occurred during delivery of the message, the server that generated the NDR, and the server that rejected the message. The following fields are present in most NDRs and are visible in the "NDR sections" figure earlier in this topic:

- **Generating server** The generating server is the SMTP server that created the NDR. The generating server takes the enhanced status code that is explained later in this topic. This code creates an easy-to-read NDR. If no remote server is listed below the e-mail address of the sender in the **Diagnostic information for administrators** section, the generating server is also the server that rejected the original e-mail message. If message delivery fails when the message is sent to another recipient in the Exchange organization, the same server typically rejects the original message and generates the NDR.
- **Rejected recipient** The rejected recipient is the e-mail address of the recipient to which delivery of the original message failed. If delivery to more than one recipient has failed, the e-mail address for each recipient is listed. The rejected recipient field also contains the following sub-fields for each e-mail address listed:
  - **Remote server** The remote server field contains the FQDN of the server that rejects delivery of the message during the Simple Mail Transfer Protocol (SMTP) conversation. The remote server field is only populated when delivery has been attempted to a remote server, and that delivery attempt has been rejected before the receiving server successfully acknowledges the message after the message body is sent. If the original message is successfully acknowledged by the receiving server and is then rejected because of content restrictions, for example, the remote server field is not populated.
  - **Enhanced status code** The enhanced status code is the code returned by the server that rejected the original message. The enhanced status code indicates why the original message was rejected. The enhanced status code is not rewritten by Exchange 2007 but is used to determine what text to display in the user information section. The enhanced status codes you're most likely to encounter are listed in "Common Enhanced Status Codes" later in this topic. For a detailed list of enhanced status codes, see RFC 3463.
  - **SMTP response** The SMTP response is the machine readable text returned by the server that rejected the original message. The SMTP response typically contains a short string that provides an explanation of the enhanced status code that is also returned. The SMTP response is not rewritten by Exchange 2010. Additionally, this response is always presented in US-ASCII format.
- **Original message headers** The original message headers section contains the message headers of the rejected message. These headers can provide useful diagnostic information, such as information that can help you determine the path that the message took before it was rejected or whether the **To** field matches the e-mail address that is specified in the rejected recipient field.

Examples of NDR Messages

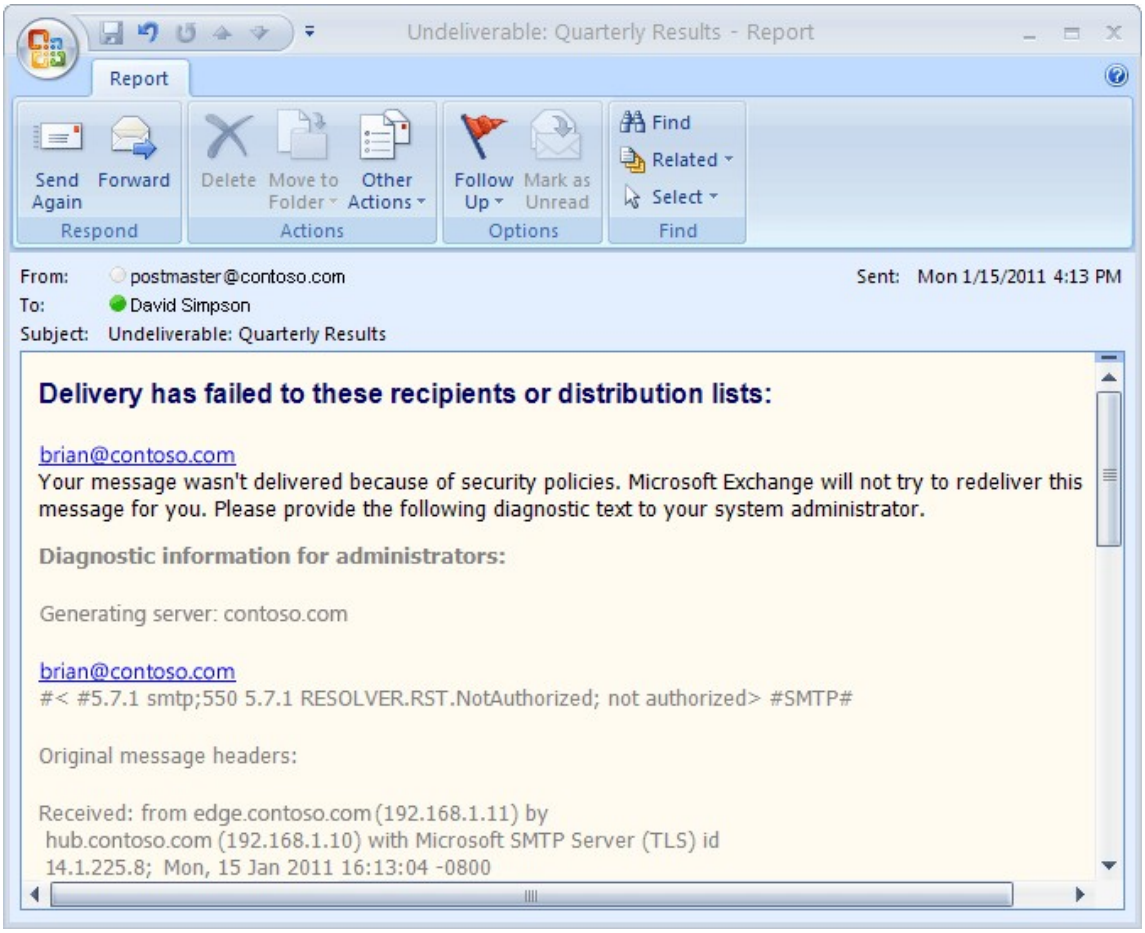
The following sections provide examples of two ways that NDR messages can be

generated:

- By the same server
- By different servers

NDR Generated and Original Message Rejected by the Same Server

The following example shows what happens when a remote e-mail organization accepts delivery of an e-mail message through an Edge Transport server, and then rejects that message because of a policy restriction on the recipient's mailbox. In this case, the sender is not allowed to send messages to the recipient. Edge Transport servers do not perform message size validation so the Edge Transport server in this example accepts the message because it has a valid recipient address and the message does not violate another content restrictions. Because the remote e-mail organization accepts the whole message, including the message contents, the remote e-mail organization is responsible for rejecting the message and for generating the NDR message to be sent to the sender.

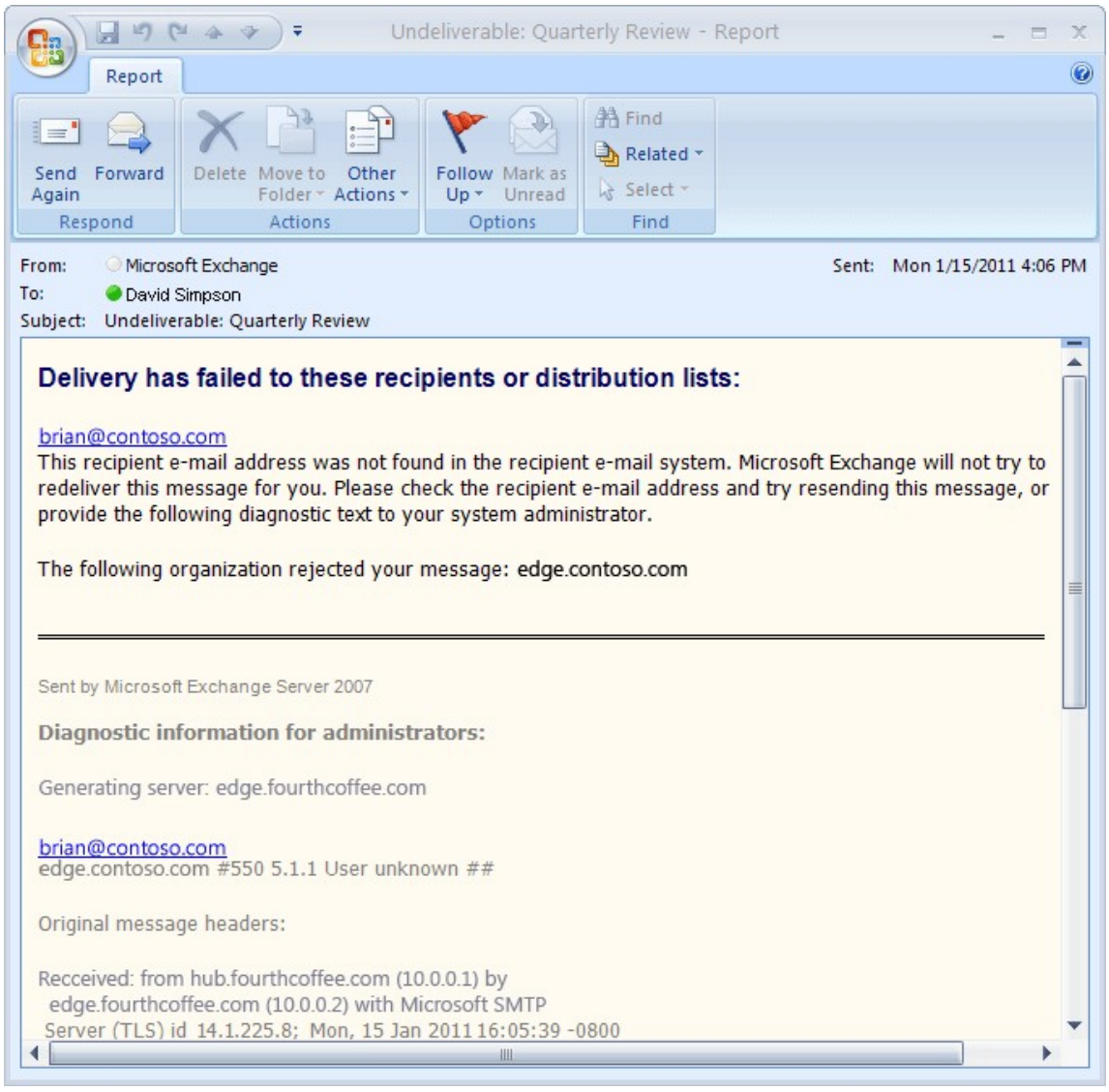


Also, messages that are rejected when they are sent to recipients that are part of the same Exchange 2010 organization are typically rejected by the same e-mail server that generates the NDR message. Messages sent to local recipients can be rejected for various reasons, such as mailboxes that have exceeded their quota, lack of authorization to send messages to the recipient address, or hardware failures that result in an extended loss of connectivity to other servers in the organization.

In both situations, no remote server is included under the e-mail address of the recipients listed in the NDR message.

NDR Generated and Original Message Rejected by Different Servers

The following example shows what happens when a remote e-mail organization rejects delivery of an e-mail message before it ever accepts the message. In this example, the remote server rejects the message and returns an enhanced status code to the local sending server because the specified recipient does not exist. The rejection happens before the receiving server ever acknowledges the message. Because the receiving server doesn't successfully acknowledge the message, the receiving server is not responsible for the message. Therefore, the local sending server generates the NDR message and sends it to the sender of the original message.



Common Enhanced Status Codes

The following table contains a list of the enhanced status codes that are returned in NDRs for the most common message delivery failures.

Enhanced status code	Description	Possible cause	Additional information

4.3.1	Insufficient system resources	An out-of-memory error occurred. A resource problem, such as a full disk, can cause this problem. Instead of getting a disk full error, you might be getting an out-of- memory error.	Ensure that your Exchange server has enough disk storage.
4.3.2	System not accepting network messages	This NDR is generated when a queue has been frozen.	You can resolve this condition by unfreezing the queue.
4.4.1	Connection timed out	The destination server is not responding. Transient network conditions can cause this error. The Exchange server tries automatically to connect to the server again and deliver the mail. If delivery fails after multiple attempts, an NDR with a permanent failure code is generated.	Monitor the situation. This may be a transient problem that may correct itself.
4.4.2	Connection dropped	A connection dropped between the servers. Transient network conditions or a server that is experiencing problems can cause this error. The sending server will retry delivery of the message for a specific time period, and then generate further status reports.	Monitor the situation as the server retries delivery. This may be a transient problem that may correct itself. This situation can also occur when the message size limit for the connection is reached, or if the message submission rate for the client IP address has exceeded the configured limit.
4.4.7	Message expired	The message in the queue has expired. The sending server tried to relay or deliver the message, but the action was not completed before the message expiration time occurred. This message can also indicate that a message header limit has been reached on a remote server, or some other protocol time-out occurred while communicating with the remote server.	This message usually indicates an issue on the receiving server. Check the validity of the recipient address, and determine if the receiving server is configured correctly to receive messages. You may have to reduce the number of recipients in the message header for the host about which you are receiving this error. If you send the message again, it is placed in the queue again. If the receiving server is available, the message is delivered.
5.0.0	HELO / EHLO	This situation is a permanent failure. Possible	Some potential resolutions include:

	requires domain address	causes include: • There is no route for the given address space; for example, an SMTP connector is configured, but this address does not match. • DNS returned an authoritative host that was not found for the domain. • An SMTP error occurred.	• On one or more SMTP connectors, add an asterisk (*) value as the SMTP address space. • Verify that DNS is working.
5.1.0	Sender denied	This NDR is caused by a general failure (bad address failure). An e-mail address or another attribute could not be found in Active Directory. Contact entries without the **targetAddress** attribute set can cause this problem. Another possible cause could be that the **homeMDB** attribute of a user could not be determined. The **homeMDB** attribute corresponds to the Exchange server on which the user's mailbox resides. Another common cause of this NDR is if you used Microsoft Office Outlook to save your e-mail message as a file, and then someone opened the message offline and replied to the message. The message property only preserves the **legacyExchangeDN** attribute when Outlook delivers the message, and therefore the lookup could fail.	Either the recipient address is incorrectly formatted, or the recipient could not be correctly resolved. The first step in resolving this error is to check the recipient address and send the message again.
5.1.1	Bad destination mailbox address	This failure may be caused by the following conditions: • The recipient e-mail address was entered incorrectly by the sender. • No recipient exists in the destination e-mail system.	This error typically occurs when the sender of the message incorrectly enters the e-mail address of the recipient. The sender should check the recipient's e-mail address and send again. This error can also occur if the recipient e-mail address was correct in the past but has changed or has been

		• The recipient mailbox has been moved and the Microsoft Office Outlook recipient cache on the sender's computer has not updated. • An invalid legacy domain name (DN) exists for the recipient mailbox Active Directory.	removed from the destination e-mail system. If the sender of the message is in the same Exchange organization as the recipient, and the recipient mailbox still exists, determine whether the recipient mailbox has been relocated to a new e-mail server. If this is the case, Outlook may not have updated the recipient cache correctly. Instruct the sender to remove the recipient address from sender's Outlook recipient cache and then create a new message. Resending the original message will result in the same failure. Other issues may cause this error, such as an invalid legacy distinguished name (DN) in Active Directory. Examine and correct the legacy DN of the recipient's mailbox. Then instruct the sender to remove the recipient address from sender's Outlook recipient cache and then create a new message. Resending the original message will result in the same failure.
5.1.2	Invalid X.400 address	The recipient has a non-SMTP address that can't be matched to a destination. The address does not appear to be local, and there are no connectors configured with address spaces that contain the recipient's address.	Verify that the recipient's address was entered correctly. If the recipient's address is in a non-SMTP e-mail system that you specifically want to provide mail delivery to, you will need to add the appropriate type of connector to your topology and configure it to provide service to the recipient's e-mail system.
5.1.3	Invalid recipient address	This message indicates that the recipient address appears incorrectly on the message.	Either the recipient address is formatted incorrectly, or the recipient could not be correctly resolved. The first step in resolving this error is to check the recipient address and send the message again.

			Also, examine the SMTP recipient policy and ensure that each mail domain for which you want to accept mail appears correctly.
5.1.4	Destination mailbox address ambiguous	Two or more recipients in the Exchange organization have the same address.	This error typically occurs because of a misconfiguration in Active Directory. Possibly because of replication problems, two recipient objects in Active Directory have the same SMTP address or Exchange Server (EX) address.
5.1.7	Invalid address	The sender has a malformed or missing SMTP address, the **mail** attribute in the directory service. The mail item cannot be delivered without a valid **mail** attribute.	Check the sender directory structure, and determine if the **mail** attribute exists.
5.2.1	Mailbox cannot be accessed	The mailbox cannot be accessed. The mailbox may be offline, disabled, or the message has been quarantined by a rule.	Check to see if the recipient database is online, the recipient mailbox is disabled, or the message has been quarantined.
5.2.2	Mailbox full	The recipient's mailbox has exceeded its storage quota and is no longer able to accept new messages.	This error occurs when the recipient's mailbox has exceeded its storage quota. The recipient must reduce the size of the mailbox or the administrator must increase the storage quota before delivery can be successful. If the recipient resides in the local Exchange 2010 organization, see Configure Storage Quotas for a Mailbox.
5.2.3	Message too large	The message is too large, and the local quota is exceeded. For example, a remote Exchange user might have a restriction on the maximum size of an incoming message.	Send the message again without attachments, or set the server or the client-side limit to allow a larger message size limit.
5.2.4	Mailing list expansion problem	The recipient is a misconfigured dynamic distribution list. Either the filter string or the base DN of the dynamic distribution list is invalid.	Set the categorizer event logging level to at least the minimum level, and send another message to the dynamic distribution list. Check the application event log for a 6025 event or a

			6026 event detailing which attribute is misconfigured on the dynamic distribution list object.
5.3.3	Unrecognized command	When the Exchange remote server reaches capacity of its disk storage to hold mail, it could respond with this NDR. This error usually occurs when the sending server is sending mail with an ESMTP BDAT command. This error also indicates a possible SMTP protocol error.	Ensure that the remote server has enough storage capacity to hold mail. Check the SMTP log.
5.3.4	Message too big for system	The message exceeds a size limit configured on a transport or mailbox database and can't be accepted. This failure can be generated by either the sending e-mail system or the recipient e-mail system.	This error occurs when the size of the message that was sent by the sender exceeds the maximum allowed message size when passing through a transport component or mailbox database. The sender must reduce the size of the message for the message to be successfully delivered. For more information about how to configure message size limits in an Exchange 2010 organization, see Configure Message Size Limits for a Mailbox or a Mail-Enabled Public Folder.
5.3.5	System incorrectly configured	A mail-looping situation was detected, which means that the server is configured to loop mail back to itself.	Check the configuration of the server's connectors for loops, and ensure that each connector is defined by a unique incoming port. If there are multiple virtual servers, ensure that none are set to "All Unassigned."
5.4.4	Invalid arguments	This NDR occurs if no route exists for message delivery, or if the categorizer could not determine the next-hop destination.	Check that the domain name specified is valid, and that a mail exchanger (MX) record exists.
5.4.6	Routing loop detected	A configuration error has caused an e-mail loop. By default, after 20 iterations of an e-mail loop, Exchange interrupts the loop and generates an NDR to the sender of the message.	This error occurs when the delivery of a message generates another message in response. That message then generates a third message, and the process is repeated, creating a loop. To help protect against exhausting system

			resources, Exchange interrupts the mail loop after 20 iterations. Mail loops are typically created because of a configuration error on the sending mail server, the receiving mail server, or both. Check the mailbox rules configuration of the recipient and sender to determine whether automatic message forwarding is enabled.
5.5.2	Send hello first	A generic SMTP error occurs when SMTP commands are sent out of sequence. For example, a server attempts to send an AUTH (authorization) command before identifying itself with an EHLO command. It is possible that this error can also occur when the system disk is full.	View the SMTP Log or a Netmon trace, and ensure that there is adequate disk storage and virtual memory available.
5.5.3	Too many recipients	The combined total of recipients on the To, Cc, and Bcc lines of the message exceeds the total number of recipients allowed in a single message.	This error occurs when the sender has included too many recipients on the message. The sender must reduce the number of recipient addresses in the message or the maximum number of recipients must be increased to allow the message to be successfully delivered. To configure the maximum number of recipients that can be included in a message, use the *RecipientLimits* parameter on the **Set-Mailbox** cmdlet. For more information, see Set-Mailbox.
5.5.4	Invalid domain name	The message contains either an invalid sender or an incorrect recipient address format. One possible cause is that the recipient address format might contain characters that are not conforming to Internet standards.	Check the recipient address for nonstandard characters.
5.5.6	Invalid message content	This message indicates a possible protocol error.	Check Event Log for possible failures.

5.7.1	Delivery not authorized	The sender of the message is not allowed to send messages to the recipient.	This error occurs when the sender tries to send a message to a recipient but the sender is not authorized to do this. This frequently occurs when a sender tries to send messages to a distribution group that has been configured to accept messages only from members of that distribution group or other authorized senders. The sender must request permission to send messages to the recipient. On an Exchange 2010 server, the following cmdlets accept the *AcceptMessageOnlyFrom* and *AcceptMessagesOnlyFromDLMembers* parameters. These enable you to determine who is authorized to send messages to the recipients that you configure: • Set-Mailbox • Set-MailUser • Set-MailContact • Set-DistributionGroup • Set-DynamicDistributionGroup This error can also occur if an Exchange 2010 transport rule rejects a message because the message matched conditions that are configured on the transport rule. For more information about transport rules, see Understanding Transport Rules.
5.7.1	Unable to relay	The sending e-mail system is not allowed to send a message to an e-mail system where that e-mail system is not the final destination of the message.	This error occurs when the sending e-mail system tries to send an anonymous message to a receiving e-mail system, and the receiving e-mail system does not accept messages for the domain or domains specified in one or more of the recipients. The following are the most common reasons for this error: • A third party tries to use a

			receiving e-mail system to send spam, and the receiving e-mail system rejects the attempt. By the nature of spam, the sender's e-mail address may have been forged and the resulting NDR could have been sent to the unsuspecting sender's e-mail address. It is difficult to avoid this situation. • A domain name service (DNS) mail exchanger (MX) record for a domain points to a receiving e-mail system where that domain is not accepted. The administrator responsible for the specific domain name must correct the DNS MX record or configure the receiving e-mail system to accept messages sent to that domain, or both. For more information about how to accept messages for a domain, see Managing Accepted and Remote Domains. • A sending e-mail system or client that should use the receiving e-mail system to relay messages does not have the correct permissions to do this. For more information

			about transport permissions, see Understanding Permissions.
5.7.1	Client was not authenticated	The sending e-mail system did not authenticate with the receiving e-mail system. The receiving e-mail system requires authentication before message submission.	This error occurs when the receiving server must be authenticated before message submission, and the sending e-mail system has not authenticated with the receiving e-mail system. The sending e-mail system administrator must configure the sending e-mail system to authenticate with the receiving e-mail system for delivery to be successful. This error can also occur if you try to accept anonymous messages from the Internet by using a Hub Transport server that has not been configured to do this. We recommend that you put an Edge Transport server in a perimeter network between the Hub Transport server and the Internet. For more information, see the following topics: Configure Internet Mail Flow Directly Through a Hub Transport Server Configure Internet Mail Flow Through a Subscribed Edge Transport Server
5.7.3	Not Authorized	The sender prohibited reassignment to the alternate recipient.	

1.7.1.10.1 Supported Locales for Use with System Messages

Supported Locales for Use with System Messages

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-11*

The following table lists the supported language locales available for use with the **New-SystemMessage** and **Set-SystemMessage** cmdlets.

Supported language locales for system messages

Language	Locale	Language	Locale
Arabic	AR	Japanese	JA
Basque	EU	Kazakh	KK
Bulgarian	BG	Korean	KO
Catalan	CA	Latvian	LV
Chinese (Simplified)	ZH-CHS	Lithuanian	LT
Chinese (Traditional)	ZH-CHT	Malay	MS
Croatian	HR	Norwegian	NB
Czech	CS	Persian	FA
Danish	DA	Polish	PL
Dutch	NL	Portuguese	PT
English	EN	Portuguese	PT-PT
Estonian	ET	Romanian	RO
Filipino (Tagalog)	FIL	Russian	RU
Finnish	FI	Serbian (Cyrillic)	SR-SP-CYRL
French	FR	Serbian (Latin)	SR-SP-LATN
Galician	GL	Slovak	SK
German	DE	Slovenian	SL
Greek	EL	Spanish	ES
Hebrew	HE	Swedish	SV
Hindi	HI	Thai	TH
Hungarian	HU	Turkish	TR
Icelandic	IS	Ukrainian	UK
Indonesian	ID	Urdu	UR
Italian	IT	Vietnamese	VI

You can use the **New-SystemMessage** cmdlet to create customized delivery status notification (DSN) and quota messages in various languages. For more information about creating customized DSNs, see Create a Custom DSN Message.

1.7.1.10.2 DSN Message Identity

DSN Message Identity

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-18*

You can identify a customized delivery status notification (DSN) message based on its syntax. The identity is the customized DSN message's GUID or a string that consists of the following values:

- **Locale** This variable specifies the locale of the language that the DSN message is displayed in. For a list of locale codes that you can use with the **New-SystemMessage** command, see Supported Locales for Use with System Messages.
- **Internal or External** This variable specifies whether the DSN message is sent only to senders who are part of the internal Microsoft Exchange Server 2010 organization or also to senders outside the Exchange 2010 organization. You can use the Internal option when you want to include a specific e-mail contact or resolution in DSN messages sent to internal senders, but don't want to expose that information to senders outside your organization.
- **DSN code** This variable specifies the DSN code of the customized DSN message.

The syntax of the DSN message identity is `<Locale>\<Internal or External>\<DSN code>`.

For each DSN code, you can create more than one customized DSN message, which can target internal senders or external senders, and different locales. For example, the following table shows some of the possible configurations for the DSN code 5.1.2 and the corresponding DSN message identities.

Example DSN configurations and identities

DSN configuration	DSN identity
Display DSN messages to internal senders with an English (en) locale	En\Internal\5.1.2
Display DSN messages to external senders with an English (en) locale	En\External\5.1.2
Display DSN messages to internal senders with a Japanese (ja) locale	Ja\Internal\5.1.2
Display DSN messages to external senders with a Japanese (ja) locale	Ja\External\5.1.2

1.7.1.10.3 DSN Message Text

DSN Message Text

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-25*

You can include text in a customized delivery status notification (DSN) message in Microsoft Exchange Server 2010, and you can format that text in HTML.

You can include any information that you want to display to the recipient of the DSN message. For example, you can include a detailed description of the DSN, contact information for your help desk, and a link to your support department's Web site. Each DSN message can contain a maximum of 512 characters.

Because DSN messages can be displayed in HTML, you can embed HTML formatting tags in the DSN text. For example, if you want to make some text in your DSN message bold, enclose the text in <B> and </B> HTML tags. The following table provides some examples of valid HTML tags that can be used in DSN message text.

Valid HTML tags for use in DSN messages

HTML tag	Description
<B>	Bold begin
</B>	Bold end
<A HREF="url">	Hyperlink begin
</A>	Hyperlink end
 	Link break
<EM>	Italic begin
</EM>	Italic end
<P>	Paragraph begin
</P>	Paragraph end

Note:

By default, Exchange 2010 sends HTML DSN messages, but you can configure whether Exchange 2010 sends HTML DSN messages to internal senders, external senders, or both. To configure this behavior, modify the *InternalDsnSendHtml* parameter and the *ExternalDsnSendHtml* parameter with the **Set-TransportServer** command.
If the *InternalDsnSendHtml* parameter is set to `$false`, Exchange 2010 suppresses HTML tags in DSN messages sent to internal senders. If the *ExternalDsnSendHtml* parameter is set to `$false`, Exchange 2010 suppresses HTML tags in DSN messages sent to external senders.

The following characters that Exchange 2010 uses in DSN message text have special meanings:

- Greater than sign (>)
- Less than sign (<)
- Ampersand (&)
- Quotation marks (")

These characters are used to determine where HTML tags begin and end, and where text that should be displayed to senders starts and stops. If you want to display these characters in your DSN messages, you must use the escape codes in the following table.

For example, if you want to display the message `"Please contact the Help Desk at <1234>."`, you must add `"Please contact the Help Desk at <1234>."` to the DSN message text.

DSN message character escape codes

Escape code	Character
<	<
>	>
"	"

&amp;	&

Important:
If you include an HTML tag in your DSN message text that contains quotation marks ("), such as <A HREF="url">, you must use single quotation marks (') around the whole DSN message text. You will receive an error message if you use double quotation marks around the whole DSN message text and around an HTML tag.

1.7.1.11 Understanding DNS Query Failure Sensitivity

Understanding DNS Query Failure Sensitivity

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-23*

You can adjust the DNS query sensitivity for slightly faster message delivery when DNS errors are encountered for the destination domain. However, depending on the DNS errors, this adjustment may cause delivery failures in certain circumstances.

DNS Queries and Remote Message Delivery

In a typical Microsoft Exchange Server 2010 organization, an Edge Transport server that's subscribed to the organization is responsible for delivering messages to external recipients. This Edge Transport server is responsible for accepting the outgoing messages from the Hub Transport server in the organization. The subscribed Edge Transport server must be able to find a destination messaging server that accepts mail for the external recipients. Depending on the destination, the messages are put in one or more remote delivery queues as they await delivery to the remote recipients. For more information about delivery queues, see Understanding Transport Queues.

The Edge Transport server queries the configured external DNS servers to find the DNS records that are required to deliver the message. The DNS servers that are configured for external DNS lookups are queried in the order in which they're listed. If one of the DNS servers is unavailable, the query goes to the next DNS server on the list. The DNS servers are queried for the following information:

- **Mail exchange (MX) records for the domain part of the external recipient** The MX record contains the fully qualified domain name (FQDN) of the messaging server that's responsible for accepting messages for the domain, and a preference value for that messaging server. A lower preference value indicates a preferred messaging server. The preference value is important if the domain has more than one MX record. To optimize fault tolerance, most organizations use multiple messaging servers and multiple MX records that have different preference values.
- **Address (A) records for the destination messaging servers** Every messaging server that's used in an MX record should have a corresponding A record. The A record is used to find the IP address of the destination messaging server. The subscribed Edge Transport server uses the IP address to open an SMTP connection with the destination messaging server. Although it's technically possible to use the FQDN of a canonical name (CNAME) record in an MX record, this practice violates RFC 974, RFC 1034, RFC 1912, and RFC 2181, and is therefore not supported by most messaging servers.
  The required combination of iterative DNS queries and recursive DNS queries

that start with a root DNS server is used to resolve the FQDN of the messaging server that's found in the MX record into an IP address.

In Exchange 2010, there's a DNS query limit that's not configurable of 5 seconds for each DNS server, and a one-minute limit for the entire DNS query.

Potential DNS Problems

Even when the external DNS settings on the Microsoft Exchange Transport server are configured correctly, problems with the DNS records for a specific domain or problems with any of the DNS servers that are used to find the authoritative DNS server for a specific domain may still occur. Generally, these problems are beyond your control and need to be resolved by the parties that own those DNS servers. These DNS-related errors may be caused by one or more of the following conditions:

- Invalid DNS records for the destination domain
- Problems with DNS server utilization
- Problems with DNS server replication

In Exchange 2010, when a DNS query results in errors, the query continues to the next DNS server only if that DNS server hasn't already returned an error for the current query.

Exchange 2010 also includes a parameter in the EdgeTransport.exe.config application configuration file that's named *DnsFaultTolerance*. This parameter has the following values:

- **Lenient** When the DNS query encounters a combination of valid MX records and invalid MX records, the DNS query continues until the DNS query time-out value of one minute is reached. The invalid MX records are discarded, and the valid MX record that has the lowest preference value is used to deliver the message to the destination messaging server.
- **Normal** When the DNS query first encounters an invalid MX record, any resolved MX records that have a preference value that's greater than or equal to the invalid MX records are immediately discarded. The remaining MX record that has the lowest preference value is used to deliver the message to the destination messaging server without waiting for the whole DNS query to time out. Although this behavior may result in faster message delivery, the potential drawback of this behavior is the DNS query may have no valid MX records if the following conditions are true:
  - The invalid MX record is the first MX record for the destination domain.
  - The valid MX records have the same precedence value as the invalid MX records.

The default value of the *DnsFaultTolerance* parameter on a Hub Transport server or Edge Transport server in Exchange 2010 is `Lenient`.

In both `Normal` mode and `Lenient` mode, the results of the DNS query for an invalid MX record are never cached. The next time that a DNS query is executed, it will try to resolve the MX records for the destination domain.

For more information about the EdgeTransport.exe.config file, see Understanding the EdgeTransport.exe.Config File.

1.7.1.12 Understanding Domain Security

Understanding Domain Security

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Domain Security refers to the set of functionality in Microsoft Exchange Server 2010 and Microsoft Office Outlook 2007 that provides a relatively low-cost alternative to S/MIME or other message-level security solutions. The purpose of the Domain Security feature set is to provide administrators a way to manage secured message paths over the Internet with business partners. After these secured message paths are configured, messages that have successfully traveled over the secured path from an authenticated sender are displayed to users as **Domain Secured** in the Outlook and Microsoft Office Outlook Web App interface.

Domain Security uses mutual Transport Layer Security (TLS) authentication to provide session-based authentication and encryption. Mutual TLS authentication differs from TLS as it's usually implemented. Typically, when TLS is implemented, the client verifies that the connection securely connects to the intended server by validating the server's certificate. This is received as part of TLS negotiation. In this scenario, the client authenticates the server before the client transmits data. However, the server doesn't authenticate the session with the client.

With mutual TLS authentication, each server verifies the connection with the other server by validating a certificate that's provided by that other server. In this scenario, where messages are received from external domains over verified connections in an Exchange 2010 environment, Outlook 2007 displays a Domain Secured icon.

Important:

It's beyond the scope of this topic to provide a detailed explanation of cryptography and certificate technologies and concepts. Before you deploy any security solution that uses cryptography and digital certificates, we recommend that you understand the basic concepts of trust, authentication, encryption, and public and private key exchange as they relate to cryptography. For more information, see the references listed at the end of this topic.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Validation of TLS Certificates

To understand the overall security and resulting trustworthiness of any mutual TLS transmission, you must understand how the underlying TLS certificate is validated.

Exchange 2010 includes a set of cmdlets to create, request, and manage TLS certificates. By default, these certificates are self-signed. A self-signed certificate is a certificate that's signed by its own creator. In Exchange 2010, the self-signed certificate is created by the computer running Microsoft Exchange by using the underlying Microsoft Windows Cryptography API (CAPI). Because the certificates are self-signed, the resulting certificates are less trustworthy than certificates that are generated by public key infrastructure (PKI) or a third-party certification authority (CA). Therefore, we recommend that you use self-signed certificates for internal mail only. Alternatively, if the receiving organizations with which you exchange domain-secured e-mail manually add your self-signed certificate to the trusted root certificate store in each of their inbound Edge Transport servers, the self-signed certificates are trusted explicitly.

For connections that traverse the Internet, it's a best practice to generate TLS certificates with a PKI or third-party CA. Generating TLS keys with a trusted PKI or third-party CA reduces the overall management of Domain Security. For more information about the options regarding trusted certificates and Domain Security, see Using PKI on the Edge Transport Server for Domain Security.

You can use the Exchange 2010 certificate cmdlets to generate certificate requests for your own PKI or for third-party CAs. For more information, see Understanding TLS Certificates.

For more information about how to configure Domain Security, see the following:

- Using Domain Security: Configuring Mutual TLS
- Domain Security White Paper

Using Exchange Hosted Services

Message-level security is enhanced by or is also available as a service from Microsoft Exchange Hosted Services.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

Resources

Housley, Russ and Tim Polk. *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*. New York: John Wiley & Son, Inc., 2001.

Adams, Carlisle and Steve Lloyd. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition. New York: John Wiley & Son, Inc., 1996.

Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure

1.7.1.12.1 Using Domain Security: Configuring Mutual TLS

Using Domain Security: Configuring Mutual TLS

Transport > Understanding Transport > Understanding Domain Security >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

This topic explains how to configure mutual Transport Layer Security (TLS) for Domain

Security, the set of functionality in Microsoft Exchange Server 2010 and Microsoft Office Outlook 2007 that provides a relatively low-cost alternative to S/MIME and other message-level security solutions.

For the purposes of this scenario, this topic explains how Exchange administrators at a fictitious company, Contoso, configure their Exchange 2010 environment to exchange domain-secured e-mail with their partner, Woodgrove Bank. Contoso administrators want to make sure that all e-mail sent to and received from Woodgrove Bank is protected with mutual TLS. Also, they want to configure Domain Security functionality so that all mail to and from Woodgrove Bank is rejected if mutual TLS can't be used.

Contoso has an internal public key infrastructure (PKI) that generates certificates. The PKI's root certificate has been signed by a major third-party certification authority (CA). Woodgrove Bank uses the same third-party CA to generate their certificates. Therefore, both Contoso and Woodgrove Bank trust the other's root CAs.

To set up mutual TLS, Exchange administrators at Contoso perform the following procedures:

Step 1: Generate a certificate request for TLS certificates

Step 2: Import certificates to Edge Transport servers

Step 3: Configure outbound Domain Security

Step 4: Configure inbound Domain Security

Step 5: Test domain-secured mail flow

Prerequisites

- This topic assumes that you have read and understood Generate Request for Third-Party Certificate Services.
- The Microsoft Exchange EdgeSync service must be fully deployed for Domain Security. Generally, configuration changes that are made to Domain Security functionality that don't use the **ExchangeCertificate** cmdlets are made within the organization and synchronized to Edge Transport servers by using the Microsoft Exchange EdgeSync service.
- Before you can successfully run mutual TLS on an Edge Transport server, you must configure the computer and PKI environment so that certificate validation and certificate revocation list checking are operable. For more information, see Using PKI on the Edge Transport Server for Domain Security.
- Even though individual configuration steps within this scenario can be accomplished with lesser rights, to complete the entire end-to-end scenario tasks, your account needs to be a member of the Organization Management management role group.

Step 1: Generate a Certificate Request for TLS Certificates

Contoso has an internal PKI that's subordinated to a third-party CA. In this scenario, subordination refers to the fact that the CA that's deployed by Contoso in the corporate infrastructure contains a root certificate that has been signed by a public third-party CA. By default, the public third-party CA is one of the trusted root certificates in the Microsoft Windows certificate store. Therefore, any client that includes the same third-party CA in its trusted root store and that connects to Contoso can authenticate to the certificate

that's presented by Contoso.

Contoso has two Edge Transport servers that require TLS certificates: mail1.contoso.com and mail2.mail.contoso.com. Therefore, the Contoso e-mail administrator must generate two certificate requests, one certificate request for each server.

The following example shows the commands that the administrator uses to generate the base64-encoded PKCS#10 certificate requests.

The Contoso administrator must run this command for CN=mail1.contoso.com.

```
$Data1 = New-ExchangeCertificate -GenerateRequest -FriendlyName "Internet certifi
Set-Content -Path "C:\Certificates\mail1-request.req" -Value $Data1
```

The Contoso administrator must run this command for CN=mail2.mail.contoso.com.

```
$Data2 = New-ExchangeCertificate -GenerateRequest -FriendlyName "Internet certifi
Set-Content -Path "C:\Certificates\mail2-request.req" -Value $Data2
```

For detailed syntax and parameter information, see New-ExchangeCertificate.

Important:

The specific details of the certificate or certificate request that you create depends on many variables. If you're generating a request, make sure that you work closely with the CA or the PKI administrator who will issue your certificate. For more information about how to create a certificate request for TLS, see Generate Request for Third-Party Certificate Services.

Return to top

Step 2: Import Certificates to Edge Transport Servers

After the Contoso administrator generates the certificate requests, the CA administrator for Contoso then uses the requests to generate the certificates for the servers. The resulting certificates must be issued as either a single certificate or a certificate chain and copied to the appropriate Edge Transport servers.

Important:

Do not use the Certificate Manager snap-in in the Microsoft Management Console (MMC) to import the certificates for TLS on the Exchange server. Using the Certificate Manager snap-in to import certificates on Exchange servers doesn't bind the request that's created in this procedure to the issued certificate. Therefore TLS might fail. You can use the Certificate Manager snap-in to import certificates and keys that are stored as .pfx files into the local computer store.

When you import the certificate to the Edge Transport server, you must also enable the certificate for the SMTP service. The Contoso administrator runs the following command on each Edge Transport server, one time for each respective certificate.

```
Import-ExchangeCertificate -FileData ([Byte[]]$(Get-Content -Path C:\Certificates
```

The preceding example imports and enables the TLS certificate by pipelining the certificate to the **Enable-ExchangeCertificate** cmdlet. You can also enable the certificate after you import it. If you do, you will need to specify the thumbprint of the certificate that you want to enable.

For detailed syntax and parameter information, see the Import-ExchangeCertificate and Enable-ExchangeCertificate topics.

Transporting Certificates and Related Keys

When you receive a certificate from your PKI or CA provider, convert the issued certificate to a .pfx (PKCS#12) file so that you can back it up as part of a disaster contingency. A .pfx file contains the certificate and related keys. In some cases, you may want to transport the certificate and keys to move them to other computers. For example, if you have multiple Edge Transport servers where you expect to send and receive e-mail that's domain secured, you can create a single certificate that will work for all servers. In this case, you must have the certificate imported and enabled for TLS on each Edge Transport server.

As long as you keep a copy of the .pfx file securely archived, you can always import and enable the certificate. The .pfx file contains the private key so it's important to physically protect the file by keeping it on storage media in a secure location.

It's important to understand that the **Import-ExchangeCertificate** cmdlet always marks the imported private key from the .pfx file as non-exportable. This functionality is by design.

When you use the Certificate Manager snap-in in MMC to import a .pfx file, you can specify private key exportability and strong-key protection.

Important:

Do not enable strong-key protection on certificates that are intended for TLS. Strong-key protection prompts the user every time that the private key is accessed. With Domain Security, the user is the SMTP service on the Edge Transport server.

Return to top

Step 3: Configure Outbound Domain Security

You must perform three steps to configure outbound Domain Security:

1. Run the **Set-TransportConfig** cmdlet to specify the domain with which you want to send domain-secured e-mail.
2. Run the **Set-SendConnector** cmdlet to set the **DomainSecureEnabled** property on the Send connector that will send mail to the domain with which you want to send domain-secured e-mail.
3. Run the **Get-SendConnector** cmdlet to verify the following:
   - The Send connector that will send mail to the domain with which you want to send domain-secured e-mail routes mail with Domain Name System (DNS).
   - The FQDN is set to match either the Subject Name or the Subject Alternative Name of certificates that you're using for Domain Security.

Because the changes that you make in these three steps are global, you must make the changes on an internal Exchange server. The configuration changes that you make will be replicated to the Edge Transport servers by using the Microsoft Exchange EdgeSync service.

Step 3a: Specify the Sender Domain in Transport Configuration

It's relatively straightforward to specify the domain with which you want to send domain-secured e-mail. The Contoso administrator runs the following command on an internal Exchange 2010 server.

```
Set-TransportConfig -TLSSendDomainSecureList woodgrovebank.com
```

The *TLSSendDomainSecureList* parameter takes a multivalued list of domain names. The

Set-TransportConfig command replaces the whole value for *TLSSendDomainSecureList* with the new value that's supplied in the cmdlet. Therefore, if you have other domains already configured and want to add a new domain, you need to either include the existing domain in the list or use a temporary variable. The following example shows how to add the woodgrovebank.com domain to the *TLSSendDomainSecureList* parameter without overwriting any existing values.

```
$TransportConfig = Get-TransportConfig
$TransportConfig.TLSSendDomainSecureList += "woodgrovebank.com"
Set-TransportConfig -TLSSendDomainSecureList $TransportConfig.TLSSendDomainSecure
```

For detailed syntax and parameter information, see Set-TransportConfig.

Step 3b: Configure the Default Send Connector

Contoso will use the default DNS-routed Send connector named Internet to send domain-secured e-mail to their partners. Because their default DNS-routed Send connector is a default Internet Send connector, it uses DNS to route mail and doesn't use a smart host. The FQDN is already set to `mail.contoso.com`. Because the certificates that the Contoso administrator created set the *DomainName* parameter of the **New-ExchangeCertificate** to `mail.contoso.com`, the Send connector can use the certificates without additional configuration.

If you've configured a subdomain for testing, you may have to update the FQDN of your Send connector to match the certificate that you've created (for example, subdomain.mail.contoso.com). On the other hand, if you've created a certificate that contains the subdomain in the Subject or Subject Alternative name fields, you don't have to update the FQDN of the Send connector.

Therefore, the only configuration that the Contoso administrator must make to the Send connector is to set the *DomainSecureEnabled* parameter. To do this, the Contoso administrator runs the following command on an internal Exchange 2010 server for the Internet Send connector.

```
Set-SendConnector Internet -DomainSecureEnabled:$true
```

For detailed syntax and parameter information, see Set-SendConnector.

Step 3c: Verify the Send Connector Configuration

After completing the configuration changes, the Contoso administrator needs to verify that the Send connector being used for Domain Security is configured correctly. To do so, the Contoso administrator needs to run the following command.

```
Get-SendConnector Internet | Format-List Name,DNSRoutingEnabled,FQDN,DomainSecure
```

This command will list the relevant parameters configured for Domain Security, allowing the Contoso administrator to verify the configuration.

For detailed syntax and parameter information, see Get-SendConnector.

Return to top

Step 4: Configure Inbound Domain Security

You must perform two steps to enable inbound Domain Security:

1. Run the **Set-TransportConfig** cmdlet to specify the domain from which you want to receive domain-secured e-mail.
2. On the Edge Transport server, use the Exchange Management Shell or the

Exchange Management Console (EMC) to enable Domain Security on the Receive connector from which you want to receive domain-secured e-mail. Because Domain Security requires mutual TLS authentication, TLS must also be enabled on the Receive connector.

Step 4a: Specify the Recipient Domain in Transport Configuration

It's relatively straightforward to specify the domain with which you want to receive domain-secured e-mail. To specify the domain, the Contoso administrator runs the following command in the Shell on an internal Exchange 2010 server or management workstation.

```
Set-TransportConfig -TLSReceiveDomainSecureList woodgrovebank.com
```

The *TLSReceiveDomainSecureList* parameter takes a multivalued list of domain names. The **Set-TransportConfig** command replaces the whole value for *TLSReceiveDomainSecureList* parameter with the new value supplied by the **Set-TransportConfig** cmdlet. Therefore, if you have other domains already configured and want to add a new domain, you need to either include the existing domain in the list or use a temporary variable. The following example shows how to add the woodgrovebank.com domain to the *TLSReceiveDomainSecureList* parameter without overwriting any existing values.

```
$TransportConfig = Get-TransportConfig
$TransportConfig.TLSReceiveDomainSecureList += "woodgrovebank.com"
Set-TransportConfig -TLSReceiveDomainSecureList $TransportConfig.TLSReceiveDomain
```

For detailed syntax and parameter information, see Set-TransportConfig.

Step 4b: Configure the Receive Connector

You must configure the Receive connector on each Edge Transport server that accepts mail from the domain from which you want to receive domain-secured e-mail. The Contoso environment is configured to have a single Internet Receive connector, with an *Identity* parameter value of Internet, on both Edge Transport servers. Therefore, to enable TLS while mail is sent to or received from Woodgrove Bank, the Contoso administrator must make sure that TLS is enabled on the default Internet Receive connector on both Edge Transport servers. To do so, the Contoso administrator runs the following command on both mail1.contoso.com and mail2.mail.contoso.com.

```
Set-ReceiveConnector Internet -DomainSecureEnabled $true -AuthMechanism TLS
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

You can also use the EMC to configure the Receive connector using the following steps.

1. On the Edge Transport server, open the EMC, click **Edge Transport**, and then in the result pane, click the **Receive Connectors** tab.
2. Select the Receive connector that accepts mail from the domain from which you want to receive domain-secured e-mail, the connector Internet in this case, and then click **Properties** in the action pane.
3. On the **Authentication** tab, select **Transport Layer Security (TLS)** and **Enable Domain Security (Mutual Auth TLS)**, and then click **OK**.

Be aware that specifying the authentication mechanism as TLS doesn't force TLS on all inbound connections.

TLS will be forced for connections from Woodgrove Bank for the following reasons:

- Woodgrove Bank is specified in the **Set-TransportConfig** cmdlet on the *TLSReceiveDomainSecureList* parameter.
- The *DomainSecureEnabled* parameter is set to `$true` on the Receive connector.

Other senders that aren't listed on the *TLSReceiveDomainSecureList* parameter in the **Set-TransportConfig** cmdlet will only use TLS if TLS is supported by the sending system.

Return to top

Step 5: Testing Domain-Secured Mail Flow

After you've configured domain-secured e-mail, you can test the connection by reviewing the performance logs and the protocol logs. Messages that have successfully authenticated over the domain-secured mail flow path are displayed in Outlook as Domain Secure messages.

Performance Counters

The Domain Security feature includes the following set of performance counters under **MSExchange Secure Mail Transport**:

- Domain-Secured Messages Received
- Domain-Secured Messages Sent
- Domain-Secured Outbound Session Failures

You can create a new counter log file for domain-secured mail flow with these performance counters to monitor the number of messages sent and received and also to monitor failed mutual TLS sessions. For more information about how to create and configure counter logs, see the Help file that's included with the **Performance Logs and Alerts** MMC snap-in.

Protocol Logs

You can review the send and receive protocol logs to determine whether TLS negotiation has been successful.

To view detailed protocol logs, you must set the protocol logging level to `Verbose` on the connectors that your organization uses to send and receive domain secured e-mail. To accomplish this, the Contoso administrator runs the following on both Edge Transport servers.

```
Set-ReceiveConnector Internet -ProtocolLoggingLevel Verbose
```

To enable protocol logging on the Send connector, the Contoso administrator runs the following on an internal Exchange server or management workstation. The configuration change is then replicated to the Edge Transport servers using the Microsoft Exchange EdgeSync service.

```
Set-SendConnector Internet -ProtocolLoggingLevel Verbose
```

For detailed syntax and parameter information, see the Set-ReceiveConnector and Set-SendConnector topics.

For more information about how to view protocol logs, see Configure Protocol Logging.

Return to top

1.7.1.12.2 Using PKI on the Edge Transport Server for Domain Security

Using PKI on the Edge Transport Server for Domain Security

Transport > Understanding Transport > Understanding Domain Security >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Domain Security relies on mutual Transport Layer Security (TLS) for authentication. Successful mutual TLS authentication relies on a trusted, validated X.509 certificate chain for the TLS certificates that are used for Domain Security.

Therefore, before you can successfully deploy Domain Security, you must configure your Edge Transport server and your X.509 public key infrastructure (PKI) to accommodate certificate trusting and certificate validation.

Important:

It's beyond the scope of this topic to provide a detailed explanation of cryptography and certificate technologies and concepts. Before you deploy any security solution that uses cryptography and X.509 certificates, we recommend that you understand the basic concepts of trust, authentication, encryption, and public and private key exchange as they relate to cryptography. For more information, see the references listed at the end of this topic.

Configuring Root Certification Authorities

To validate a given X.509 certificate, you must trust the root certification authority (CA) that issued the certificate. A root CA is the most trusted CA, which is at the top of a CA hierarchy. The root CA has a self-signed certificate. When you run an application that relies on certificate authentication, each certificate must have a certificate chain that ends in a certificate in the trusted root container of the local computer. The trusted root container contains certificates from root certification authorities.

To successfully send domain-secured e-mail, you must be able to validate the receiving server's X.509 certificate. Similarly, when someone sends domain-secured e-mail to your organization, the sending server must be able to validate your certificate.

There are two types of trusted root CAs that you can use to implement Domain Security: Built-in third-party root CAs and private root CAs.

Third-Party Root Certification Authorities

Microsoft Windows includes a set of built-in third-party root CAs. If you trust the certificates issued by these third-party root CAs, this means you can verify certificates issued by these CAs. If your organization and your partner organizations are using the default Windows installation and trust the built-in third-party root CAs, trust is automatic. In this scenario, additional trust configuration is not required.

Private Trusted Root Certification Authorities

A private trusted root CA is a root CA that has been deployed by a private or internal PKI. For example, when your organization or the organization that you exchange domain-secured e-mail with has deployed an internal PKI with its own root certificate, you must make additional trust configurations.

When private root CAs are used, you must update the Windows trusted root certificate store on the Edge Transport server for Domain Security to function correctly.

You can configure trust in two ways: direct root trust and cross-certification. You must understand that whenever the transport service picks a certificate, it validates the certificate before it uses it. Therefore, if you're using a private root CA to issue your certificates, you must include the private root CA in the trusted root certificate store on each Edge Transport server that sends or receives domain-secured e-mail.

Direct Root Trust

If you want to trust a certificate that has been issued by a private root CA, you can manually add that root certificate to the trusted root certificate store on the Edge Transport server computer. For more information about how to manually add certificates

to the local certificate store, see the Help file for the Certificate Manager snap-in in Microsoft Management Console (MMC).

Cross-Certification

Cross-certification occurs when one CA signs a certificate that is generated by a different CA. Cross-certification is used to build trust from one PKI with another PKI. In the context of Domain Security, if you have your own PKI, instead of using direct manual trust for a root authority of a partner with an internal PKI, you might create a cross-certificate for the partner CA under your root authority. In this case, trust is established because the cross-certificate ultimately chains back to your trusted root.

You must understand that if you have an internal PKI and are using cross-certification, you must manually update the root certificate store on each Edge Transport server that receives domain-secured e-mail so that each Edge Transport server can validate certificates when they receive e-mail from partners that are trusted through cross-certificates.

For more information about how to manually add certificates to the local certificate store, see the Help file for the Certificate Manager snap-in in MMC.

Configuring Access to the Certificate Revocation List

Whenever the Transport service retrieves a certificate, it validates the certificate chain and validates the certificate. Validation of the certificate is a process in which many attributes of the certificate are confirmed. Most of these attributes can be confirmed on the local computer by the application that requests the certificate. For example, the intended use of the certificate, the expiration dates on the certificate, and similar attributes are verifiable outside the context of a PKI. However, verification that the certificate has not been revoked must be validated with the CA that issued the certificate. Therefore, most CAs make a certificate revocation list (CRL) available to the public to validate the revocation status.

To successfully use Domain Security, CRLs for CAs that you use or are used by your partners must be available to the Edge Transport servers that send and receive domain-secured e-mail. If the revocation check fails, the receiving Exchange server issues a temporary protocol rejection of the message. A transient revocation failure can occur. For example, the Web server that is used to publish the CRL can fail. Or, general network connectivity issues between the Edge Transport server and the CRL distribution point could fail the revocation check. Therefore, transient revocation failures only cause temporary mail delivery delays because the sending server will retry later. However, CRL validation is required for successful domain-secured e-mail transmission.

You must enable the following scenarios:

- **Your Edge Transport servers must be able to access CRLs for external CAs** Each partner with which you exchange domain-secured e-mail must have publicly available CRLs that your organization's Edge Transport server can contact. In some cases, CRLs are only available with Lightweight Directory Access Protocol (LDAP). In most cases, with public CAs, CRLs are published via HTTP. Make sure that the appropriate outbound ports and proxies are configured to let the Edge Transport server contact the CRL. You can determine which protocol a given CRL distribution point accepts by opening a certificate in MMC and viewing the **CRL Distribution Points** field.
- **You must make the CRL for the CA that issues your certificates publicly available** You must understand that even when an Edge Transport server retrieves a certificate from your own organization, it validates the certificate chain to validate the certificate. Therefore, the CRL for your CA must be available to your own Edge Transport servers. In addition, all partners that

you exchange domain-secured e-mail with must be able to access the CRL for the CA that issues your certificates.

Configuring Proxy Settings for WinHTTP

Exchange 2010 transport servers rely on the underlying Microsoft Windows HTTP Services (WinHTTP) to manage all HTTP and HTTPS traffic. Both Hub Transport servers and Edge Transport servers may use HTTP to access updates for Microsoft Exchange 2010 Standard Anti-spam Filter Updates and for CRL validation.

For more information, see Configure Proxy Settings for WinHTTP.

Testing the PKI and Proxy Configuration

To verify your PKI and proxy configuration for a specific Edge Transport server, use Certutil.exe to verify the certificate chain for your Edge Transport server certificate. Certutil.exe is a command-line tool that is installed as part of Certificate Services in Windows Server 2008 operating systems. For more information, see Test PKI and Proxy Configuration.

1.7.1.12.3 Test PKI and Proxy Configuration

Test PKI and Proxy Configuration

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

To verify your public key infrastructure (PKI) and proxy configuration for a specific Edge Transport server, use Certutil.exe to verify the certificate chain for your Edge Transport server certificate. Certutil.exe is a command-line tool installed as part of Certificate Services in the Windows Server 2008 operating system. For more information, see Certutil.

Before you can run **Certutil** to verify the certificate chain for a specific certificate, the certificate must first be in file (.cer) format. Therefore, you must first export the certificate, but not the private keys, to the DER (.cer) file format.

The first procedure in this topic shows you how to add the Certificate Manager snap-in to the Microsoft Management Console (MMC). The second procedure explains how to use the Certificate Manager to export a certificate. The third procedure shows how you can run the **Certutil** command to verify the certificate chain.

Step 1: Add Certificate Manager to the Microsoft Management Console

To perform this procedure, the account you use must be delegated membership in the local Administrators group.

1. Click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**.
3. In the **Add/Remove Snap-in** box, click **Add**.
4. In the **Available Snap-ins** list, click **Certificates**, and then click **Add**.
5. Click **Computer Account**, and then click **Next**.
6. Click the **Local computer (the computer this console is running on)** option,

and then click **Finish**.
7. Click **OK**.

Step 2: Export the certificate

To perform this procedure, the account you use must be delegated membership in the local Administrators group.

1. Open the Certificate Manager that you created in Step 1.
2. Expand the **Certificates (Local Computer)** folder and the **Personal** folder, and then click the **Certificates** folder.
3. In the details pane, right-click the certificate that you will use for Domain Security, click **All Task**, and then select **Export**. The Certificate Export Wizard will open.
4. On the **Welcome** page, click **Next**.
5. On the **Export Private Key** page, select **No, do not export the private key**, and then click **Next**.
6. On the **Export File Format** page, select **DER encoded binary X.509 (.CER)**, and then click **Next**.
7. On the **File to Export** page, enter the path and file name where you want to save the exported certificate, and then click **Next**.
8. On the **Finish** page, verify the settings and then click **Finish**.

Step 3: Verify the certificate chain for the certificate

To perform this procedure, the account you use must be delegated membership in the local Administrators group.

On the Edge Transport server, open a Command Prompt window, and type the following command.

```
Certutil -verify c:\CertificateName.cer
```

In this example, `CertificateName` is the Edge Transport server certificate that you exported in the previous procedure.

1.7.1.13 Understanding Edge Subscriptions

Understanding Edge Subscriptions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-02-01*

This topic provides detailed information about Edge Subscriptions and the EdgeSync synchronization process. Edge Subscriptions are used to populate the Active Directory Lightweight Directory Services (AD LDS) instance on the Microsoft Exchange Server 2010 Edge Transport server role with Active Directory data.

In Exchange 2010, the Edge Transport server role is deployed in your organization's perimeter network. Designed to minimize the attack surface, the Edge Transport server handles all Internet-facing mail flow and provides SMTP relay and smart host services for the Exchange organization. Additional layers of message protection and security are provided by a series of agents that run on the Edge Transport server and act on messages as they're processed by the message transport components. These agents

support the features that provide protection against viruses and spam and apply transport rules to control message flow.

Although creating an Edge Subscription is optional, subscribing an Edge Transport server to the Exchange organization provides a simpler management experience for the administrator and enhances the available anti-spam features. You must create an Edge Subscription if you plan to use recipient lookup or safelist aggregation, or if you plan to help secure SMTP communications with partner domains by using mutual Transport Layer Security (TLS).

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Edge Subscription Process

In a typical deployment scenario, the computer that has the Edge Transport server role installed doesn't have access to Active Directory. All the configuration and recipient information that the Edge Transport server has to process messages is stored in AD LDS. Creating an Edge Subscription establishes secure, automatic replication of information from Active Directory to AD LDS. The Edge Subscription process provisions the credentials that are used to establish a secure LDAP connection between Hub Transport servers and a subscribed Edge Transport server. The Microsoft Exchange EdgeSync service that runs on Hub Transport servers then performs periodic one-way synchronization to transfer data to AD LDS and keep that data up to date. This process reduces the administration that you must perform in the perimeter network by letting you perform required configuration on the Hub Transport server role and then write that information to the Edge Transport server.

You subscribe an Edge Transport server to the Active Directory site that contains the Hub Transport servers that will directly exchange messages with your Edge Transport servers. The Edge Subscription process creates an Active Directory site membership affiliation for the Edge Transport server. The site affiliation enables Hub Transport servers in the Exchange organization to relay messages to the Edge Transport server for delivery to the Internet without having to configure explicit Send connectors.

One or more Edge Transport servers can be subscribed to a single Active Directory site. However, an Edge Transport server can't be subscribed to more than one Active Directory site. If you have more than one Edge Transport server deployed, each server can be subscribed to a different Active Directory site. Each Edge Transport server requires an individual Edge Subscription.

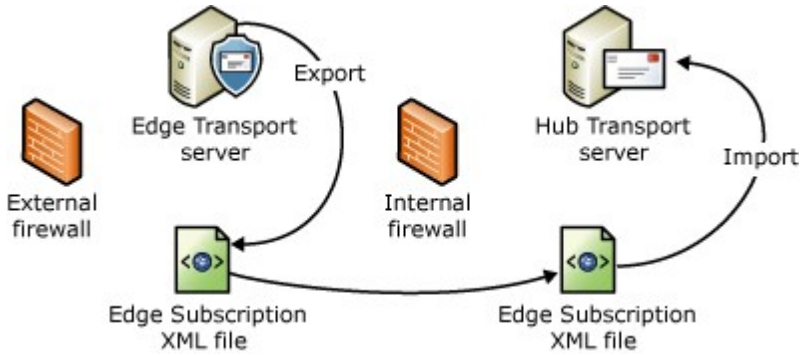
To deploy an Edge Transport server and subscribe it to an Active Directory site, follow these steps:

1. Install the Edge Transport server role.
2. Verify that the Hub Transport servers and the Edge Transport server can locate one another by using Domain Name System (DNS) name resolution.
3. Configure the objects and settings to be replicated to the Edge Transport server.
4. On the Edge Transport server, create and export an Edge Subscription file.

For more information about this step, see Create an Edge Subscription File on an Edge Transport Server.

5. Copy the Edge Subscription file to a Hub Transport server or a file share that's accessible from the Active Directory site that has your Hub Transport servers.
6. Import the Edge Subscription file to your Active Directory site to which you want to subscribe your Edge Transport server. For more information about this step, see Import an Edge Subscription File to an Active Directory Site.

The following figure illustrates the Edge Subscription process.



Configuration Changes Made When a New Edge Subscription Is Created

When you run the **New-EdgeSubscription** cmdlet on the Edge Transport server to create an Edge Subscription file, the following actions occur:

- An AD LDS account is created. This account is called the EdgeSync bootstrap replication account (ESBRA). These credentials are used to authenticate the first EdgeSync connection to the Edge Transport server. The account is configured to expire 1,440 minutes (24 hours) after it's created. Therefore, you must complete the subscription process before that time expires. If the ESBRA expires before the Edge Subscription process is complete, you must run the **New-EdgeSubscription** cmdlet on the Edge Transport server again to create an Edge Subscription file.
- The ESBRA credentials are retrieved from AD LDS and written to the Edge Subscription file. The public key for the Edge Transport server's self-signed certificate is also exported to the Edge Subscription file. The credentials that are written to the Edge Subscription file are specific to the server from which the file is exported.
- Any previously created configuration objects in a class that will now be replicated to AD LDS from Active Directory are deleted from AD LDS and the Exchange Management Shell commands used to configure those objects are disabled. You can still use the cmdlets that let you view those objects. The following cmdlets are disabled on the Edge Transport server when you run the **New-EdgeSubscription** cmdlet:
  - **Set-SendConnector**
  - **New-SendConnector**
  - **Remove-SendConnector**
  - **New-AcceptedDomain**
  - **Set-AcceptedDomain**
  - **Remove-AcceptedDomain**
  - **New-MessageClassification**
  - **Set-MessageClassification**
  - **Remove-MessageClassification**
  - **New-RemoteDomain**
  - **Set-RemoteDomain**
  - **Remove-RemoteDomain**

When you import the Edge Subscription file on the Hub Transport server by running the **New-EdgeSubscription** cmdlet in the Shell or by using the New Edge Subscription wizard in the Exchange Management Console, the following actions occur:

- The Edge Subscription is created, establishing a record of an Edge Transport server that has been joined to an Exchange organization and to which the Microsoft Exchange EdgeSync service will propagate configuration data. This step creates the edge configuration object in Active Directory.
- Each Hub Transport server in the Active Directory site receives notification from Active Directory that a new Edge Transport server has been subscribed. The Hub Transport server retrieves the ESBRA from the Edge Subscription file. The Hub Transport server then encrypts the ESBRA by using the public key of the Edge Transport server's self-signed certificate. The encrypted credentials are then written to the edge configuration object.
- Each Hub Transport server also encrypts the ESBRA by using its own public key and then stores the credentials in its own configuration object.
- EdgeSync replication accounts (ESRAs) are created in Active Directory for each Edge Transport-Hub Transport server pair. Each Hub Transport server stores its ESRA credentials as an attribute of the Hub Transport server configuration object.
- Send connectors are automatically created to relay messages outbound from the Edge Transport server to the Internet, and inbound from the Edge Transport server to the Exchange organization.
- The Microsoft Exchange EdgeSync service that runs on Hub Transport servers uses the ESBRA credentials to establish a secure LDAP connection between a Hub Transport server and the Edge Transport server and performs the initial replication of data. The following data is replicated to AD LDS:
  - Topology data
  - Configuration data
  - Recipient data
  - ESRA credentials
- The Microsoft Exchange Credential Service that runs on the Edge Transport server installs the ESRA credentials. These credentials are used to authenticate and secure later synchronization connections.
- The EdgeSync synchronization schedule is established.

The Microsoft Exchange EdgeSync service that's running on the Hub Transport servers in the Active Directory site to which the Edge Transport server is subscribed will now perform one-way replication of data from Active Directory to AD LDS on a regular schedule. You can also use the **Start-EdgeSynchronization** cmdlet in the Shell to override the EdgeSync synchronization schedule and immediately start synchronization.

For more information about ESRA accounts and how they're used to help secure the EdgeSync synchronization process, see Understanding Edge Subscription Credentials.

Send Connectors Created During Edge Subscription Process

By default, when you complete the Edge Subscription process by importing the Edge Subscription file to a Hub Transport server, the Send connectors that are required to enable end-to-end mail flow between the Internet and the Exchange organization are created automatically. Any existing Send connectors on the Edge Transport server are deleted. Even though that's the recommended method, you can also select to suppress automatic creation of Send connectors and configure Send connectors manually. For more information about manually configuring Send connectors, see Configure Mail Flow Between an Edge Transport Server and Hub Transport Servers Without Using EdgeSync.

The Edge Subscription process provisions the following Send connectors:

- A Send connector that's configured to relay e-mail messages from the Exchange organization to the Internet
- A Send connector that's configured to relay e-mail messages from the Edge

Transport server to the Exchange organization

Also, by subscribing an Edge Transport server to the Exchange organization, you enable Hub Transport servers that are located in the Active Directory site to which the Edge Transport server is subscribed to use the intra-organization Send connector to relay messages to that Edge Transport server.

Automatically Create a Send Connector to Send Messages to the Internet

By default, when you run the **New-EdgeSubscription** cmdlet in the Shell on the Hub Transport server, the *CreateInternetSendConnector* parameter is set to `$true`. This creates the Send connector that's required to send messages to the Internet. The following table shows the default configuration of this Send connector.

Automatic Internet Send connector configuration

Parameter	Value
Name	EdgeSync - <*Site Name*> to Internet
Address Space	SMTP:*;100
Source Servers	Edge Subscription name **Note:** The name of the Edge Subscription is the same as the name of the subscribed Edge Transport server.
Enabled	True
DNS Routing Enabled	True
Domain Secure Enabled (Mutual Auth TLS)	True

If more than one Edge Transport server is subscribed to the same Active Directory site, additional Send connectors to the Internet aren't created. Instead, all Edge Subscriptions are added to the same Send connector as source servers. This configuration causes outbound connections to the Internet to be load balanced between the subscribed Edge Transport servers.

This Send connector is configured to send e-mail messages from the Exchange organization to all remote SMTP domains. It will use DNS routing to resolve domain names to MX resource records. You can modify the configuration of this connector manually. However, if you must route outbound e-mail through a smart host, for example, you can suppress creation of this connector and manually configure a Send connector to the Internet.

Note:

A Send connector that's configured to use a smart host to route e-mail must have the *DNSRoutingEnabled* parameter set to `$false`. If the *DNSRoutingEnabled* parameter is set to `$false`, the *DomainSecureEnabled* parameter must also be set to `$false`.

Automatically Create an Inbound Send Connector

By default, when you run the **New-EdgeSubscription** cmdlet in the Shell on the Hub Transport server, the *CreateInboundSendConnector* is parameter set to `$true`. This creates the Send connector that's required to send messages to the Exchange organization. The following table shows the configuration of this Send connector.

Automatic inbound Send connector configuration

Parameter	Value

Name	EdgeSync - Inbound to *<Site Name>*
Address Space	SMTP:--;1
Source Servers	Edge Subscription name
Enabled	True
DNS Routing Enabled	False
Smart Hosts	--

The **--** placeholder in the address space for the inbound Send connector represents the authoritative and internal relay accepted domains for the Exchange organization and is the literal character displayed. Any messages that the Edge Transport server receives for authoritative and internal relay accepted domains are routed to this Send connector and relayed to the smart hosts.

The **--** placeholder in the list of smart hosts represents all the Hub Transport servers that are located in the subscribed Active Directory site and is the literal character displayed. Hub Transport servers that are added to an Active Directory site after an Edge Subscription has been established don't participate in the EdgeSync synchronization process. However, they are automatically added to the list of smart hosts for the inbound Send connector. If more than one Hub Transport server is located in the subscribed Active Directory site, inbound connections will be load balanced across the smart hosts.

You can't modify the address space or list of smart hosts for the automatically created inbound Send connector. However, you can set the value of the *CreateInboundSendConnector* parameter to `$false` when creating an Edge Subscription, and manually configure a Send connector from the Edge Transport server to the Exchange organization.

Intra-Organization Send Connector

The intra-organization Send connector is an implicit and hidden Send connector that's automatically computed by Exchange 2010 and enables Hub Transport servers in the same organization to relay messages to each other without using explicit Send connectors. Because a configuration object that has an Active Directory site association exists in Active Directory for an Edge Subscription, the intra-organization Send connector will also be used to relay messages to that Edge Transport server.

Only Hub Transport servers that are located in the same Active Directory site to which the Edge Transport server is subscribed can send and receive e-mail directly to or from the subscribed Edge Transport server. If you have a multiple site forest and Exchange 2010 is deployed in more than one site, the Hub Transport servers in non-subscribed sites will route outbound e-mail to the subscribed site. A Hub Transport server in the subscribed site will route outbound e-mail to the Edge Transport server.

Creating Additional Send Connectors After Edge Subscription is Completed

After an Edge Transport server is subscribed to an Active Directory site, the tasks for creating and modifying Send connectors are disabled on the Edge Transport server. If you want to create a Send connector for which the Edge Transport server is a source server, you create the Send connector inside the Exchange organization. You can specify one or more Edge Subscriptions as the source server for a Send connector. You can't specify both Hub Transport servers and Edge Subscriptions as source servers for the same Send connector. The Send connector will be replicated to the AD LDS instance on the Edge Transport server that's configured as a source server the next time that configuration data is synchronized by the EdgeSync synchronization process. If you list more than one Edge Subscription as a source server, connections to that Send connector will be load balanced between the subscribed Edge Transport servers. However, the Edge Transport

servers have to be subscribed to the same Active Directory site for load balancing to occur. If Edge Subscriptions in different Active Directory sites are configured as source servers on the same Send connector, Hub Transport servers will route only to the closest source server.

You have to create Send connectors manually in the following scenarios:

- You've suppressed automatic creation of the Internet or inbound Send connectors.
- You've accepted domains that are configured as external relay domains.

Suppressing Automatic Creation of Send Connectors

Depending on the topology of your Exchange organization, you may decide to suppress automatic creation of Send connectors. The following scenarios provide examples of topologies that require that you suppress automatic creation of Send connectors.

Partitioning Mail Flow

You may decide to partition the inbound and outbound mail processing between two Edge Transport servers. In this scenario, one Edge Transport server is responsible for processing outbound mail flow and a second Edge Transport server is responsible for processing inbound mail flow. To achieve this scenario, you configure the Edge Subscriptions as follows:

- For the Edge Transport server that processes only outbound mail flow, run the following command in the Shell on the Hub Transport server.

```
New-EdgeSubscription -FileData ([byte[]]$(Get-Content -Path "C:\EdgeSer
```

- For the Edge Transport server that processes only inbound mail flow, run the following command in the Shell on the Hub Transport server.

```
New-EdgeSubscription -FileData ([byte[]]$(Get-Content -Path "C:\EdgeSer
```

Routing Outbound E-Mail to a Smart Host

If your Exchange organization routes all outbound e-mail through a smart host, the default automatically created Send connector to the Internet won't have the correct configuration.

In this scenario, you run the following command in the Shell on the Hub Transport server to suppress automatic creation of the Send connector to the Internet.

```
New-EdgeSubscription -FileData ([byte[]]$(Get-Content -Path "C:\EdgeServerSubscri
```

After the Edge Subscription process is complete, manually create a Send connector to the Internet. Create the Send connector inside the Exchange organization and select the Edge Subscription as the source server for the connector. Select the **Custom** usage and configure one or more smart hosts. The Send connector will be replicated to the AD LDS instance on the Edge Transport server the next time that EdgeSync synchronizes configuration data. You can also force EdgeSync synchronization to immediately start by running the **Start-EdgeSynchronization** cmdlet in the Shell on a Hub Transport server.

The following code provides an example of how to use the Shell to configure a Send connector for a subscribed Edge Transport server to route messages for all Internet address spaces through a smart host. This task is run inside the Exchange organization, not on the Edge Transport server.

```
New-SendConnector -Name "EdgeSync - Site-A to Internet" -Usage Custom -AddressSpa
```

Important:

This example doesn't specify any smart host authentication mechanism. Make sure that you configure the correct authentication mechanism and provide all necessary credentials when you create a smart host connector in your own Exchange organization.

Configuring Send Connectors for External Relay Domains

If you've accepted domains in your Exchange organization that are configured as external relay domains, you have to manually create a Send connector for those address spaces. Messages that are being delivered to external relay domains are relayed by the Edge Transport server. The Edge Subscription process doesn't automatically create and configure Send connectors for external relay domains. Therefore, you have to configure Send connectors for those domains and specify one or more Edge Subscriptions as the source server for those Send connectors.

The DNS MX resource record for an external relay domain resolves to your Edge Transport server. Configure a Send connector that relays e-mail to an external relay domain to use a smart host for routing. If you configure the Send connector for an external relay domain to use DNS routing, a routing loop will occur. For more information about external relay domains, see Understanding Accepted Domains.

Return to top

Microsoft Exchange EdgeSync Service

After you subscribe an Edge Transport server to an Active Directory site, the EdgeSync service that runs on the Hub Transport servers will replicate configuration and recipient data to the Edge Transport servers using the Microsoft Exchange EdgeSync service. The service replicates the following data from Active Directory to AD LDS:

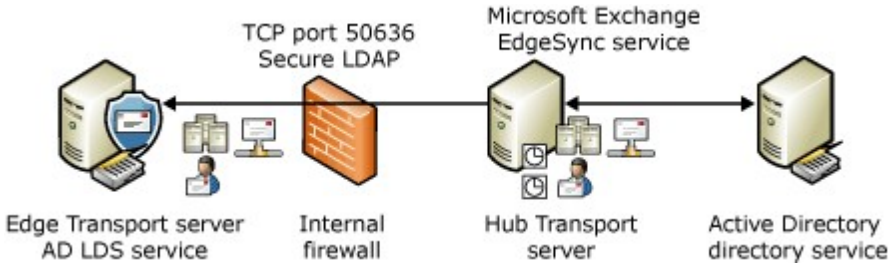
- Send connector configuration
- Accepted domains
- Remote domains
- Message classifications
- Safe Senders Lists
- Blocked Senders Lists
- Recipients
- List of send and receive domains used in domain secure communications with partners
- List of SMTP servers listed as internal in your organization's transport configuration
- List of Hub Transport servers in the subscribed Active Directory site

For more information about the data that's replicated to AD LDS and how it's used, see EdgeSync Replication Data.

The Microsoft Exchange EdgeSync service uses a secure LDAP channel to transfer this data. A mutually authenticated and authorized secure LDAP channel is established from the Hub Transport server to the Edge Transport server.

To replicate data to AD LDS, the Hub Transport server binds to a global catalog server to retrieve updated data. The Microsoft Exchange EdgeSync service initiates a secure LDAP session between a Hub Transport server and the subscribed Edge Transport server over the non-standard TCP port 50636.

The following figure illustrates the EdgeSync synchronization process.



When you first subscribe an Edge Transport server to an Active Directory site, the initial replication that populates AD LDS with data from Active Directory can take some time, depending on the quantity of data in the directory service. After the initial replication is complete, the EdgeSync service only synchronizes the new and changed objects and removes any objects that have been deleted from Active Directory.

Synchronization Schedule

Different types of data synchronize on different schedules. The EdgeSync synchronization schedule specifies the maximum length of time between EdgeSync synchronization intervals. EdgeSync synchronization occurs at the following intervals:

- Configuration data is scheduled to be synchronized at 3-minute intervals.
- Recipient data is scheduled to be synchronized at 5-minute intervals.
- Topology data is reloaded every 5 minutes.

You use the **Set-EdgeSyncServiceConfig** cmdlet to configure the EdgeSync synchronization schedule intervals. If you use the **Start-EdgeSynchronization** cmdlet in the Shell on the Hub Transport server to force Edge Subscription synchronization to occur immediately, you override the timer that determines the next time that EdgeSync synchronization is scheduled to occur.

Selection of Hub Transport Server

A subscribed Edge Transport server is associated with a particular Active Directory site. If more than one Hub Transport server exists in the site, any of them can replicate data to the subscribed Edge Transport servers. To avoid contention among the Hub Transport servers when synchronizing, the selection of the preferred Hub Transport server occurs as follows:

1. The first Hub Transport server in the Active Directory site to perform a topology scan and discover the new Edge Subscription performs the initial replication. Because this discovery is based on the timing of the topology scan, any Hub Transport server in the site may perform the initial replication.
2. The Hub Transport server that performs the initial replication establishes an EdgeSync lease option and sets a lock on the Edge Subscription. The lease option establishes that Hub Transport server as the preferred server to provide synchronization services to that Edge Transport server. The lock prevents the Microsoft Exchange EdgeSync service on another Hub Transport server from taking over the lease option.
3. The EdgeSync lease option lasts for one hour. No other Microsoft Exchange EdgeSync service can take over the option from another Hub Transport server during this one-hour period unless a manual synchronization occurs before this period expires. If the preferred Hub Transport server isn't available to provide the Microsoft Exchange EdgeSync service when manual synchronization is performed, after a five-minute wait, the lock is released and another Microsoft Exchange EdgeSync service takes over the lease option and performs synchronization.
4. If manual synchronization isn't performed, synchronization occurs based on the EdgeSync synchronization schedule. If the preferred server isn't available when scheduled synchronization occurs, after a five-minute wait, the lock is released and another Microsoft Exchange EdgeSync service takes over the lease option and performs synchronization.

This method of locking and leasing prevents more than one instance of the Microsoft Exchange EdgeSync service from pushing data to the same Edge Transport server at the same time.

Note:

If you have both Exchange 2010 and Exchange Server 2007 Hub Transport servers in the Active Directory site to which your Edge Transport server is subscribed, Exchange 2010 Hub Transport servers will always take precedence over Exchange 2007 Hub Transport servers.

Note:

When an Edge Transport server is subscribed to an Active Directory site, all the Hub Transport servers that are installed in that Active Directory site at that time can participate in the EdgeSync synchronization process. If one of those servers is removed, the Microsoft Exchange EdgeSync service that's running on the remaining Hub Transport servers will continue the data synchronization process. However, if new Hub Transport servers are installed in the Active Directory site, they won't participate in the EdgeSync synchronization process automatically. To enable those Hub Transport servers to participate in the EdgeSync synchronization process, you have to subscribe the Edge Transport server again.

The following table lists the EdgeSync properties that are related to the locking and leasing process. You can use the **Set-EdgeSyncServiceConfig** cmdlet to configure these properties.

EdgeSync lease properties

Property name	Value	Description
Lock duration	5 minutes	This setting determines for how long a particular Microsoft Exchange EdgeSync service will acquire a lock. If the Microsoft Exchange EdgeSync service on the Hub Transport server that's holding this lock doesn't respond, it will take five minutes for the Microsoft Exchange EdgeSync service on another Hub Transport server to take over the lease. Forcing EdgeSync synchronization doesn't override this value.
Option duration	1 hour	This setting determines for how long a Microsoft Exchange EdgeSync service can declare a lease option on an Edge Transport server. If the Microsoft Exchange EdgeSync service holding the lease is unavailable and doesn't restart during this option period, no other Microsoft Exchange EdgeSync service will take over the lease option, unless you force EdgeSync

		synchronization.
Lock renewal	1 minute	This setting determines how frequently the lock field is updated when a Microsoft Exchange EdgeSync service has acquired a lock to an Edge Transport server.

Preparing to Run the EdgeSync Service

Before you can subscribe your Edge Transport server to your Exchange organization, you must make sure that your infrastructure and your Hub Transport servers are prepared for the EdgeSync service. The following list summarizes the things you need to do to prepare for EdgeSync synchronization:

- Verify that the perimeter network firewall that separates the Edge Transport server from the Exchange organization is configured to enable communications through the correct ports. The Edge Transport server uses non-standard LDAP ports. You can modify the ports that are used by AD LDS by using the ConfigureAdam.ps1 script that's provided with Exchange 2010 if your environment requires specific ports. For more information, see Modify AD LDS Configuration. However, don't modify the ports after you create the Edge Subscription. If you modify the ports after you create the Edge Subscription, you must remove the Edge Subscription and then create a subscription. By default, the following LDAP ports are used to access AD LDS:
  - **LDAP** Port 50389/TCP is used locally to bind to the AD LDS instance. This port doesn't have to be open on the perimeter network firewall.
  - **Secure LDAP** Port 50636/TCP is used for directory synchronization from Hub Transport servers to AD LDS. This port must be open for successful EdgeSync synchronization.
- Verify that DNS host name resolution is successful from the Edge Transport server to the Hub Transport servers, and from the Hub Transport servers to the Edge Transport server.
- License the Edge Transport server. The licensing information for the Edge Transport server is captured when the Edge Subscription is created and is shown in the EMC for the Exchange organization. For subscribed Edge Transport servers to appear as licensed, they must be subscribed to the Exchange organization after the license key is applied on the Edge Transport server. If the license key is applied on the Edge Transport server after you perform the Edge Subscription process, the licensing information isn't updated in the Exchange organization, and you must resubscribe the Edge Transport server.
- Configure the following settings for propagation to the Edge Transport server role:
  - **Internal SMTP servers** Use the **Set-TransportConfig** cmdlet to configure the *InternalSMTPServers* parameter. This parameter specifies a list of internal SMTP server IP addresses or IP address ranges that should be ignored by Sender ID and connection filtering.
  - **Accepted domains** Configure all authoritative domains, internal relay domains, and external relay domains.
  - **Remote domains** Configure remote domain settings.

Return to top

Managing Edge Subscriptions

This section provides background information about various Edge Subscription management tasks. For step-by-step instructions, see Managing Edge Subscriptions.

Adding an Edge Transport Server

You can subscribe one or more Edge Transport servers to a single Active Directory site. If you deploy additional Edge Transport servers in your perimeter network and subscribe them to the same Active Directory site where an Edge Subscription already exists, the following actions occur:

- A new Edge Subscription object is created in Active Directory.
- Additional ESRA accounts are created for each Hub Transport server in the Active Directory site. These accounts are replicated to AD LDS and used by the EdgeSync synchronization process during synchronization with the new server.
- The new Edge Subscription is added to the source server list of the automatic Send connector to the Internet. Messages submitted to that connector for processing will be load balanced between the subscribed Edge Transport servers.
- An inbound Send connector from the Edge Transport server to the Exchange organization is automatically created.
- EdgeSync synchronization to the Edge Transport server starts.

For detailed steps about creating an Edge Subscription, see the following topics:

- Create an Edge Subscription File on an Edge Transport Server
- Import an Edge Subscription File to an Active Directory Site

Adding or Removing a Hub Transport Server

If a Hub Transport server is added to the Active Directory site to which an Edge Transport server is already subscribed, it doesn't automatically participate in the EdgeSync synchronization process. To enable a newly deployed Hub Transport server to participate in the EdgeSync synchronization process, you must resubscribe each Edge Transport server to the Active Directory site.

Removing a Hub Transport server from an Active Directory site where an Edge Transport server is subscribed won't affect EdgeSync synchronization, unless that Hub Transport server is the last Hub Transport server in that site. If you remove all Hub Transport servers from the Active Directory site where an Edge Transport server is subscribed, the subscribed Edge Transport servers are orphaned.

Resubscribing an Edge Transport Server

Occasionally you may have to resubscribe an Edge Transport server to an Active Directory site. When the Edge Subscription is re-created, new credentials are generated and the complete Edge Subscription process must be followed. This process is used in the following scenarios:

- New Hub Transport servers have been deployed in the subscribed Active Directory site, and you want the new server to participate in EdgeSync synchronization.
- The license key for the Edge Transport server was applied after the Edge Subscription was created. The licensing information for the Edge Transport server is captured when the Edge Subscription is created and is shown in the EMC for the Exchange organization. For subscribed Edge Transport servers to appear as licensed, they must be subscribed to the Exchange organization after the license key is applied on the Edge Transport server. If the license key is applied on the Edge Transport server after you perform the Edge Subscription process, the licensing information isn't updated in the Exchange organization and you must resubscribe the Edge Transport server.
- The ESRA credentials are compromised.

Important:

To resubscribe an Edge Transport server, export a new Edge Subscription file on the Edge Transport server and then import the XML file on a Hub Transport server. You must resubscribe the Edge Transport server to the same Active

Directory site to which it was originally subscribed. You don't have to first remove the original Edge Subscription. The resubscription process will overwrite the existing Edge Subscription.

Removing an Edge Subscription

There are some scenarios where you may have to remove an Edge Subscription from the Exchange organization or from both the Exchange organization and the Edge Transport server. If the Edge Transport server will be resubscribed to the Exchange organization, don't remove the Edge Subscription from the Edge Transport server. When you remove the Edge Subscription from an Edge Transport server, all replicated data is deleted from AD LDS. This can take a long time if you have lots of recipient data.

The following list provides examples of situations that require you to remove the Edge Subscription.

- You no longer want the Edge Transport server to participate in the EdgeSync synchronization process. In this scenario, you must remove the Edge Subscription from both the Edge Transport server and from the Exchange organization.
- An Edge Transport server is being decommissioned. In this scenario, you must remove the Edge Subscription from the Exchange organization only. If you uninstall the Edge Transport server role from the computer, the AD LDS instance and all Active Directory data that's stored in AD LDS is also removed.
- You want to change the Active Directory site association for the Edge Subscription. In this scenario, you must remove the Edge Subscription from only the Exchange organization. After the Edge Subscription is removed from the Exchange organization, you can resubscribe the Edge Transport server to a different Active Directory site.

When you remove the Edge Subscription from the Exchange organization, the effect is as follows:

- Synchronization of information from Active Directory to AD LDS stops.
- The ESRA accounts are removed from both Active Directory and AD LDS.
- The computer that has the Edge Transport server role installed is removed from the source server list of any Send connector.
- The automatic inbound Send connector from the Edge Transport server to the Exchange organization is removed from AD LDS.

When you remove the Edge Subscription from an Edge Transport server, the effect is as follows:

- You can no longer use the Edge Transport server features that rely on Active Directory data.
- Replicated data is removed from AD LDS.
- The tasks that were disabled when the Edge Subscription was created are enabled again to allow for local configuration.

For step-by-step instructions about how to remove an Edge Subscription, see Remove an Edge Subscription.

Verifying EdgeSync Results

You can use the **Test-EdgeSynchronization** diagnostic cmdlet to verify that the edge synchronization is working. This cmdlet provides a report of the synchronization status of subscribed Edge Transport servers. It can be run manually or called by Microsoft System Center Operations Manager 2007. When the task is called by System Center Operations Manager 2007, alerts are generated if an Edge Transport server isn't synchronized.

The output of this cmdlet lets you view which objects haven't been synchronized to the Edge Transport server. The task compares the data that's stored in Active Directory and the data that's stored in AD LDS. Any inconsistencies in data are reported in the results output by this command.

You can use the *ExcludeRecipientTest* parameter with the **Test-EdgeSynchronization** cmdlet to exclude validation of recipient data synchronization. If you include this parameter, only the synchronization of configuration objects is validated. Validating that recipient data is synchronized will take longer than validating only configuration data.

For detailed steps, see Verify EdgeSync Results for a Recipient.

Return to top

1.7.1.13.1 EdgeSync Replication Data

EdgeSync Replication Data

Transport > Understanding Transport > Understanding Edge Subscriptions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The computer that has the Edge Transport server role installed doesn't have access to Active Directory. To perform recipient lookup and safelist aggregation tasks, and to implement domain security by using mutual Transport Layer Security (TLS) authentication, the Edge Transport server requires data that resides in Active Directory. This data is replicated to the Edge Transport server using the EdgeSync process and the Edge Transport server stores all replicated information in Active Directory Lightweight Directory Services (AD LDS).

This topic focuses on the data that's replicated from Active Directory to the AD LDS instance on a Microsoft Exchange Server 2010 Edge Transport server when the Edge Transport server is subscribed to an Active Directory site. To learn more about the EdgeSync process and Edge Subscriptions, see Understanding Edge Subscriptions.

The following data are replicated from Active Directory to AD LDS:

- Edge Subscription information
- Configuration information
- Recipient information
- Topology information

The following sections describe these types of data and the way they're used by the Edge Transport server.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Edge Subscription Information

Exchange 2010 extends both the Active Directory and AD LDS schemas to provide attributes on the **ms-Exch-ExchangeServer** object to represent the data needed to control the EdgeSync synchronization process. These attributes provide the following three functions that are important to the EdgeSync synchronization process:

- They provide automatic provisioning and maintenance of the credentials that are used to help secure the LDAP connection between a Hub Transport server and a subscribed Edge Transport server.
- They arbitrate the synchronization lock and lease process that makes sure that only one Hub Transport server at a time will try to synchronize with an individual Edge Transport server. For more information about the lock and

lease process, see Understanding Edge Subscriptions.
- They optimize the EdgeSync synchronization process to maintain a record of the current synchronization status and avoid excessive manual synchronization.

The following table lists the schema extensions that are specific to Edge Subscriptions. The values assigned to these attributes are maintained by the Edge Subscription and EdgeSync synchronization process. You shouldn't manually edit these attributes by using editing tools, such as Ldp.exe or Active Directory Service Interfaces (ADSI) Edit.

Edge Subscription schema extensions

Attribute name	Description
ms-Exch-Server-EKPK-Public-Key	This attribute represents the current public key for the certificate being used by the server. This value is stored by both Edge Transport servers and Hub Transport servers. The public key is used to encrypt the credentials that are used to authenticate the server during LDAP and SMTP communication.
ms-Exch-EdgeSync-Credential	This attribute represents the list of credentials that the Microsoft Exchange EdgeSync service uses to establish an authenticated LDAP session to AD LDS. On Hub Transport servers, this attribute contains only the credentials that the Hub Transport server uses to authenticate to the subscribed Edge Transport servers. On Edge Transport servers, this attribute contains the credentials of each Hub Transport server in the subscribed Active Directory site that participates in the EdgeSync synchronization process. This attribute is only present on Hub Transport servers that run the EdgeSync synchronization process and on subscribed Edge Transport servers.
ms-Exch-Edge-Sync-Lease	This attribute is used to arbitrate between Hub Transport servers when more than one Hub Transport server tries to replicate to the same Edge Transport server.
ms-Exch-Edge-Sync-Status	This attribute is only present in AD LDS on the Edge Transport server object. This attribute tracks the status of replication to an AD LDS instance and includes information about replication.

Configuration Information

When you subscribe an Edge Transport server to the organization, you can manage the configuration objects that are common to the Edge Transport server and the Exchange organization from inside the organization. These changes are then replicated to the Edge Transport server by using the Microsoft Exchange EdgeSync service. This process helps maintain a consistent configuration across all servers involved in message processing.

A subset of the configuration data for the Exchange organization must also be maintained on the Edge Transport server. During the EdgeSync synchronization process, the

configuration data that the Edge Transport server needs is written to the configuration partition of AD LDS. The configuration data written to AD LDS includes the following:

- **Hub Transport servers** The fully qualified domain name (FQDN) of each Hub Transport server in the subscribed Active Directory site is made available to the local AD LDS store on the Edge Transport server. This information is used to derive a list of smart host servers for the inbound Send connector.
- **Accepted domains** All authoritative, internal relay, and external relay domains configured for the Exchange organization are written to AD LDS. Having the accepted domains available to the Edge Transport server enables the Exchange organization to perform domain filtering and reject invalid SMTP traffic into their organization as early as possible. For more information about accepted domains, see Understanding Accepted Domains.
- **Message classifications** If message classifications are available on the Edge Transport server, transport agents and content conversion can act on message classifications in the perimeter network. For example, the Attachment Filter agent can apply the Attachment Removed classification when it removes an attachment. Therefore, informational text will be displayed to a Microsoft Outlook user or a Microsoft Office Outlook Web App user to tell the recipient what happened. Agents that are developed for use by third-party applications can use message classifications in a similar manner. Also, message classifications may have to be translated by the Edge Transport server from a GUID in an X-header to Transport Neutral Encapsulation Format (TNEF) as a localized recipient description.
- **Remote domains** All remote domain policies configured for the Exchange organization are written to AD LDS. Remote domain policies control out-of-office message settings and message format settings for a remote domain. For more information about remote domains, see Understanding Remote Domains.
- **Send connectors** By default, Send connectors required to enable end-to-end mail flow between the Exchange organization and the Internet are automatically created. Any existing Send connectors on the Edge Transport server are deleted. If you want to configure additional Send connectors, you configure the Send connector inside the Exchange organization and select the Edge Subscription as the source server for the connector. For more information, see Understanding Edge Subscriptions.
- **Internal SMTP servers** The value for the **InternalSMTPServers** attribute is stored on the **TransportConfig** object for both the Exchange organization and the local Edge Transport server. During the EdgeSync synchronization process, the value that's stored on the local Edge Transport server object is overwritten with the value that's stored on this object for the Exchange organization. This attribute specifies a list of internal SMTP server IP addresses or IP address ranges that should be ignored by Sender ID and connection filtering.
- **Domain Secure lists** The **TLSReceiveDomainSecureList** and the **TLSSendDomainSecureList** attributes are stored on the **TransportConfig** object for both the Exchange organization and the local Edge Transport server. During the EdgeSync synchronization process, the value that's stored on the local Edge Transport server object is overwritten with the value that's stored on this object for the Exchange organization. These attributes specify the list of remote domains that are configured for mutual TLS authentication.

Recipient Information

The recipient information that's replicated to AD LDS includes only a subset of the recipient attributes. Only the data that the Edge Transport server must have to perform certain anti-spam tasks is replicated. The recipient information replicated to AD LDS includes the following:

- **Recipients** The list of recipients in the Exchange organization is replicated to AD LDS. Each recipient is identified by the GUID assigned to it in Active

Directory. If you configure a recipient's user account to deny receipt of mail from outside the organization, the recipient isn't replicated to AD LDS. If you disable or delete the mailbox for a recipient, it isn't replicated to AD LDS.

- **Proxy addresses** All proxy addresses assigned to each recipient are replicated to AD LDS as hashed data. This is a one-way hash that uses Secure Hash Algorithm (SHA)-256. SHA-256 generates a 256-bit message digest of the original data. Storing proxy addresses as hashed data helps secure this information in case the Edge Transport server or AD LDS is compromised. Proxy addresses are referenced when the Edge Transport server performs the recipient lookup anti-spam task.
- **Safe Senders List, Blocked Senders List, and Safe Recipients List** The Safe Senders Lists, Blocked Senders Lists and Safe Recipients Lists that are defined in each recipient's Outlook instance are aggregated and replicated to AD LDS. These settings are stored on the mailbox store where the recipient's mailbox resides. An Outlook user's safelist collection is the combined data from the user's Safe Senders List, Safe Recipients List, Blocked Senders List, and external contacts. Having safelist collection data available in AD LDS enables the Edge Transport server to screen senders appropriately, reducing the operational overhead involved with filtering mail. This information is sent as hashed data.

  Important:
  Although the safe recipient data is stored in Outlook and can be aggregated into the safelist collection on the AD LDS instance on the Edge Transport server, the content filtering functionality doesn't act on safe recipient data.

- **Per recipient anti-spam settings** By using the **Set-Mailbox** cmdlet, you can assign anti-spam threshold settings per recipient that differ from the organization-wide anti-spam settings. If you configure per recipient anti-spam settings, these settings override the organization-wide settings. By replicating these settings to AD LDS, the per recipient settings can be considered before the message is relayed to the Exchange organization. This information is sent as hashed data.

Topology Information

The topology information includes notification of newly subscribed Edge Transport servers or removed Edge Subscriptions. This data is refreshed every five minutes.

1.7.1.13.2 Understanding Edge Subscription Credentials

Understanding Edge Subscription Credentials

Transport > Understanding Transport > Understanding Edge Subscriptions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-18*

This topic explains how the Edge Subscription process provisions the credentials that are used to help secure the EdgeSync synchronization process in Microsoft Exchange Server 2010 and how the Microsoft Exchange EdgeSync service uses those credentials to establish a secure LDAP connection between a Hub Transport server and an Edge Transport server. To learn more about the Edge Subscription process, see Understanding Edge Subscriptions.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Edge Subscription Process

The Edge Transport server is subscribed to an Active Directory site to establish a synchronization relationship between the Hub Transport servers in an Active Directory site and the subscribed Edge Transport server. The credentials that are provisioned during the Edge Subscription process are used to help secure the LDAP connection between a Hub Transport server and an Edge Transport server in the perimeter network.

When you run the **New-EdgeSubscription** cmdlet in the Exchange Management Shell on an Edge Transport server, the EdgeSync bootstrap replication account (ESBRA) credentials are created in the Active Directory Lightweight Directory Services (AD LDS) directory on the local server and then written to the Edge Subscription file. These credentials are used only to establish the initial synchronization and will expire 1,440 minutes (24 hours) after the Edge Subscription file is created. If the Edge Subscription process isn't completed within that time, you must run the **New-EdgeSubscription** cmdlet in the Shell on the Edge Transport server again to create an Edge Subscription file.

The following table describes the data contained in the Edge Subscription XML file.

Edge Subscription file contents

Subscription data	Description
EdgeServerName	The NetBIOS name of the Edge Transport server. The name of the Edge Subscription in Active Directory will match this name.
EdgeServerFQDN	The fully qualified domain name (FQDN) of the Edge Transport server. The Hub Transport servers in the subscribed Active Directory site must be able to locate the Edge Transport server by using Domain Name System (DNS) to resolve the FQDN.
EdgeCertificateBlob	The public key of the Edge Transport server's self-signed certificate.
ESRAUsername	The name assigned to the ESBRA. The ESBRA account has the following format: ESRA.*Edge Transport server name*. ESRA means EdgeSync replication account.
ESRAPassword	The password assigned to the ESBRA. The password is generated by using a random number generator and is stored in the Edge Subscription file in clear text.

EffectiveDate	The creation date of the Edge Subscription file.
Duration	The length of time that these credentials will be valid before they expire. The ESBRA account is valid for only 24 hours.
AdamSslPort	The secure LDAP port to which the EdgeSync service binds when synchronizing data from Active Directory to AD LDS. By default, this is TCP port 50636.
ProductID	The licensing information for the Edge Transport server. After an Edge Transport server is subscribed to Active Directory, the licensing information about the Edge Transport server is displayed in the Exchange Management Console for the Exchange organization. You must license the Edge Transport server before you create the Edge Subscription for this information to be displayed correctly.
VersionNumber	The version number of the Edge Subscription file.
SerialNumber	The version of Exchange Server that is installed on the Edge Transport server.

Important:
The ESBRA credentials are written to the Edge Subscription file in clear text. You must protect this file throughout the subscription process. After the Edge Subscription file is imported to your Exchange organization, you should immediately delete the Edge Subscription file from the Edge Transport server, the network share you used to import the file to your Exchange organization, and any removable media.

Return to top

EdgeSync Replication Accounts

EdgeSync replication accounts (ESRA) are an important part of EdgeSync security. Authentication and authorization of the ESRA is the mechanism used to help secure the connection between an Edge Transport server and a Hub Transport server.

The ESBRA contained in the Edge Subscription file is used to establish a secure LDAP connection during the initial synchronization. After the Edge Subscription file is imported to a Hub Transport server in the Active Directory site to which the Edge Transport server is being subscribed, additional ESRA accounts are created in Active Directory for each Edge Transport-Hub Transport server pair. During initial synchronization, the newly created ESRA credentials are replicated to AD LDS. These ESRA credentials are used to help secure later synchronization sessions.

Each EdgeSync replication account is assigned the properties described in the following table.

Ms-Exch-EdgeSyncCredential properties

Property name	Type	Description
TargetServerFQDN	String	The Edge Transport server

		that will accept these credentials.
SourceServerFQDN	String	The Hub Transport server that will present these credentials. This value is empty if the credential is the bootstrap credential.
EffectiveTime	DateTime (UTC)	When to start using this credential.
ExpirationTime	DateTime (UTC)	When to stop using this credential.
UserName	String	The user name that's used to authenticate.
Password	Byte	The password that's used to authenticate. The password is encrypted by using **ms-Exch-EdgeSync-Certificate**.

The following sections of this topic describe how the ESRA credentials are provisioned and used during the EdgeSync synchronization process.

Provisioning the EdgeSync Bootstrap Replication Account

When the **New-EdgeSubscription** cmdlet is run on the Edge Transport server, the ESBRA is provisioned as follows:

- A self-signed certificate (Edge-Cert) is created on the Edge Transport server. The private key is stored in the local computer store and the public key is written to the Edge Subscription file.
- The ESBRA (ESRA.Edge) is created in AD LDS, and the credentials are written to the Edge Subscription file.
- The Edge Subscription file is exported by copying it to removable media. The file is now ready to import to a Hub Transport server.

Provisioning EdgeSync Replication Accounts in Active Directory

When the Edge Subscription file is imported on a Hub Transport server, the following steps occur to establish a record of the Edge Subscription in Active Directory and to provision additional ESRA credentials.

1. An Edge Transport server configuration object is created in Active Directory. The Edge-Cert certificate is written to this object as an attribute.
2. Every Hub Transport server in the subscribed Active Directory site receives an Active Directory notification that a new Edge Subscription has been registered. As soon as the notification is received, each Hub Transport server retrieves the ESRA.Edge account and encrypts the account by using the Edge-Cert public key. The encrypted ESRA.Edge account is written to the Edge Transport server configuration object.
3. Each Hub Transport server creates a self-signed certificate (Hub-Cert). The private key is stored in the local computer store and the public key is stored in the Hub Transport server configuration object in Active Directory.
4. Each Hub Transport server encrypts the ESRA.Edge account by using the public key of its own Hub-Cert certificate and then stores it in its own configuration object.
5. Each Hub Transport server generates an ESRA for each existing Edge Transport server configuration object in Active Directory (ESRA.Hub.Edge). The account name is generated by using the following naming convention: ESRA.*<Hub Transport server NetBIOS Name>*.*<Edge Transport server NetBIOS Name>*.*<Effective Date UTC Time>*

Example: ESRA.Hub.Edge.01032010
The password for ESRA.Hub.Edge is generated by a random number generator and is encrypted by using the public key of the Hub-Cert certificate. The generated password has the maximum length allowed for Microsoft Windows Server.

6. Each ESRA.Hub.Edge account is encrypted by using the public key of the Edge-Cert certificate and is stored on the Edge Transport server configuration object in Active Directory.

The following sections of this topic explain how these accounts are used during the EdgeSync synchronization process.

Return to top

Authenticating Initial Replication

The ESBRA account, ESRA.Edge, is used only when establishing the initial synchronization session. During the first EdgeSync synchronization session, the additional ESRA accounts, ESRA.Hub.Edge, are replicated to AD LDS. These accounts are used to authenticate later EdgeSync synchronization sessions.

The Hub Transport server that performs the initial replication is determined randomly. The first Hub Transport server in the Active Directory site to perform a topology scan and discover the new Edge Subscription performs the initial replication. Because this discovery is based on the timing of the topology scan, any Hub Transport server in the site may perform the initial replication.

The Microsoft Exchange EdgeSync service initiates a secure LDAP session from the Hub Transport server to the Edge Transport server. The Edge Transport server presents its self-signed certificate and the Hub Transport server verifies that the certificate matches the certificate that's stored on the Edge Transport server configuration object in Active Directory. After the Edge Transport server's identity is verified, the Hub Transport server provides the credentials of the ESRA.Edge account to the Edge Transport server. The Edge Transport server verifies the credentials against the account that's stored in AD LDS.

The Microsoft Exchange EdgeSync service on the Hub Transport server then pushes the topology, configuration, and recipient data from Active Directory to AD LDS. The change to the Edge Transport server configuration object in Active Directory is replicated to AD LDS. AD LDS receives the newly added ESRA.Hub.Edge entries and the Microsoft Exchange Credential Service creates the corresponding AD LDS account. These accounts are now available to authenticate later scheduled EdgeSync synchronization sessions.

Microsoft Exchange Credential Service

The Microsoft Exchange Credential Service is part of the Edge Subscription process. It runs only on the Edge Transport server. This service creates the reciprocal ESRA accounts in AD LDS so that a Hub Transport server can authenticate to an Edge Transport server to perform EdgeSync synchronization. The Microsoft Exchange EdgeSync service doesn't communicate directly with the Microsoft Exchange Credential Service. The Microsoft Exchange Credential Service communicates with AD LDS and installs the ESRA credentials whenever the Hub Transport server updates them.

Return to top

Authenticating Scheduled Synchronization Sessions

After initial EdgeSync synchronization finishes, the EdgeSync synchronization schedule is

established and data that has changed in Active Directory is regularly updated in AD LDS. A Hub Transport server initiates a secure LDAP session with the AD LDS instance on the Edge Transport server. AD LDS proves its identity to that Hub Transport server by presenting its self-signed certificate. The Hub Transport server presents its ESRA.Hub.Edge credentials to AD LDS. The ESRA.Hub.Edge password is encrypted by using the Hub Transport server's self-signed certificate's public key. This means that only that particular Hub Transport server can use those credentials to authenticate to AD LDS.

Return to top

Renewing EdgeSync Replication Accounts

The password for the ESRA account must comply with the local server's password policy. To prevent the password renewal process from causing temporary authentication failure, a second ESRA.Hub.Edge account is created seven days before the first ESRA.Hub.Edge account expires with an effective time that's three days before the first ESRA expiration time. As soon as the second ESRA account becomes effective, EdgeSync stops using the first account and starts to use the second account. When the expiration time for the first account is reached, those ESRA credentials are deleted. This renewal process will continue until the Edge Subscription is removed.

Return to top

1.7.1.14 Understanding Edge Transport Server Cloned Configuration

Understanding Edge Transport Server Cloned Configuration

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Microsoft Exchange Server 2010 Edge Transport server role stores its configuration information in Active Directory Lightweight Directory Services (AD LDS). You can install more than one Edge Transport server in the perimeter network and use Domain Name System (DNS) round robin, a simple mechanism that's used by DNS servers to share and distribute loads for network resources, to help balance network traffic among the Edge Transport servers.

To make sure that all Edge Transport servers that you deploy are using the same configuration information, you can use the provided cloned configuration scripts in the Exchange Management Shell to duplicate the configuration of a source server to a target server.

You use *cloned configuration* to deploy new Edge Transport servers based on a configured source server. The configuration information for the source server is duplicated and then exported to an XML file. The XML file is then imported to the target server.

This topic provides an overview of the cloned configuration process. For detailed steps about configuring your Edge Transport servers using cloned configuration, see Configure Edge Transport Server Using Cloned Configuration.

Cloned Configuration and EdgeSync

Run the EdgeSync process after you import the cloned configuration. To perform recipient lookup and message security tasks, the computer that has the Edge Transport server role

installed requires data that resides in Active Directory. *EdgeSync* is a collection of processes that are run on a computer that has the Hub Transport server role installed to establish one-way replication of recipient and configuration information from Active Directory to the AD LDS instance on an Edge Transport server. The Microsoft Exchange EdgeSync service copies only the information that's required for the Edge Transport server to perform anti-spam tasks and the information about the connector configuration that's required to enable end-to-end mail flow. The Microsoft Exchange EdgeSync service performs scheduled updates so that the information in AD LDS remains current.

Cloned configuration doesn't duplicate the Edge Subscription settings of a server. The certificates that are used by the Microsoft Exchange EdgeSync service aren't cloned. You must run the EdgeSync process separately for each Edge Transport server. The Microsoft Exchange EdgeSync service overwrites any settings that are included in both cloned configuration information and in EdgeSync replication information. These settings include Send connectors, Receive connectors, accepted domains, and remote domains.

Cloned Configuration Process

The cloned configuration process consists of three steps:

1. Export the configuration on the source server.
   In this step, you run the ExportEdgeConfig.ps1 script to export the source server's configuration information to an intermediate XML file.
2. Validate the configuration on the target server.
   In this step, you run the ImportEdgeConfig.ps1 script. This script checks the existing information in the intermediate XML file to see whether the settings that were exported are valid for the target server and then creates an answer file. The answer file specifies the server-specific information that's used during the next step when you import the configuration on the target server. The answer file contains entries for each source server setting that isn't valid for the target server. You can modify these settings so that they're valid for the target server. If all settings are valid, the answer file contains no entries.
3. Import the configuration on the target server.
   In this step, the ImportEdgeConfig.ps1 script uses the intermediate XML file and the answer file to clone an existing configuration or to restore the server to a specific configuration.

These steps are described in detail in the following sections.

Step 1: Export the Configuration

After you install and configure the Edge Transport server role, run the ExportEdgeConfig.ps1 script. This script retrieves the source server's configuration information and stores the information in an intermediate XML file.

The following information is exported from the source server and stored in the intermediate XML file:

- Transport server-related information and log file path information. The following file paths are exported:
  - ReceiveProtocolLogPath
  - SendProtocolLogPath
  - MessageTrackingLogPath
  - PickupDirectoryPath
  - RoutingTableLogPath
- Transport agent-related information that includes the status and priority settings of each transport agent.
- All Send connector-related information. If any Send connectors are configured to use credentials, the password is written to the intermediate XML file as an encrypted string. You can use the *-key* parameter with the ImportEdgeConfig.ps1 and ExportEdgeConfig.ps1 scripts to specify the 32-

byte string to use for password encryption and decryption. If you don't use the *-key* parameter, a default encryption key is used.
- Receive connector-related information. To modify the local network binding and port properties, you must modify the configuration information in the answer file that's created in the validate configuration step.
- Accepted domain configuration.
- Remote domain configuration.
- Anti-spam features configuration settings. The following information is exported:
  - IP Allow list information. Only the IP Allow list entries that were manually configured by the administrator are exported.
  - IP Block list information.
  - Content filter configuration.
  - Recipient filter configuration.
  - Address rewrite entries.
  - Attachment filter entries.

Step 2: Validate the Configuration

The target server is an Exchange 2010 server that has a clean installation of the Edge Transport server role. Run the ImportEdgeConfig.ps1 script on the target server to validate the existing information in the intermediate XML file and to create the answer file. The answer file specifies the server-specific information that's used during the next step in the cloned configuration process when you import the configuration on the target server. The answer file contains entries for each source server setting that isn't valid for the target server. You can modify these settings so that they're valid for the target server. If all settings are valid, the answer file contains no entries. The intermediate XML file can be used for different target servers. The answer file is specific to a target server.

The ImportEdgeConfig.ps1 script performs the following tasks during this step:

- The script verifies that the data paths and log paths can be created on the target server. If the paths can't be created, a blank path is inserted into the answer file.
- For each Send connector in the XML file, the script adds a blank entry for the source IP address in the answer file.
- For each Receive connector in the XML file, the script adds a blank entry for the local network bindings in the answer file.

You must manually modify the answer file to provide the following information about server-specific settings:

- Fill in the data paths and log paths. If these paths are left blank in the answer file, the paths that are configured in the intermediate XML file are used in the next step when you import the configuration on the target server.
- For each Send connector entry, fill in the source IP address. If this field is left blank, an error occurs in the import configuration step.
- For each Receive connector entry, fill in the local network bindings. If the local network bindings are left blank, an error occurs in the next step when you import the configuration on the target server.

Step 3: Import the Configuration

Perform this step on any target server to clone the configuration of an existing Edge Transport server or to restore the server to a specific configuration. Run the ImportEdgeConfig.ps1 script to validate and import the new configuration. After you run this script, the target server's configuration matches the settings in the intermediate XML file and the answer file.

Important:

It's a best practice to back up the existing server configuration before you run the import configuration process, so that if the cloning operation fails, the server can be restored to the previous stable state.

This step uses the server-specific information that's provided in the answer file. If a setting isn't specified in the answer file, the data in the intermediate XML file is used. Before the script modifies the configuration, the script validates the data in the intermediate XML file and the answer file.

The following configuration settings of the target server are modified during the import configuration step:

- The transport agent configuration is modified.
- The existing connectors on the target server are removed, and the connectors that are present in the intermediate XML file are added.
- The existing accepted domains are removed, and the accepted domain entries in the intermediate XML file are added.
- The existing remote domains are removed, and the remote domain entries in the intermediate XML file are added.
- The existing IP Allow list entries are removed, and the IP Allow list entries in the intermediate remote domains file are added.
- The existing IP Block list entries are removed, and the IP Block list entries in the intermediate remote domains file are added.
- The following anti-spam configuration is cloned to the target server:
  - Content filter configuration
  - Recipient filter configuration
  - Address rewrite entries
  - Attachment filter entries

Transport Configuration Information

The settings of the transport configuration object define server-wide e-mail transport settings for an Edge Transport server. When you import the intermediate XML file to the target server, all the settings of the transport configuration object except for the following are imported:

- General names and creation dates from the exported XML file
- Send connector information
- Receive connector information
- Attachment filter entries
- The **MaxDumpsterSizePerStorageGroup** attribute entry

After the import process is complete, you may also configure the settings by using the **Set-TransportConfig** cmdlet. For more information, see Set-TransportConfig.

The following table describes the attributes that are associated with the transport configuration object and the default values. You configure this object on both Hub Transport servers and Edge Transport servers. However, many attributes apply only to Hub Transport servers and configuring those attributes on an Edge Transport server will have no effect.

Transport configuration attributes and default values

Attribute	Description	Default value
ClearCategories	This attribute specifies whether to clear Microsoft Office Outlook categories during content conversion.	True
GenerateCopyOfDSNFor	This attribute specifies the delivery status notification (DSN) codes that cause the DSN message to be copied to the postmaster e-mail	5.4.8, 5.4.6, 5.4.4, 5.2.4, 5.2.0, 5.1.4

	address. DSN codes are entered as *x.y.z* and are separated by commas.	
InternalSMTPServers	This attribute specifies a list of internal SMTP server IP addresses or IP address ranges that should be ignored by Sender ID and connection filtering.	Null
JournalingReportNdrTo	This attribute specifies the e-mail address to which journal reports are sent if the journaling mailbox is unavailable. This attribute doesn't apply to the configuration of an Edge Transport server.	Null
MaxDumpsterSizePerStorageGroup	This attribute specifies the maximum size of the transport dumpster on a Hub Transport server. This attribute doesn't apply to the configuration of an Edge Transport server.	18 MB
MaxDumpsterTime	This attribute specifies how long an e-mail message should remain in the transport dumpster on a Hub Transport server. This attribute doesn't apply to the configuration of an Edge Transport server.	7.00:00:00
MaxReceiveSize	This attribute specifies the maximum message size that can be received by recipients in the organization. This attribute doesn't apply to the configuration of an Edge Transport server.	10 MB
MaxRecipientEnvelopeLimit	This attribute specifies the maximum number of recipients that are allowed in a single e-mail message. This attribute doesn't apply to the configuration of an Edge Transport server.	5,000
MaxSendSize	This attribute specifies the maximum message size that can be sent by senders in the organization. This attribute doesn't apply to the configuration of an Edge Transport server.	10 MB

TLSReceiveDomainSecureList	This attribute specifies the remote domains that will use mutual Transport Layer Security (TLS) authentication through Receive connectors configured to support Domain Security. Multiple domains may be separated by commas. The wildcard character (*) isn't supported in the domains that are listed in this attribute.	Null
TLSSendDomainSecureList	This attribute specifies the remote domains that will use mutual TLS authentication when e-mail is sent through a Send connector configured to support Domain Security and the address space of the target domain. Multiple domains may be separated by commas. The wildcard character (*) isn't supported in the domains that are listed in this attribute.	Null
VerifySecureSubmitEnabled	This attribute verifies that e-mail clients that are submitting messages from mailboxes on Mailbox servers are using encrypted MAPI submission. This attribute doesn't apply to the configuration of an Edge Transport server. The valid values for this attribute are `$true` or `$false`.	False
VoicemailJournalingEnabled	This attribute specifies whether Unified Messaging voice mail is journaled by the Journaling agent. This attribute doesn't apply to the configuration of an Edge Transport server.	True
Xexch50Enabled	This attribute specifies whether Xexch50 authentication should be enabled for backward compatibility with Exchange Server 2003 servers.	True

Note:

If the Edge Transport server is subscribed to the Exchange organization later, the value of the **InternalSMTPServers** attribute is overwritten during the EdgeSync process. For more information, see Understanding Edge Subscriptions.

1.7.1.15 Understanding the EdgeTransport.exe.Config File

Understanding the EdgeTransport.exe.Config File

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-09*

The EdgeTransport.exe.config file is an XML application configuration file that is associated with the EdgeTransport.exe file. By default, it's located in the C:\Program Files\Microsoft \Exchange Server\V14\Bin directory.

EdgeTransport.exe and MSExchangeTransport.exe are the executable files that are used by the Microsoft Exchange Transport service. This service runs on every Hub Transport server or Edge Transport server. Changes that are saved to the EdgeTransport.exe.config file are applied after the Microsoft Exchange Transport service is restarted. The default value is enforced if either of the following conditions is true:

- A configuration option is missing.
- A configuration option is present and contains the default value.

The following example shows the typical structure of the EdgeTransport.exe.config file:

```
<configuration>

<runtime>

<gcServer enabled="true" />

</runtime>

<appSettings>

<add key="Configuration Option" value="Value" />

...

</appSettings>

</configuration>
```

You can add new configuration options or modify existing configuration options in the <appSettings> section.

Note:

The parameter names in the <add key=../> section are case sensitive.

1.7.1.16 Understanding Exchange 2010 Support for X.400 Authoritative Domains

Understanding Exchange 2010 Support for X.400 Authoritative Domains

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-18*

This topic describes the support that Microsoft Exchange Server 2010 provides for X.400 domains. Exchange 2010 enables the configuration of one or more X.400 authoritative domain namespaces by using Exchange Management Shell commands.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

X.400 Addresses

An X.400 address is an address that's defined as part of a suite of e-mail standards that are defined by International Telecommunication Union - Telecommunication [Standardization Sector] (ITU-T) recommendations. An X.400 address uses a hierarchical naming system and consists of a series of attributes, the sum of which form the X.400 address. Some attributes in the address specify the organization. Other attributes specify the recipient. The sum of all the organizational attributes specifies a unique node in the X.400 address hierarchy.

Exchange 2010 doesn't support the following X.400 scenarios:

- Sharing an X.400 address node with another e-mail system. In Exchange 2010, you can share an SMTP domain namespace by configuring an internal relay accepted domain. You can't use this configuration for an X.400 namespace. Exchange 2010 must be authoritative for the X.400 domain. Alternatively, the X.400 domain must be configured as an external relay subdomain of an authoritative X.400 domain.
- Configuring an X.400 authoritative domain on the Edge Transport server.
- Configuring an X.400 authoritative domain in the Exchange Management Console. You must use the Shell to configure X.400 authoritative domains.
- Routing or relaying directly to an X.400 message transfer agent (MTA). Exchange 2010 must route through a source server that's running Microsoft Exchange Server 2003 and hosting an X.400 connector, or through a third-party Exchange 2010 X.400 connector.

Return to top

Configuring X.400 Authoritative Domains

You configure an X.400 authoritative domain on the Hub Transport server role. When an

organization is configured as authoritative for a particular domain, it's assumed that the organization hosts all the mailboxes for recipients in that domain. After you create an X.400 authoritative domain name, you can create an e-mail address policy that specifies that domain in the e-mail proxy address. The Exchange organization accepts e-mail that's addressed to recipients who have been assigned an X.400 e-mail proxy address that uses the X.400 authoritative domain namespace. Any X.400 recipient addresses in the authoritative namespace that don't resolve to a mailbox or a contact in Active Directory are treated as an error and cause messages to result in a non-delivery report (NDR). If the message that causes the error is a delivery status notification (DSN), such as an NDR, it's deleted.

Exchange 2010 supports non-authoritative X.400 domains if they're a subdomain of an authoritative domain. You use the *X400ExternalRelay* parameter of the **New-X400AuthoritativeDomain** cmdlet to define any exceptions where the Exchange organization isn't authoritative for a subdomain of the authoritative X.400 domain. By default, the value of the *X400ExternalRelay* parameter is set to `$false`. Therefore, a recipient resolution failure for an e-mail message that's sent to a recipient in the X.400 subdomain results in an NDR. If the value of the *X400ExternalRelay* parameter is set to `$true`, Exchange doesn't treat recipient resolution failures as an error and routes messages that are addressed to a recipient in the X.400 subdomain to an external address.

Defining an X.400 Namespace

By default, when you configure an X.400 authoritative domain, the Exchange organization is considered authoritative for all X.400 addresses in the hierarchy.

An X.400 address consists of a series of attributes that define organizational components and specify recipients. The X.400 namespace that's specified in the *X400DomainName* parameter can only include the X.400 organizational components. The following table lists the attributes that you can use to define an X.400 domain namespace in Exchange 2010. The attributes are listed in hierarchical order.

X.400 organizational components

Attribute abbreviation	Organizational component	Required/Optional	Maximum character length
C	**Country** The value of the **Country** attribute is the two-letter country/region designation from International Organization for Standardization (ISO) 3166. This attribute identifies the country or region of the X.400 domain namespace.	Required	2
A	**ADMD** The value of the Administration Management Domain (**ADMD**) typically identifies a public mail service provider. Valid values are decided on a country or regional basis.	Required	16
P	**PRMD** The value of	Optional	16

	the Private Management Domain (**PRMD**)defines the top level domain in the namespace of the Exchange organization.		
O	**Organization** The value of the **Organization** attribute is unique within the context of the **PRMD** or of the **ADMD** if there is no **PRMD**.	Optional	64
OU1	**Organizational unit 1** The value of each organizational unit identifies a unique address element within the scope of the immediately superior address element in the hierarchy.	Optional	64
OU2	**Organizational unit 2** The value of each organizational unit identifies a unique address element within the scope of the immediately superior address element in the hierarchy.	Optional	64
OU3	**Organizational unit 3** The value of each organizational unit identifies a unique address element within the scope of the immediately superior address element in the hierarchy.	Optional	64
OU4	**Organizational unit 4** The value of each organizational unit identifies a unique address element within the scope of the immediately superior address element in the hierarchy.	Optional	64

When you specify the X.400 namespace, the address attributes must be separated by semicolons and the address must be enclosed in quotation marks ("), as in the following example.

```
"C=US;A=ATT;P=Contoso;O=Example"
```

X.400 domain names can only include the following ASCII characters:

- A to Z
- a to z
- 0–9
- These punctuation and special characters: (space) ' () + , - . / : = ?

The inclusion of a wildcard character, such as an asterisk (*), isn't supported in the X.400 authoritative namespace. Each attribute can appear only one time in the X.400 namespace.

Any address in the hierarchy that's subordinate to the defined organizational components must resolve to a recipient or contact in Active Directory, unless an exception has been defined for a subdomain by specifying the *X400ExternalRelay* parameter as `$true`. If the categorizer can't resolve a recipient, an NDR is generated for a message. If the message is a DSN, it's deleted.

For example, if you've configured an X.400 authoritative domain as `"C=US;A=ATT;O=Contoso"`, the Exchange organization is also considered authoritative for the X.400 namespace `"C=US;A=ATT;O=Contoso;OU1=Tailspin Toys"`. If all the recipients for Tailspin Toys are located in another organization, each of those recipients must be represented as a contact in the Active Directory of the Contoso organization. If you can't do this, the Tailspin Toys namespace must be defined as an external relay subdomain.

Return to top

Recipient Resolution and Routing for X.400 Authoritative Domains

To determine how to handle routing of e-mail messages, the Exchange 2010 categorizer compares the recipient addresses to the list of domains for which the Exchange organization is authoritative. This enables the categorizer to determine when to route an X.400 addressed message to an external system and when to generate an NDR for a message if the recipient isn't found in the authoritative namespace. If a message is being sent to a recipient address in an X.400 domain for which the Exchange organization is authoritative, the message is delivered to valid recipients, In addition, an NDR is returned to the sender for any recipient that doesn't appear in Active Directory. If a message is being sent to an X.400 domain for which the Exchange organization isn't authoritative, the message is routed externally through an X.400 connector.

After an X.400 authoritative namespace has been defined, the Exchange organization is assumed to be responsible for message delivery to all recipients that have e-mail proxy addresses that match the namespace. Therefore, X.400 addressed messages that are received by an Exchange 2010 Hub Transport server are processed as follows:

- If the recipient address resolves to a recipient in Active Directory, the message is delivered.
- An NDR is returned to the sender if all the following conditions are true:
  - The recipient address doesn't resolve to a recipient in Active Directory.
  - The recipient address matches an X.400 namespace for which Exchange is authoritative.
  - The e-mail is a message.

- The e-mail is deleted if all the following conditions are true:
  - The recipient address doesn't resolve to a recipient in Active Directory.
  - The recipient address matches an X.400 namespace for which Exchange is authoritative.
  - The e-mail is a DSN.
- The e-mail is routed to an X.400 connector if all the following conditions are true:
  - The recipient address doesn't resolve to a recipient in Active Directory.
  - The recipient address doesn't match an X.400 namespace for which Exchange is authoritative.
  - The e-mail is routed to an X.400 connector.

Although you can configure recipients to receive e-mail that's addressed to an X.400 namespace, Exchange 2010 doesn't provide native transport support for X.400. To send or receive X.400 e-mail messages to or from remote X.400 domains, you must maintain one or more X.400 connectors on an Exchange 2003 server, or configure a Foreign connector to the X.400 backbone.

Exchange 2010 doesn't have an X.400 MTA. Therefore, Exchange 2010 can't convert messages to the X.400 format. An X.400 connector that's hosted on an Exchange 2003 server or a Foreign connector must process the message so that conversion to an X.400 message occurs. To transport X.400 messages, Exchange 2010 routes the message over SMTP as a MIME-encapsulated Transport Neutral Encapsulation Format (TNEF) message.

For more information about how to create an X.400 connector on Exchange 2003, see How to Create an X.400 Connector. For more information about how to create a Foreign connector, see Create a Foreign Connector.

Return to top

1.7.1.17 Understanding Foreign Connectors

Understanding Foreign Connectors

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-26*

A Foreign connector can only be installed on a computer that's running Microsoft Exchange Server 2010 and that has the Hub Transport server role installed. A Foreign connector uses a Drop directory to send messages to a local messaging server that doesn't use SMTP as its primary transport mechanism.

Overview of Foreign Connectors

Exchange 2010 Hub Transport servers require Foreign connectors to deliver messages to foreign gateway servers that don't use SMTP to transmit messages. Third-party fax gateway servers are examples of foreign gateway servers. A Foreign connector controls outbound connections from the Hub Transport server to the foreign gateway server. The outbound messages are put in a Drop directory on the Hub Transport server or in a network file share on a remote server. Each Foreign connector uses its own Drop directory. The foreign gateway server must be configured to obtain messages from the Drop directory that's specified for that Foreign connector.

Foreign connectors that are created on Hub Transport servers are stored in Active

Directory and are available to all Hub Transport servers in the organization. In Active Directory, a Foreign connector is created as an object in the connections container. When a Hub Transport server in the organization routes messages to an address space configured on a Foreign connector, the message is delivered to a source Hub Transport server for that Foreign connector to be relayed to the destination domain. You can specify several different Hub Transport servers in your organization as source servers for a Foreign connector. This provides fault tolerance for the Foreign connector. If a Hub Transport server that contains the Foreign connector is unavailable, the messages that are destined for the Foreign connector's address space are relayed by using any of the other defined and available Hub Transport servers. To provide this fault tolerance, you must make sure that the Drop directory that's specified by the Foreign connector is accessible by all Hub Transport servers that are designated as source servers for that Foreign connector.

Foreign gateway servers can send messages into the Exchange 2010 organization by using the Replay directory that exists on the Hub Transport server. Correctly formatted e-mail message files that you copy to the Replay directory are submitted for delivery.

For more information about the Replay directory, see Understanding the Pickup and Replay Directories.

Defining the Usage of a Foreign Connector by Using Address Spaces and Connector Scope

The address space for a Foreign connector specifies the recipient domains to which the Foreign connector will route e-mail. You can specify SMTP address spaces or non-SMTP address spaces. In Exchange 2010, the complete syntax for specifying an address space is as follows.

```
<AddressSpaceType>:<AddressSpace>;<AddressSpaceCost>
```

You can use the scope of a Foreign connector to control the visibility of the Foreign connector within the Exchange organization. By default, all Foreign connectors that you create are usable by all the Hub Transport servers in the Exchange organization. However, you can limit the scope of any Foreign connector so that it's only usable by other Hub Transport servers that exist in the same Active Directory site.

The connector scope is specified by using the *IsScopedConnector* parameter in the **New-ForeignConnector** cmdlet or the **Set-ForeignConnector** cmdlet. When the value of this parameter is `$false`, the connector can be used by all Hub Transport servers in the Exchange organization. When the value of this parameter is `$true`, the connector can only be used by Hub Transport servers in the same Active Directory site.

Foreign Connector DSN Handling

When a message is sent with a delivery confirmation request to an address that's serviced by a Foreign connector, the sender should be notified if the recipient's messaging server can't correctly process the delivery confirmation request. A Relayed delivery status notification (DSN) notifies the sender that the recipient's messaging system is unable to forward delivery confirmation requests. By default, Relayed DSN messages aren't generated for messages sent to the address spaces that are serviced by a Foreign connector. DSN messages are defined in RFC 1894. For more information about DSN messages, see Managing Delivery Status Notifications.

Delivery Agent Connectors

Exchange 2010 introduces a new feature called Delivery Agent connector, which is also used to route messages to foreign systems that don't use the SMTP protocol. When a message is routed to a Delivery Agent connector, the associated delivery agent performs

the content conversion and message delivery. Delivery Agent connectors allow queue management of Foreign connectors, thereby eliminating the need for storing messages on the file system in a Drop directory. They provide greater control over the message delivery to the foreign systems. To learn more, see Understanding Delivery Agents.

1.7.1.18 Understanding Group Metrics

Understanding Group Metrics

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-07*

Group metrics is the collection of the following data about distribution groups and dynamic distribution groups in your organization:

- Number of members
- Number of members who are external to your organization

Group metrics data is used to support MailTips in Microsoft Exchange Server 2010. MailTips are informative messages displayed to senders while they're composing messages. For more information about MailTips, including a full list of MailTips available in Exchange 2010, see Understanding MailTips.

Group metrics data is used when deciding whether to display the following MailTips:

- **Large Audience** This MailTip is displayed when a sender adds a distribution group whose membership count is considered a large audience as configured in your organization. By default, any message addressed to more than 25 recipients is considered a large audience.
- **External Recipients** This MailTip is displayed when a sender adds a distribution group that has members who are external to your organization.

Determining these characteristics of distribution groups and dynamic distribution groups isn't a simple task. MailTips are evaluated every time a recipient is added to a message composed by a user. Calculating this information while senders compose messages isn't feasible because it would delay the display of MailTips, and it could have an adverse performance impact depending on the size of your organization.

To provide this valuable information to senders without an adverse performance impact, Exchange calculates group metrics data as a background process that can be scheduled to run during nonbusiness hours. When evaluating recipients for MailTips, Exchange reads the group metrics data.

Looking for management tasks related to MailTips? See Managing MailTips.

Group Metrics Generation and Distribution

By default, group metrics data is generated on the same Mailbox server that generates the offline address book (OAB). This is the case even if you explicitly disable group metrics generation on that server using the **Set-MailboxServer** cmdlet. The Mailbox server generates full group metrics data for all distribution groups and dynamic distribution groups every Sunday, and incremental updates for any groups that were modified since the last full generation. The day of the full group metrics data generation is fixed, but you can configure the time it's generated daily. By default, group metrics data is generated daily at a random time within two hours of midnight.

The following files are associated with group metrics:

- **GroupMetrics-<*date*>T<*time*>.bin** This binary file is the main group metrics data file. It contains the membership and external members count for all distribution groups and dynamic distribution groups in your organization. The date and time sections of the file name are separated by hyphens. For example, a group metrics data file created on January 18, 2010 at 20:00 (8:00 P.M.) has the following file name: GroupMetrics-2010-01-18T20-00-00.bin.
- **GroupMetrics-<*servername*>.xml** This XML file contains information about the Mailbox server configured to generate the group metrics data. This file is required by the Microsoft Exchange File Distribution service, and it points to the binary file that needs to be distributed.
- **ChangedGroups.txt** This file contains the list of groups that were updated the last time group metrics data was generated.

Group metrics data won't be generated by default in the following scenarios:

- You don't use OABs in your organization, or you use only public folders for OAB distribution.
- The server responsible for OAB generation is a server running Microsoft Exchange Server 2007 with the Mailbox server role installed.

If any of these scenarios apply to you, you must configure an Exchange 2010 Mailbox server manually to start generating group metrics. For detailed steps, see Configure Group Metrics.

The group metrics data is distributed to the Client Access servers using the Microsoft Exchange File Distribution service. The Microsoft Exchange File Distribution service queries Active Directory for a list of Mailbox servers that have group metrics generation enabled, and then copies the group metrics data from the closest Mailbox server every eight hours.

1.7.1.19 Understanding Header Firewall

Understanding Header Firewall

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-27*

In Microsoft Exchange Server 2010, *header firewall* is a mechanism that removes specific header fields from inbound and outbound messages. Computers that are running Exchange 2010 that have the Hub Transport server role or the Edge Transport server role installed insert custom X-header fields into the message header. An *X-header* is a user-defined, unofficial header field that exists in the message header. X-headers aren't specifically mentioned in RFC 2822, but the use of an undefined header field starting with **X-** has become an accepted way to add unofficial header fields to a message. Messaging applications, such as anti-spam, antivirus, and messaging server applications may add their own X-headers to a message. X-header fields are usually preserved but ignored by messaging servers and clients that don't use them.

The X-header fields contain details about the actions that are performed on the message by the transport server, such as the spam confidence level (SCL), content filtering results, and rules processing status. Revealing this information to unauthorized sources could pose a potential security risk.

Header firewall prevents the spoofing of these X-headers by removing them from inbound messages that enter the Exchange organization from untrusted sources. Header firewall prevents the disclosure of these X-headers by removing them from outbound messages that will go to untrusted destinations outside the Exchange organization. Header firewall

also prevents the spoofing of standard routing headers that are used to track the routing history of a message.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Custom Organization X-Headers and Forest X-Headers That Are Used in Exchange 2010

Organization X-headers start with **X-MS-Exchange-Organization-**. Forest X-headers start with **X-MS-Exchange-Forest-**.

The following table describes some of the organization X-headers and forest X-headers that are used in messages in an Exchange 2010 organization.

Some of the organization X-headers and forest X-headers that are used in messages in an Exchange 2010 organization

X-header	Description
X-MS-Exchange-Forest-RulesExecuted	This X-header lists the transport rules that were performed on the message.
X-MS-Exchange-Organization-Antispam-Report	This X-header is a summary report of the anti-spam filter results that have been applied to the message by the Content Filter agent.
X-MS-Exchange-Organization-AuthAs	This X-header is always present when the security of a message has been evaluated. This X-header specifies the authentication source. The possible values are `Anonymous`, `Internal`, `External`, or `Partner`.
X-MS-Exchange-Organization-AuthDomain	This X-header is populated during Domain Secure authentication. The value is the fully qualified domain name (FQDN) of the remote authenticated domain.
X-MS-Exchange-Organization-AuthMechanism	This X-header specifies the authentication mechanism for the submission of the message. The value is a 2-digit hexadecimal number.
X-MS-Exchange-Organization-AuthSource	This X-header specifies the FQDN of the

	server computer that evaluated the authentication of the message on behalf of the organization.
X-MS-Exchange-Organization-Journal-Report	This X-header identifies journal reports in transport. As soon as the message leaves the transport server, the header becomes X-MS-Journal-Report.
X-MS-Exchange-Organization-OriginalArrivalTime	This X-header identifies the time when the message first entered the Exchange organization.
X-MS-Exchange-Organization-Original-Sender	This X-header identifies the original sender of a quarantined message when it first entered the Exchange organization.
X-MS-Exchange-Organization-OriginalSize	This X-header identifies the original size of a quarantined message when it first entered the Exchange organization.
X-MS-Exchange-Organization-Original-Scl	This X-header identifies the original SCL of a quarantined message when it first entered the Exchange organization.
X-MS-Exchange-Organization-PCL	This X-header identifies the phishing confidence level. The possible phishing confidence level values are from 1 through 8. A larger value indicates a suspicious message. For more information, see Understanding Anti-Spam Stamps.
X-MS-Exchange-Organization-Quarantine	This X-header indicates that the message has been quarantined in the spam quarantine mailbox and a delivery status notification (DSN) has been sent. Alternatively, it indicates that the message was quarantined and released by the administrator. This X-header field prevents the released message from being submitted to the spam quarantine mailbox again. For more information, see Release Quarantined Messages from the Spam Quarantine Mailbox.
X-MS-Exchange-Organization-SCL	This X-header identifies the SCL of the message. The possible SCL values are from 0 through 9. A larger value indicates a suspicious message. The special value -1 exempts the message from processing by the Content Filter agent. For more information, see Understanding Content Filtering.
X-MS-Exchange-Organization-SenderIdResult	This X-header contains the results of the Sender ID agent. The Sender ID agent uses the sender policy framework (SPF) to compare the message's source IP address to the domain that's used in the sender's e-mail address. The Sender ID results are used to calculate the SCL of a message. For

	more information, see Understanding Sender ID.

Return to top

Header Firewall for Organization X-Headers and Forest X-Headers

Exchange 2010 applies header firewall to organization X-headers and forest X-headers that exist in messages in the following ways:

- Permissions that can be used to preserve or remove specific X-headers in messages are assigned to Send connectors or Receive connectors.
- Header firewall is automatically implemented for X-headers in messages during other types of message submission.

How Header Firewall Is Applied to Organization X-Headers and Forest X-headers in Messages

Header firewall for organization X-headers and forest X-headers that exist in inbound messages consists of two specific permissions that are assigned to a Receive connector that's configured on a Hub Transport server or an Edge Transport server:

- If the permissions are assigned to the Receive connector, header firewall isn't applied to the message. The organization X-headers or forest X-headers in the message are preserved.
- If the permissions aren't applied to the Receive connector, header firewall is applied to the message. The organization X-headers or forest X-headers are removed from the message.

The following table describes the header firewall permissions for organization X-headers and forest X-headers that are available on a Receive connector.

Header firewall permissions for organization X-headers and forest X-headers that are available on a Receive connector for inbound messages

Permission	By default, the security principals that have the permission assigned	Permission group that has the security principals as members	By default, the usage type that assigns the permission groups to the Receive connector	Description
Ms-Exch-Accept-Headers-Organization	• Hub Transport servers • Edge Transport servers • Exchange Servers **Note:** On Hub Transport servers only	ExchangeServers	Internal	This permission applies to organization X-headers. Organization X-headers start with **X-MS-Exchange-Organization-**. If this permission isn't granted,

				the receiving server removes any organization headers from the message.
Ms-Exch-Accept-Headers-Forest	• Hub Transport servers • Edge Transport servers • Exchange Servers **Note:** On Hub Transport servers only	ExchangeServers	`Internal`	This permission applies to forest X-headers. Forest X-headers start with **X-MS-Exchange-Forest-**. If this permission isn't granted, the receiving server removes any forest headers from the message.

If you want to apply header firewall to organization X-headers and forest X-headers in a custom Receive connector scenario, use any of the following methods:

- Create a Receive connector and select a usage type other than `Internal`. The Receive connector usage type can only be set when you create the connector. For more information, see Create an SMTP Receive Connector.
- Modify an existing Receive connector and remove the ExchangeServers permission group. For more information, see Configure Receive Connector Properties.
- Use the **Remove-ADPermission** cmdlet to remove the Ms-Exch-Accept-Headers-Organization permission and the Ms-Exch-Accept-Headers-Forest permission from a security principal that's configured on the Receive connector. This method doesn't work if the permission has been assigned to the security principal by using a permission group. You can't modify the assigned permissions or the group membership of a permission group. For more information, see Remove-ADPermission.
- Use the **Add-ADPermission** cmdlet to deny the Ms-Exch-Accept-Headers-Organization permission and the Ms-Exch-Accept-Headers-Forest permission to a security principal that's configured on the Receive connector. For more information, see Add-ADPermission.

How Header Firewall Is Applied to Organization X-Headers and Forest X-Headers in Outbound Messages

Header firewall for organization X-headers and forest X-headers that exist in outbound messages consists of two specific permissions that are assigned to a Send connector that's configured on a Hub Transport server or an Edge Transport server:

- If the permissions are assigned to the Send connector, header firewall isn't applied to the message. The organization X-headers or forest X-headers in the message are preserved.
- If the permissions aren't applied to the Send connector, header firewall is applied to the message. The organization X-headers and forest X-headers are removed from the message.

The following table describes the header firewall permissions for organization X-headers and forest X-headers that are available on a Send connector.

Header firewall permissions for organization X-headers and forest X-headers that are available on a Send connector for outbound messages

Permission	By default, the security principals that have the permission assigned	By default, the usage type that assigns the security principals to the Send connector	Description
Ms-Exch-Send-Headers-Organization	• Hub Transport servers • Edge Transport servers • Exchange Servers **Note:** On Hub Transport servers only • Externally Secured servers • Exchange Legacy Interop universal security group • Exchange Server 2003 bridgehead servers	`Internal`	This permission applies to organization X-headers. Organization X-headers start with **X-MS-Exchange-Organization-**. If this permission isn't granted, the sending server removes any organization headers from the message.
Ms-Exch-Send-Headers-Forest	• Hub Transport servers • Edge Transport servers • Exchange Servers **Note:** On Hub Transport servers only • Externally Secured servers • Exchange Legacy Interop universal security group • Exchange 2003 bridgehead servers	`Internal`	This permission applies to forest X-headers. Forest X-headers start with **X-MS-Exchange-Forest-**. If this permission isn't granted, the sending server removes any forest headers from the message.

If you want to apply header firewall for organization X-headers or forest X-headers in a custom Send connector scenario, use the any of the following methods:

- Create a Send connector and select a usage type other than `Internal` or `Partner`. The Send connector usage type can only be set when you create the connector. For more information, see Create an SMTP Send Connector.
- Remove a security principal that assigns the Ms-Exch-Send-Headers-Organization permission and the Ms-Exch-Send-Headers-Forest permission from the connector. For more information, see Configure Send Connector Properties.
- Use the **Remove-ADPermission** cmdlet to remove the Ms-Exch-Send-Headers-Organization permission and the Ms-Exch-Send-Headers-Forest permission

from one of the security principals that's configured on the Send connector. For more information, see Remove-ADPermission.

- Use the **Add-ADPermission** cmdlet to deny the Ms-Exch-Send-Headers-Organization permission and the Ms-Exch-Send-Headers-Forest permission to one of the security principals that's configured on the Send connector. For more information, see Add-ADPermission.

How Header Firewall Is Applied to Organization X-Headers and Forest X-Headers from Other Message Sources

Messages can enter the Exchange 2010 transport pipeline on a Hub Transport server or an Edge Transport server without using Send connectors or Receive connectors. Header firewall for organization X-headers and forest X-headers is applied to messages originating from these other message sources as described in the following list:

- **Pickup directory** The Pickup directory is used by administrators or applications to submit message files. Header firewall for organization X-headers and forest X-headers is always applied to the message files in the Pickup directory. For more information about the Pickup directory, see Understanding the Pickup and Replay Directories.
- **Replay directory** The Replay directory is used to resubmit messages that have been exported from Exchange 2010 message queues. How header firewall for organization X-headers and forest X-headers is applied in these messages is controlled by the `X-CreatedBy:` header field in the message file:
  - If the value of this header field is `MSExchange14`, header firewall isn't applied to the message.
  - If the value of `X-CreatedBy:` isn't `MSExchange14`, header firewall is applied.
  - If the `X-CreatedBy:` header field doesn't exist in the message file, header firewall is applied.

  For more information about the Replay directory, see Understanding the Pickup and Replay Directories.
- **Drop directory** The Drop directory is used by Foreign connectors on Hub Transport servers to send messages to messaging servers that don't use SMTP to transfer messages. Header firewall for organization X-headers and forest X-headers is always applied to message files before they're put in the Drop directory. For more information about Foreign connectors, see Understanding Foreign Connectors.
- **Store driver** The store driver exists on Hub Transport servers to transport messages to and from mailboxes on Mailbox servers. For outgoing messages that are created and submitted from mailboxes, header firewall for organization X-headers and forest X-headers is always applied. For incoming messages, header firewall for organization X-headers and forest X-headers is selectively applied. The X-headers that are specified in the following list aren't blocked by header firewall for inbound messages to mailbox recipients:
  - X-MS-Exchange-Organization-SCL
  - X-MS-Exchange-Organization-AuthDomain
  - X-MS-Exchange-Organization-AuthMechanism
  - X-MS-Exchange-Organization-AuthSource
  - X-MS-Exchange-Organization-AuthAs
  - X-MS-Exchange-Organization-OriginalArrivalTime
  - X-MS-Exchange-Organization-OriginalSize

  For more information about the store driver, see Understanding Transport Pipeline.
- **DSN messages** Header firewall for organization X-headers and forest X-headers is always applied to the original message or the original message header that's attached to the DSN message. For more information about DSN messages, see Managing Delivery Status Notifications.
- **Agent submission** Header firewall for organization X-headers and forest X-headers isn't applied to messages that are submitted by agents.

Return to top

Header Firewall for Routing Headers

Routing headers are standard SMTP header fields that are defined in RFC 2821 and RFC 2822. Routing headers stamp a message by using information about the different messaging servers that were used to deliver the message to the recipient. The available routing headers are described in the following list:

- **Received:** A different instance of this header field is added to the message header by every messaging server that accepted and forwarded the message to the recipient. The `Received:` header typically includes the name of the messaging server and a date-timestamp.
- **Resent-*:** Resent header fields are informational header fields that can be used to determine whether a message has been forwarded by a user. The following resent header fields are available: `Resent-Date:`, `Resent-From:`, `Resent-Sender:`, `Resent-To:`, `Resent-Cc:`, `Resent-Bcc:`, and `Resent-Message-ID:`.
  The Resent fields are used so that the message appears to the recipient as if it was sent directly by the original sender. The recipient can view the message header to discover who forwarded the message.

Routing headers that are inserted into messages can be used to misrepresent the routing path that a message traveled to reach a recipient. Exchange 2010 uses two different ways to apply header firewall to routing headers that exist in messages:

- Permissions are assigned to Send connectors or Receive connectors that can be used to preserve or remove routing headers in messages.
- Header firewall is automatically implemented for routing headers in messages during other types of message submission.

How Header Firewall Is Applied to Routing Headers in Inbound Messages

Receive connectors have the Ms-Exch-Accept-Headers-Routing permission that's used to accept or reject any routing headers that exist in an inbound message:

- If this permission is granted, all routing headers are preserved in the inbound message.
- If this permission isn't granted, all routing headers are removed from the inbound message.

The following table describes the default application of the Ms-Exch-Accept-Headers-Routing permission on a Receive connector.

Default application of the Ms-Exch-Accept-Headers-Routing permission on a Receive connector

By default, the security principals that have the permission assigned	Permission group that has the security principals as members	By default, the usage type that assigns the permission groups to the Receive connector
Anonymous user account	Anonymous	`Internet`
Authenticated user accounts	ExchangeUsers	`Client` (unavailable on Edge Transport servers)
• Hub Transport servers • Edge Transport servers • Exchange Servers	ExchangeServers	`Internal`

Note: Hub Transport servers only • Externally Secured servers		
Exchange Legacy Interop universal security group	ExchangeLegacyServers	Internal
Partner Server account	Partner	• Internet • Partner

The Ms-Exch-Accept-Headers-Routing permission is assigned to all usage types except Custom. If you want to apply header firewall to routing headers in a custom Receive connector scenario, follow these steps:

1. Perform one of the following actions:
   - Create a Receive connector and select the usage type Custom. Don't assign any permission groups to the Receive connector. You can't modify the assigned permissions or the group membership of a permission group.
   - Modify an existing Receive connector, and set the *PermissionGroups* parameter to the value None.
2. Use the **Add-ADPermission** cmdlet to add the appropriate security principals that are required on the Receive connector. Make sure that no security principals have the Ms-Exch-Accept-Headers-Routing permission assigned to them. If it's necessary, use the **Add-ADPermission** cmdlet to deny the Ms-Exch-Accept-Headers-Routing permission to the security principal that you want to configure to use the Receive connector.

For more information, see the following topics:

- Create an SMTP Receive Connector
- Configure Receive Connector Properties
- Add-ADPermission
- Remove-ADPermission

How Header Firewall Is Applied to Routing Headers in Outbound Messages

Send connectors have the Ms-Exch-Send-Headers-Routing permission that's used to allow or remove any routing headers that exist in an outbound message:

- If this permission is granted, all routing headers are preserved in the outbound message.
- If this permission isn't granted, all routing headers are removed from the outbound message.

The following table describes the default application of the Ms-Exch-Send-Headers-Routing permission on a Send connector.

Default application of the Ms-Exch-Send-Headers-Routing permission on a Send connector

By default, the security principals that have the permission assigned	By default, the usage type that assigns the security principals to the Send connector
• Hub Transport servers • Edge Transport servers • Exchange Servers **Note:** On Hub Transport servers only	Internal

• Externally Secured servers • Exchange Legacy Interop universal security group • Exchange 2003 bridgehead servers	
Anonymous User Account	`Internet`
Partner Servers	`Partner`

The Ms-Exch-Send-Headers-Routing permission is assigned to all usage types except `Custom`. If you want to apply header firewall to routing headers in a custom Send connector scenario, use the any of following methods:

- Create a Send connector and select the usage type `Custom`. The Send connector usage type can only be set when you create the connector. For more information, see Create an SMTP Send Connector.
- Remove a security principal that assigns the Ms-Exch-Send-Headers-Routing permission from the connector. For more information, see Configure Send Connector Properties.
- Use the **Remove-ADPermission** cmdlet to remove the Ms-Exch-Send-Headers-Routing permission from one of the security principals that's configured on the Send connector. For more information, see Remove-ADPermission.
- Use the **Add-ADPermission** cmdlet to deny the Ms-Exch-Send-Headers-Routing permission to one of the security principals that's configured on the Send connector. For more information, see Add-ADPermission.

How Header Firewall Is Applied to Routing Headers from Other Message Sources

Messages can enter the Exchange 2010 transport pipeline on a Hub Transport server or an Edge Transport server without using Send connectors or Receive connectors. Header firewall for routing headers is applied to the other message sources that are described in the following list:

- **Pickup directory** The Pickup directory is used by administrators or applications to submit message files. Header firewall for routing headers is always applied to the message files in the Pickup directory. For more information about the Pickup directory, see Understanding the Pickup and Replay Directories.
- **Store driver** The store driver exists on Hub Transport servers to transport messages to and from mailboxes on Mailbox servers. Header firewall for routing headers is always applied to all messages that are sent from mailboxes on Mailbox servers. Header firewall for routing headers isn't applied to incoming messages for delivery to mailbox recipients. For more information about the store driver, see Understanding Transport Pipeline.
- **DSN messages** Header firewall for routing headers is always applied to the original message or the original message header that's attached to the DSN message. For more information about DSN messages, see Managing Delivery Status Notifications.
- **Replay directory, Drop directory, and agent submission** Header firewall for routing headers isn't applied to messages that are submitted by the Replay directory, the Drop directory, or agents.

Return to top

Header Firewall and Earlier Versions of Exchange

Exchange 2003 and earlier versions of Exchange don't use the organization X-headers or forest X-headers. Exchange 2010 treats versions of Exchange earlier than Exchange 2007

as untrusted message sources. Header firewall is applied to all organization X-headers and forest X-headers in messages coming from servers that are running earlier versions of Exchange. Header firewall for organization X-headers and forest X-headers is also applied to messages that are delivered to servers that are running earlier versions of Exchange that exist in the Exchange organization.

Earlier versions of Exchange use the proprietary verb X-EXCH50 to transmit information about messages and recipients that can't be included in the e-mail message. The information is transmitted as the Exch50 binary large object (BLOB). The Exch50 BLOB is a collection of binary data that's stored as a single object. Exch50 contains data such as the SCL, address rewriting information, and other MAPI properties that don't have MIME representation. Because X-EXCH50 is a proprietary Extended Simple Mail Transfer Protocol (ESMTP) verb, Exch50 data can't be propagated by a server that doesn't have Exchange installed. For more information, see Exchange 2003 - Planning Roadmap for Upgrade and Coexistence.

Routing group connectors between servers that have Exchange 2010 or Exchange 2003 installed are automatically configured to support sending and receiving Exch50 data. Send connectors and Receive connectors have permissions that enable the Exch50 command.

The following table describes the permissions that allow the Exch50 command on a Receive connector for inbound messages. If one of these permissions isn't granted, and a message is sent that contains the Exch50 command, the server accepts the message, but doesn't include the Exch50 command.

Permissions that allow the Exch50 command on a Receive connector for inbound messages

Permission	By default, the security principals that have the permission assigned	Permission group that has the security principals as members	By default, the usage type that assigns the permission groups to the Receive connector
Ms-Exch-Accept-Exch50	• Hub Transport servers • Edge Transport servers • Exchange Servers **Note:** On Hub Transport servers only • Externally Secured servers	ExchangeServers	`Internal`
Ms-Exch-Accept-Exch50	Exchange Legacy Interop universal security group	ExchangeLegacyServers	`Internal`

If you want to block the Exch50 command in a custom Receive connector scenario, use the any of following methods:

- Create a Receive connector and select a usage type other than `Internal`. The Receive connector usage type can only be set when you create the connector. For more information, see Create an SMTP Receive Connector.
- Modify an existing Receive connector and remove the ExchangeServers permission group. For more information, see Configure Receive Connector Properties.
- Use the **Remove-ADPermission** cmdlet to remove the Ms-Exch-Accept-Exch50 permission from a security principal that's configured on the Receive connector.

This method doesn't work if the permission has been assigned to the security principal by using a permission group. You can't modify the assigned permissions or the group membership of a permission group. For more information, see Remove-ADPermission.

- Use the **Add-ADPermission** cmdlet to deny the Ms-Exch-Accept-Exch50 permission to a security principal that's configured on the Receive connector. For more information, see Add-ADPermission.

The following table describes the permission that allows the Exch50 command on a Send connector for outbound messages. If this permission isn't granted and a message is sent that contains the Exch50 command, the server sends the message, but doesn't include the Exch50 command.

Permission that allows the Exch50 command on a Send connector for outbound messages

Permission	By default, the security principals that have the permission assigned	By default, the usage type that assigns the security principals to the Send connector
Ms-Exch-Send-Exch50	• Hub Transport servers • Edge Transport servers • Exchange Servers **Note:** On Hub Transport servers only • Externally Secured servers • Exchange Legacy Interop universal security group • Exchange 2003 bridgehead servers	`Internal`

If you want to block the Exch50 command in a custom Send connector scenario, you can use the any of following methods:

- Create a Send connector and select a usage type other than `Internal`. The Send connector usage type can only be set when you create the connector. For more information, see Create an SMTP Send Connector.
- Remove a security principal that assigns the Ms-Exch-Send-Exch50 permission from the connector.
- Use the **Remove-ADPermission** cmdlet to remove the Ms-Exch-Send-Exch50 permission from one of the security principals that's configured on the Send connector. For more information, see Remove-ADPermission.
- Use the **Add-ADPermission** cmdlet to deny the Ms-Exch-Send-Exch50 permission to one of the security principals that's configured on the Send connector. For more information, see Add-ADPermission.

Return to top

1.7.1.20 Understanding SMTP Failover and Load Balancing in Transport

Understanding SMTP Failover and Load Balancing in Transport

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-01-13*

When you have multiple Hub Transport servers in your organization, Exchange automatically distributes the mail traffic among all the Hub Transport servers in your organization. The load distribution is successful in distributing the load evenly when all servers are available. However, when one or more servers are unavailable, the load distribution may become uneven among the remaining servers, especially if your organization is distributed across multiple Active Directory sites.

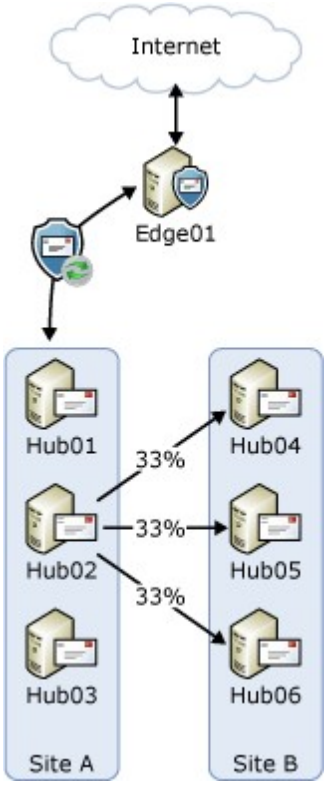
In Microsoft Exchange Server 2010 Service Pack 1 (SP1), several improvements were made to the decision-making mechanism for distributing the load among Hub Transport servers.

Looking for management tasks related to message routing? See Managing Message Routing.

Contents

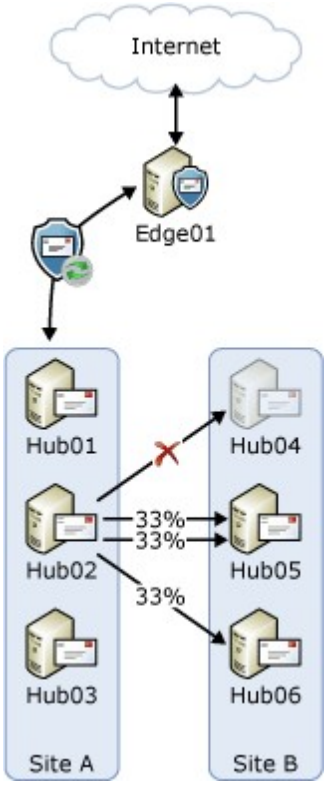
Exchange Server 2010 RTM Behavior

In the release to manufacturing (RTM) version of Exchange 2010, when a transport server needs to route several messages to the same destination, the server initially determines the next hop for those messages. If there are multiple target servers for that next hop, it load balances the connection used to deliver messages equally among the target servers using the round robin manner provided by enhanced Domain Name System (DNS). For example, consider a topology where you have two Active Directory sites with three Hub Transport servers in each (as shown in the following figure). When a Hub Transport server in Site A, for example Hub02, needs to send messages to Site B, the next hop for that message is Site B. There are three possible targets in the next hop: Hub04, Hub05, and Hub06. The server will distribute the number of connections evenly across those three targets as shown in the following figure. This action results in an even distribution of messages across the connections over time.



Similarly, the Hub Transport servers in Site B will distribute the number of messages sent to recipients in Site A evenly across Hub01, Hub02, and Hub03. Also, because Edge01 is subscribed to Site A, the targets for the next hop for messages sent to the Internet are Hub01, Hub02, and Hub03.

A problem arises if one or more of the servers are unavailable in the next hop. For example, assume that Hub04 in Site B is unavailable for scheduled maintenance. The servers in Site A don't maintain availability status of each server in Site B. The servers in Site A will distribute the load destined for Site B among the three Hub Transport servers in that site. However, approximately one third of those connections would be sent to Hub04 but won't succeed. These connections will fail over to the next available server, and one of the Hub Transport servers in Site B will process substantially more load than the other server as shown in the following figure.



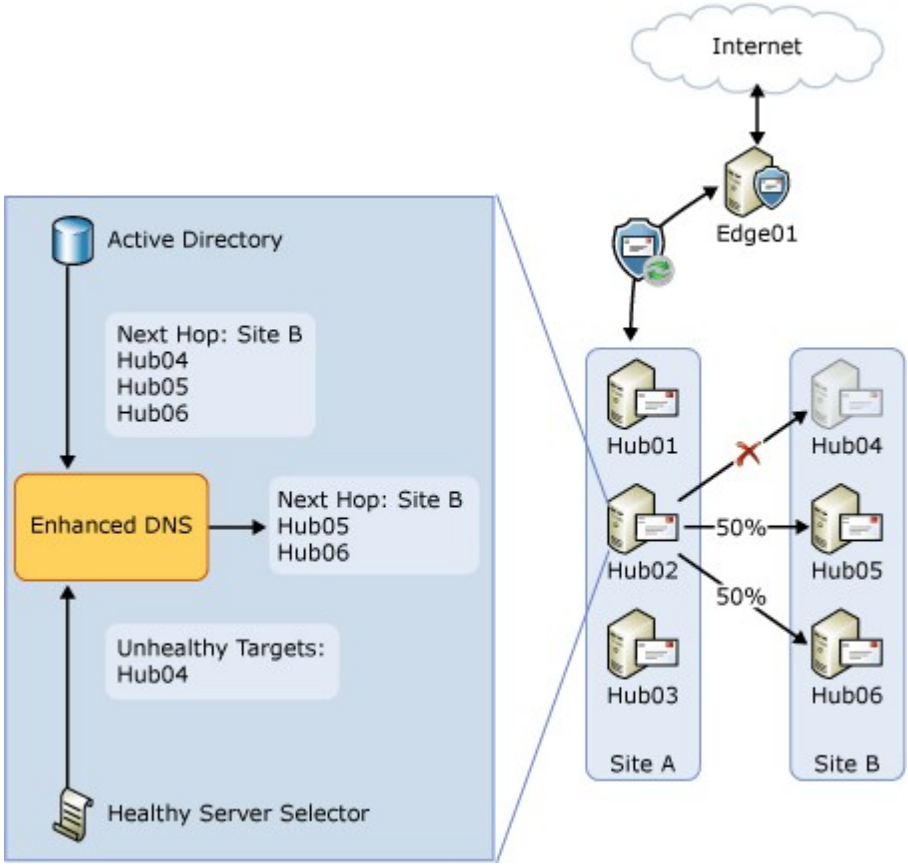
This undesirable behavior may occur whenever there's an unavailable server in the next hop that typically has more than two targets. The next hop could be another Active Directory site as shown in the preceding example, or a connector that has multiple Hub Transport servers listed as the source server (for example, the Send connector to the subscribed Edge Transport server in the topology shown in the preceding figures).

This isn't an issue for mail submissions from Mailbox servers. The mail submission service will detect unavailable Hub Transport servers in a site, and won't attempt to deliver to those servers. In the example shown previously, although one of the Hub Transport servers in Site B may have a heavier load from intersite traffic, the load generated by Mailbox servers in Site B will be evenly split between Hub05 and Hub06.

Return to top

Exchange 2010 SP1 Improvements

To address the issue described in the previous section, a new component called *Healthy Server Selector* was added in Exchange 2010 SP1. Healthy Server Selector maintains a list of servers that are unavailable. This list is used by enhanced DNS to filter out any unavailable servers when applying round robin logic for load balancing. To demonstrate how Healthy Server Selector helps with load balancing, consider the problematic condition shown in the preceding figure. In Exchange 2010 SP1, enhanced DNS will first compile the list of potential targets in the next hop, Site B. It will then ask Healthy Server Selector to filter the list. Healthy Server Selector will report that Hub04 for the next hop Site B is unhealthy. Enhanced DNS will remove Hub04 from the list of potential targets for the next hop Site B, and will use round robin load balancing only between Hub05 and Hub06 as shown in the following figure.



Healthy Server Selector

In its simplest form, Healthy Server Selector tracks servers deemed unhealthy so that those servers aren't included in round robin load balancing. From a Healthy Server Selector perspective, a definition of an unhealthy server is one to which a connection attempt returns any Windows sockets (Winsock) error code.

For each unhealthy server, Healthy Server Selector keeps the following information:

- Server IP address
- Retry count
- Last retry time

Retry Behavior

When a server is marked as unhealthy, Healthy Server Selector will ensure that connections to that specific server are tried again to detect when that server comes online. Healthy Server Selector uses the following settings to determine how frequently connections will be retried to an unhealthy server:

- **QueueGlitchRetryInterval and QueueGlitchRetryCount** These settings determine how many times and at what interval Healthy Server Selector retries connections to a specific server when it's first marked unhealthy. These settings are configured in the EdgeTransport.exe.config file. The default values for these settings are 1 minute and 4 retry attempts. These values mean that a connection to an unhealthy server will be attempted every minute four times in a default configuration.
- **TransientFailureRetryInterval and TransientFailureRetryCount** If the unhealthy server is unavailable, these settings are used by Healthy Server Selector to determine the frequency of the next set of retry attempts. These settings are configured for each transport server. The default values are 5 minutes (10 minutes on an Edge Transport server) and 6 retry attempts. These values mean that a connection to an unhealthy server will be attempted

every five minutes six times after the first four minutes in a default configuration.

- **OutboundConnectionFailureRetryInterval** If the unhealthy server is unavailable, Healthy Server Selector will continue to retry the connection by the frequency specified in this parameter. This setting is configured for each transport server. The default value is 10 minutes (30 minutes on an Edge Transport server). This means that a connection will be attempted to an unhealthy server every 10 minutes after the first 34 minutes in a default configuration.

For step-by-step instructions about how to configure these settings, see Configure Message Retry, Resubmit, and Expiration Intervals.

When it's time to retry a connection, Healthy Server Selector allows only one connection attempt to the unhealthy server. If that connection succeeds, the SMTP outbound component will notify Healthy Server Selector that the connection is successful. At that point, Healthy Server Selector removes the server from the list of unhealthy servers.

Healthy Server Selector and Shadow Redundancy

The shadow redundancy component of transport includes a heartbeat feature. The heartbeat is a simple SMTP connection used to query the status of messages previously submitted to a target server. Healthy Server Selector filtering won't prevent the Shadow Redundancy Manager from issuing heartbeat connection attempts. If a server has shadow messages that were submitted to a server that's unhealthy, it will attempt to make heartbeat connections to that server. If a heartbeat connection succeeds to an unhealthy server, that target server is immediately removed from the list of unhealthy servers by Healthy Server Selector.

To learn more about shadow redundancy and the heartbeat, see Understanding Shadow Redundancy.

Diagnostic Information

In Exchange 2010 SP1, the connectivity logs include diagnostic information for Healthy Server Selector and the enhanced load balancing features. When a server is added to the unhealthy servers list by Healthy Server Selector, the event is logged in the connectivity log. To locate this event, search for the phrase **MarkedUnhealthy** in the connectivity log. On the line that contains this phrase, you can find the following information:

- Target host IP address
- Target host fully qualified domain name (FQDN)
- Winsock error received
- Status: `MarkedUnhealthy`
- Current failure count
- Next retry time

From this entry, you can identify the reason for the failure by evaluating the Winsock error code. For a complete list of Winsock error codes and their definitions, see Windows Sockets Error Codes.

You can also determine how many connection attempts have failed and the next scheduled retry attempt to the target server by analyzing the **Current Failure Count** and **Next Retry Time** fields.

You must have connectivity logging enabled on your transport servers to be able to see this diagnostic information. Connectivity logging is disabled by default on Hub Transport and Edge Transport servers. For more information about configuring connectivity logging, see Configure Connectivity Logging.

Return to top

Windows Network Load Balancing or Third-Party Load Balancing Solutions with Transport Servers

As discussed earlier in this topic, Exchange 2010 automatically load balances all intra-organization message traffic between Edge Transport, Hub Transport, and Mailbox servers using enhanced DNS. However, this functionality doesn't cover the load balancing of messages received from non-Exchange sources such as external mail servers, third-party anti-spam or antivirus solutions, any internal mail servers outside your Exchange organization, line-of-business (LOB) applications, and POP-based or IMAP-based e-mail clients.

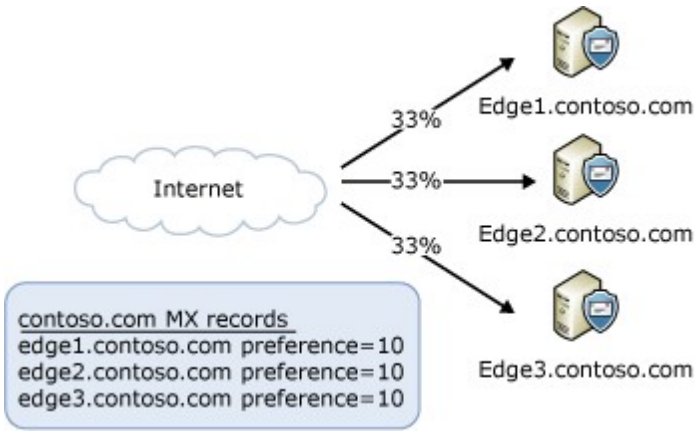
If you have one or more of these mail sources, you may choose to load balance incoming SMTP traffic using a unified SMTP namespace (such as smtp.contoso.com) that distributes external e-mail messages across the transport servers within the organization. Windows Network Load Balancing (NLB) or a hardware-based load balancing solution from a third-party vendor are both supported. For a list of load balancers that have been tested by the vendor and reviewed by Microsoft to meet Exchange 2010 requirements, see Microsoft Unified Communications Load Balancer Deployment.

Important:

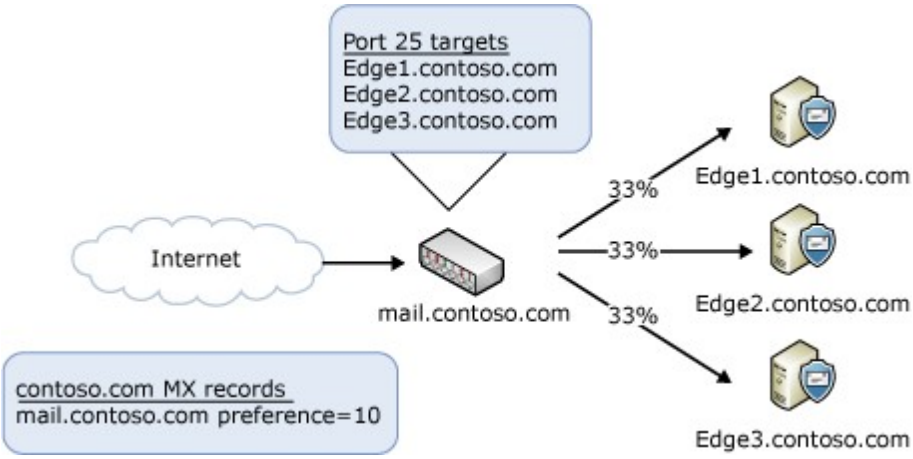
Using a load balancing solution to handle message traffic between the Exchange servers in your organization isn't supported. You must exclude message traffic between Exchange servers from any load balancing solution you deploy in your environment.

Load Balancing Inbound Internet Messages Among Your Edge Transport Servers

The most common situation is handling incoming messages from the Internet. You don't need to deploy a load balancing solution to distribute the load across your Edge Transport servers. You can accomplish this by using DNS round robin and mail exchange records (MX records) that have the same preference value, as shown in the following figure.



If you choose to use Windows NLB or a hardware load balancing solution to distribute incoming Internet messages, you need to publish a single MX record that points to your load balancing solution. The load balancer will distribute incoming messages to all the Edge Transport servers listed in its configuration, as shown in the following figure.

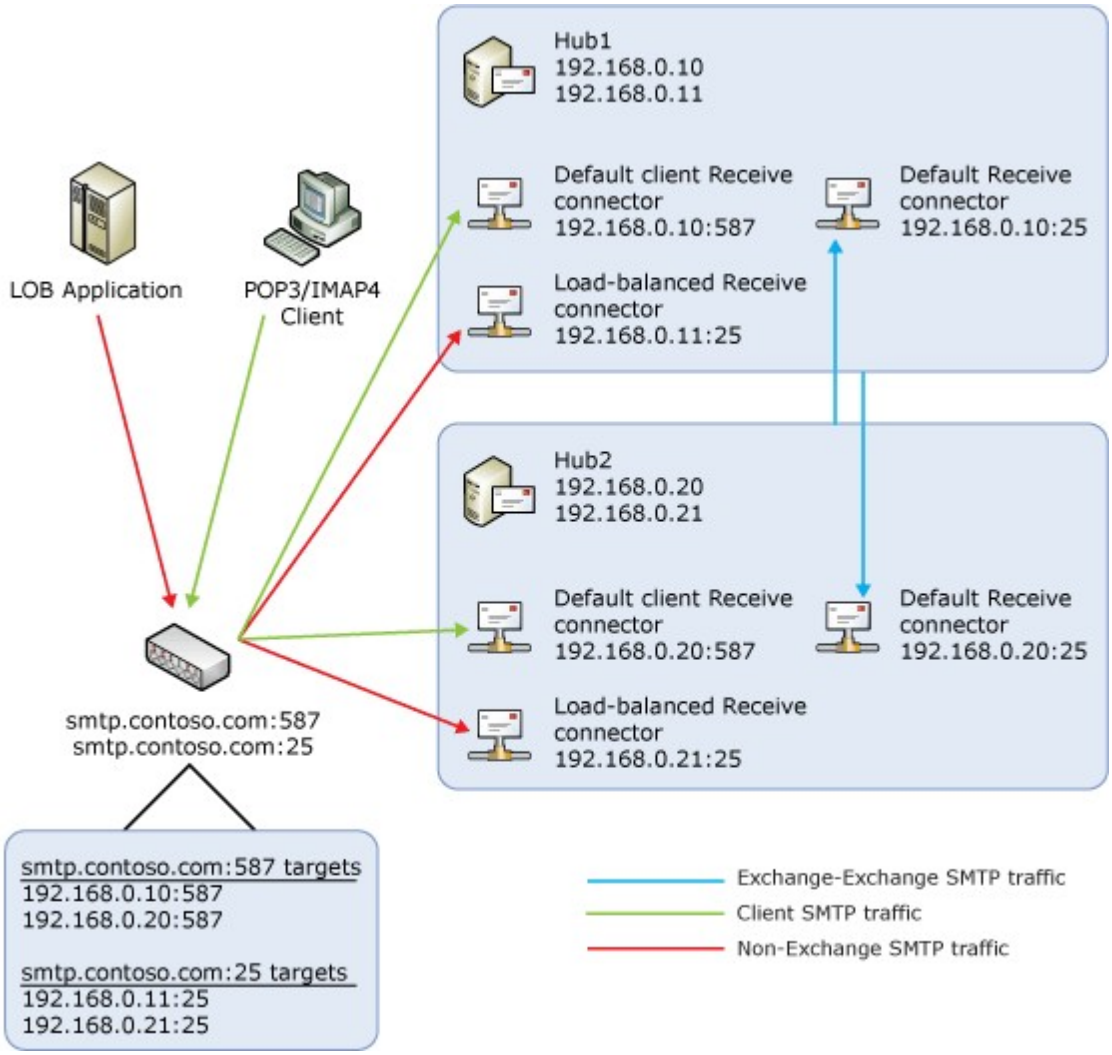


Load Balancing Non-Exchange Messages Among Your Hub Transport Servers

Exchange 2010 uses Receive connectors to accept incoming messages. By default, when an Exchange 2010 Hub Transport server receives an e-mail message via SMTP over TCP port 25, it's processed by the Receive connector named Default Receive connector.

When a POP or IMAP client submits an e-mail message to an Exchange 2010 Hub Transport server, the message is submitted over TCP port 587 by default. This means e-mail messages submitted from POP or IMAP clients are processed by a separate Receive connector named Default Client Receive connector.

If you plan on placing a load balancing solution in front of your Hub Transport servers, you should create a separate Receive connector for that purpose and make sure that only traffic processed by that particular connector is subject to load balancing. This can be achieved by adding an additional IP address to the Hub Transport server and associating this IP address with the new Receive connector. In addition, the **Exchange Server authentication** option should be disabled on the Receive connector to ensure Exchange traffic doesn’t route over it. The following figure shows a configuration where a load balancer is used to distribute messages received from POP3 or IMAP4 clients and non-Exchange SMTP servers among two Hub Transport servers.



Windows Network Load Balancing

Windows NLB is the most common software load balancer used for Exchange servers. There are some limitations associated with deploying Windows NLB with Exchange 2010 Hub Transport servers:

- Windows NLB can't be used on Exchange servers where the Hub Transport and Mailbox server roles coexist and the server also participates in a database availability group (DAG).
  This is because the Windows NLB feature is incompatible with Windows failover clustering. If you use an Exchange 2010 DAG and you want to use Windows NLB, you need to have the Hub Transport server role and the Mailbox server role running on separate computers. In addition, Windows NLB impacts message routing when the DAG member and Hub Transport server role coexist on the same server. To learn more, see Hub Transport and Mailbox Server Roles Coexistence When Using DAGs.
- We don't recommend putting more than eight Hub Transport servers in an array that's load balanced by Windows NLB. If you need to load balance more than eight Hub Transport servers, you should deploy a hardware-based solution.
- Windows NLB doesn't detect service outages.
  It only detects server outages by IP address. If the Exchange Transport service fails, but the server is still functioning, Windows NLB won't detect the failure and will still route incoming e-mail messages to that Hub Transport

server. Manual intervention is required to remove the Hub Transport server experiencing the outage from the load balancing pool.

- Windows NLB configuration can result in port flooding, which can overwhelm networks.
  This is because Windows NLB has been designed in such a way that it simultaneously delivers all incoming client packets to all switch ports. Although this behavior enables Windows NLB to deliver very high throughput, it may cause high switch occupancy.

For detailed steps about configuring Windows NLB, see Configure Windows Network Load Balancing for Hub Transport Servers.

Hardware Load Balancing

If you have more than eight Hub Transport servers for which you want to load balance non-Exchange message traffic, you need a more scalable load balancing solution. Although there are robust software load balancing solutions available, a hardware load balancing solution provides the most capacity.

Unlike Windows NLB, which only detects server outages by IP address, a hardware load balancer can be configured to detect the failure of the Exchange Transport service and can route incoming e-mail messages to other Hub Transport servers without any manual intervention.

For detailed steps about configuring a hardware load balancing solution, see Configure Hardware Load Balancing for Hub Transport Servers.

1.7.1.21 Understanding MailTips

Understanding MailTips

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

MailTips are informative messages displayed to users while they're composing a message. Microsoft Exchange Server 2010 analyzes the message, including the list of recipients to which it's addressed, and if it detects a potential problem, it notifies the user with MailTips prior to sending the message. With the help of the information provided by MailTips, senders can adjust the message they're composing to avoid undesirable situations or non-delivery reports (NDRs).

The following unproductive messaging scenarios are common in any messaging environment:

- NDRs resulting from messages that violate restrictions configured in an organization such as message size restrictions or maximum number of recipients per message.
- NDRs resulting from messages sent to recipients that don't exist, recipients that are restricted, or users whose mailboxes are full.
- Sending messages to users with Automatic Replies configured.

All of these scenarios involve the user sending a message, expecting it to be delivered, and instead receiving a response stating that the message isn't delivered. Even in the best-case scenario, like the automatic reply, these events result in lost productivity. In the case of an NDR, this scenario could result in a costly call to the Help desk.

There are also several scenarios where sending a message won't result in an error, but

can have undesirable, even embarrassing consequences:

- Messages sent to extremely large distribution groups.
- Messages sent to inappropriate distribution groups.
- Messages inadvertently sent to recipients outside your organization.
- Selecting **Reply to All** to a message that was received as a Bcc recipient.

All of these problematic scenarios can be mitigated by informing users of the possible outcome of sending the message as they're composing the message. For example, if senders know that the size of the message they're trying to send exceeds the corporate policy, they won't attempt to send the message. Similarly, if senders are notified that the message they're sending will be delivered to people outside the organization, they're more likely to ensure that the content and the tone of the message are appropriate.

By addressing the scenarios listed earlier, MailTips can help you to:

- Reduce the cost of processing and storing messages by preventing NDRs.
- Reduce the volume of Help desk calls caused by NDRs.
- Increase productivity by avoiding communications that won't succeed, for example, breaking the cycle of sending an e-mail message, receiving an automatic reply, and then redirecting the message.
- Inform your users as they compose e-mail messages about various policies configured in your organization that impose limits on the messages sent.
- Direct your users to the correct distribution groups.
- Reduce the risk of inadvertent disclosure of information to people outside your organization.

Important:
MailTips aren't designed to enforce specific policies. They simply inform the senders about the nature of the message they're composing so they can make necessary adjustments.

Looking for management tasks related to MailTips? See Managing MailTips.

MailTips in Exchange 2010

The following table provides a list of MailTips in Exchange 2010.

Exchange 2010 MailTips

MailTip	Scenario
Invalid Internal Recipient	The Invalid Internal Recipient MailTip is displayed if the sender adds a recipient that appears to be internal to the organization but doesn't exist in Active Directory. This could happen if the sender addresses a message to a user who is no longer with the company but whose address resolves due to name resolution cache or an entry in the sender's Contacts folder. It can also happen if the sender types an SMTP address with a domain for which Exchange is authoritative and the address doesn't resolve to an existing recipient. The MailTip indicates the invalid recipient and gives the sender the option to remove the recipient from the message.
Mailbox Full	The Mailbox Full MailTip is displayed if the sender adds a recipient whose mailbox is full and your

	organization has implemented a Prohibit Receive restriction for mailboxes over a specified size. The MailTip indicates the recipient whose mailbox is full and gives the sender the option to remove the recipient from the message. The MailTip is accurate at the time of display. If the message isn't immediately sent, the MailTip is updated every two hours. This also applies to messages that were saved in the Drafts folder and reopened after two hours.
Automatic Replies	The Automatic Replies MailTip is displayed if the sender adds a recipient who has turned on Automatic Replies. The MailTip indicates the recipient has Automatic Replies turned on and also displays the first 250 characters of the automatic reply configured by the recipient. The MailTip is accurate at the time of display. If the message isn't immediately sent, the MailTip is updated every two hours. This also applies to messages that were saved in the Drafts folder and reopened after two hours. If part of your user mailboxes are hosted on Exchange Online and you're in a coexistence with Exchange Online scenario, the setting on the remote domain object that represents the remote part of your organization has a direct effect on how this MailTip is processed. In Exchange 2010, users can configure different Automatic Replies for internal and external senders. If the remote domain is configured as an internal domain (by setting the *IsInternal* parameter on the remote domain object to `$true`), the internal automatic reply is returned to all users in the organization regardless of where their mailbox resides. However, if the remote domain isn't configured as an internal domain, the internal automatic reply is returned to all users whose mailboxes are in the local domain and the external automatic reply is returned to users whose mailboxes are in the remote domain.
Custom	A custom MailTip is displayed if the sender adds a recipient for whom a customized MailTip is configured. A custom MailTip can be useful for providing specific information about a recipient. For example, you can create a custom MailTip for a distribution group explaining its purpose to reduce its misuse. By default, custom MailTips aren't displayed if the

	sender isn't allowed to send to that recipient. In that case, the Restricted Recipient MailTip is displayed. However, you can change this configuration and have the custom MailTip also display. For more information about configuring custom MailTips, see Configure Custom MailTips for Recipients.
Restricted Recipient	The Restricted Recipient MailTip is displayed if the sender adds a recipient for which delivery restrictions are configured prohibiting this sender from sending messages. The MailTip indicates the recipient to which the sender isn't allowed to send messages and gives the sender the option to remove the recipient from the message. It also clearly informs the sender that the message won't be delivered if sent. If the restricted recipient is an external recipient, or if it's a distribution group that contains external recipients, this information is also provided to the sender. However, the following MailTips, if applicable, are suppressed: • Automatic Replies • Mailbox Full • Custom MailTip • Moderated Recipient • Oversize Message
External Recipients	The External Recipients MailTip is displayed if the sender adds a recipient that's external, or adds a distribution group that contains external recipients. This MailTip informs senders if a message they're composing will leave the organization, helping them make the correct decisions about wording, tone, and content. By default, this MailTip is turned off. You can turn it on using the **Set-OrganizationConfig** cmdlet. For details, see Configure Organizational Settings for MailTips. If part of your user mailboxes are hosted on Exchange Online and you're in coexistence with an Exchange Online scenario, the setting on the remote domain object that represents the remote part of your organization has a direct effect on how this MailTip is processed. If the remote domain is configured as an internal domain (by setting the *IsInternal* parameter on the remote domain object to `$true`), any recipients in this remote domain will be treated as internal and therefore the External Recipients MailTip won't be displayed. However, if the remote domain isn't configured as an internal domain, the recipients in that domain will be considered external and this

	MailTip will be displayed when a message is being composed to those recipients. **Note:** This MailTip isn't evaluated when composing a message to a distribution group in the remote domain.
Large Audience	The Large Audience MailTip is displayed if the sender adds a distribution group that has more than the large audience size configured in your organization. By default, Exchange displays this MailTip for messages to distribution groups that have more than 25 members. For information about configuring the large audience size for your organization, see Configure Organizational Settings for MailTips. The size of distribution groups isn't calculated each time. Instead, the distribution group information is read from the group metrics data. For more information about group metrics, see Understanding Group Metrics.
Moderated Recipient	The Moderated Recipient MailTip is displayed if the sender adds a recipient that's moderated. The MailTip indicates which recipient is moderated and informs the sender that this may result in delay of the delivery. If the sender is also the moderator, this MailTip isn't displayed. It's also not displayed if the sender has been explicitly allowed to send messages to the recipient (by adding the sender's name to the Accept Messages Only From list for the recipient).
Reply-All on Bcc	The Reply-All on Bcc MailTip is displayed if the sender receives a Bcc copy of a message and selects **Reply to All**. When a user selects **Reply to All** to such a message, the fact that the user received a Bcc of that message is revealed to the rest of the audience to which the message was sent. In almost all cases, this is an undesirable situation, and this MailTip informs the user of this condition. **Note:** This MailTip is only supported in Microsoft Office Outlook Web App.
Oversize Message	The Oversize Message MailTip is displayed if the message the sender is composing is larger than configured message size limits in your organization. The MailTip is displayed if the message size violates one of the following size restrictions: • Maximum send size setting on the sender's mailbox

	• Maximum receive size setting on the recipient's mailbox • Maximum message size restriction for the organization • Maximum Request Length setting (for Outlook Web App only) **Note:** Due to the complexity of the implementation, the message size limits on the connectors in your organization aren't taken into account. **Note:** This MailTip isn't displayed in Outlook Web App.

MailTips Architecture

MailTips are implemented as a Web service in Exchange 2010. When a sender is composing a message, the client software makes an Exchange Web service call to the server running Exchange 2010 with the Client Access server role installed to get the list of MailTips. The Exchange 2010 server responds with the list of MailTips that apply to that message, and the client software displays the MailTips to the sender.

The following messaging clients support MailTips:

- Outlook Web App
- Microsoft Outlook 2010

The following actions by the sender trigger MailTips to be evaluated or updated:

- Add a recipient
- Add an attachment
- Reply or reply to all
- Open a message, which is already addressed to recipients, from the Drafts folder

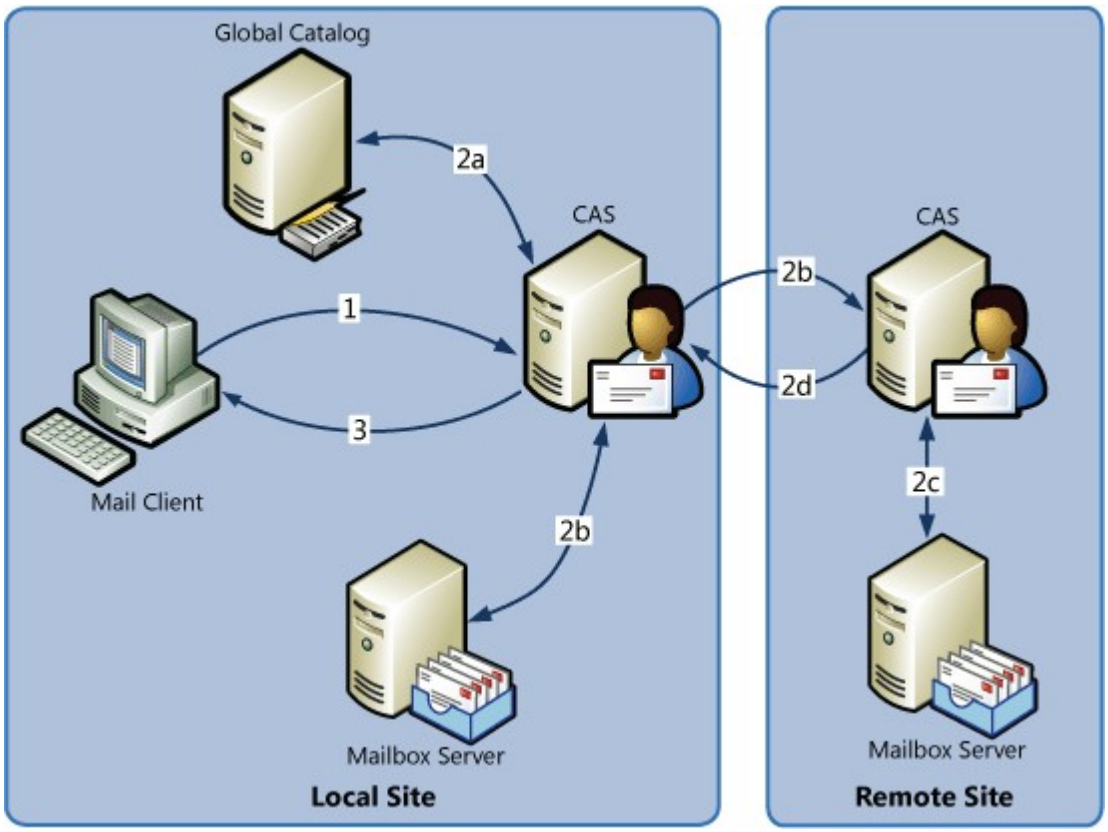
The client caches the MailTips so removing and adding the same recipient won't result in the client querying the Client Access server again.

When the Client Access server is queried, it compiles the list of applicable MailTips and returns them all in one batch. As a result, all MailTips are displayed to the user at the same time and don't arrive one at a time, distracting the sender.

The Client Access server uses the following sources to compile MailTips for a specific message:

- Active Directory
- Recipient mailboxes
- Local group metrics data

Each time a sender adds a recipient to a message, a sequence of events occurs to evaluate MailTips, as shown in the following figure.



As shown in the preceding figure:

1. The mail client queries the Web service on the Client Access server for MailTips that apply to the recipients in the message.
2. The Client Access server gathers MailTip data:
   - 2.a. The Client Access server queries Active Directory and reads group metrics data.
   - 2.b. If the recipient is a mailbox that's located on a Mailbox server in the local site, the Client Access server queries the Mailbox server to gather the Automatic Replies and Mailbox Full MailTips. If the recipient's mailbox is in another site, the Client Access server requests MailTips information from the Client Access server in the remote site.
   - 2.c. The Client Access server in the remote site queries the local Mailbox server for MailTip data.
   - 2.d. The remote Client Access server proxies the results back to the requesting Client Access server.
3. The Client Access server returns MailTip data back to the client.

Limits on MailTips

MailTips are subject to the following restrictions:

- MailTips aren't supported when working in offline mode with Outlook.
- When a message is addressed to a distribution group, the MailTips for individual recipients that are members of that distribution group aren't evaluated. However, if any of the members is an external recipient, the External Recipients MailTip is displayed, which shows the sender the number of external recipients in the distribution group.
- If the message is addressed to more than 200 recipients, individual mailbox MailTips aren't evaluated due to performance reasons.
- Custom MailTips are limited to 250 characters.
- If the sender starts composing a message and leaves it open for an extended

period of time, the Automatic Replies and Mailbox Full MailTips are evaluated every two hours.

MailTips in Complex Topologies

MailTips that rely on the recipients' mailbox data are evaluated by making a connection to the Mailbox servers that hold those recipients. The Mailbox Full and Automatic Replies MailTips are in this category. For these MailTips, the Client Access server directly queries the Mailbox server using RPC, but only if the recipients are in the same site. For recipients that reside in other sites or forests, this information is gathered via server-to-server Web requests between Client Access servers.

MailTips over Organization Relationships

Microsoft Exchange Server 2010 Service Pack 1 (SP1) allows you to configure organization relationships with Exchange Online or other organizations. Establishing an organization relationship allows you to enhance the user experience when dealing with the other organization with features including sharing free/busy data between the two organizations, configuring secure message flow, and enabling message tracking across the two organizations. For more information about organization relationships, see Understanding Federation.

When MailTips are enabled over an organization relationship, the local Client Access servers will proxy the Client Access servers in the remote organization. The behavior is similar to how mailbox-specific MailTips are handled for users in remote Active Directory sites. The one difference is the Client Access servers will proxy all MailTips types over an organization relationship, not just the mailbox-specific MailTips.

You have granular control over which MailTip types are returned over an organization relationship in addition to just allowing or preventing returning MailTips. The following two sections explain these settings in detail.

Controlling the MailTips Access Level

There may be many reasons to establish an organization relationship. Depending on the specific situation, you may want to restrict certain types of MailTips. Specifically, you can either allow all MailTips to be returned or only a limited set that would prevent NDRs. You can configure this setting with the *MailTipsAccessLevel* parameter of the **Set-OrganizationRelationship** cmdlet. The following table shows which MailTips are returned over the organization relationship.

MailTip	All	Limited
Large Audience	Yes	No
Automatic Replies	Yes If the remote domain of the recipient is specified as internal, the internal automatic reply is displayed. Otherwise, the external automatic reply is displayed.	Yes The external automatic reply is displayed.
Moderated Recipient	Yes	No
Oversize Message	Yes	Yes
Restricted Recipient	Yes	Yes
Mailbox Full	Yes	No
Custom MailTips	Yes	No
External Recipients	Yes	Yes

	If the remote domain of the recipient is specified as internal, this MailTip is suppressed. Otherwise, the external MailTip is returned.	If the remote domain of the recipient is specified as internal, this MailTip is suppressed. Otherwise, the external MailTip is returned.

For detailed steps about how to configure MailTips access levels, see Configure Organizational Settings for MailTips.

Controlling the MailTips Access Scope

When you enable MailTips over an organization relationship and set the access level to All, the recipient-specific MailTips, Mailbox Full, Automatic Replies, and custom MailTips, are returned for all users. However, you may only want to allow these MailTips for a specific set of users. For example, if you set up an organization relationship with a partner, you may want to allow these MailTips only for the users that work with that partner.

To achieve this, you need to first create a group and add all users for whom you want to share recipient-specific MailTips to that group. You can then specify that group on the organization relationship.

After you implement this restriction, your Client Access servers will first verify whether the recipient for whom they received a MailTips query is part of this group. If the recipient is a member of this group, the Client Access servers will proxy back all MailTips including the recipient-specific MailTips. Otherwise they won't include the recipient-specific MailTips in their response.

For detailed steps about how to configure MailTips access levels, see Configure Organizational Settings for MailTips.

Performance and Scalability

The following table lists some of the common performance concerns regarding MailTips and how these concerns are addressed.

Common performance concerns for MailTips

Performance concerns	Mitigation of concern
Discovering the size of distribution groups and dynamic distribution groups, and whether they include external recipients, seems like an expensive operation.	Distribution groups and dynamic distribution groups aren't evaluated when a message is being composed. This information is calculated daily by the group metrics generation service and is distributed to all Client Access servers. For more information, see Understanding Group Metrics.
Discovering the delivery restrictions for all recipients in a message with a large number of recipients can be resource- intensive.	Delivery restrictions aren't evaluated if a message has more than 200 recipients. Also, delivery restrictions aren't evaluated for the members of distribution groups and dynamic distribution groups. This is done only for recipients that are explicitly added to the message. If a user expands a distribution group, delivery restrictions for all members will be

	evaluated, as long as the total number of recipients doesn't exceed 200.
It may take a long time to collect information from various sites in complex topologies.	If the requested information isn't returned within 10 seconds, the operation times out. Exchange won't display any new MailTips to the sender after 10 seconds.

1.7.1.22 Understanding Message Routing

Understanding Message Routing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-12*

The primary task of Hub Transport and Edge Transport servers in your organization is to route messages received from users and external sources to their ultimate destinations. This topic explains how Microsoft Exchange Server 2010 routes messages in your organization.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Overview of Message Routing in Exchange 2010

Routing decisions are made during message categorization. The categorizer is a component of the Microsoft Exchange Transport service that processes all incoming messages and determines what to do with the messages based on information about the intended recipients. The categorizer processes messages in several dependent phases and also uses other components of the Microsoft Exchange Transport service during message processing. After a message is received by an Exchange 2010 transport server, and after the preliminary processing that occurs during SMTP Receive is complete, the message is delivered to the Submission queue. Messages move from the Submission

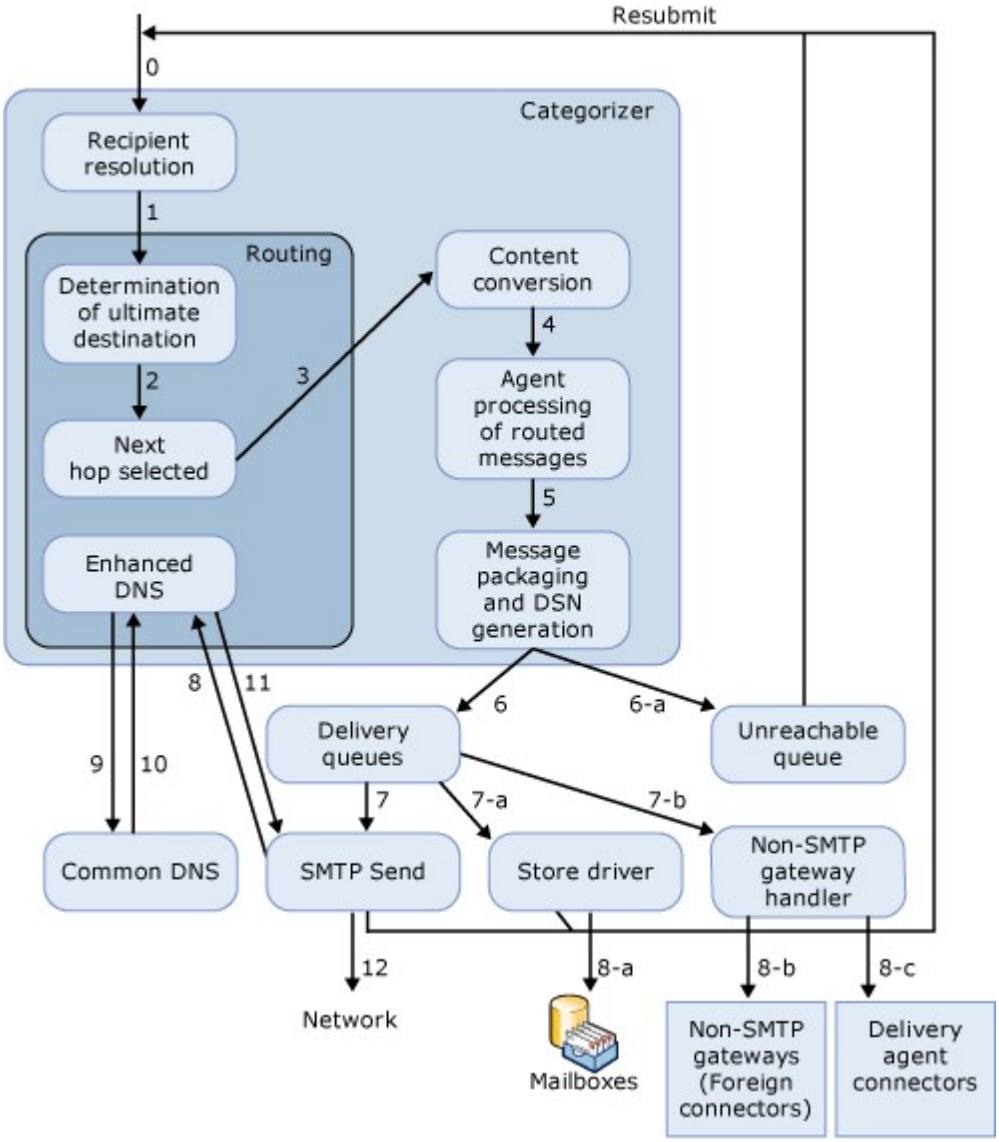
queue through the categorizer in the following phases:

1. **Agent processing of submitted messages** Some agent processing on the Hub Transport server occurs when the message is received for categorization. The agents that are applied during this phase include the optional Microsoft Forefront Protection for Exchange Server antivirus agent and the Journaling agent.
2. **Recipient resolution** During this phase, the recipient's e-mail address is resolved to determine whether the recipient has a mailbox in the Exchange organization or an external e-mail address.
3. **Routing** After information about the recipient is resolved, the routing component of the categorizer determines the ultimate destination for the message and the route to that destination, selects the next segment, or hop, for message relay, and resolves the next hop information to a list of physical servers and IP addresses.
4. **Content conversion** Before a message is relayed to its next hop, content conversion occurs so that the message is sent in a format that's readable by the recipient. *Content conversion* transforms e-mail messages from one format to another format for mail flow or storage, such as MAPI to MIME, or UUENCODE to base64 encoded, or for appropriate rendering that's specific to an e-mail client, such as HTML, rich text format (RTF), or plain text.
5. **Agent processing of routed messages** After the routing decisions for a particular message are made, the Transport Rules agent and the Journaling agent are applied on the Hub Transport server. The Journaling agent is applied both when the message is submitted and when it's routed so that any changes that are made to the message by the Transport Rules agent, for example, when it modifies a delivery address or applies a message-specific journaling requirement, don't bypass the Journaling agent.
6. **Message packaging and DSN generation** The final categorized message is assembled and moved to a delivery queue. A delivery status notification (DSN) may also be generated during this phase.

Messages are next processed by SMTP Send, the store driver, delivery agents, or the foreign gateway connection handler. The component that's used depends on the ultimate destination. A delivery queue is dynamically generated for each hop. The messages are queued in these delivery queues after a routing decision is made. If a route can't be found for a recipient, the messages are queued to the Unreachable queue.

The following figure shows how message processing occurs in the different routing phases and how messages are queued for delivery to the next hop destination.

Routing context in mail flow



Return to top

Routing Components

To make routing decisions, Exchange 2010 must access configuration information that's stored in Active Directory. On an Edge Transport server, configuration information is stored in and accessed from the Active Directory Lightweight Directory Services (AD LDS) instance on the local server. Microsoft Windows and Exchange 2010 services work together to create mappings of the configuration data. These mappings are cached in routing tables. Exchange 2010 references these tables when it makes routing decisions. The cache is updated when the routing topology changes. The Exchange services that are used during message transport are common to both the Hub Transport server role and the Edge Transport server role. However, the Edge Transport server role doesn't cache information about the Active Directory topology.

The following configuration and service components are important to message routing:

- **Active Directory sites** An Active Directory site represents the routing boundary for Hub Transport servers. A Hub Transport server delivers directly

to Mailbox servers, distribution group expansion servers, and to source servers for connectors in the local Active Directory site and to Edge Transport servers subscribed to that site. However, a Hub Transport server must relay messages to another Hub Transport server for recipients, expansion servers, and connectors that are located in remote Active Directory sites. The Hub Transport server role must be deployed in every Active Directory site that contains other Exchange 2010 server roles.

- **Active Directory IP site links** Active Directory IP site links define logical paths between Active Directory sites. Exchange 2010 references the IP site link objects to determine the least-cost routing path of remote Active Directory sites.
- **Send connectors** Send connectors are used for sending messages to other SMTP hosts. The address space configuration on Send connectors are used to make routing decisions. When a message is delivered to an external domain, the routing destination is typically a Send connector. An Exchange organization that accepts messages for more than one e-mail domain may decide to create Send connectors that are dedicated to each address space. For more information about Send connector selection for routing messages to external domains, see External Message Routing.
- **Delivery agents** Delivery agents are used to route messages to foreign systems that don't use SMTP protocol for message transfer. The address space and protocol configuration of delivery agents are used when making routing decisions.
- **Foreign connectors** Foreign connectors use drop directories to send messages to foreign systems that don't use SMTP protocol for message transfer. Exchange uses the configuration of Foreign connectors when making routing decisions.
- **Routing groups** Routing groups represent a routing boundary for Exchange Server 2003. If Exchange 2010 is deployed in an existing Exchange 2003 organization, routing must consider the location of servers within routing groups to deliver a message to a mailbox or a connector that resides on Exchange 2003. To implement compatibility with Exchange 2003, all computers running Exchange 2010 deployed in the organization belong to a single, global routing group.
- **Routing group connectors** Routing group connectors define logical paths between Exchange routing groups. If Exchange 2010 is deployed in an existing Exchange 2003 organization, messages are routed between server versions through routing group connectors. When the first Hub Transport server is deployed, the setup process prompts you to create a routing group connector from the global Exchange 2010 routing group to a legacy routing group. For more information about message routing in an environment where more than one version of Exchange is deployed, see Internal Message Routing.
- **Microsoft Exchange Transport service** The Microsoft Exchange Transport service is the SMTP provider for Exchange 2010 and controls every component of message processing, from SMTP IN to SMTP OUT. A series of configurable SMTP Receive agents are triggered at various SMTP events. The Microsoft Exchange Transport service enables these agents to process messages as they pass through SMTP transport and perform anti-spam, antivirus, and other tasks before messages are submitted to the categorizer. The Microsoft Exchange Transport service also uses the topology discovery module for Exchange topology discovery.
- **Microsoft Exchange Active Directory Topology service** The Microsoft Exchange Active Directory Topology service is responsible for locating the domain controllers and global catalog servers that Exchange 2010 can use to retrieve configuration and recipient data from Active Directory. The Microsoft Exchange Active Directory Topology service is also responsible for keeping Active Directory site affinity for an Exchange 2010 server up to date.
- **Routing tables** The routing tables hold the information that the routing component uses to make routing decisions. The routing table is composed of a

map of topology components and their relationship to one another.

- **DNS** Exchange 2010 uses an enhanced Domain Name System (DNS) client, a component of the Microsoft Exchange Transport service, to resolve the next hop selection to a list of target server names. The standard DNS client is used to resolve that list of server names to IP addresses. Enhanced DNS also provides load-balancing functionality for Exchange 2010 transport servers by using round robin.
- **SMTP** SMTP is used for communication when messages are relayed between SMTP servers. An SMTP server can be a Hub Transport server, Edge Transport server, Exchange 2003 server, or a smart host. A Hub Transport server uses remote procedure call (RPC) to deliver messages directly to Mailbox servers that have the same Active Directory site membership as the Hub Transport server.

Return to top

Using Active Directory Sites for Routing

An Active Directory site is a logical configuration component that's based on the physical aspects of the network. The primary purpose for creating an Active Directory site is to define which subnets in the network are connected in a way that optimizes control of Active Directory replication traffic. The Active Directory site represents a routing boundary for Exchange 2010. Computers that have the Hub Transport server role installed make routing decisions based on the Active Directory site topology.

Determining Site Membership

By default, an Active Directory forest contains only one Active Directory site. The default name for this Active Directory site is Default-First-Site-Name. If no other Active Directory sites are created, all domain member computers in the forest are members of Default-First-Site-Name. You don't have to configure a subnet-to-site association. If additional Active Directory sites are created, you must specify the subnets that are assigned to that Active Directory site.

Each Active Directory site is associated with one or more IP subnets. An administrator assigns Active Directory site membership to computers that are configured as domain controllers and global catalog servers. Other domain member computers, such as Exchange servers, are assigned Active Directory site membership automatically when they're configured to use an IP address that's in an IP subnet that's associated with an Active Directory site. Computers that have the same Active Directory site membership are presumed to have good network connectivity. A server is always a member of a single Active Directory site.

When an application can determine the Active Directory site membership of the computer where it's installed and of other computers in the forest, and then use that information to control communication flow, it's a site-aware application. When site-aware applications must use the services of another server, such as a domain controller or global catalog server, priority is given to the servers that have the same Active Directory site membership as the computer that's requesting those services.

Exchange 2010 is a site-aware application and uses the Active Directory topology for message routing and to communicate with the services that are running on computers that have other Exchange 2010 server roles installed. The Active Directory site isn't only the routing boundary. It's also the service discovery boundary.

Determining site membership for a domain member computer depends on a series of DNS queries to compare the local IP address to defined subnets and then determine the appropriate site membership association. To reduce the overhead that's associated with DNS queries, the Exchange 2010 Active Directory schema additions include the **msExchServerSite** attribute for the Exchange server object. The value of this attribute is

the distinguished name of the Active Directory site of an Exchange server. This attribute is a property of each Exchange server object. When site membership affinity is stored as an attribute of the server object, the current topology can be read directly from Active Directory instead of relying on DNS queries and a site membership association is enabled for a non-domain computer, such as a subscribed Edge Transport server.

The value for the **msExchServerSite** attribute is populated and kept up to date by the Microsoft Exchange Active Directory Topology service. When a Windows-based computer starts, the Net Logon service determines site membership for the computer. The Net Logon service uses that information to locate domain controllers that are located in the same Active Directory site as the local computer and then directs authorization and authentication requests to those servers. The Microsoft Exchange Active Directory Topology service uses the DsGetSiteName API call to retrieve the site membership value from the Net Logon service and writes the Active Directory site's distinguished name to the **msExchServerSite** attribute for the Exchange server object in Active Directory.

The following table shows how an organization might define Active Directory sites. In this example, three Active Directory sites are defined, and each Active Directory site is associated with more than one IP subnet.

Example of an Active Directory site-to-subnet association

Active Directory site name	Associated IP subnets
Site A	192.168.1.0/24 192.168.2.0/24
Site B	192.168.3.0/24 192.168.4.0/24
Site C	192.168.5.0/24 192.168.6.0/24

If a server named HubTransportA has the IP address of 192.168.1.1, it's a member of Site A. By changing the IP address of a server, you may change its site membership. If you change the IP address of HubTransportA to 192.168.2.1, it won't change the server's Active Directory site membership because that subnet is also associated with Site A. However, if you move the server and the IP address changes to 192.168.3.1, the server would be considered a member of Site B.

A change in site membership can also occur if you change the association of subnets to Active Directory sites. For example, if you remove the subnet 192.168.3.0 from association with Site B and associate it with Site A, the site membership of a server that has the IP address of 192.168.3.1 also changes to Site A. Whenever a change in site membership occurs, Exchange 2010 must update its configuration data so that the change is considered when Exchange 2010 makes routing decisions. Some latency occurs between the time that a change in an Active Directory site membership occurs and the topology change is fully propagated. The following communication must occur in the following order to propagate topology changes:

1. The change in site membership is written to a domain controller. The updated information replicates between the domain controllers in each Active Directory site in the forest. The time that's required for the change to propagate fully throughout the forest depends on the Active Directory replication topology and schedule as defined by site links.
2. The Net Logon service runs on all Windows-based computers and polls frequently for changes in Active Directory site membership. The Net Logon service polls at five-minute intervals. Therefore, the change is detected by

the Net Logon service within five minutes of the local domain controller receiving the update.

3. The Microsoft Exchange Active Directory Topology service queries the Net Logon service at 15-minute intervals to determine the Active Directory site membership of the local Exchange server. If a change is detected, the Microsoft Exchange Active Directory Topology service updates the **MsExchServerSite** attribute.
4. The changed site attribute value of the Exchange server configuration object is then replicated throughout the organization. The Exchange servers in the organization detect this change. Then the routing tables are updated with the new Active Directory site membership attribute value.

Some latency occurs between the time that an Active Directory site membership change takes effect and the time that the updated information is available to another Exchange 2010 server. For more information about how Exchange 2010 handles these types of configuration changes, see "Rerouting and the Unreachable Queue" later in this topic.

IP Site Links

Site links are logical paths between Active Directory sites. A site link object represents a set of sites that can communicate at a uniform cost through a specified intersite transport. Site links don't correspond to the actual path taken by network packets on the physical network. However, the cost assigned to the site link by the administrator typically relates to the underlying network reliability, speed, and available bandwidth. For example, the Active Directory administrator would assign a lower cost to a network connection with a speed of 100 megabits per second (Mbps) than to a network connection with a speed of 10 Mbps.

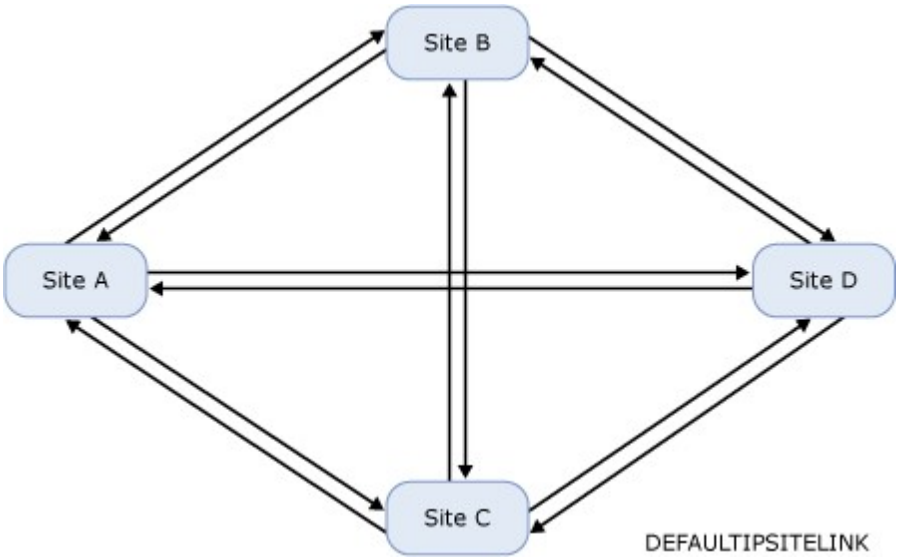
By default, all site links are transitive. This means that if Site A has a link to Site B, and Site B has a link to Site C, Site A is transitively linked to Site C. The transitive link between Site A and Site C is also known as a *site-link bridge*.

An Active Directory site link can be configured to use either IP or SMTP as the transport protocol for communication. An SMTP site link is limited in the types of data that can be replicated by using that protocol and is designed to provide a store and forward mechanism for replication between Active Directory sites that don't have a reliable network link. An IP site link isn't limited in the types of data that can be replicated across it. Exchange 2010 uses only IP site links to determine its routing topology. The cost that's assigned to the IP site link will be considered by the routing component of Exchange 2010 when calculating a routing table. These costs are used to calculate the least-cost routing path to the ultimate destination for a message.

Every Active Directory site must be associated with at least one IP site link. There is a single default IP site link named DEFAULTIPSITELINK. When you create an Active Directory site, you must associate that site to an IP site link. You can create additional IP site links to implement the desired topology, or you can associate every Active Directory site to the DEFAULTIPSITELINK. Each Active Directory site that's part of an IP site link can communicate directly with every other site in that link at a uniform cost.

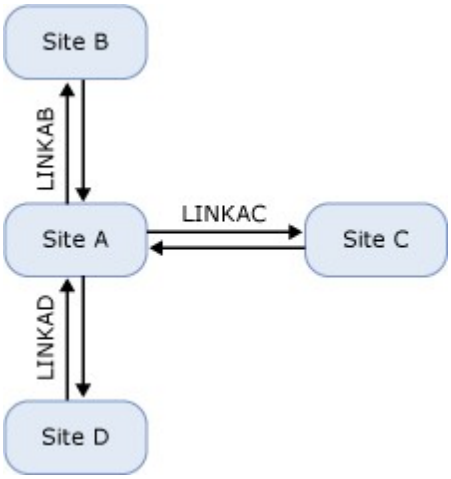
In the following figure, four Active Directory sites are configured in the forest. Every site has been associated with the DEFAULTIPSITELINK. Therefore, each Active Directory site communicates directly with every other site by using the same cost metric. More than one communication path is indicated, but only a single IP site link is defined.

Full mesh topology with a single IP site link



In the following figure, four Active Directory sites are configured in the forest. In this topology, the administrator has configured IP site links to create a *hub-and-spoke topology* of Active Directory sites. Each spoke site can communicate directly with the central site, and the spoke sites can communicate with one another by using the transitive IP site links.

Hub-and-spoke topology of Active Directory IP site links



It's important to note that Exchange uses site links only when determining the least-cost path, but will always try to deliver messages directly to the destination Hub Transport server. For example, if a user in Site B in the topology shown in the preceding figure sends a message to another user in Site C, the Hub Transport server in Site B will connect directly to the Hub Transport server in Site C. If you want to force messages to go through Site A, you must enable that site as a hub site. For more information about hub sites, see "Implementing Hub Sites" later in this topic.

An Active Directory administrator implements the topology that best represents the connectivity and communication requirements of the forest. Because the same topology is used by Exchange 2010, you must make sure that the current topology supports efficient messaging communication.

The default cost for a site link is 100. A valid site link cost can be any number from 1

through 99,999. If you specify redundant links, the link with the lowest cost assignment is always preferred. An Exchange organization administrator can assign an Exchange-specific cost to an IP site link. If an Exchange cost is assigned to an IP site link, it will be used by Exchange 2010. Otherwise, the Active Directory cost is used. For more information about how to set an Exchange cost on an IP site link, see "Controlling IP Site Link Costs" later in this topic. An administrator who has membership in the Enterprise Administrators group can create additional IP site links.

For more information about Active Directory site configuration, see Designing the Site Topology.

Controlling IP Site Link Costs

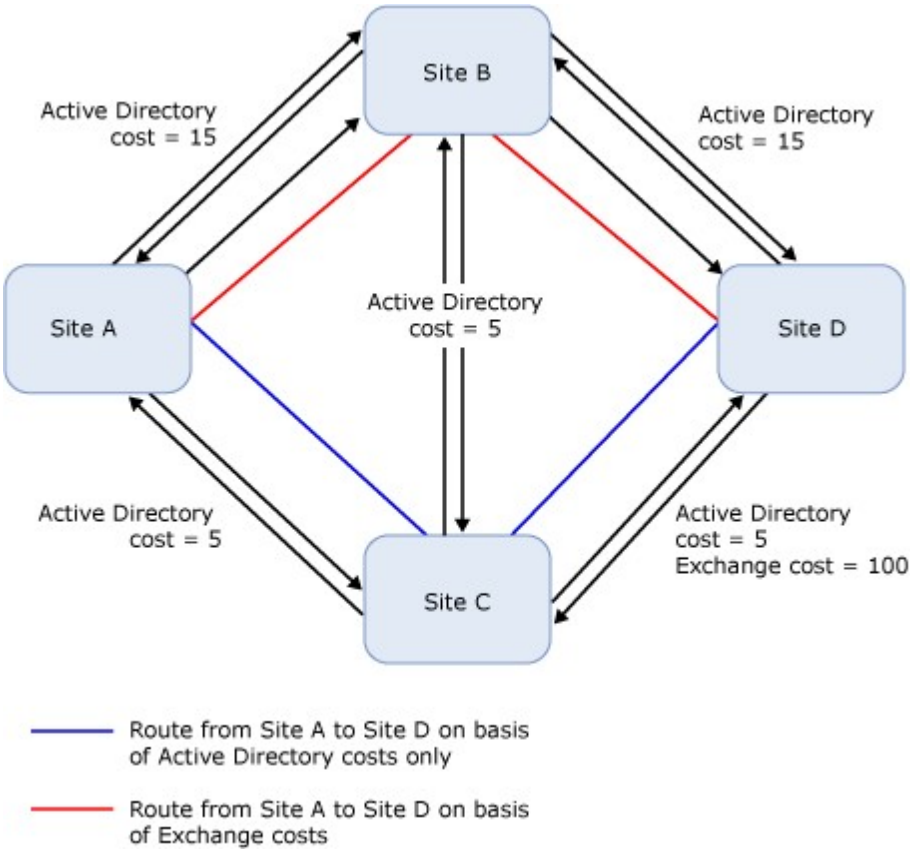
Active Directory IP site links costs are based on relative network speed compared to all network connections in the WAN and are designed to produce a reliable and efficient replication topology. Therefore, in most cases, the existing IP site link costs should work well for Exchange 2010 message routing. However, if after documenting the existing Active Directory site and IP site link topology, you verify that the Active Directory IP site link costs and traffic flow patterns aren't optimal for Exchange 2010, you can make adjustments to the costs evaluated by Exchange. Changing the cost assigned to the IP site link by using Active Directory tools would impact the entire environment. Instead, use the **Set-AdSiteLink** cmdlet in the Exchange Management Shell to assign an Exchange-specific cost to the IP site link. For example, to set a different cost on the IP site link SITELINKAB for message routing purposes, run the following command in the Shell.

```
Set-AdSiteLink -Identity SITELINKAB -ExchangeCost 25
```

When an Exchange cost is assigned to an IP site link, the Exchange cost overrides the Active Directory cost for message routing purposes, and routing only considers the Exchange cost when it evaluates the least-cost routing path.

Adjusting IP site link costs can be useful when the message routing topology has to diverge from the Active Directory replication topology. Exchange costs can be used to force all message routes to use a hub site. Exchange costs can also be used to control where messages are queued when communication to an Active Directory site fails. The following figure shows an Active Directory topology with four sites.

Topology with Exchange costs configured on IP site links



In the preceding figure, the network connection between Site C and Site D is a low bandwidth connection that's only used for Active Directory replication and shouldn't be used for message routing. However, the Active Directory IP site link costs cause that link to be included in the least-cost routing path from any other Active Directory site to Site D. Therefore, messages are delivered to the Site D queue in Site C. The Exchange administrator prefers that the least-cost routing path include Site B instead so that if Site D is unavailable, the messages will queue at Site B. Configuring a high Exchange cost on the IP site link between Site C and Site D prevents that IP site link from being included in the least-cost routing path to Site D.

Exchange 2010 provides support for configuration of a maximum message size limit on an Active Directory IP site link. By default, Exchange 2010 doesn't impose a maximum message size limit on messages that are relayed between Hub Transport servers in different Active Directory sites. If you use the **Set-AdSiteLink** cmdlet to configure a maximum message size on an Active Directory IP site link, routing generates a non-delivery report (NDR) for any message that has a size larger than the maximum message size limit that's configured on any Active Directory site link in the least-cost routing path. This configuration is useful for restricting the size of messages that are sent to remote Active Directory sites that must communicate over low-bandwidth connections. For more information, see Understanding Message Size Limits.

Implementing Hub Sites

In your Exchange organization, you may have to force all message delivery to be relayed through a particular Active Directory site. In this scenario, connectivity may prevent direct SMTP relay between sites. Therefore, messages must be relayed through an interim site before they're sent to their destination. Because of an Exchange organization's internal policies, an administrator may also want to relay all messages through a particular site. You can use Shell cmdlets to designate an Active Directory site as a hub site. By designating an Active Directory site as a hub site, you cause additional overall overhead

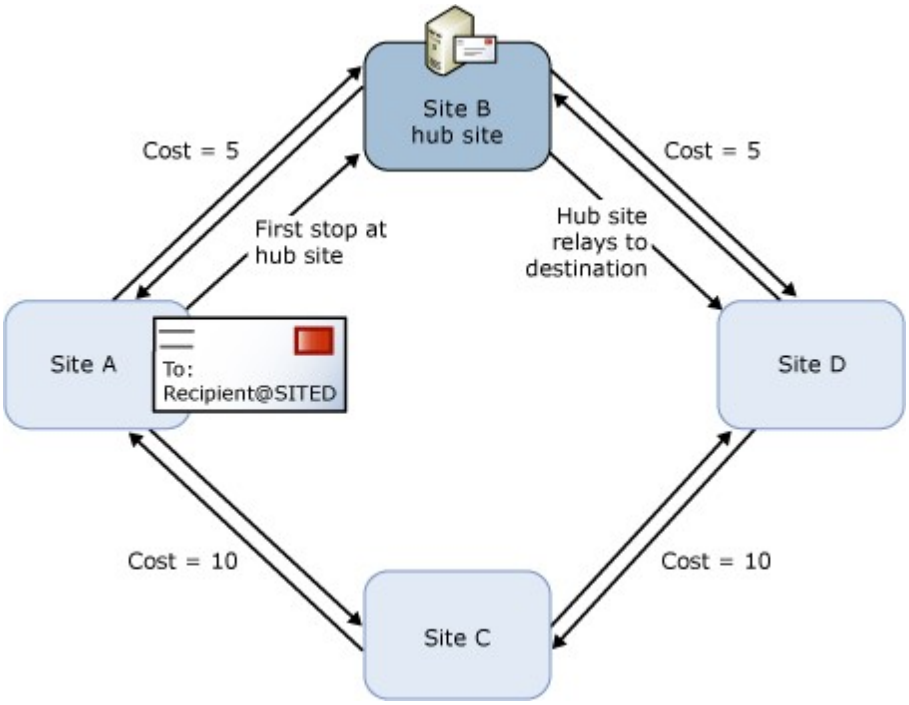
because more servers are involved in message delivery. For example, consider a message that's sent from Site A to Site E. If the least-cost routing path is Site A-Site B-Site C-Site D-Site E, and you designate Site C as a hub site, the message is relayed from Site A to Site C and then relayed from Site C to Site E.

You use the **Set-AdSite** cmdlet to specify an Active Directory site as a hub site. Whenever a hub site exists along the least-cost routing path for message delivery, the messages queue and are processed by the Hub Transport servers in the hub site before they're relayed to their ultimate destination.

After the least-cost routing path is chosen, routing determines whether there's a hub site along that routing path. If a hub site is configured, messages stop at a Hub Transport server in the hub site before they're relayed to the target destination. If there's more than one hub site along the least-cost routing path, messages stop at each hub site along the routing path.

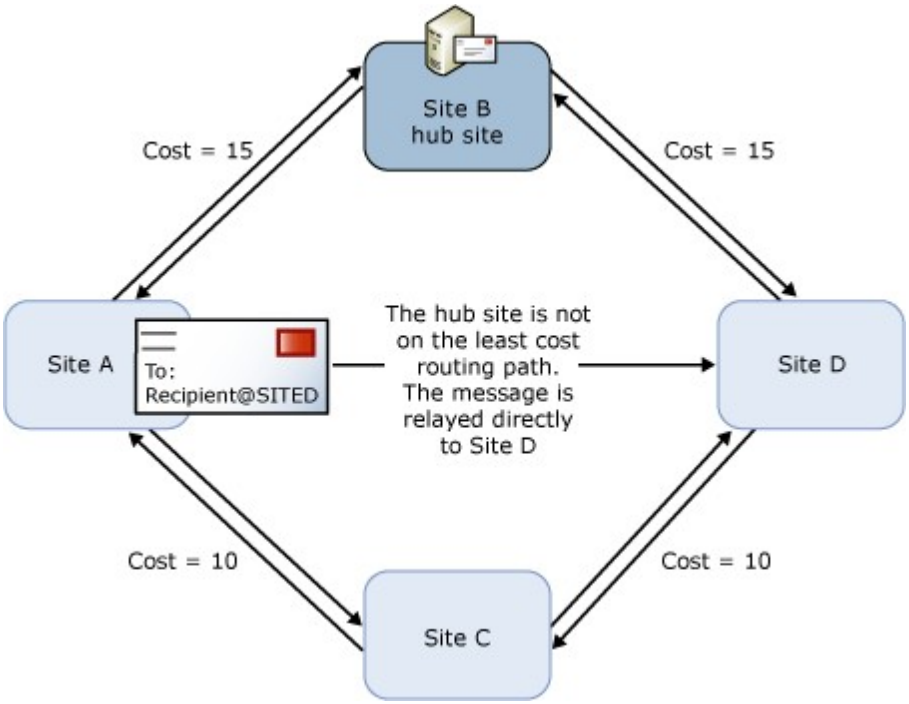
This variation to direct relay routing only is in effect when the hub site is located along the least-cost routing path. The following figure shows the correct use of a hub site. In this diagram, Site B is configured as a hub site. Messages that are relayed from Site A to Site D are relayed to Site B before they're delivered to Site D.

Message delivery with a hub site



The following figure shows how IP site link costs affect routing to a hub site. In this scenario, Site B has been designated as a hub site. However, because it doesn't exist along the least-cost routing path between any other sites, queuing at Site B before delivery to the destination doesn't occur. An Active Directory site is never used as a hub site if it isn't on the least-cost routing path between two other sites.

Misconfigured hub site



You can configure any Active Directory site as a hub site. However, for this configuration to work correctly, you must have deployed at least one Hub Transport server in the hub site.

Topology Discovery

The Exchange 2010 topology relies on the Active Directory site topology and doesn't have its own configuration. The Active Directory topology is made available to Exchange 2010 by the following required elements:

- The Microsoft Exchange Active Directory Topology service
- The topology discovery module inside the Microsoft Exchange Transport service

The Microsoft Exchange Active Directory Topology service runs on all Exchange 2010 server roles, except the Edge Transport server role. These Exchange 2010 servers use the Microsoft Exchange Active Directory Topology service to discover the domain controllers and global catalog servers that can be used by the Exchange servers to read and write Active Directory data. Exchange 2010 binds to the identified directory servers whenever Exchange has to read from or write to Active Directory.

The topology discovery module is part of the Microsoft Exchange Transport service and provides information about the Active Directory topology to Exchange servers. This API discovers the Exchange servers and roles in the organization and determines their relationship to the Active Directory configuration objects. Configuration data is retrieved from Active Directory and then cached so that it can be accessed by the Exchange services that are running on that computer.

The topology discovery module performs the following steps to generate an Exchange routing topology:

1. Data is read from Active Directory. All the following objects are retrieved:
   - Active Directory sites.
   - IP site links.
   - All Exchange servers. This includes information about the Exchange 2010 server roles deployed on those servers.
2. The data that's retrieved in step 1 is used to create the initial topology and

to begin linking and mapping the related configuration objects.
3. Exchange servers are matched to Active Directory sites by retrieving the site attribute value from the Exchange server object that's stored in Active Directory.
4. Routing tables are updated with the collection of information retrieved.

This process makes every Exchange 2010 server aware of the other Exchange servers in the organization and of how close the Exchange servers are to one another.

Return to top

Exchange 2010 Routing Tables

When the Microsoft Exchange Transport service starts, it calculates a set of routing tables that's based on the snapshot of information that's retrieved from Active Directory or, on an Edge Transport server, from AD LDS. The configuration information that's stored in AD LDS includes available connectors and accepted domains, but doesn't include topology data.

The routing component refers to the routing tables to determine how to route messages to recipients. When configuration changes are made, the routing tables are rebuilt. The new routing tables are used to route new incoming messages. Messages in remote delivery queues are also rerouted if the routing component determines that they're affected by the configuration changes. For more information about message rerouting, see "Rerouting and the Unreachable Queue" later in this topic.

The following configuration data is retrieved from Active Directory and made available to the routing component of Hub Transport servers:

- Active Directory sites
- Active Directory IP site links
- Exchange servers and their relationship to Active Directory sites
- SMTP connectors
- Non-SMTP connectors

  Note:
  Non-SMTP connectors include Exchange 2010 delivery agent connectors, Foreign connectors, and in coexistence scenarios, any non-SMTP connectors hosted by Exchange 2003.

- Routing groups
- Routing group connectors
- Mailbox stores (private message databases (MDBs))
- Public folder stores (public MDBs)
- Public folder hierarchies

Based on this data, the routing component of the Microsoft Exchange Transport service populates routing tables to help streamline routing decisions. The routing table correlates the data to create a topology map. This topology map contains the following elements:

- **Linked connectors map** This map correlates the identifiers of Receive connectors on the local server to the linked Send connector.
- **Server map** All Exchange 2010 and Exchange 2007 Hub Transport servers, Edge Transport servers, Mailbox servers, and Exchange 2003 servers in the organization are contained in the server map. This map correlates the distinguished name of each Exchange server to server routing data. This includes the total cost to reach that server.
- **Legacy server map** All Exchange Server 2007 Hub Transport servers, Edge Transport servers, Mailbox servers, and Exchange 2003 servers in the organization are contained in the legacy server map. This map correlates the legacy distinguished name of each Exchange server to server routing data.

This includes the total cost to reach that server. This map supports store override functionality. Store override functionality is specific to public folders. For more information, see "Routing to Public Folders" in Internal Message Routing.

- **MDB map** All MDBs in the organization are contained in the MDB map. This map correlates the distinguished name of each MDB to server routing data. This includes the total cost to reach that server.
- **Active Directory site map** This map correlates each Active Directory site to a structure that contains the least-cost routing path from the local site to every other site. The map includes any hub sites along the least-cost routing path. Each routing path hop also identifies all Hub Transport servers in that site that will be used by the enhanced DNS component.
- **Routing groups map** This map associates the total cost and first hop routing group connector for the least-cost routing path from the Exchange 2010 routing group to each legacy routing group.
- **Send connectors map** This map identifies the Send connectors configured in the organization and the source servers for each connector.

The routing tables are built every time that a transport server is started and recalculated when configuration changes are received. Configuration changes can be detected in any of the following ways:

- **Active Directory change notifications** There is a delay between the time that a notification is received and the time that the change is written to the routing tables. This delay lets the routing component batch the changes and process more than one change in a single operation. By default, each notification causes the routing component to delay processing by five seconds. For example, if five notifications are received exactly one second after the previous notification, routing delays processing the change for a total of nine seconds.
- **Configuration reloading caused by service control commands** The routing component reloads the configuration data when the Microsoft Exchange Transport service is restarted.
- **Periodic reload to track changes that aren't supported by Active Directory notifications** By default, routing will periodically reload the configuration data to make sure that all changes are tracked. The configuration reload occurs at six-hour intervals.

The information in the routing tables is logged to routing logs. By default, these logs are located in the C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Routing folder. A new log is generated every time that the routing tables are calculated. If for some reason the Hub Transport server is unable to contact Active Directory, routing continues to make routing decisions based on the currently cached data, even though that data may not be up to date. For more information, see Understanding Routing Table Logging.

Return to top

Receiving Messages for Routing

A message can arrive at a Hub Transport server in any of the following ways:

- E-mail is received from an Internet-facing SMTP server for delivery to a recipient in the Exchange organization or to a recipient in an internal relay accepted domain.
- E-mail is received from another Hub Transport server in the Exchange organization for delivery to a recipient mailbox that's located on a Mailbox server in that Active Directory site.
- E-mail is received from SMTP clients. These are typically POP3 or IMAP4 users that may exist in your environment.
- E-mail is received from Pickup and Replay directories on a Hub Transport

server. These directories are typically used by Foreign connectors to transmit messages to your Exchange infrastructure.
- E-mail is retrieved from an Exchange 2010 Mailbox server by the Hub Transport server.
- E-mail is received from an Exchange 2007 or Exchange 2003 server for delivery to a recipient mailbox that's located on an Exchange 2010 Mailbox server.

Processing of all e-mail that's received by a Hub Transport server for categorization begins in the Submission queue.

Receiving Messages from Edge Transport Servers, Other Exchange Hub Transport Servers, and SMTP Clients

In this scenario, messages are received from Edge Transport servers, Hub Transport servers, or other third-party SMTP hosts by using standard SMTP connections. The remote host initiates an SMTP connection and transfers the messages to the Hub Transport server. Hub Transport servers use Receive connectors for accepting incoming SMTP connections. Each Hub Transport server has two Receive connectors created during setup. One of these connectors is used to receive authenticated SMTP connections from other Exchange servers. The second one is used to receive SMTP connections from SMTP clients used by POP3 or IMAP4 users in your organization. These two Receive connectors have different permissions configured that are appropriate for their intended use. To learn more about Receive connectors, see Understanding Receive Connectors.

By default, Hub Transport servers don't accept unauthenticated anonymous connections. If you need to enable this functionality, we recommend that you create a separate Receive connector to handle the anonymous connections. For more information, see Allow Anonymous Relay on a Receive Connector.

Collecting Messages from Pickup and Replay Directories

Messaging systems that don't use SMTP as the transfer protocol can be connected to your Exchange organization using Foreign connectors. When a message is sent to an Exchange user from a remote system, the Foreign connector writes that message to a special directory on the Hub Transport server called the Pickup directory. The Hub Transport server periodically checks the Pickup directory for new messages. When it detects a new message, the Hub Transport server then converts the message to an Exchange e-mail message and routes it as a regular message. To learn more about how the Pickup and Replay directories are used, see Understanding the Pickup and Replay Directories.

Retrieving Messages from a Mailbox Server

In this scenario, the Microsoft Exchange Mail Submission service that runs on Mailbox servers notifies a Hub Transport server that's located in the same Active Directory site that messages are ready for retrieval from a sender's outbox. Each Mailbox server maintains a list of Hub Transport servers that are located in the same Active Directory site. This list of Hub Transport servers is known as the submission server list. The server discovery process repeats every ten minutes to keep the list up to date.

If more than one Hub Transport server is located in the same Active Directory site as the Mailbox server that's submitting a notification that mail is ready for retrieval, the following process is used to select the server:

- If the local Mailbox server is also running the Hub Transport server role and it is not participating in a database availability group (DAG), the local server is notified. If the local Microsoft Exchange Transport service isn't running or the local Hub Transport server can't process new mail submissions because of back pressure, another available Hub Transport server is notified. For more information about back pressure, see Understanding Back Pressure.
- If the local Mailbox server is also running the Hub Transport server role and is also participating in a DAG, it first tries to notify any Hub Transport server in the site before notifying the local Hub Transport server. This is done to avoid having redundant copies of messages on the same server hardware. To learn

more about coexisting Mailbox and Hub Transport server roles when using DAGs, see Hub Transport and Mailbox Server Roles Coexistence When Using DAGs.

- If the local Mailbox server isn't running the Hub Transport server role, notifications are load balanced among Hub Transport servers by using round robin.
- If the selected Hub Transport server can't be contacted, the Microsoft Exchange Mail Submission service fails over to a different Hub Transport server in the same Active Directory site. The failing server is marked as inactive, and the next Hub Transport server in the submission server list is selected. If no Hub Transport servers in the local Active Directory site are available, the submission server list is empty. In this case, an event is logged and mail submission notifications are temporarily stopped. Hub Transport servers that are marked as inactive are retried after five minutes.

By default, the Microsoft Exchange Mail Submission service load balances notification events across the Hub Transport servers in a site so that each Hub Transport server receives an equal distribution of notification events to process. In some circumstances, providing an equal distribution may not be an optimal solution. Not all Hub Transport servers have the same capacity, and some messages require additional processing. For example, a message that has a large attachment or many recipients takes longer for a Hub Transport server to process than a small message that's addressed to only one recipient. If you want to create a static list of Hub Transport servers that a Mailbox server should notify, you can use the **Set-MailboxServer** cmdlet in the Shell. Use the *SubmissionServerOverrideList* parameter to specify a list of Hub Transport servers that the local Mailbox server will notify when it has mail for retrieval. For more information about how to configure this setting, see Set-MailboxServer.

After a Hub Transport server receives a mail submission notification from a Mailbox server, it uses the store driver to retrieve the message from the mailbox database and put it in the Submission queue on the Hub Transport server. The transfer of the message from the Mailbox server to the Hub Transport server happens by using Exchange RPC.

Receiving Messages from Legacy Exchange Servers

Due to the changes made to the Exchange Server Object (XSO) model in Exchange 2010, Exchange 2010 Hub Transport servers can't pick up messages from and deliver messages to Exchange 2007 Mailbox servers. Similarly Exchange 2007 Hub Transport servers can't communicate with Exchange 2010 Mailbox servers. All messages sent from Exchange 2007 recipients are first picked up from the Mailbox servers by Exchange 2007 Hub Transport servers and are then relayed to Exchange 2010 Hub Transport servers. To learn more about message routing when coexisting with Exchange 2007, see Upgrade from Exchange 2007 Transport.

As opposed to Active Directory sites, Exchange 2003 uses routing groups to route messages. Routing groups are connected to each other using routing group connectors. To support coexistence between these two routing topologies, all Exchange 2010 servers are automatically added to a single routing group when Exchange 2010 is installed in an Exchange 2003 organization. All messages that originate on Exchange 2003 mailboxes are delivered to the Exchange 2010 environment through the routing group connectors between the Exchange 2010 routing group and the Exchange 2003 routing groups. To learn more about message routing when coexisting with Exchange 2003, see Upgrade from Exchange 2003 Transport.

Return to top

Routing Messages

After a Hub Transport server or an Edge Transport server receives a message, it determines the ultimate destination and uses the Exchange topology and connector

configurations to determine the least-cost routing path. After the routing path is determined, the message is delivered to the next hop on the routing path.

Although this topic explains how Exchange makes routing decisions in general, the following two topics provide additional information about specific routing scenarios. The internal message routing topic discusses message delivery to Mailbox servers, public folders, and legacy servers. The external message routing topic discusses routing messages to recipients that are outside your Exchange organization. The topic also discusses the roles of Send connectors, delivery agent connectors, and Foreign connectors.

- Internal Message Routing
- External Message Routing

Determining the Ultimate Destination

The previous section described the various sources from which a Hub Transport server can receive messages. When a message is received by a Hub Transport server, the message must be categorized. The first phase of message categorization is recipient resolution. After the recipient has been resolved, the ultimate destination can be determined. The next phase, routing, determines how to best reach that destination. A single, deterministic route is selected. That route isn't recalculated unless the routing configuration changes.

From the perspective of the sending server, each delivery queue represents the destination for a particular message. When the Hub Transport server or Edge Transport server selects the destination for a message, the destination is stamped on the recipient as the **NextHopSolutionKey** attribute. If a single message is being sent to more than one recipient, each recipient has the **NextHopSolutionKey** attribute. The receiving server also performs message categorization and queues the message for delivery. After a message is queued, you can examine the delivery type for a particular queue to determine whether a message will be relayed again when it reaches the next hop destination.

The destination for a message can be classified as one of the following delivery types:

- **DNS connector delivery** The messages are queued for delivery to an external recipient by using an SMTP Send connector for which the local server is a source server. The connector is configured to use DNS to resolve the recipient addresses.
- **Smart host connector delivery** The messages are queued for delivery to an external recipient by using an SMTP Send connector for which the local server is a source server. The connector is configured to use a smart host for delivery.
- **SMTP relay in an Active Directory site to an Edge Transport server** The messages are queued for delivery to an external recipient by using an SMTP Send connector for which the source server is an Edge Transport server that's subscribed to the local Active Directory site.
- **SMTP relay in an Active Directory site to a Hub Transport server** The messages are queued for delivery to a Hub Transport server that's located in the same Active Directory site as the local server. The destination server can be an Exchange 2007 Hub Transport server, the source server for a Send connector, a delivery agent connector or Foreign connector, the source server of a routing group connector, or a distribution group expansion server.
- **SMTP relay to a remote Active Directory site** The messages are queued for delivery to a Hub Transport server that's located in a remote Active Directory site. The ultimate destination server in the remote Active Directory site can be any of the following:
  - The source server for a connector that's configured to transport messages for external recipients
  - The source server for a routing group connector
  - A distribution group expansion server
  - A Mailbox server that's located in the remote Active Directory site

The messages are delivered to one of the Hub Transport servers in the destination site. The receiving server relays the message within the Active Directory site if it's necessary.

- **SMTP relay to a legacy routing group** The messages are queued for delivery to the first hop routing group connector used to reach an Exchange 2003 routing group. The ultimate destination server can be any of the following:
  - The source server for a connector
  - An expansion server
  - An Exchange 2003 bridgehead server that delivers messages addressed to mailbox recipients that are located in the routing group
- **MAPI delivery** The messages are queued for delivery to a recipient's mailbox, a public folder, or a public folder store that's located on a Mailbox server that's located in the local Active Directory site.
- **Non-SMTP gateway delivery** The messages are queued for delivery to an external recipient by using a delivery agent connector or Foreign connector for which the local server is a source server. This delivery type is used only when the messages are being delivered to delivery agent connectors or the Foreign connector drop directory on the local server.
- **Unreachable** A route to the recipient couldn't be determined and the messages are located in the Unreachable queue.

Determining the Least-Cost Routing Path

The least-cost routing path to the remote Active Directory site is determined by the calculation of all the costs assigned to the Active Directory IP site links that exist between the two sites. The links are bridged, and a direct connection occurs. Exchange 2010 Hub Transport servers always select a single, deterministic least-cost routing path. Availability of the underlying connection or destination server is never a consideration in routing path selection, and no alternative routing path is considered.

The least-cost routing path calculation is used to determine a backoff path when message delivery to the next hop fails. In Exchange 2010, *backoff* is a mechanism used to deliver messages at an interim hop along the least-cost routing path when direct relay fails for any reason, such as network issues or servers going offline. The routing component tries to deliver messages as close to the destination as possible by backing off, hop by hop, along the least-cost routing path until a connection is made. First, a connection attempt is made to each Hub Transport server in the destination Active Directory site. If no Hub Transport servers in the Active Directory site respond, the least-cost routing path is checked to determine how to start backing off from the delivery site. The goal is to deliver the message as close as possible to the destination and queue it at a Hub Transport server in that Active Directory site.

Depending on the individual message routing scenario, the following factors may influence the selection of a least-cost routing path:

- **Linked connectors** If the Receive connector that the message is received on is linked to a Send connector, messages are routed to that Send connector regardless of cost. This configuration always takes precedence.
- **The cost assigned to the IP site links and routing group connectors that must be traversed to reach the destination** If more than one routing path exists between a source server and a destination server, the routing path with the lowest aggregate cost is selected.
- **The address space assigned to a Send connector** The Send connector with the most specific address space match to the destination is selected.
- **The cost assigned to the address space configured on a Send connector** If more than one Send connector is assigned the same address space, the routing component compares the cost assigned to the address space. The Send connector with the lowest cost is selected.
- **Connector scope** A connector may be limited to use by Exchange 2010 servers that are located in the same Active Directory site as the source transport servers for the connector. In earlier versions of Exchange, the

connector scope could be limited to servers that have the same routing group membership.

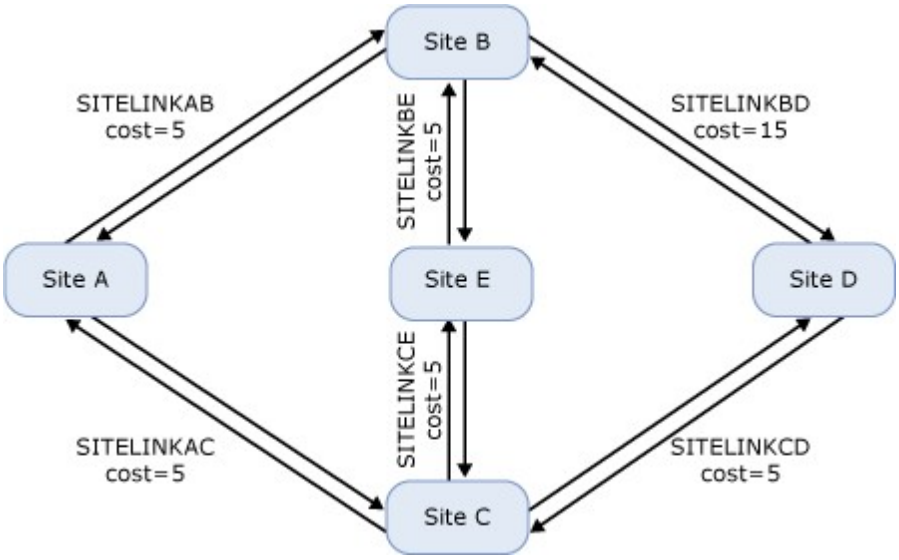
- **Message size restrictions** The message size constraint specified on a connector must be larger than the size of the message being routed. Connectors with a message size restriction that's less than the size of the message are eliminated from routing consideration.
- **The proximity of the destination to the sending server** Routing will prefer the server that's closest, in this order: local server, server in the same Active Directory site, or server in a remote Active Directory site or routing group.
- **The name assigned to an Active Directory site** If more than one routing path results in the same aggregate cost, the routing component makes an alphanumeric comparison of the name of the Active Directory sites that precede the target site along each routing path. The routing path where the Active Directory site nearest to the destination is lowest in alphanumeric order is used.
- **The name assigned to a routing group connector** If more than one routing path results in the same aggregate cost, the routing component makes an alphanumeric comparison of the name of the routing group connectors that come before the target destination along each routing path. The routing path where the routing group connector nearest to the destination is lowest in alphanumeric order is used.
- **The connector state** The Exchange 2010 routing component only considers enabled connectors when it calculates the routing path. However, earlier versions of Exchange don't consider connector state.

The following logic is used to select the routing path:

1. First, calculate the least-cost routing path by adding the cost of the IP site links and of any routing group connectors that must be traversed to reach the destination. If the destination is a connector, the cost assigned to the address space is added to the cost to reach the selected connector. If multiple routing paths are possible, only the routing path with the lowest aggregate cost is used.
2. If more than one routing path has the same aggregate cost, the number of hops in each path is evaluated and the routing path with the least number of hops is used.
3. If more than one routing path is still available, the name assigned to the Active Directory sites or routing group connectors before the destination are considered. The routing path where the Active Directory site nearest the destination is lowest in alphanumeric order is used. If the site nearest the destination is the same for all routing paths being evaluated, an earlier site name is considered.

The following figure shows the routing topology for an Exchange organization. This topology is used in the following examples to demonstrate the logic used by the routing algorithm to select the least-cost routing path.

Exchange 2010 routing topology



Example 1 A message that's being relayed from Site A to Site D can follow two possible routing paths: Site A-Site B-Site D and Site A-Site C-Site D. The costs assigned to the IP site links in each routing path are added to determine the total cost to route the message. In this example, the routing path Site A-Site B-Site D has an aggregate cost of 20. The routing path Site A-Site C-Site D has an aggregate cost of 10. Routing selects path Site A-Site C-Site D.

Example 2 A message is being relayed from Site B to Site D. There are three possible routing paths: Site B-Site D with a cost of 15, Site B-Site E-Site C-Site D with a cost of 15, and Site B-Site A-Site C-Site D with a cost of 15. Because more than one routing path results in the same cost, routing selects the routing path Site B-Site D. This has the least number of hops.

Example 3 A message is being relayed from Site A to Site E. There are two possible routing paths: Site A-Site B-Site E with a cost of 10, and Site A-Site C-Site E with a cost of 10. Both routing paths have the same cost and same number of hops. The alphanumeric order of the Active Directory sites immediately before Site E is compared. Site B has a lower alphanumeric value than Site C. Therefore, routing selects the routing path Site A-Site B-Site E.

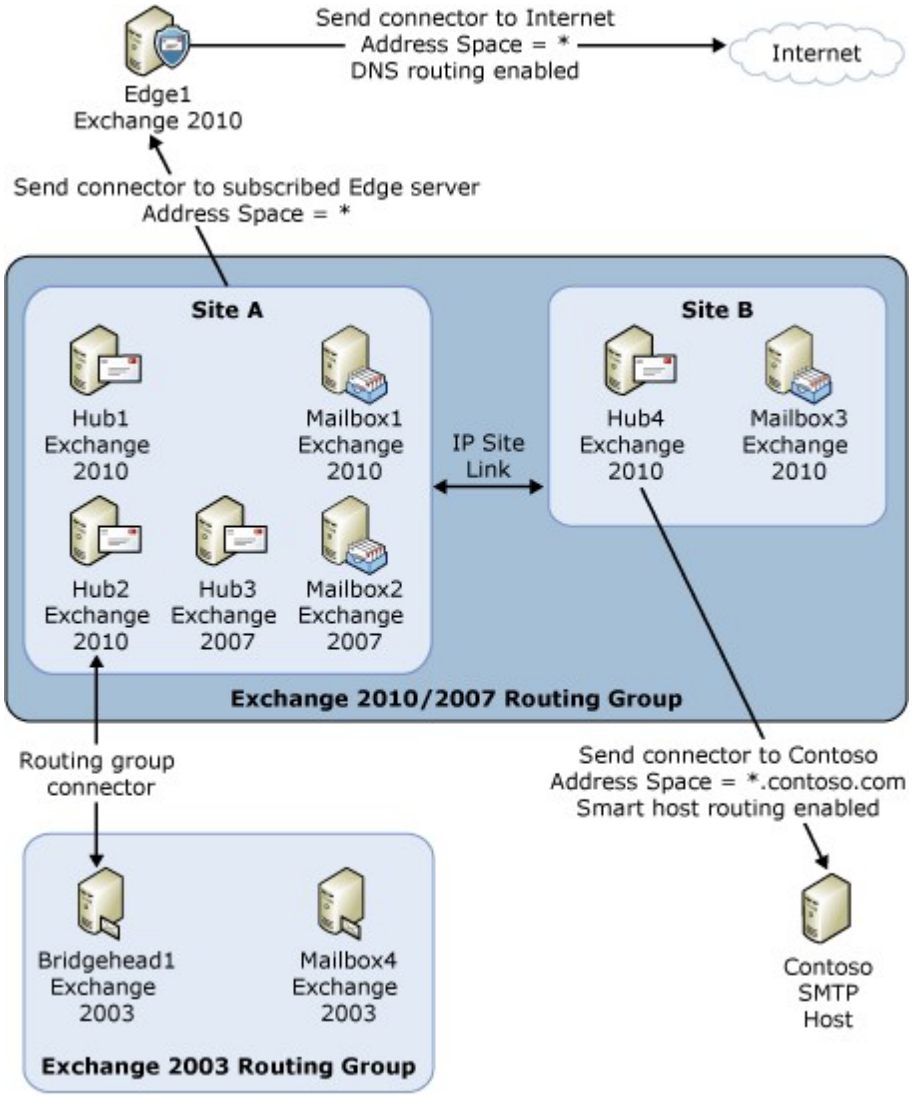
After the least-cost routing path has been determined, the Exchange 2010 routing component doesn't consider alternative routing paths.

Next Hop Selection

Exchange 2010 Hub Transport servers don't relay to each Active Directory site along the least-cost routing path. After the routing path is determined, the message is relayed directly from the source server to the next hop. The next hop selection tries to deliver the messages as close as possible to the ultimate destination. Additional intrasite relay may be required to arrive at the ultimate destination. When routing to legacy routing groups, direct relay to the Active Directory site where the source server for the first hop routing group connector resides occurs. After the message is relayed to the legacy environment, standard legacy routing occurs.

The following figure shows a simple Exchange topology and illustrates many of the Exchange routing components.

Exchange topology and routing components



Using the preceding figure as a reference, a message that's sent from Mailbox1 in Site A, to the external recipient joe@contoso.com is processed as follows:

1. The Microsoft Exchange Mailbox Submission service that's running on Mailbox1 notifies an Exchange 2010 Hub Transport server that's located in the same Active Directory site of the new mail item for transport.
2. Using RPC, the store driver component on an Exchange 2010 Hub Transport server in the same Active Directory site retrieves the message and puts it in the Submission queue on the local server.
3. From the Submission queue, the message moves through categorization. The categorizer first performs recipient resolution and determines that joe@contoso.com is an external recipient.
4. The routing component selects the best connector through which to route the message and calculates the least-cost routing path to that connector. In this example, a Send connector has the address space *.contoso.com and is the connector selected by the routing component. All the source servers for this Send connector are located in Site B.
5. The routing component determines the next hop required to reach a source server for the Send connector. The Hub Transport server in Site A queues the message for SMTP delivery to Site B.
6. If the receiving server in Site B is a source server for the Send connector, it

queues the message for delivery to that Send connector. If the receiving server isn't a source server for the *.contoso.com Send connector, the message is relayed by using SMTP to a Hub Transport server in Site B that's the source server for the connector.

The following table provides additional examples of the next hop selection for several recipients based on the topology shown in the preceding figure. It isn't a complete list of all routing possibilities. It simply provides examples that are most common in a topology like the one shown in the preceding figure.

Examples of next hop selection in the preceding figure

Receiving server	Ultimate destination	Next hop	Queue delivery type
Hub1	Mailbox1	Mailbox1	MAPI delivery
Hub1	Mailbox2	Hub3	SMTP relay in an Active Directory site
Hub1	Mailbox3	Site B	SMTP relay to a remote Active Directory site
Hub1	Mailbox4	Routing group connector	SMTP relay to a legacy routing group
Hub1	Recipient@fourthcoffee.com	Edge1	SMTP relay to Edge Transport
Hub3	Mailbox1	Hub1 or Hub2	SMTP relay in an Active Directory site
Hub4	Mailbox1	Site A	SMTP relay to a remote Active Directory site
Hub4	Mailbox4	Site A	SMTP relay to a remote Active Directory site
Hub4	Recipient@contoso.com	Contoso SMTP Host	Smart host delivery
Hub4	Recipient@fourthcoffee.com	Site A	SMTP relay to a remote Active Directory site
Edge1	Recipient@fourthcoffee.com	Fourth Coffee SMTP Host	DNS delivery

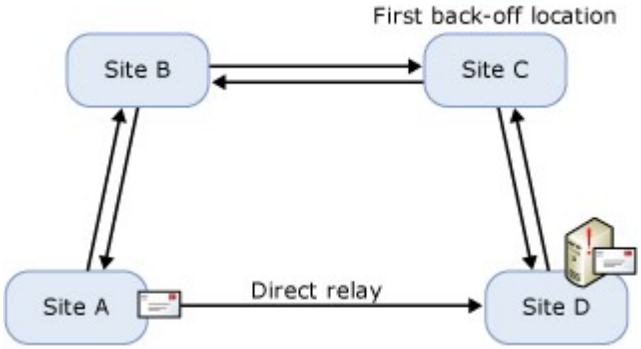
After the least-cost routing path has been calculated and the next hop destination has been chosen, Exchange 2010 routing tries to relay the message directly to the destination, unless a hub site is configured along the least-cost routing path.

Queue at Point of Failure

The least-cost routing path calculation is used to determine a backoff path when message delivery to the next hop fails. Exchange 2010 tries to deliver messages as close to the destination as possible by backing off, hop by hop, along the least-cost routing path until a connection is made. This behavior is known as *queue at point of failure*. When the messages are queued at the point in the delivery path where communication failed, it not only speeds up delivery after the problem is resolved, but it will also help you determine why the message delivery failed.

In the topology shown in the following figure, if a message is being delivered from Site A to Site D, the least-cost routing path may be Site A-Site B-Site C-Site D. Delivery will first be tried directly from Site A to Site D. If no Hub Transport server in Site D responds, delivery will be tried to the Hub Transport servers in Site C. This process continues until a Hub Transport server accepts the message. If all intermediate sites are unavailable, the message will be queued at the source site. If the message is queued in Site C, you can start investigating the failure at the Hub Transport servers in Site D or the network connectivity between Site C and Site D.

Queue at point of failure



When the message is queued at the point of failure, the queue is put in a retry state and delivery attempts continue based on the message retry intervals until delivery succeeds or the message expires. The queue is automatically resubmitted for categorization again after a default interval of 12 hours. Queues that have a connector as the next hop destination aren't automatically resubmitted unless a configuration change that causes resubmission occurs. For more information, see Message Rerouting and the Unreachable Queue.

You can use the Mail Flow Troubleshooter to help diagnose problems with mail flow. This tool is a component of the Microsoft Exchange Troubleshooting Assistant and can be run from the Toolbox of the Exchange Management Console.

In more complex topologies, the least-cost routing path between two Active Directory sites can contain many intermediate Active Directory sites. If a network issue occurs somewhere early along the routing path, it may be too inefficient to back off site by site from the end and try to deliver to every one of the intermediate sites. If the routing path is longer than four hops, binary backoff is implemented until four or fewer sites are remaining. *Binary backoff* means that the next connection attempt is made at the halfway point in the routing path. For example, if the least-cost routing path from Active Directory Site A to Site G is A - B - C - D - E - F - G and the network failure occurs at the link between Site B and Site C, the first connection attempt is made to all Hub Transport servers in Site G. When the connection attempt fails, the next attempt is made to all Hub Transport servers in Site D. This is halfway to Site G. When that connection attempt fails, connection attempts are made to Site C, and Site B because they're closer than four links to the source site. The message will eventually be queued on a Hub Transport server in Site B until the B-C link connectivity is restored.

Delayed Fan-Out

A single e-mail message can be addressed to more than one recipient. These recipients may have internal mailboxes, or they may be external recipients. To route a single message to more than one recipient, the following steps occur:

1. **Recipient resolution** Each recipient of the message is resolved to a delivery destination.
2. **Routing** The least-cost routing path for each recipient is determined. This includes whether a hub site is configured.

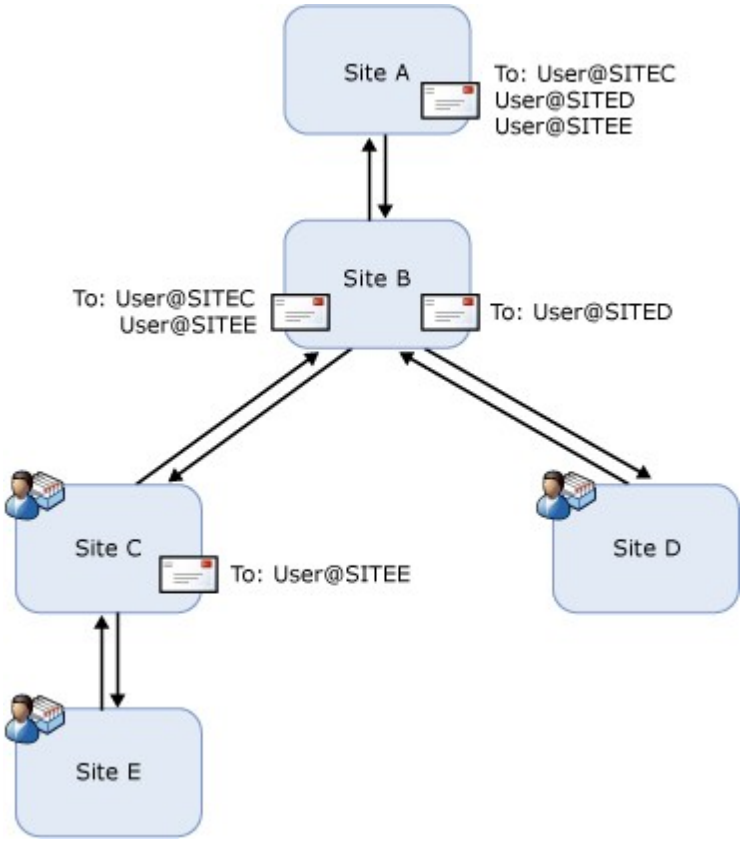
3. **Message splitting** To route the message to recipients that have different delivery locations, the message must be split into multiple copies.

After each recipient has been resolved and a routing path to each delivery destination is determined, Exchange 2010 compares the routing path for each recipient. To preserve bandwidth, the bifurcation, or splitting of the message into multiple copies, doesn't occur until a fork in the routing path is encountered.

For example, if multiple recipients of a single message share part or all of the least-cost routing path, a single copy of the message is sent until the message reaches the point in the routing path where a fork occurs. When the divergence in routing paths occurs, the message splits to create a separate copy for each recipient.

In the following figure, a single message is sent from Site A to recipients in Site C, Site D, and Site E. The least-cost routing path is shared until the message reaches Site B. In this scenario, a single copy of the message that contains all recipients is relayed to Site B. This represents the first fork in the routing path. From Site B, a single message copy is routed to the recipient in Site D, and a single copy is relayed to Site C. In Site C, the message splits again. A copy of the message is delivered to the recipient in Site C. And, a copy of the message is relayed to Site E for delivery to the recipient in that site.

Delayed message fan-out



Return to top

Rerouting and the Unreachable Queue

If routing is unable to determine a route for a valid recipient for any reason, the messages are put in the Unreachable queue. Messages in this queue are rerouted when

configuration changes are processed and routing tables are recalculated. Messages aren't rerouted in the following scenarios. Instead, an NDR is returned to the sender. The following scenarios result in a message being routed to the Unreachable queue:

- The recipient is a non-SMTP address and a matching connector for the address space can't be found.
- The message doesn't meet the message size restrictions of any matching connector.

Not all configuration changes require resubmission of the messages in the queue. For example, a change to the list of smart hosts for a connector doesn't cause messages to be rerouted. For more information about how messages are rerouted, see Message Rerouting and the Unreachable Queue.

Return to top

1.7.1.22.1 External Message Routing

External Message Routing

Transport > Understanding Transport > Understanding Message Routing >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

Microsoft Exchange Server 2010 handles the routing of messages to external recipients. An external recipient is any message recipient that doesn't have a mailbox in the Exchange organization. Exchange uses Send connectors to route messages to external SMTP domains. If the external recipient isn't on an SMTP messaging system, a Delivery Agent connector or a Foreign connector is used instead.

For more information about how Exchange makes routing decisions, see Understanding Message Routing.

Looking for management tasks related to message routing? See Managing Message Routing.

Contents

Send Connectors

To route messages to external SMTP domains, you must configure at least one Send connector to relay messages to the Internet. You can configure a Send connector and define the address space as the asterisk (*) wildcard character. The * character indicates

that the Send connector can be used to relay messages to all external SMTP addresses. You can also configure Send connectors to relay messages to specific address spaces when Send connector restrictions, such as message size, vary for those external domains.

When you configure a Send connector, you must select at least one source server for that Send connector. The source servers are the transport servers associated with that connector to handle message delivery. The source server for a Send connector can be a Hub Transport server, an Edge Transport server, or an Edge server subscribed to an Active Directory site. You can configure more than one source server for a Send connector to provide load balancing and fault tolerance for the address spaces defined on that Send connector. However, each Exchange 2010 source transport server you specify must be in the same Active Directory site.

For more information about how to configure your Exchange organization to send and receive Internet e-mail, see Managing Message Routing.

When Exchange is processing a message sent to an external recipient, the routing component of the Microsoft Exchange Transport service must select the best Send connector through which to route the message, and then calculate the least cost routing path to reach that Send connector.

To learn more about Send connectors, see Understanding Send Connectors.

Return to top

Delivery Agent Connectors

Delivery Agent connectors are used to route messages addressed to messaging systems that don't use SMTP. When a message is routed to a Delivery Agent connector, the associated delivery agent performs the content conversion and message delivery. Delivery Agent connectors allow queue management for non-SMTP messages, thereby eliminating the need for storing messages on the file system in the Drop and Pickup directories. For more information, see Understanding Delivery Agents.

Return to top

Foreign Connectors

Foreign connectors are used to send messages to third-party messaging systems. Each Foreign connector uses a Drop directory configured on the source Hub Transport servers for receiving messages. The foreign gateway server must be configured to obtain messages from the Drop directory specified for that Foreign connector. For more information about Foreign connectors, see Understanding Foreign Connectors.

Return to top

Connector Considerations

Restrictions applied to the connectors may eliminate a specific connector from routing consideration. The following configuration options on connectors can determine whether those connectors are considered when making routing decisions. For more information about configuring connectors, see Managing Connectors.

Connector State

You can disable and enable any connector in your organization. If a connector is disabled, it's not considered when routing messages. For example, if an Exchange 2010 Send connector is disabled, messages aren't routed to that connector.

Note:
Exchange Server 2003 doesn't detect the disabled state of connectors. Therefore, if Exchange 2003 is deployed in the same organization, it may route to that connector.

Connector Scope

Routing only considers connectors in scope for the sending server. By default, no scope limitation is applied to connectors, and they are available to all Hub Transport servers in the organization. However, you can specify a local scope for a connector. If you configure a connector as scoped, the availability of that connector is limited to Hub Transport servers located in the same Active Directory site as the source servers for the connector. Scoped connectors aren't considered when routing by Hub Transport servers in other Active Directory sites.

Address Space

The address space for a connector specifies the following:

- Recipient domains to which this connector routes e-mail
- Address space type
- Cost assigned to the address space for that connector

When you create a Send connector, the address space type is always configured as SMTP by default. Even though you can also specify a non-SMTP address space for a Send connector, the messages are still sent using SMTP. If you need to use a different transport protocol for transmitting messages to their destination, you must use a Delivery Agent connector or a Foreign connector.

When the Microsoft Exchange Transport service selects a connector for routing, it only considers connectors that have a matching address space for the destination domain. You can use the wildcard character * in an address space to indicate all domains, all domains that have a particular top-level domain, such as *.com, or a second-level domain and all its subdomains, such as *.contoso.com. When you configure a connector for a particular domain, e-mail sent to that domain is always routed through that connector.

If more than one connector matches the address space for the destination recipient domain, the connector with the more precise address match is selected. For example, if Send connector C1 is configured to have the address space *.contoso.com and Send connector C2 is configured to have the address space northamerica.contoso.com, e-mail addressed to *user*@europe.subdomain.contoso.com is routed to Send connector C1 and e-mail addressed to *user*@northamerica.contoso.com is routed to Send connector C2. Even though the latter address matches the address spaces on both connectors, the address space of C2 is a better match.

Message Size Restrictions

A message size restriction on a connector may also remove that connector from consideration during routing path selection if the message being routed is larger than the size restriction configured on that Send connector.

Cost

Connector cost is used to set selection priority when more than one connector is configured for the same address space. During routing, when the connector selection is made, the lowest cost routing path to the destination is selected. By adjusting connector costs, you can control the preferred routing path for mail flow in your organization and to the Internet. When you create a connector, the default cost is set to 1.

Return to top

Selecting the Routing Path to an External Recipient

When a message is sent to an external recipient, Exchange 2010 will always select a single connector through which to send the message. The selected connector must meet the message size constraints. After Exchange 2010 has eliminated all connectors whose message size restrictions are less than the size of the message being routed, routing applies the following criteria to determine which connector it will select:

1. From the list of all the connectors configured in the Exchange organization, Exchange narrows the list to connectors that satisfy all the following criteria:
   - In the scope for the local server
   - Enabled
   - With an address space that matches the recipient's e-mail domain
2. From the resulting list, Exchange selects the connector with the most specific address space match.

If more than one connector meets the address space match criteria, Exchange 2010 routing evaluates the following criteria to select a connector:

1. **Connector cost** The cost of the connector is the sum of the cost assigned to all the IP site links between the source Active Directory site and the Active Directory site that contains the source servers for the connector, and the cost assigned to the connector. The connector with the lowest aggregate cost is selected. If more than one connector has the same cost, the selection process continues to the next step.
2. **Proximity** The source server that has the closest proximity to the routing server is selected. This means that the local server is chosen over another Hub Transport server in the same Active Directory site, and a server in the local Active Directory site is chosen over a source server in a remote Active Directory site. If more than one connector matches the criteria, the selection process continues to the next step.
3. **Alphanumerically lower connector name** If more than one routing path has the same cost and proximity, the connector with the name that has the lowest alphanumeric value is selected.

Routing Path Selection When Coexisting with Exchange 2003

In a coexistence scenario, the selection varies slightly depending on whether the source server for the selected connector is an Exchange 2010 or Exchange 2003 server.

If more than one connector meets the address space match criteria, and they are all are hosted on servers running Exchange 2003, the following selection method is used:

1. **Connector cost** The cost of the connector is the sum of the cost assigned to all the routing group connectors between the routing server and the routing group that contains the source servers for the connector and the cost assigned to the connector.
2. **Alphanumerically lower connector name** If more than one routing path has the same cost and proximity, the connector with the name that has the lowest alphanumeric value is selected.

If more than one connector meets the address space match criteria, and they are spread across Exchange 2010 and Exchange 2003, Exchange 2010 will always prefer Exchange 2010 connectors.

When a connector is selected, if there are legacy servers listed as source servers as well as Exchange 2010 servers, messages are routed to the Exchange 2010 servers. When all things are equal, Exchange 2010 will always route the messages to other Exchange 2010 servers.

After a connector is selected by using the previous criteria, there may be more than one routing path to reach the Active Directory site where the source server for the selected connector is located. In this case, the lowest cost routing path to the connector is calculated by using the logic used for intra-organizational routing. For more information, see Internal Message Routing.

Handling Messages That Can't Be Routed

If no connector satisfies all criteria required to select a connector according to the logic described earlier, one of the following actions occurs:

- If there is no matching connector for an SMTP address space, the recipient is marked as unreachable and the message is routed to the Unreachable queue.
- If the message size exceeds the connector size restriction for all connectors, a non-delivery report (NDR) is returned to the sender.
- If there is no matching connector for a non-SMTP address space, an NDR is returned to the sender.

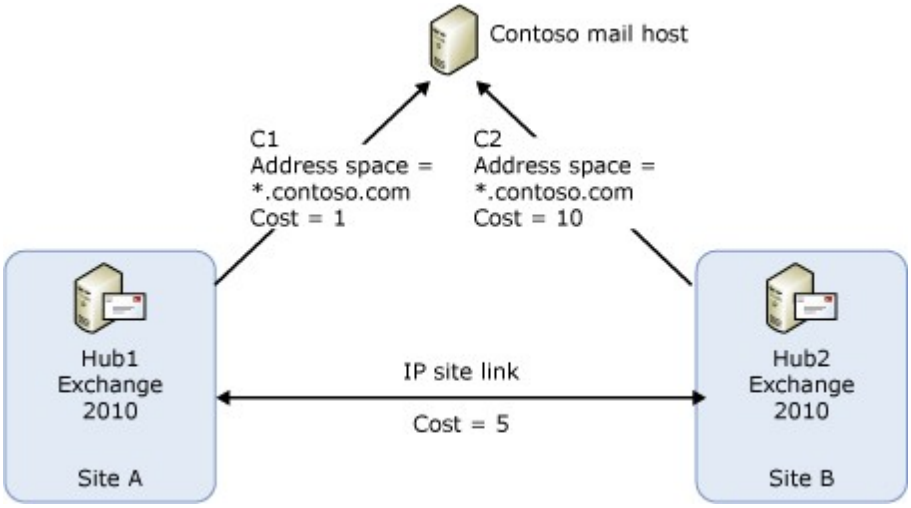
Return to top

Routing Examples

The following examples illustrate how messages are routed to external recipients.

Example 1: Selecting a Connector Based on Address Space Match

In this topology, a message is being routed from Active Directory Site A to the external recipient, john@subdomain.contoso.com. The following figure shows that two connectors can route messages to this address space.



The following table shows the configuration of two Send connectors in an Exchange 2010 topology.

Examples of Send connector configurations

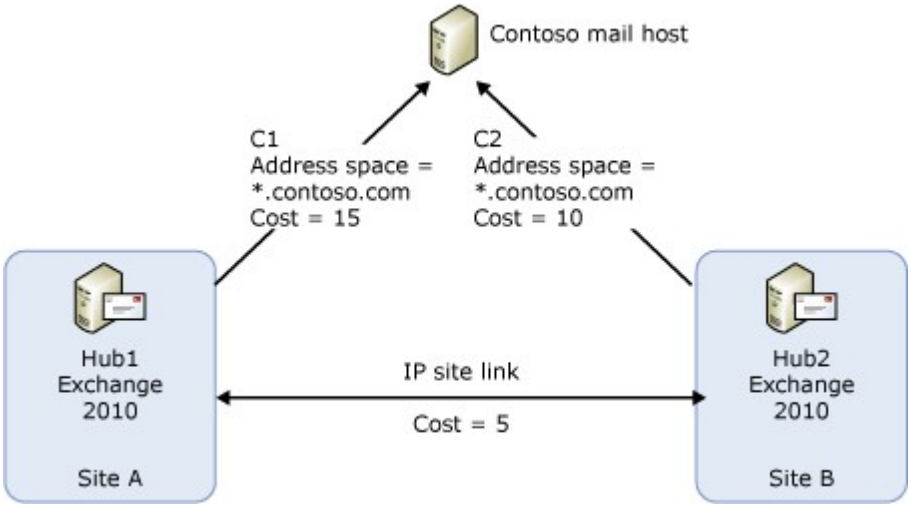
Send connector name	Address space	Connector cost	Source servers	Message size restrictions
C1	*.contoso.com	1	Hub Transport servers in Active Directory Site A	None
C2	subdomain.contoso.com	10	Hub Transport servers in Active Directory Site B	None

In this scenario, the message is routed by using C2 because the most specific address space match is chosen. C1 has a lower routing cost, and the source servers are located in

the same site as the Hub Transport server processing the message. However, the address space match takes priority over the other factors.

Example 2: Selecting a Connector Based on Proximity

In this scenario, a message is being routed by a Hub Transport server located in Active Directory Site A to the external recipient, john@subdomain.contoso.com, as shown in the following figure.



The following assumptions apply:

- The routing server isn't listed as a source server for any Send connector.
- The IP site link between Site A and Site B is assigned a cost of 5.
- Two Send connectors can route messages to the address space. The following table shows the connector configuration.

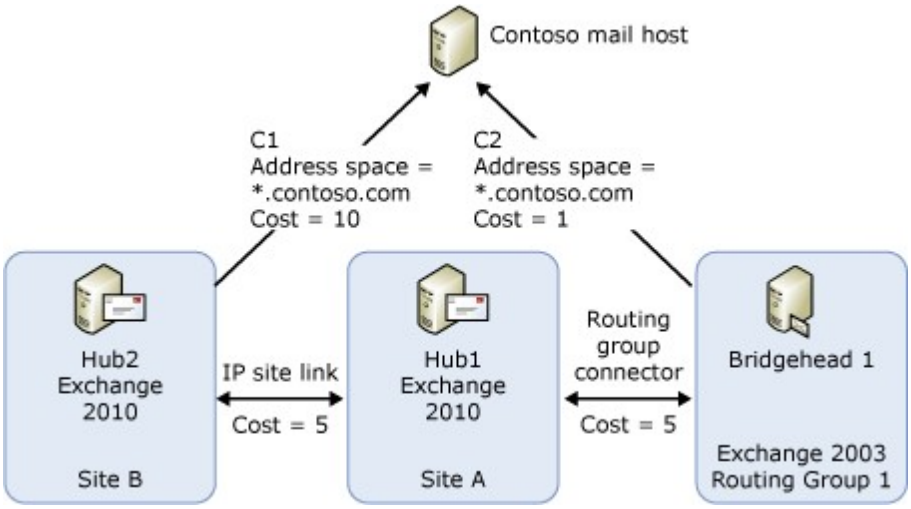
Alternative Send connector configuration

Send connector name	Address space	Address space cost	Source servers	Message size restrictions
C1	subdomain.contoso.com	15	Hub Transport servers in Active Directory Site A	None
C2	subdomain.contoso.com	10	Hub Transport servers in Active Directory Site B	None

Because both connectors have the same address space match, the connector cost is evaluated next. The cost assigned to connector C2 is added to the cost of the IP site link between Active Directory Site A and Site B, for a combined cost of 15. The source servers for connector C1 are located in the local Active Directory site. Therefore, the IP site link cost to reach the connector is 0, for a total cost of 15. In this scenario, both connectors match the address space equally and have an equal cost. Routing selects connector C1 because it has a closer proximity.

Example 3: Selecting a Connector Based on Exchange Version

In the next example, a message is being relayed from Active Directory Site A to the external recipient, john@contoso.com, as shown in the following figure.



The following assumptions apply:

- There are two Send connectors that match the destination address space equally.
- The source servers for the routing group connector between Exchange 2003 and Exchange 2010 are located in Site A.
- The routing group connector has a routing cost of 5.
- The IP site link between Site A and Site B is assigned a cost of 5.
- The source server for one of the Send connectors is an Exchange 2003 server located in routing group 1. The following table shows the connector configuration.

Connectors configured on different versions of Exchange

Connector name	Address space	Address space cost	Source servers	Message size restrictions
C1	*.contoso.com	10	Hub Transport servers in Active Directory Site B	None
C2	*.contoso.com	1	Exchange 2003 bridgehead servers in routing group 1	None

In this scenario, the aggregate cost of using connector C1 is 15, which is the sum of the IP site link cost and the Send connector cost. The aggregate cost of using connector C2 is 6, which is the sum of the routing group connector cost and the Send connector cost. However, even though C1 has a lower routing cost, Exchange will still route the message to the Exchange 2010 connector.

Return to top

1.7.1.22.2 Message Rerouting and the Unreachable Queue

Message Rerouting and the Unreachable Queue

Transport > Understanding Transport > Understanding Message Routing >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

In Microsoft Exchange Server 2010, there are message routing scenarios where a message that isn't delivered is put in the Unreachable queue or rerouted.

The decision to put a message in the Unreachable queue is made during the routing phase of categorization. If a routing path can't be calculated for a message during the routing phase, the message is sent to the Unreachable queue.

The decision to reroute a message occurs during the message delivery phase in the SMTP Send connector process. If there are configuration changes that require a message in the queue to be resubmitted, the message is resubmitted for categorization in the message delivery phase and rerouted with the new configuration information. Depending on the type of configuration change, some or all resubmitted messages may be sent to the Unreachable queue or to a different delivery queue.

For more information about how the least-cost routing path is computed, see Understanding Message Routing. For more information about how the categorizer works, see Understanding Transport Pipeline.

Looking for management tasks related to message routing? See Managing Message Routing.

Message Rerouting

There are two types of message delivery in Exchange:

- *Local delivery* refers to delivery of messages sent to a recipient with a mailbox in the same Active Directory site as the Hub Transport server on which categorization occurred.
- *Remote delivery* refers to delivery of messages to recipients in other Active Directory sites of the Exchange organization and to external recipients. Remote delivery queues are the main focus of message rerouting. Remote delivery can be affected by configuration changes in various ways.

The routing component of the categorizer tries to detect whether messages in a queue must be rerouted during enhanced Domain Name System (DNS) resolution. During enhanced DNS resolution, routing tries to detect if a queue has to be rerouted. In this phase, the **NextHopSolutionKey** attribute is resolved to a list of targets. This enables routing to automatically detect any configuration changes that invalidate or modify the **NextHopSolutionKey** attribute. If routing detects that configuration changes require rerouting of messages in a queue, the messages in the affected queue are resubmitted to the categorizer and the least cost path is recalculated, taking the new configuration changes into account.

The store driver, which delivers inbound messages to the Exchange databases, may also reroute messages. It resubmits a message for rerouting if either of the following conditions is true:

- The message is in a MAPI delivery queue, and the next hop has been selected, but the message hasn't been delivered.
- The destination mailbox is moved to another Mailbox server.

If a Mailbox server is unavailable when the store driver tries to deliver the messages to that Mailbox server, the store driver puts the message queue in a retry state. If continued attempts to contact the Mailbox server are unsuccessful, when the retry interval expires, all messages in the queue are resubmitted to the categorizer.

If a message is located in a non-SMTP gateway delivery queue (a queue being routed to a

Delivery Agent connector or a Foreign connector), the foreign gateway connection handler determines whether the configuration change requires rerouting. The foreign gateway connection handler is a component of the Microsoft Exchange Transport service that manages delivery of messages to Delivery Agent connector queues and Foreign connector Drop directories. For example, deleting or disabling a Foreign connector requires rerouting messages to another connector.

The following list summarizes the types of configuration changes that affect message routing. Each configuration change is discussed in detail later in this topic:

- **Invalid next hop** The next hop for the message has been deleted or modified, therefore invalidating the previously calculated routing path. The next hop for a message may be an Active Directory site, a connector, or a transport server (either a Hub Transport server or Edge Transport server).
- **Changes to next hop** The configuration of the next hop has changed in a way that affects connectivity. For example, changes to the list of Hub Transport servers in the remote Active Directory site cause the next hop connection to be modified.
- **Less preferred routing paths** When configuration changes occur along a previously computed routing path, messages already routed are delivered if the routing path is reachable. But new messages are rerouted with the updated configuration changes.
- **Unavailable next hop** Network connectivity or target server availability cause the next hop to be unavailable for connectivity. However, the next hop doesn't change. An example is when the Hub Transport servers in an Active Directory site are offline.
- **Additional scenarios where rerouting occurs** In some cases, configuration changes may be caused when DNS MX resource record resolution fails for a DNS connector or a smart host connector.
- **Configuration changes that cause message rerouting or delay** When specific configuration changes are detected during the message delivery phase, routing actions occur, and messages are rerouted or delivery is delayed.

Invalid Next Hop

Configuration changes can invalidate a previously calculated next hop. In these circumstances, the routing component of the categorizer can detect the configuration change and reroute to compensate for that change.

Delivery to an SMTP Connector on the Local Computer

When a message is being delivered to an SMTP connector on the local computer, the server that received the message for relay to its destination is also the source server for the Send connector through which the message is routed. This kind of delivery occurs when either of the following conditions is true:

- The message was received on a linked Receive connector.
- The recipient has an external address, and a source server for the selected connector is the local computer.

If the Send connector selected by the routing component of the categorizer is deleted or disabled, the configuration change is detected during the message delivery phase. This causes all messages in the queue to be categorized again.

If the configuration of the Send connector is changed to remove the local server as a source server of the connector, the configuration change is detected during the message delivery phase, and all messages in the queue are categorized again.

A change of the address resolution method of the Send connector causes the queue to be rerouted. A Send connector can be configured to use DNS to resolve MX records and route messages automatically or it can be configured to route all messages through one or

more smart hosts. If you change the address resolution of a Send connector, the messages routed through that Send connector are rerouted.

SMTP Relay in an Active Directory Site

SMTP message relay in an Active Directory site occurs in the following scenarios:

- The recipient has an external address, and at least one of the source servers for the Send connector is an Exchange 2010 Hub Transport server located in the local Active Directory site.
- The recipient has an external address, and at least one of the source servers for the Send connector is an Exchange 2010 Edge Transport server subscribed to the local Active Directory site.
- The recipient's mailbox is located on a server that runs Exchange Server 2007 in the local Active Directory site.
- The recipient's mailbox is located on a server that runs Exchange Server 2003, and at least one of the source servers for the selected routing group connector is an Exchange 2010 Hub Transport server in the local Active Directory site.
- The recipient is a distribution group, and the expansion server for the group is an Exchange 2010 Hub Transport server in the local Active Directory site.

In the first four scenarios, if the Send connector is deleted or disabled, the configuration change is detected during the message delivery phase, and the queue is resubmitted.

In the last scenario, the messages are queued for delivery to an expansion server and the **NextHopSolutionKey** attribute contains the fully qualified domain name (FQDN) of the expansion server for the distribution group. If the Hub Transport server role is uninstalled from the specified expansion server, that configuration change is detected during the message delivery phase, and the queue is resubmitted.

SMTP Relay to a Remote Active Directory Site

When a message is being delivered to a remote Active Directory site, the next hop is a different Active Directory site than the Hub Transport server processing the message. This kind of delivery occurs in the following scenarios:

- The recipient is a resolved user, mailbox database, or public folder, and the destination computer is an Exchange 2010 server in a remote Active Directory site.
- The recipient is an external address, and the source servers of the Send connector selected for that address are Exchange 2010 servers in a remote Active Directory site.
- The recipient is an external address, and the source servers of the Foreign connector selected by the routing component of the categorizer are Exchange 2010 servers in a remote Active Directory site.
- The recipient is a distribution group, and the expansion server is an Exchange 2010 Hub Transport server in a remote Active Directory site.
- The recipient's mailbox is located on an Exchange 2003 server, and the closest Hub Transport server listed as a source server for the selected routing group connector is located in a remote Active Directory site.

In these scenarios, if the remote Active Directory site is deleted, the configuration change is detected during the message delivery phase, and the queue is resubmitted.

SMTP Relay to an Exchange 2003 Server

When a message is being delivered to an Exchange 2003 server, the Exchange 2010 Hub Transport server relays the message through a routing group connector to an Exchange 2003 server. This delivery type occurs in the following scenarios:

- The recipient is a resolved user, mailbox database, or public folder located on an Exchange 2003 server.
- The recipient is an external address, and the source servers for the SMTP connector selected for that address are Exchange 2003 servers.

- The recipient is an external address, and the source servers for the selected Foreign connector for that address are Exchange 2003 servers.
- The recipient is a distribution group, and the designated expansion server is an Exchange 2003 server.

In these scenarios, if the routing group connector is deleted, the configuration change is detected during the message delivery phase, and the queue is resubmitted.

Changes to Next Hop

In some scenarios, the next hop isn't invalidated. However, it's modified in a way that affects the connection to a next hop target. Such configuration changes are automatically detected during the message delivery phase, and messages are delivered to the new targets.

The following types of changes cause an update of the list of next hop targets:

- Changes to the target server list of a routing group connector.
- Changes to the list of Hub Transport servers in the remote Active Directory site.
- Changes to the list of Hub Transport servers or Edge Transport servers in the local Active Directory site.
- The introduction of hub sites along a previously calculated routing path. When this change is detected during the message delivery phase, the IP address list returned to the resolve request is adjusted so that the message is sent to the hub site.

Less Preferred Routing Paths

If a configuration change causes the previously calculated routing path to become less preferred or removes the routing path from consideration, the routing path is still reachable and the messages can still be delivered along the previously calculated routing path. The following configuration changes are in this category:

- Message size restrictions are added along the routing path. This causes messages that exceed the size limit to be routed along a different routing path.
- A routing path with better cost or proximity is created.
- The address space of the connector changes.
- Other connector-related changes occur, such as the enabling of a connector or modification of the scope for a connector. For example, if a connector whose scope is changed from global to scoped is in the local Active Directory site, the change has no effect. If the connector is in a remote Active Directory site, the change isn't detected during the message delivery phase because the messages are queued to the remote Active Directory site instead of to the connector.
- As the routing path tries to SMTP-relay to a Mailbox server in the remote Active Directory site, the Mailbox server moves from a remote Active Directory site to a local Active Directory site.
- The routing path is trying to reach the expansion server for a distribution group when it's no longer an expansion server.

In these scenarios, existing messages are delivered along the already calculated routing path. Because the routing path exists and is reachable, messages already routed are unaffected by these configuration changes. However, newly submitted messages are routed by using the updated configuration.

Unavailable Next Hop

In this scenario, a configuration change or network connectivity change doesn't invalidate the next hop to which messages are routed but a configuration change or network connectivity change makes the next hop unavailable. This means that an SMTP connection can't be established to the next hop target for some reason. Possible reasons are as follows:

- An attempt is made to establish an SMTP connection with a currently offline Hub Transport server in the local site.
- A remote Active Directory site has unavailable or offline Hub Transport servers.
- A remote routing group has unavailable or offline Exchange 2003 bridgehead servers.
- Remote domains are unavailable because of network connectivity issues.

Message delivery failures caused by network connectivity problems aren't detected by the routing component of the categorizer. When an SMTP connection can't be established to the next hop target, the SMTP Send connector retries the queue. The *MaxIdleTimeBeforeResubmit* parameter, which is located in the EdgeTransport.exe.config file, has a default value of 12 hours. After the configurable retry interval (*MaxIdleTimeBeforeResubmit*) has expired without successfully establishing a connection, all messages from the delivery queue are resubmitted to the Submission queue. If the connectivity problem still exists, this process is repeated. If the connectivity problem is resolved, messages are delivered as soon as message retry is successful. Or, a configuration change that modifies the next hop destination may resolve the problem. For example, if the problem is caused by all the Hub Transport servers in a destination site being offline, and you move mailboxes to a server in a different site, the next hop would change to the new site.

Note:

The automatic resubmission from the message delivery queue to the Submission queue only happens for queues that aren't connector queues. Connector queues remain in retry mode until the problem is fixed, or the messages expire and a non-delivery report (NDR) is sent.

Additional Scenarios Where Rerouting Occurs

In addition to the scenarios described earlier in this section, the following scenarios cause messages to be rerouted during the message delivery phase:

- DNS MX resolution fails for a DNS connector. If the DNS MX resolution fails because the authoritative host for the MX record wasn't found, an NDR for the messages in the queue is sent immediately. If other types of failures exist, the queue is put into retry mode until a connection is established or the messages expire.
- DNS MX resolution fails for a smart host connector. The queue is put into retry mode until the messages expire.

Configuration Changes That Cause Message Rerouting or Delay

The following table summarizes the routing actions taken when specific configuration changes are detected during the message delivery phase, and messages are rerouted or delivery is delayed.

Configuration changes that cause message rerouting and delay

Routing scenario	Configuration change and routing action	
Message is routed to a DNS connector configured on the local server.	**Configuration change**	**Routing action**
	The connector is deleted.	The queue is resubmitted.
	The connector is changed to a smart host connector.	The queue is resubmitted.
	The connector is modified to remove the local server from the source server list.	The queue is resubmitted.

	A fatal DNS MX resolution failure occurs.	An NDR is sent.
	A DNS MX resolution failure that isn't fatal occurs.	The queue is retried until messages expire.
	The connector is disabled.	The queue is resubmitted.
Message is routed to a smart host connector configured on the local server.	**Configuration change**	**Routing action**
	The connector is deleted.	The queue is resubmitted.
	The connector is modified to remove the local server from the source server list.	The queue is resubmitted.
	The connector is changed to a DNS connector.	The queue is resubmitted.
	The smart host list for the connector is modified.	The updated smart hosts list is automatically detected and used during the message delivery phase.
	Any DNS MX resolution failure occurs.	The queue is retried until messages expire.
	The connector is disabled.	The queue is resubmitted.
	The SMTP server is offline or the destination isn't running an SMTP server.	The queue is retried until messages expire.
Message is routed to a connector with a source Hub Transport server or Edge Transport server in the local Active Directory site.	**Configuration change**	**Routing action**
	The connector is deleted.	The queue is resubmitted.
	The source server list for the connector is modified to remove or add Hub Transport or Edge Transport servers in the local Active Directory site.	Changes to source servers in the local site are automatically detected and used during the message delivery phase.
	The source server list for the connector is modified to remove all	The queue is resubmitted.

	Hub Transport or Edge Transport servers in the local Active Directory site.	
Message is routed to an expansion server for a distribution group in the local Active Directory site.	**Configuration change**	**Routing action**
	The server is no longer configured for the Hub Transport server role.	The queue is resubmitted.
Message is routed to a transport server in the local Active Directory site.	**Configuration change**	**Routing action**
	The server is offline or the Microsoft Exchange Transport service isn't running.	The queue is resubmitted after an interval.
Message is routed to a remote Active Directory site.	**Configuration change**	**Routing action**
	The remote Active Directory site is deleted.	The queue is resubmitted.
	The link to the remote Active Directory site is deleted. Therefore, the site is unreachable from the local site.	The queue is resubmitted.
	The list of Hub Transport servers in the remote Active Directory site changes.	Changes are automatically detected and used during the message delivery phase.
	All Hub Transport servers in the remote Active Directory site are removed.	The queue is resubmitted.
	Hub sites are introduced along the routing path of the destination Active Directory site.	Changes are automatically detected and used during the message delivery phase so that the messages are relayed to the hub site.
	All Hub Transport servers in the remote Active Directory site are offline.	The queue is resubmitted after an interval.
	The remote site is the delayed fan-out point, and all Hub Transport	The queue is resubmitted after an interval.

<table>
<tr><td></td><td><table><tr><td>servers in the site are offline.</td><td></td></tr></table></td></tr>
<tr><td>The message is routed to an Exchange 2003 server in a remote routing group.</td><td><table>
<tr><th>Configuration change</th><th>Routing action</th></tr>
<tr><td>The connector is deleted.</td><td>The queue is resubmitted.</td></tr>
<tr><td>The source Hub Transport server list for the connector changes to remove the local server from the list.</td><td>The queue is resubmitted.</td></tr>
<tr><td>The target bridgehead server list for the connector is changed by removing or adding bridgehead servers in the remote routing group.</td><td>Changes are automatically detected and used during the message delivery phase.</td></tr>
<tr><td>All Exchange 2003 bridgehead servers in the remote routing groups are offline.</td><td>The queue is retried until messages expire.</td></tr>
</table></td></tr>
<tr><td>The message is routed to a destination, and there are configuration changes, but the destination is still reachable.</td><td><table>
<tr><th>Configuration change</th><th>Routing action</th></tr>
<tr><td>The routing path becomes less preferred because a new routing path appears with a reduced cost or closer proximity, or both.</td><td>Changes are automatically detected and used during the message delivery phase.</td></tr>
<tr><td>The routing path is removed for a message because maximum message size restrictions are added along the path.</td><td>Changes are automatically detected and used during the message delivery phase.</td></tr>
<tr><td>A previously disabled routing path comes into consideration with a reduced cost because the connector is enabled, put back in scope, or has no message size restrictions.</td><td>Changes are automatically detected and used during the message delivery phase.</td></tr>
<tr><td>The connector address space changes.</td><td>Changes are automatically detected and used</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>during the message delivery phase.</td></tr>
<tr><td>The connector is changed to add local Hub Transport or Edge Transport servers to the source server list.</td><td>Changes are automatically detected and used during the message delivery phase.</td></tr>
<tr><td>The message is relayed to a Mailbox server in the remote Active Directory site, while the Mailbox server housing the destination mailbox database is moved to a different site.</td><td>Changes are automatically detected and used during the message delivery phase.</td></tr>
<tr><td>The message is relayed to a distribution group expansion server when it's no longer an expansion server. (The distribution group's HomeMTA attribute is modified.)</td><td>Changes are automatically detected and used during the message delivery phase.</td></tr>
</table>
</td></tr>
<tr><td>The message is routed by using MAPI delivery to a Mailbox server.</td><td>
<table>
<tr><th>Configuration change</th><th>Routing action</th></tr>
<tr><td>The mailbox moves to a different Mailbox server.</td><td>The store driver detects the change and resubmits the messages.</td></tr>
<tr><td>The Mailbox server is offline.</td><td>The queue is retried and resubmitted after an interval.</td></tr>
</table>
</td></tr>
<tr><td>The message is routed by using a non-SMTP gateway to a non-SMTP connector configured on the local server.</td><td>
<table>
<tr><th>Configuration change</th><th>Routing action</th></tr>
<tr><td>A Foreign connector is deleted.</td><td>The queue is resubmitted.</td></tr>
<tr><td>A Foreign connector is modified to remove the local server from the source server list.</td><td>The queue is resubmitted.</td></tr>
<tr><td>The connector is disabled.</td><td>The queue is resubmitted.</td></tr>
<tr><td>The Drop directory isn't found.</td><td>The queue is retried until messages expire.</td></tr>
</table>
</td></tr>
</table>

Unreachable Queue

The Unreachable queue contains messages that can't be routed to their destinations. Typically, an unreachable destination is caused by misspelled e-mail addresses, or configuration changes that have modified the routing path for delivery. Regardless of destination, all messages that have unreachable recipients reside in this queue.

The decision to put a message in the Unreachable queue is made during the routing phase of categorization. If a routing path can't be calculated for a message during the routing phase, the message is sent to the Unreachable queue. Messages in the Unreachable queue are rerouted after configuration changes are processed. There is only one Unreachable queue for each Exchange 2010 transport server.

During categorization, messages are put in the Unreachable queue when the following conditions are true:

- The recipient is a valid Active Directory recipient object. However, a routing path can't be calculated for that recipient.
- The recipient is an external SMTP address and a matching connector can't be found for the address space. A matching connector may also be ignored by the routing component of the categorizer because it's disabled or configured incorrectly.
- The recipient is a distribution group. The expansion server for the distribution group is invalid or doesn't have the Hub Transport server role installed.
- The recipient is an SMTP address recipient of a message received on a Receive connector linked to a Send connector that's ignored by the routing component of the categorizer because it's disabled or configured incorrectly in some way.

In the following scenarios, messages aren't put in the Unreachable queue, and NDRs are sent instead:

- The routing path can't be calculated for a recipient because constraints, such as message size restrictions, prevent delivery of the message using the single, deterministic route calculated by the categorizer.
- The recipient is a non-SMTP address and a matching connector can't be found. Or the matching connector is disabled or configured incorrectly.
- The recipient is a non-SMTP address recipient received on a Receive connector linked to a Send connector that's ignored by the routing component of the categorizer because the Send connector is disabled or configured incorrectly.

Messages in the Unreachable queue are resubmitted to the categorizer when the routing tables are rebuilt because of configuration changes. The old routing tables and new routing tables are compared. The Unreachable queue is resubmitted only if the old routing tables and new routing tables aren't the same.

Scenarios Where Messages Are Put in the Unreachable Queue

This section describes some scenarios where messages are put in the Unreachable queue.

Routing group connector between an Exchange 2010 organization and Exchange 2003 organization doesn't exist

A routing group connector between the Exchange 2010 routing group and Exchange 2003 routing groups hasn't been configured, or the last routing group connector between the Exchange 2010 routing group and Exchange 2003 routing groups has been removed. No routing group connector exists to provide a routing path to the Exchange 2003 recipients. To resolve this problem, first verify that the routing group connector is missing. If that's the case, you can create a routing group connector. For more information, see Create Additional Routing Group Connectors from Exchange 2010 to Exchange 2003. If a routing group connector does exist, the message is in the Unreachable queue for some other reason. Check the configuration of the routing group connector.

Destination Active Directory site doesn't have Hub Transport servers

The destination Active Directory site has no Hub Transport servers. In this scenario, messages to recipients in that site are sent to the Unreachable queue. To resolve this problem, deploy a Hub Transport server in the Active Directory site. For more information, see Overview of the Hub Transport Server Role.

Active Directory site link doesn't exist between two Active Directory sites

An Active Directory site link has been removed and as a result, a disconnected Active Directory site contains Exchange 2010 servers. To resolve this problem, create an Active Directory site link by using Active Directory Sites and Services.

Other issues

When a message is put in the Unreachable queue, the last error message specifies why the message was placed in the Unreachable queue. If more than one recipient of the same message is routed to the Unreachable queue, but for different reasons, the last error available on each recipient specifies the reason for each. When inconsistencies are found during routing table computation, events are logged in the Application log of Windows Event Viewer. The last error message and these events can help you determine the configuration error and make corrections so that messages in the Unreachable queue can be routed successfully.

You can also manually force the messages in queues to be resubmitted. For more information, see Resubmit Messages in Queues.

1.7.1.22.3 Internal Message Routing

Internal Message Routing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

Internal message delivery involves a routing process that relays e-mail in the following ways:

- From a server running Microsoft Exchange Server 2010 that has the Hub Transport server role installed to an Exchange Server 2007 or Exchange 2010 Hub Transport server in a different Active Directory site
- From an Exchange 2010 Hub Transport server to an Exchange 2010 Mailbox server located in the same Active Directory site
- From an Exchange 2010 Hub Transport server to a Hub Transport server running Exchange 2007 for delivery to a recipient mailbox located on an Exchange 2007 server
- From an Exchange 2010 Hub Transport server to a server running Exchange Server 2003 for delivery to a recipient mailbox located on an Exchange 2003 server
- From an Exchange 2010 Hub Transport server to an Exchange 2010 Mailbox server for delivery to a mail-enabled public folder

For more information about how Exchange makes routing decisions, see Understanding Message Routing.

Looking for management tasks related to message routing? See Managing Message Routing.

Contents

Routing Messages for Delivery to Exchange 2003 Servers

Routing to Public Folders

Routing Messages for Delivery to Exchange 2010 Servers

In Exchange 2010, after a message is received by the Hub Transport server, the message is added to the Submission queue. Messages move from the Submission queue through the categorizer. When the message is categorized, a recipient's e-mail address is resolved to an object in Active Directory. This query determines the mailbox associated with that e-mail address and which Mailbox server is hosting that mailbox.

After information about the recipient is resolved, the next step is resolving the Mailbox server to an Active Directory site. This Active Directory site information is stamped on the message as the **NextHopSolutionKey** attribute. The enhanced DNS component of the Microsoft Exchange Transport service accesses the topology information to determine which Hub Transport servers are located in the same site as the destination Mailbox server. A list of Hub Transport servers in the Active Directory site is then referenced to determine where to route the message. If the destination Mailbox server is located in the same site as the querying Hub Transport server, that Hub Transport server queues the message for local delivery. If the destination Mailbox server is located in a different site, the local Hub Transport server queues the message for remote delivery to that Active Directory site.

A message queued for local delivery is submitted to the destination mailbox store by the store driver. The message is transferred from the Hub Transport server to the Mailbox server by using an Exchange remote procedure call (RPC).

A message queued for delivery to a remote Active Directory site is transferred by using SMTP. Before the message is relayed, the routing component of the categorizer selects the least cost routing path. The method for determining the least-cost routing path is explained in detail in "Determining the Least-Cost Routing Path" in Understanding Message Routing.

Return to top

Routing Messages for Delivery to Exchange 2007 Servers

Due to the changes made to the Exchange Server Object (XSO) model in Exchange 2010, Exchange 2010 Hub Transport servers can't pick up messages from and deliver messages to Exchange 2007 Mailbox servers. Similarly, Exchange 2007 Hub Transport servers can't communicate with Exchange 2010 Mailbox servers. As a result, to have both Exchange 2010 and Exchange 2007 in the same Active Directory site, you must maintain both versions of Hub Transport servers in that site.

When a Hub Transport server queries Active Directory to determine the Mailbox server hosting the destination mailbox, it also retrieves the version of the Mailbox server. If the Mailbox server is an Exchange 2007 server that's in the same site as the Hub Transport server, the Hub Transport server will relay the message to an Exchange 2007 Hub Transport server in the same Active Directory site. The process of using the version information to make routing decisions is called *versioned routing* and is explained in detail in Upgrade from Exchange 2007 Transport.

If the Mailbox server is in a different Active Directory site, the message is queued for delivery to that remote site and is transferred by using SMTP.

Return to top

Routing Messages for Delivery to Exchange 2003 Servers

The routing topology and components of Exchange 2010 differ significantly from those of Exchange 2003 but generally correlate in the following ways:

- The Active Directory site in Exchange 2010 correlates to routing groups in Exchange 2003.
- IP site links in Exchange 2010 correlate to the concept of routing group connectors in Exchange 2003.
- The functionality of the Hub Transport server role in Exchange 2010 correlates to the functionality of a dedicated bridgehead server in Exchange 2003.

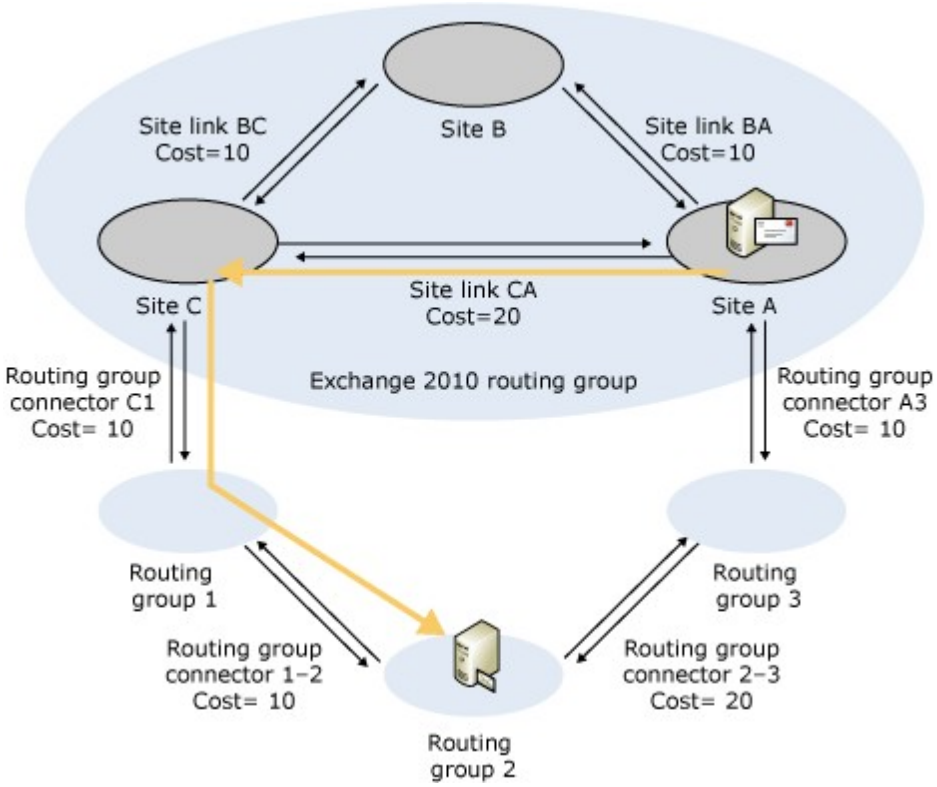
However, each Exchange version differs in the method used to determine routing paths. For more information about the routing differences, see Upgrade from Exchange 2003 Transport.

A message relayed from a Hub Transport server to an Exchange 2003 server for delivery to a recipient mailbox located on an Exchange 2003 server must be relayed across a routing group connector. All Exchange 2010 servers are associated with a single routing group named Exchange Routing Group (DWBGZMFD01QNBJR) for the purposes of routing to earlier versions of Exchange when Exchange 2010 coexists in the same organization with Exchange 2003. Placement of Exchange 2010 and earlier versions of Exchange in the same routing group isn't supported. Therefore, at least one routing group connector will always separate Exchange 2010 servers from Exchange 2003 servers.

When an Exchange 2010 Hub Transport server determines the least-cost routing path to an Exchange 2003 server, the routing component of the Microsoft Exchange Transport service uses the following algorithm to select the least-cost routing path to a computer running Exchange 2003:

1. Examine all possible routing paths across routing group connectors and select the routing path that has the least total cost.
2. If more than one routing path has the same cost, examine all possible routing paths across IP site links to reach the first routing group connector and select the routing path that has the lowest total IP site link cost.
3. If more than one routing path has the same routing group cost and has the same IP site link cost, select the routing path that includes the least number of hops.
4. If more than one routing path has the same routing group cost, the same IP site link cost, and the same number of hops, select the routing path where the name of the last Active Directory site before the destination site has the lowest alphanumeric value.

The following figure shows an example of a routing topology where Exchange 2010 and Exchange 2003 coexist.

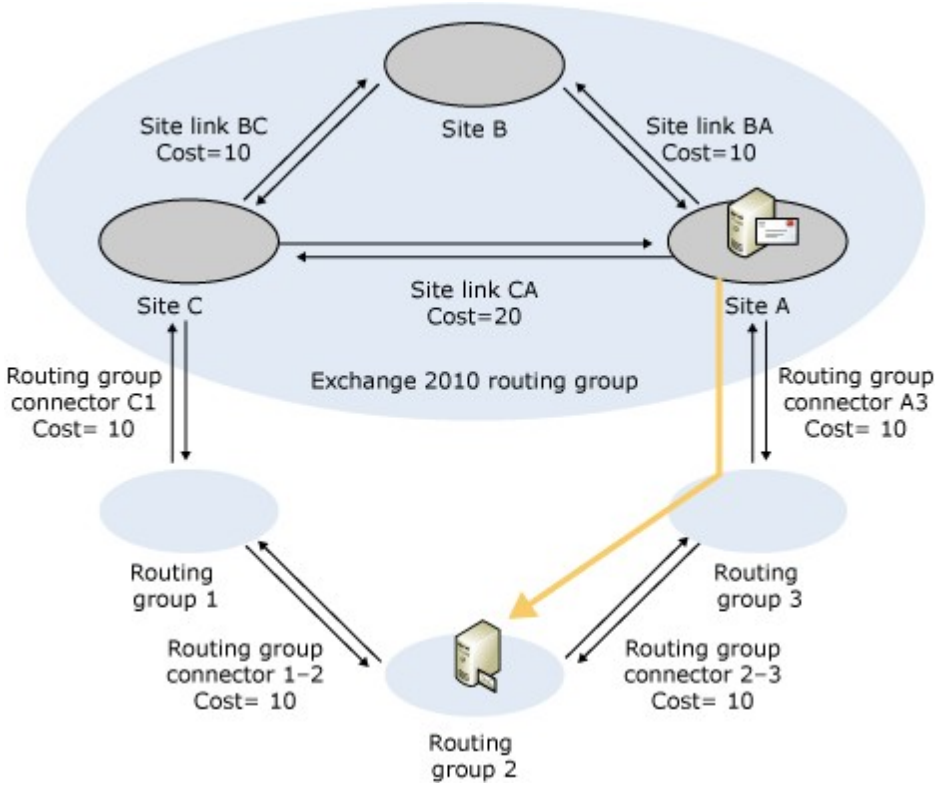


In this example, a message is being routed from a Hub Transport server in Site A to an Exchange 2003 server located in routing group 2. Two possible routing paths exist to reach routing group 2:

- Option 1: From routing group connector A3 at a cost of 10, to routing group connector 2-3 at a cost of 20. This routing path has a total cost of 30.
- Option 2: From routing group connector C1 at a cost of 10, to routing group connector 1-2 at a cost of 10. This routing path has a total cost of 20.

In this example, Option 2 has a lower total routing group connector cost, and the message is routed from the Hub Transport server in Site A, to a Hub Transport server in Site C where it's queued for delivery by using routing group connector C1.

The previous example shows how the routing decisions may not result in optimal routing due to the assigned costs on the routing group connectors. To maintain optimal routing, you may need to modify the routing group connector costs you have in your organization. The following figure shows the same topology, but with the cost of routing group connector 2-3 changed to 10.



Again, two possible routing paths are available to reach routing group 2:

- Option 1: From routing group connector A3 at a cost of 10, to routing group connector 2-3 at a cost of 10. This routing path has a total cost of 20.
- Option 2: From routing group connector C1 at a cost of 10, to routing group connector 1-2 at a cost of 10. This routing path has a total cost of 20.

In this scenario, both options have the same total routing group connector cost. Routing next evaluates the cost of the IP site links that must be crossed to reach the first routing group connector. From Site A, the IP site link cost to reach routing group connector A3 is zero, and the cost to reach routing group connector C1 is 20. Therefore, the routing path described in Option 1 is selected.

Return to top

Routing to Public Folders

Public folders can be mail-enabled in Exchange. Users can send messages to mail-enabled public folders just like any other recipient. When a Hub Transport server receives a message sent to a mail-enabled public folder, the following routing process applies:

1. The categorizer must determine which public folder hierarchy in which the public folder resides.
2. The categorizer looks up the **homeMDB** attribute for the public folder. The **homeMDB** attribute identifies the public folder hierarchy where the destination public folder is located.
3. Based on the routing table calculations performed by the Microsoft Exchange Transport service, and described in "Selecting the Destination Public Folder Database" later in this topic, the preferred public folder database is used to determine which public folder hierarchy contains a replica of the destination public folder.
   If the preferred public folder database is located in the same Active Directory

site as the routing Hub Transport server, message processing proceeds as described in step 4 in this section.
If the preferred public folder database is located in a remote Active Directory site, the message is relayed to that site by using the least cost routing path. The message categorization process described in step 1 and step 2 earlier in this section are repeated by the Hub Transport server that receives the message in the remote site.
If the preferred public folder database is located on an Exchange 2007 or Exchange 2003 server, the message is relayed to the Exchange 2007 Hub Transport server or the Exchange 2003 bridgehead server, and message delivery is determined by the earlier version of Exchange.

4. The Hub Transport server establishes a connection to the store driver on the Mailbox server that contains the preferred public folder database. The public folder database is queried to determine whether content for the public folder is available. The identity of the destination folder is referenced by the **legacyExchangeDN** attribute, and content availability is determined by the value of the **IsContentAvailable** attribute. The store driver either accepts the message for delivery, or if the folder contents aren't available locally, the store driver responds with a list of alternative servers that contain a replica of that public folder.
   The behavior of returning an alternative list of servers is known as *store override*. The alternative list of servers that contain the public folder replica is listed in the same order provided in client folder referrals, and the top entry is chosen by transport. This referral is provided to routing as the destination to which the message should be routed. For more information about client folder referrals, see Configure Public Folder Referrals.
5. If store override occurs, the Hub Transport server uses the routing table to determine the least cost routing path to the server that contains the preferred public folder replica and routes the message to that destination.
6. The message is delivered to the public folder store.

Selecting the Destination Public Folder Database

Public folders are stored in databases created on Mailbox servers. For efficiency and fault tolerance, you can replicate the content in your public folders to multiple Mailbox servers. Public folder content exists only in Exchange databases configured to have a replica of a specific folder, whereas the hierarchy is replicated to all public folder databases. Content and hierarchy information are replicated separately.

Public folder hierarchies are retrieved when routing tables are calculated. The top-level hierarchy object has a list of all the public folder databases to which that hierarchy is replicated. This list of public folder databases is stored as the **msExchOwningPFTreeBL** attribute in Active Directory. The **msExchOwningPFTreeBL** attribute always lists the most recently added public folder databases at the top of the list.

In Exchange 2010, the preferred public folder hierarchy database is selected by using the following criteria:

1. **Ranking by the age of the public folder database** By default, public folder databases that have an age threshold of less than two days aren't considered unless the age of all public folder databases is less than the threshold or the age is unknown.
2. **Proximity** Thelocal server is preferred. If the local server doesn't contain a replica of the public folder database, a server in the same Active Directory site is preferred. If the local Active Directory site doesn't contain a replica of the public folder database, a server in a remote Active Directory site or routing group is selected as the preferred destination.
3. **Cost** If more than one remote Active Directory site or routing group contains a replica of the public folder database, the server in the Active Directory site or routing group that has the least cost routing path from the local Active Directory site is selected as the preferred destination.

If more than one server still meets the criteria, the first server in the replica list returned by Active Directory is selected.

After the hierarchy is read, Exchange then determines which public folder databases have replicas of the content. To make sure that correct message delivery can occur to the public folder replica, a preferred public folder database is selected by the routing component of the Microsoft Exchange Transport service from the **msExchOwningPFTreeBL** list. This selection is made by using the following evaluation process:

1. If only a single instance of a public folder database exists, the server that hosts that database is selected.
2. If the list contains any public folder databases located on servers running Exchange 2007 or Exchange Server 2003, these public folder databases are removed from consideration as the preferred public folder database if a replica also exists on an Exchange 2010 Mailbox server.
3. If more than one Exchange 2010 public folder database is available, the following criteria are used to select a preferred public folder database:
   3.a. **Ranking by the age of the public folder database** The older a public folder database is, the more likely it is to have a replica of the target public folder. Therefore, all public folder databases listed in the **msExchOwningPFTreeBL** list are ranked according to their date of creation by using a configurable number of days as a baseline. The age ranking for each public folder database can be one of the following, listed from best to worst:
      - More than baseline days old
      - Less than baseline days old
      - Unknown

      The public folder database that has the best age rating is selected as the preferred public folder database. By default, the baseline age for public folder replicas is two days (48 hours). You can modify this value by editing the **PFReplicaAgeThreshold** key in the EdgeTransport.exe.config file. This file is located in the *%ProgramFiles%*\Microsoft \Exchange Server\V14\Bin directory on a computer running Exchange 2010.
   3.b. **Proximity** If more than one public folder database has the best age rating, the Mailbox server that has the best proximity rating is selected. The proximity rating for each public folder database can be one of the following, listed from best to worst:
      - **Local server** If the local server contains a replica of the public folder database, it's selected as the preferred destination for routing to public folders contained in that hierarchy.
      - **Server located in the local Active Directory site** If more than one server on the list is located in the local Active Directory site, the first server on the list is selected as the preferred destination for routing to public folders contained in that hierarchy.
      - **Server located in a remote Active Directory site** If the list contains servers from multiple remote Active Directory sites, the server in the Active Directory site that has the least cost routing path from the local Active Directory site is selected as the preferred destination for routing to public folders contained in that hierarchy. If there is more than one server in that site that has a replica of the public folder database, the first server on the list is selected. If more than one remote Active Directory site has the same value for the least cost routing path, the first server on the list is selected.
4. If no public folder database replica is located on an Exchange 2010 Mailbox server, a public folder database located on an Exchange 2007 server is

selected as the preferred destination. If there are no Exchange 2007 servers, a public folder database located on an Exchange 2003 computer is selected as the preferred destination for routing to public folders contained in that hierarchy. In either case, the destination public folder database is selected by the age ranking of the public folder database. The age ranking is determined by using the same method as for an Exchange 2010 server. If more than one public folder database has the same age ranking, the first server on the list is selected.

Return to top

1.7.1.22.4 Using Exchange 2010 Transport to Relay Application Server SMTP Traffic

Using Exchange 2010 Transport to Relay Application Server SMTP Traffic

Transport > Understanding Transport > Understanding Message Routing >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-01-16*

In Microsoft Exchange Server 2010, the Receive connector and load-balancing concepts remain the same as in Exchange Server 2007. Here's a quick review of those concepts. In Exchange 2007, Receive connectors are used to accept incoming messages. By default, when an Exchange Server 2007 Hub Transport server receives an e-mail message via SMTP over TCP port 25, it's processed by the Receive connector named "Default Receive connector".

In addition, Exchange 2007 automatically load-balances all intra-organization message traffic between Edge Transport, Hub Transport, and Mailbox servers using enhanced DNS. However, this functionality doesn't cover the load-balancing of messages received from non-Exchange sources, such as external mail servers, third-party anti-spam or antivirus solutions, any internal mail servers outside your Exchange organization, line-of-business (LOB) applications, and POP-based or IMAP-based e-mail clients.

For more information about how you configure load balancing for messages received from non-Exchange sources, see Understanding SMTP Failover and Load Balancing in Transport.

If you place a load-balancing solution in front of your Hub Transport servers, you need to create a separate Receive connector for that purpose and make sure that only traffic processed by that specific connector is subject to load balancing. This is achieved by adding an additional IP address to the Hub Transport server and associating this IP address with the new Receive connector.

Changes in Behavior with Exchange 2010

Exchange 2010 introduces the *shadow redundancy* feature which provides redundancy for messages for the entire time they're in transit. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all of the next hops for that message have completed delivery.

Because shadow redundancy is an Exchange 2010 feature, shadow redundancy is only supported by Exchange 2010 servers. If an Exchange 2010 transport server receives messages from a previous version of Exchange Server or a non-Exchange source, the source server can't send the expected XSHADOW command. Therefore, shadow redundancy isn't used. Non-Exchange sources include external mail servers, third-party

anti-spam or antivirus solutions, any internal mail servers outside your Exchange organization or line-of-business (LOB) applications the source server.

However, when an Exchange 2010 transport server receives a message from a non-Exchange 2010 source, Exchange attempts to achieve shadow redundancy by delaying the acknowledgement to the sending server until it verifies that the message has been successfully delivered to all next hops internally. This way, if the Exchange 2010 server fails, the sending server assumes that the message was never delivered to Exchange and attempts delivery again.

The delayed acknowledgement time-out is controlled by the MaxAcknowledgementDelay attribute of each Receive connector. The default value is 30 seconds.

For more information about shadow redundancy, see Understanding Shadow Redundancy.

Customers who have upgraded from Exchange 2007 to Exchange 2010 and use dedicated Receive connectors for the purpose of relaying messages from sources such as line-of-business (LOB) applications may see a significant decrease in SMTP throughput. This decrease in throughput is because of the default delayed acknowledgement time-out of 30 seconds configured for a Receive connector. To increase the SMTP throughput for the relay Receive connector, we recommend you either lower the time-out value for the delayed acknowledgement attribute or disable it completely. Whether you should lower or disable the time-out value depends on the amount of messages that go through the relay Receive connector. A good approach is to first lower the value and then verify whether SMTP throughput still suffers and, if it does, then disable the feature completely.

Important:

Although disabling delayed acknowledgements for a Receive connector increases SMTP throughput, it also means that you no longer benefit from the features provided by shadow redundancy. For this reason, we recommend the use of storage hardware redundancy for transport servers for which delayed acknowledgements are disabled.

Use the Shell to configure the maximum acknowledgement delay on a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

Note:

You can't use the Exchange Management Console to configure the maximum acknowledgement delay on a Receive connector.

This example lowers the time-out value for a Receive connector named “SMTP Application relay” from 30 to 15 seconds.

```
Set-ReceiveConnector "SMTP Application relay" -MaxAcknowledgementDelay 15
```

This example disables delayed acknowledgement on the Receive connector.

```
Set-ReceiveConnector "SMTP Application relay" -MaxAcknowledgementDelay 0
```

Important:

It isn’t possible to disable shadow redundancy for a Receive connector. Instead, you must do this on the Exchange organization level. For detailed syntax and parameter information, see Set-TransportConfig.

Message Throttling Policy Considerations

When relaying application server SMTP traffic through an Exchange 2010 transport server,

there are Receive connector specific message throttling policy options that may need to be adjusted, so the overall SMTP throughput doesn't suffer. For example, the *MessageRateLimit* parameter specifies the maximum number of messages that a Receive connector accepts from a single IP address per minute. On Hub Transport servers, this parameter is set to a value of Unlimited, which means SMTP throughput won't be affected. But, for an Edge Transport server, it's set to accept 600 messages per minute. Depending on the relay application server SMTP traffic in your specific environment, you may need to raise this limit.

This example raises the message rate limit for a Receive connector named "SMTP Application relay" from 600 to 2000.

```
Set-ReceiveConnector "SMTP Application relay" -MessageRateLimit 2000
```

Another Receive connector specific option that can have an impact on overall SMTP throughput from a relay application server is expressed in the value of the *MessageRateSource* parameter. With this parameter, you specify how the message submission rate is calculated. It can be set to None, IPAddress, User, or All. By default, the parameter is set to IPAddress, which means the message submission rate is calculated for sending hosts. If this parameter has a negative impact on SMTP throughput from your relay application servers, you should consider setting the value to None.

This example disables the *MessageRateSource* parameter for a Receive connector named "SMTP Application relay".

```
Set-ReceiveConnector "SMTP Application relay" -MessageRateSource None
```

If you're planning to use a dedicated transport server for relay application server SMTP traffic, you should also consider increasing the maximum number of connections that a Receive connector will serve at the same time from a single IP address. This is done using the *MaxInboundConnectionPercentagePerSource* parameter. The value for this parameter is expressed as the percentage of available remaining connections on a Receive connector. By default, the value is set to 2 percent.

This example changes the value of MaxInboundConnectionPercentagePerSource for a Receive connector named "SMTP Application relay" from 2 to 30 percent.

```
Set-ReceiveConnector "SMTP Application relay" - MaxInboundConnectionPercentagePer
```

For detailed syntax and parameter information for the above Receive connector specific parameters, see Set-ReceiveConnector.

1.7.1.23 Understanding Message Size Limits

Understanding Message Size Limits

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can apply message size limits to individual messages that move through the Microsoft Exchange Server 2010 organization. You can restrict the total size of a message or the size of the individual components of a message, such as the message header, the message attachments, and the number of recipients. You can apply limits globally for the whole Exchange 2010 organization, or specifically for a particular connector or user object.

As you plan the message size limits for your Exchange 2010 organization, consider the following questions:

- What size limits should I impose on all incoming messages?
- What size limits should I impose on all outgoing messages?
- Does my Exchange 2010 organization have a mailbox quota?
- How do the message size limits that I have chosen relate to the mailbox quota size?
- Are there users in my Exchange 2010 organization who must send or receive messages that are larger than the specified allowed size?
- Does my Exchange 2010 network topology include other messaging systems or distinctly separate business units that have different message size limits?

This topic provides guidance to help you answer these questions.

Looking for management tasks related to Transport servers? See Managing Transport Servers.

Types of Message Size Limits

Following are the basic categories of the size limits available for individual messages:

- **Message header size limits** These limits apply to the total size of all message header fields that are present in a message. The size of the message body or attachments isn't considered. Because the header fields are plain text, the size of the header is determined by the number of characters in each header field and by the total number of header fields. Each character of text consumes 1 byte.

  Note:
  Some third-party firewalls or proxy servers apply their own message header size limits. These third-party firewalls or proxy servers may have difficulty processing messages that contain attachment file names that are greater than 50 characters or attachment file names that contain non-US-ASCII characters.

- **Message size limits** These limits apply to the total size of a message, which includes the message header, the message body, and any attachments. Message size limits may be imposed on incoming messages or outgoing messages. For internal message flow, Exchange 2010 uses the custom `X-MS-Exchange-Organization-OriginalSize:` message header to record the original message size of the message as it enters the Exchange 2010 organization. Whenever the message is checked against the specified message size limits, the lower value of the current message size or the original message size header is used. The size of the message can change because of content conversion, encoding, and agent processing.
- **Attachment size limits** These limits apply to the maximum allowed size of a single attachment within a message. The message may contain many attachments that greatly increase the overall size of the message. However, an attachment size limit applies to the size of an individual attachment only.
- **Recipient limits** These limits apply to the total number of message recipients. When a message is first composed, the recipients exist in the `To:`, `Cc:`, and `Bcc:` header fields. When the message is submitted for delivery, the message recipients are converted into `RCPT TO:` entries in the message envelope. A distribution group is counted as a single recipient during message submission.

Scope of Limits

Following are the basic categories for the scope of the limits available for individual messages:

- **Organizational limits** These limits apply to all Exchange 2010 and Exchange 2007 servers that exist in the organization. The specified message limits apply to all Exchange 2010 and Exchange 2007 servers that have the Hub Transport server role installed. On an Edge Transport server, the specified limits apply to the specific server.
- **Global limits** Global limits are used when Exchange Server 2003 servers coexist with your Exchange 2010 deployment. The global limits are stored in a different location in Active Directory than the organizational limits and are primarily used by Exchange Server 2003 servers. In an environment where you have both Exchange 2010 and Exchange Server 2003 servers in the same organization, changes that you make to the organizational limits are automatically copied to the corresponding global limits. In Exchange 2010, you can modify the organizational limits by using the **Set-TransportConfig** cmdlet in the Exchange Management Shell, or by configuring the Hub Transport server organization configuration properties in the Exchange Management Console.
- **Connector limits** These limits apply to any messages that use the specified Send connector, Receive connector, Delivery Agent connector, or Foreign connector for message delivery. Connectors are defined on Hub Transport servers or Edge Transport servers.
- **Active Directory site links** Hub Transport servers use Active Directory sites and the costs that are assigned to the Active Directory IP site links to determine the least-cost routing path from each Hub Transport server in the organization to every other Hub Transport server in the organization. You can assign specific message size limits to the Active Directory site links in your organization. For example, you may want to apply a lower message size limit to an Active Directory site link that represents a connection to a remote office with a low-bandwidth connection. Any messages that exceed the maximum message size limit on any Active Directory site link included in the least-cost routing path won't be delivered and will generate a delivery status notification (DSN) with a value of 5.3.4. For more information about message routing in Exchange 2010, see Planning to Use Active Directory Sites for Routing Mail.
- **Routing group connectors** A routing group connector is used to send and receive messages between Exchange 2010 Hub Transport servers and Exchange Server 2003 bridgehead servers when the organization is running more than one version of Microsoft Exchange. Any messages that exceed the maximum message size limit on any routing group connector won't be delivered. They will generate a DSN with the value of 5.3.4. For more information about routing group connectors, see Upgrade from Exchange 2003 Transport.
- **Server limits** These limits apply to a specific Hub Transport server or Edge Transport server. You can set the specified message limits independently on each Hub Transport server or Edge Transport server.
  If you are using Outlook Web App, the maximum HTTP request size limit setting on the Client Access servers also controls the size of messages that Outlook Web App users can send. For more information, see Configure Maximum Message Size in Outlook Web App.
- **User limits** These limits apply to a specific user object, such as a mailbox, contact, distribution group, or public folder.

Organizational Limits

The following table shows the organizational limits, including information about how to configure the limits in the Exchange Management Shell or the Exchange Management Console (EMC).

Organizational limits

Size limit	Default value in Exchange 2010	Shell configuration	EMC configuration
Maximum size for	10 MB	Cmdlet: **Set-TransportConfig**	Organization

messages received		Parameter: *MaxReceiveSize*	Configuration > Hub Transport > Global Settings > Transport Settings > General tab
Maximum size for messages sent	10 MB	Cmdlet: **Set-TransportConfig** Parameter: *MaxSendSize*	Organization Configuration > Hub Transport > Global Settings > Transport Settings > General tab
Maximum number of recipients per message **Note:** When a message is first processed by a Hub Transport server, an X-header named `X-MS-Exchange-Organization-OriginalSize:` is inserted into the message header. Any Hub Transport servers that are involved in the future delivery of the message will use this value for the message size. Conversion encoding and agent processing can increase the size of the message as it flows through the Exchange organization.	5000	Cmdlet: **Set-TransportConfig** Parameter: *MaxRecipientEnvelopeLimit*	Organization Configuration > Hub Transport > Global Settings > Transport Settings > General tab
Maximum attachment size in Transport rules that apply to all Hub Transport servers in the organization	Not configured	Cmdlets: **New-TransportRule**, **Set-TransportRule** Parameter: *AttachmentSizeOver*	Organization Configuration > Hub Transport > Transport Rules New Transport Rule wizard or Edit Transport Rule wizard

Global Limits

The following table shows the global limits, including information about where to configure the limits in Exchange System Manager in Exchange Server 2003.

Global limits

Size limit	Default value	Exchange System Manager configuration
Maximum size for messages received	10240 KB (10 MB)	• *delivContLength* in Active Directory • **Incoming message size** in

		Exchange System Manager **Global Settings**
Maximum size for messages sent	10240 KB (10 MB)	• *submissionContLength* in Active Directory • **Outgoing message size** in Exchange System Manager **Global Settings**
Maximum number of recipients per message	5000	• *msExchRecipLimit* in Active Directory • **Maximum number of recipients** in Exchange System Manager **Global Settings**

Connector Limits

The following table shows the connector limits, including information about how to configure the limits in the Exchange Management Shell or the Exchange Management Console (EMC).

Connector limits

Size limit	Default value	Shell configuration	EMC configuration
Maximum header size through a Receive connector	64 KB	Cmdlets: **New-ReceiveConnector**, **Set-ReceiveConnector** Parameter: *MaxHeaderSize*	N/A
Maximum message size through a Receive connector	10 MB	Cmdlets: **New-ReceiveConnector**, **Set-ReceiveConnector** Parameter: *MaxMessageSize*	Server Configuration > Hub Transport > Receive Connectors > Receive Connector properties > General tab Edge Transport > Receive Connectors > Receive Connector properties > General tab
Maximum number of recipients per message through a Receive connector	200 for the Default Client Receive connector 5,000 for the Default Receive connector on Hub Transport servers 200 for the Default Receive connector on Edge Transport servers **Note:** If the number of recipients is exceeded for an anonymous	Cmdlets: **New-ReceiveConnector**, **Set-ReceiveConnector** Parameter: *MaxRecipientsPerMessage*	N/A

	sender, the message is accepted for the first 200 recipients. Most SMTP messaging servers detect that a recipient limit is in effect. The SMTP messaging server continues to resend the message in groups of 200 recipients until the message is delivered to all recipients.		
Maximum message size through a Send connector	10 MB	Cmdlets: **New-SendConnector**, **Set-SendConnector** Parameter: *MaxMessageSize*	Organization Configuration > Hub Transport > Send Connectors > Send Connector properties > General tab Edge Transport > Send Connectors > Send Connector properties > General tab
Maximum message size through an Active Directory site link	Unlimited	Cmdlet: **Set-AdSiteLink** Parameter: *MaxMessageSize*	N/A
Maximum message size through a routing group connector	Unlimited	Cmdlet: **Set-RoutingGroupConnector** Parameter: *MaxMessageSize*	N/A
Maximum message size through a delivery agent connector	Unlimited	Cmdlets: **New-DeliveryAgentConnector**, **Set-DeliveryAgentConnector** Parameter: *MaxMessageSize*	N/A
Maximum message size through a foreign connector	Unlimited	**Cmdlet: Set-ForeignConnector** Parameter: *MaxMessageSize*	N/A

Server Limits

The following table shows the server limits, including information about how to configure the limits in the Exchange Management Shell or the Exchange Management Console (EMC).

Server limits

Size limit	Default value	Shell configuration	EMC configuration
Transport rule on an Edge Transport server that only applies to the specific server	Not configured	Cmdlets: **New-TransportRule**, **Set-TransportRule** Parameter: *AttachmentSizeOver*	Edge Transport > Transport Rules New Transport Rule wizard or Edit Transport Rule wizard
Maximum header size for messages in the pickup directory	64 KB	Cmdlet: **Set-TransportServer** Parameter: *PickupDirectoryMaxHeaderSize*	Not applicable
Maximum number of recipients per message for messages in the pickup directory	100	Cmdlet: **Set-TransportServer** Parameter: *PickupDirectoryMaxRecipientsPerMessage*	Not applicable

In addition, you can configure the maximum HTTP request length on your Client Access servers that service Microsoft Office Outlook Web App clients. The value configured for this setting will also affect the message size users can submit. For example, if you set this value lower than other message size limits in your organization, your users will not be able to send large messages using Outlook Web App even though they can send the same message using Outlook.

You can configure this setting by modifying the *maxRequestLength* parameter in the web.config file on your Client Access servers. By default, this file is located in the <Exchange install directory>\V14\ClientAccess\Owa folder. The default value is 30000 KB.

User Limits

The following table shows message size limits that you can configure at the recipient level, including information about how to configure the limits in the Exchange Management Shell or the Exchange Management Console (EMC).

User limits

Size Limit	Default value	Shell configuration	EMC configuration
Maximum message size that can be sent by this recipient	Unlimited	Cmdlets: **Set-DistributionGroup** **Set-DynamicDistributionGroup** **Set-Mailbox** **Set-MailContact** **Set-MailUser** **Set-MailPublicFolder**	For mailboxes: Recipient Configuration > Mailbox Properties > Mail Flow Settings tab For mail public folders: Public Folder Management Console > Public Folder properties > Mail Flow Settings tab **Note:** This setting isn't

		Parameter: *MaxSendSize*	configurable using the EMC for other recipient types.
Maximum message size that can be sent to this recipient	Unlimited	Cmdlets: **Set-DistributionGroup** **Set-DynamicDistributionGroup** **Set-Mailbox** **Set-MailContact** **Set-MailUser** **Set-MailPublicFolder** Parameter: *MaxReceiveSize*	For all recipient types except Mail Public Folders: Recipient Configuration > Recipient Properties > Mail Flow Settings tab For Mail Public Folders: Public Folder Management Console > Public Folder properties > Mail Flow Settings tab
Maximum number of recipients per message sent by this recipient	Unlimited	Cmdlets: **Set-Mailbox**, **Set-MailUser** Parameter: *RecipientLimits* Cmdlet: **Set-MailUser** Parameter: *MaxRecipientsPerMessage*	N/A

Order of Precedence for Message Size Limits

You can set different message size limits at different levels in the Exchange organization. As a message is routed through your Transport infrastructure, it may be subjected to several different message size restrictions. You should plan your message size restrictions in a way that makes sure that messages in the transport pipeline are rejected as early as possible if they violate message size limits. Generally speaking, you should set more restrictive limits at the points where messages enter your infrastructure. For example, any message size restrictions on your Edge server Receive connectors that receive messages from the Internet should be less than or equal to the message size restrictions you configure for your internal Exchange organization. It would be a waste of system resources for the Edge Transport server to accept and process a message from the Internet that would be rejected by your Hub Transport servers. Make sure that your organization, server, and connector limits are configured in a way that minimizes any unnecessary processing of messages.

One exception to this approach is the user limits. User level limits take precedence over other message size restrictions. Therefore, you can configure a user to exceed the default

message size limits for your organization. For example, you can allow a specific group of user mailboxes to send larger messages than the rest of the organization by configuring custom send and receive limits for those users.

The exceptions for the user limits only apply to message exchanges between authenticated users. If a message is sent to or received by a recipient on the Internet, the organizational limits will be applied. For example, assume that you have an organizational message size restriction of 10 MB, but you have configured the users in your marketing department to send and receive messages up to 50 MB. These users will be able to exchange large messages with each other, but they still won't be able to receive large messages from Internet users because such messages will be coming from unauthenticated senders.

Messages Exempt from Size Limits

The following list shows the types of messages generated by a Hub Transport server or an Edge Transport server and exempted from all message size limits:

- System messages
- Agent-generated message
- Delivery status notification (DSN) messages
- Journal report messages
- Quarantined messages

However, these messages are still subject to the organizational value for maximum number of recipients in a message. This value is set by the *MaxRecipientEnvelopeLimit* parameter that you can configure by using the **Set-TransportConfig** cmdlet in the Shell.

Differences in Message Size Limits Between Exchange 2003 and Exchange 2010

The primary difference in message size limits between Exchange Server 2003 and Exchange Server 2010 is in the handling of recipient limits. Exchange 2003 treats each member of an expanded distribution list as one recipient. Exchange 2010 treats a distribution group as one recipient. This change was implemented to avoid the partial message delivery scenarios that may occur in Exchange 2003.

Partial message delivery occurs in Exchange 2003 if the number of individual recipients and the recipients that are contained within the distribution list exceeds the specified recipient limit. The total number of message recipients isn't known until after distribution list expansion. Message delivery occurs as the distribution list is expanded until the number of recipients reaches the specified limit. The remaining recipients do not receive the message, but at least the sender receives a non-delivery report (NDR) for each unsuccessful delivery. However, if delivery failure reporting is disabled for the distribution list, the remaining recipients wouldn't receive the message, and the sender would not know who did not receive the message.

1.7.1.24 Understanding Message Throttling

Understanding Message Throttling

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-07*

This topic explains the message throttling options that are available in Microsoft Exchange Server 2010. It also describes enhancements to the message throttling functionality that are included in Service Pack 1 (SP1) of Microsoft Exchange Server 2010. *Message throttling* refers to a group of limits that are set on the number of messages and connections that can be processed by a computer that is running Exchange 2010 with either the Hub Transport server role or the Edge Transport server role installed. These limits prevent the accidental or intentional exhaustion of system resources on the transport server.

For more information about management tasks related to managing transport servers, see Managing Transport Servers.

Contents

Message Throttling Scope

Message throttling involves a variety of limits on message processing rates, SMTP connection rates, and SMTP session time-out values. These limits work together to protect a Hub Transport server or Edge Transport server from being overwhelmed by accepting and delivering messages. Although a large backlog of messages and connections may be waiting to be processed, the message throttling limits enable the transport server to process the messages and connections in an orderly manner.

In addition to message throttling, with Exchange 2010 you can also put size limits on the individual components of messages, such as the number of recipients, the size of the message header, or the size of individual attachments. For more information about message size limits, see Understanding Message Size Limits.

Another Exchange 2010 feature that helps avoid overwhelming the system resources of an Exchange 2010 transport server is *back pressure*. Back pressure is a system resource monitoring feature on Hub Transport servers and Edge Transport servers. When a monitored system resource, such as hard disk utilization or memory utilization, exceeds the specified threshold, the Exchange transport server reduces the rate at which it accepts new connections and messages, and focuses on delivering existing messages. When the utilization of the monitored system resources returns to normal levels, the Exchange transport server slowly increases the rate at which it accepts new connections and then establishes a normal level. For more information, see Understanding Back Pressure.

Message Throttling Enhancements in Exchange 2010 SP1

Exchange 2010 SP1 includes additional features that enhance the message throttling functionality. These enhancements address the following issues that administrators may experience in a messaging environment:

- Because more resources are required to send messages that have large attachments or that are sent to multiple recipients, other message delivery operations may experience increased latency.
- A high rate of mailbox delivery operations may reduce the user interactive mailbox experience. For example, users may experience slow refresh or update times when they access their mailboxes.
- No centralized method is available to control how a specific user may inadvertently affect the resources of a Transport server. Such an effect may occur if the user sends messages that have high delivery costs in terms of number of recipients or total message size or both.

To provide more consistent message throughput and predictable message delivery latency, Exchange 2010 SP1 establishes an accumulated cost for messages. This cost is based on the following criteria:

- Message size
- Number of recipients
- Frequency of transmission

Transport servers that run on Exchange 2010 SP1 track the average delivery cost of messages that are sent by individual users. By using message costs, Exchange 2010 SP1 provides a group of settings that can control the effect that a user or connection has on an Exchange organization. This group of settings is known as a *throttling policy*. When a user repeatedly sends costly messages, such as messages that have large attachments or messages that are sent to many recipients, the Exchange 2010 SP1-based transport servers use a throttling policy to assign a lower priority to higher-cost messages from the user while continuing to deliver lower-cost messages. This new behavior adds a "quality of service" aspect to the message throttling functionality in Exchange 2010.

Note:

Message throttling doesn't affect the message priority from a user's perspective. Messages still retain the original priority set by the user. For example, messages retain a setting of Important or Urgent, and so on.

To support this new functionality, Exchange 2010 SP1 uses the following mechanisms:

- **Internal prioritization agent** This agent is triggered on the **OnResolvedMessage** event and assigns a lower priority to messages from the same sender that have a high accumulated cost. This cost is measured over a period of one minute and affects messages that have more than 500 P1 and P2 recipients or that are larger than 1 megabyte (MB).
- **Quota-based priority queuing for the MapiDelivery queue type** This mechanism causes Exchange to deliver messages in a normal-priority queue more frequently than messages in a low-priority queue. By default, the normal-to-low message ratio is 20:1. However, new messages from a lower priority queue are never delivered sooner than new items from a higher priority queue. For example, consider the following scenario:
  .1.Twenty normal priority messages are delivered. By default, the next delivered message is a lower priority message.
  .2.Two new messages are received by the Transport server: One message from a higher priority queue and one message from a lower priority queue.
  In this scenario, the message from the higher priority queue is delivered first. Then, the message from the lower priority queue is delivered.
- **Throttle concurrent connections based on messaging database health** This mechanism monitors the health of the Exchange messaging database (MDB) health and throttles concurrent connections to Exchange transport servers based on an assigned Health Measure value. The MDB is monitored by the Resource Health Monitor API on the Hub Transport server and is assigned a health value from -1 through 100. This value is based on the RPC performance

statistics that are included with each RPC response from the Store.exe process. The Resource Health framework uses both the **Requests/Second** rate performance counter and the **Average RPC Latency** performance counter to calculate a health value for the database. To help maintain a consistent interactive user experience, Exchange reduces the number of concurrent connections as the health value decreases. The following health value ranges are available:

.1. **-1:** This value indicates that the MDB health state is unknown. This value is assigned when the database starts. In this scenario, the database is considered healthy.
.2. **0:** This value is assigned if the database is in an unhealthy state. In this state, the database should not be contacted.
.3. **1 through 99:** These values represent a fair health state. A lower value represents a less healthy database.
.4. **100:** This value represents a healthy database.

The Microsoft Exchange Throttling service in Exchange 2010 SP1 provides the framework for mail flow throttling. This service is installed when you install the Mailbox Server role. The Exchange 2010 Throttling service keeps track of mail flow throttling settings for a specific user and caches the throttling information in memory. Mail flow throttling settings are also known as a *budget*. Restarting the Exchange 2010 Throttling service also resets mail flow throttling budgets.

You can use the throttling policy cmdlets that are available in Exchange 2010 SP1 to configure individual budget settings for a throttling policy. A budget is the amount of access that a user or application may have for a specific setting. A budget represents how many connections a user may have or how much activity a user may be permitted for each one-minute period. For example, a budget may be configured to set the amount of time that a user may spend using a specific feature in Exchange, such as ActiveSync, Outlook Web App, or Exchange Web Services. This threshold is stored in a throttling policy and defines the budget.

Time settings for a budget are set as a percentage of one minute. Therefore, a threshold of 100 percent represents 60 seconds. For example, assume that you want to specify Outlook Web App policy settings that limit the amount of time during which a user may run Outlook Web App code on a Client Access server and the amount of time the user may communicate with the Client Access server to 600 milliseconds over a one-minute period. To accomplish this, you need to set the value to 1 percent of one minute (600 milliseconds) for both of the following parameters:

- **OWAPercentTimeInCAS:** 1
- **OWAPercentTimeInMailboxRPC:** 1

A user who has this policy applied has a budget of OWAPercentTimeInCAS of 600 milliseconds and of OWAPercentageTimeInMailboxRPC of 600 milliseconds. In this scenario, when the user is logged into Outlook Web App, the user can run Client Access code for up to 600 milliseconds. After the 600 millisecond-period, the connection is considered over budget and the Exchange server doesn't allow any further Outlook Web App action until one minute after the budget limit is reached. After the one-minute period, the user can run Outlook Web App client access code for another 600 milliseconds.

These Exchange 2010 SP1 features, together with the features in the release to manufacturing (RTM) version of Exchange 2010, let an Exchange administrator maintain a consistent user experience without having to deploy more servers than are required to meet the normal workload.

Message Throttling Options on Transport Servers

You can set the message throttling options at the following locations:

- On the transport server
- On a Send connector
- On a Receive connector

You can set all the message throttling options that are available on Hub Transport servers or Edge Transport servers in the Exchange Management Shell. You can also set some of the same options by configuring the transport server properties in the Exchange Management Console (EMC).

The following table shows the message throttling options that are available on Hub Transport servers or Edge Transport servers.

Message throttling options on Hub Transport or Edge Transport servers

Source	Parameter	Description
Set-TransportServer	*MaxConcurrentMailboxDeliveries*	This parameter specifies the maximum number of delivery threads that the Hub Transport server can have open at the same time to deliver messages to mailboxes. The store driver on the Hub Transport server is responsible for delivering messages to and from Mailbox servers. This limit applies to the delivery of messages to any mailboxes in the Exchange organization. The default value of the *MaxConcurrentMailboxDeliveries* parameter is 20.
Set-TransportServer	*MaxConcurrentMailboxSubmissions*	This parameter specifies the maximum number of delivery threads that the Hub Transport server can have open at the same time to accept messages from mailboxes. The store driver on the Hub Transport server is responsible for delivering messages to and from Mailbox servers. This limit applies to the acceptance of new messages from any mailboxes in the Exchange organization. The default value of the *MaxConcurrentMailboxSubmissions* parameter is 20.
Set-TransportServer	*MaxConnectionRatePerMinute*	This parameter specifies the maximum rate at which new inbound connections can be opened to the Hub Transport server or the Edge Transport

		server. These connections are opened to any Receive connectors that exist on the server. The default value for the *MaxConnectionRatePerMinute* parameter is 1200 connections per minute.
Set-TransportServer or Transport server properties	*MaxOutboundConnections*	This parameter specifies the maximum number of concurrent outbound connections that the Hub Transport server or Edge Transport server can have open at the same time. The outbound connections occur by using the Send connectors that exist on the server. The value that's specified by the *MaxOutboundConnections* parameter applies to all the Send connectors that exist on the transport server. The default value of the *MaxOutboundConnections* parameter is 1000. If you enter a value of `unlimited`, no limit is imposed on the number of outbound connections. This value can also be configured using the EMC.
Set-TransportServer or Transport server properties	*MaxPerDomainOutboundConnections*	This parameter specifies the maximum number of connections that an Internet-facing Hub Transport server or Edge Transport server can have open to any single remote domain. The outbound connections to remote domains occur by using Send connectors that exist on the server. The default value of the *MaxPerDomainOutboundConnections* parameter is 20. If you enter a value of `unlimited`, no limit is imposed on the number of outbound connections per domain. This value can also be configured using the EMC.
Set-TransportServer	*PickupDirectoryMaxMessagesPerMinute*	This parameter specifies the rate of message processing for both the Pickup directory

		and Replay directory. Each directory can independently process message files at the rate that's specified by the *PickupDirectoryMaxMessagesPerMinute* parameter. By default, the Pickup directory can process 100 messages per minute, and the Replay directory can process 100 messages per minute at the same time. The Pickup directory and the Replay directory scan for new message files once every 5 seconds, or 12 times per minute. This 5-second polling interval isn't configurable. This means the maximum number of messages that can be processed during each polling interval is the value that you assign to the *PickupDirectoryMaxMessagesPerMinute* parameter divided by 12 (*PickupDirectoryMaxMessagesPerMinute*/12). By default, a maximum of just over eight messages can be processed during each 5-second polling interval.

For more information, see the following topics:

- Configure Edge Transport Server Properties
- Configure Hub Transport Server Properties
- Set-TransportServer

Message Throttling Option on Send Connectors

The following table shows the message throttling option that's available on Send connectors that are configured in your organization or an Edge Transport server. You must use the Shell to configure this option.

Message throttling option available on Send connectors

Source	Parameter	Description
Set-SendConnector	*ConnectionInactivityTimeOut*	This parameter specifies the maximum time that an open SMTP connection with a destination messaging server can remain idle before the connection is closed. The default value is 10 minutes.

For more information, see Set-SendConnector.

Message Throttling Options on Receive Connectors

The following table shows the message throttling options that are available on Receive connectors that are configured on a Hub Transport server or an Edge Transport server. You must use the Shell to configure these options.

Message throttling options available on Receive connectors

Source	Parameter	Description
Set-ReceiveConnector	*ConnectionInactivityTimeOut*	This parameter specifies the maximum time that an open SMTP connection with a source messaging server can remain idle before the connection is closed. The default value for a Receive connector that's configured on a Hub Transport server is 5 minutes. The default value for a Receive connector that's configured on an Edge Transport server is 1 minute.
Set-ReceiveConnector	*ConnectionTimeOut*	This parameter specifies the maximum time that an SMTP connection with a source messaging server can remain open, even if the source messaging server is transmitting data. The default value for a Receive connector that's configured on a Hub Transport server is 10 minutes The default value for a Receive connector that's configured on an Edge Transport server is 5 minutes. The value specified by the *ConnectionTimeout* parameter must be larger than the value specified by the *ConnectionInactivityTimeout* parameter.
Set-ReceiveConnector	*MaxInboundConnection*	This parameter specifies the maximum number of inbound SMTP connections that this Receive connector allows at the same time. The default value is 5000.
Set-ReceiveConnector	*MaxInboundConnectionPercentagePerSource*	This parameter specifies the maximum number of SMTP

		connections that a Receive connector allows at the same time from a single source messaging server. The value is expressed as the percentage of available remaining connections on a Receive connector. The maximum number of connections that are permitted by the Receive connector is defined by the *MaxInboundConnection* parameter. The default value of the *MaxInboundConnectionPercentagePerSource* parameter is 2 percent.
Set-ReceiveConnector	*MaxInboundConnectionPerSource*	This parameter specifies the maximum number of SMTP connections that a Receive connector allows at the same time from a single source messaging server. The default value is 100.
Set-ReceiveConnector	*MaxProtocolErrors*	This parameter specifies the maximum number of SMTP protocol errors that a Receive connector allows before the Receive connector closes the connection with the source messaging server. The default value is 5.
Set-ReceiveConnector	*TarpitInterval*	This parameter specifies the delay that's used in *tarpitting*. Tarpitting is the practice of artificially delaying SMTP responses for specific SMTP communication patterns that indicate a directory harvest attack or other unwelcome messages. A *directory harvest attack* is an attempt to collect valid e-mail addresses from a particular organization to use as a target for unsolicited commercial e-mail. The delay that's specified by the *TarpitInterval* parameter only applies to anonymous connections. The default value of the *TarpitInterval* parameter is 5 seconds. For more information, see Understanding Recipient Filtering.

For more information, see Set-ReceiveConnector.

Message Throttling Policies

In Exchange 2010 SP1, each mailbox has a ThrottlingPolicy setting. The default value for this setting is $Null. You can use the **Set-Mailbox** command together with the *ThrottlingPolicy* parameter to configure a throttling policy for a mailbox.

A default throttling policy exists to provide a default set budget configuration for users who connect to Exchange. To configure customized budget settings for one or more users, create a new throttling policy. Then, apply the policy to the appropriate user or group.

Important:
We recommend that you do not modify the default throttling policy.

You can set all the message throttling options that are available on Mailbox servers in the Exchange Management Shell. The following cmdlets are available to manage throttling policies:

- **Get-ThrottlingPolicy**
- **Remove-ThrottlingPolicy**
- **New-ThrottlingPolicy**
- **Set-ThrottlingPolicy**

For more information, see Understanding Client Throttling Policies.

You can use the **New-ThrottlingPolicy** and **Set-ThrottlingPolicy** cmdlets to configure how much activity a user can perform against Exchange over a specific connection or time period. These settings make up a user's budget. You can establish throttling policies to control access to the following Exchange features:

- Exchange ActiveSync
- Exchange Web Services
- Outlook Web App
- Unified Messaging
- IMAP4
- POP3
- Outlook client connections (MAPI or RPC connections)
- Mail flow settings
- PowerShell commands
- CPU usages

For more information about the policy settings available for use with the throttling policy cmdlets, see New-ThrottlingPolicy and Set-ThrottlingPolicy.

For more information about how to configure Transport servers, see the following topics:

- Configure Edge Transport Server Properties
- Configure Hub Transport Server Properties
- Set-TransportServer

1.7.1.25 Understanding Moderated Transport

Understanding Moderated Transport

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-05*

Using the moderated transport feature in Microsoft Exchange Server 2010, you can require all e-mail messages sent to specific recipients be approved by moderators. You can configure any type of recipient as a moderated recipient, and Exchange 2010 Hub Transport servers will ensure that all messages sent to those recipients go through an approval process.

In any type of organization, you may need to restrict access to specific recipients. The most common scenario is the need to control messages sent to large distribution groups. Depending on your organization's requirements, you may also need to control the messages sent to executive mailboxes or partner contacts. You can use moderated recipients to accomplish these tasks.

Note:

Previous versions of Exchange don't support moderated recipients. If a message sent to a moderated distribution group is expanded on a Hub Transport server running Exchange Server 2007, it will be delivered to all members of that distribution group, bypassing the moderation process. If you have Exchange 2007 Hub Transport servers in your Exchange 2010 organization, and you want to use moderated distribution groups, you must designate an Exchange 2010 Hub Transport server as the expansion server for the moderated distribution groups. Doing this ensures that all messages sent to the distribution group are moderated.

Moderated transport relies on the Exchange 2010 approval framework. For more information about the approval framework, see Understanding Approval Framework.

Looking for management tasks related to transport servers? See Managing Transport Servers.

Moderated Transport

The moderated transport application consists of the following components:

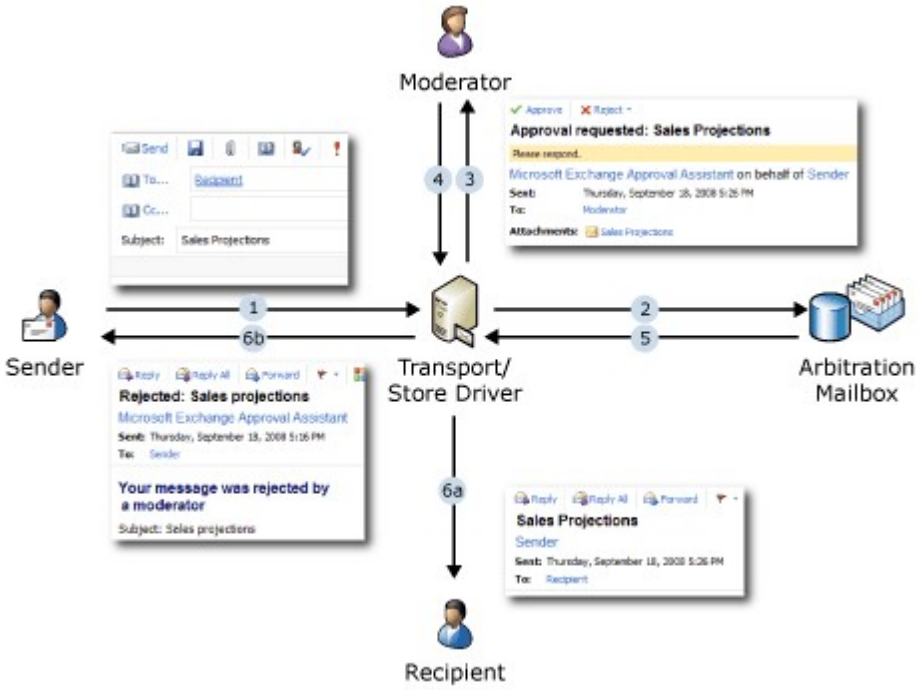
- **Categorizer** The transport categorizer initiates the approval process. When the categorizer detects a moderated recipient while processing a message, it reroutes the message to the arbitration mailbox.
- **Store driver** The store driver processes the messages that the categorizer marks for moderation. When the store driver encounters such a message, it stores the original message in the arbitration mailbox and sends approval requests to the moderators. When a moderator responds with a decision, the store driver marks that decision on the message that's stored in the arbitration mailbox. If an approved message is submitted again by the Information Assistant, the store driver removes the approval workflow wrappers so the message that's delivered is identical to the original message submitted by the sender.
- **Information Assistant** The Information Assistant process monitors the arbitration mailbox. The Information Assistant resubmits any approved messages to the submission queue for delivery to the intended recipients, or it deletes rejected messages. The Information Assistant is also responsible for sending rejection notifications to the sender. In addition, it cleans up the arbitration mailbox by deleting any stale or orphaned messages from the arbitration mailbox. For example, if a moderator simply deletes an approval

request instead of making a decision, the corresponding message waiting for approval in the arbitration mailbox needs to be removed by the Information Assistant.

- **Arbitration mailbox** The arbitration mailbox is used to store the original message that's awaiting approval. By default, one arbitration mailbox is created for moderated transport during setup. It's used for all moderated recipients. You can add additional arbitration mailboxes for load balancing purposes. If you're using multiple arbitration mailboxes, you need to specify which mailbox to use for each moderated recipient.

Message Flow for Moderated Recipients

When a user sends a message to a recipient for whom message moderation is enabled, the message follows a path to its destination, as shown in the following figure and described in the following steps.



1. The sender creates a message and sends it to the moderated recipient.
2. The categorizer intercepts the message, marks it for moderation, and then reroutes it to the arbitration mailbox.
3. The store driver stores the message in the arbitration mailbox and sends an approval request to the moderator.
4. The moderator uses the buttons in the approval request to either accept or reject the message.
5. The store driver marks the moderator's decision on the original message stored in the arbitration mailbox.
6. The Information Assistant reads the approval status on the message stored in the arbitration mailbox, and then processes the message depending on the moderator's decision:
   6.a. If the moderator has approved the message, the Information Assistant resubmits the message to the submission queue, and the message is delivered to the recipient.
   6.b. If the moderator has rejected the message, the Information Assistant deletes the message from the arbitration mailbox and notifies the sender that the message was rejected.

Note:
If the moderator doesn't respond to the message within five days, the Information Assistant will delete the message from the arbitration mailbox and notify the sender that their message has expired.

Handling Multiple Moderated Recipients

It's possible to send a message to a group of recipients that includes both moderated recipients and recipients that aren't moderated. In this case, a separate approval process occurs for each moderated recipient.

Consider a message that's sent to 12 recipients, one of which is a moderated distribution group. The categorizer splits this message into two messages. One message is delivered immediately to the 11 recipients that aren't moderated, and the second message is submitted to the approval process for the moderated distribution group.

If a message is intended for more than one moderated recipient, a separate copy is created for each moderated recipient and is submitted to the approval process.

A moderated distribution group may contain other moderated recipients. In this case, after the message to the distribution group is approved, a separate approval process occurs for each moderated recipient that's a member of the distribution group. However, you can also enable the automatic approval of the distribution group members after the message to the moderated distribution group is approved. To do this, you set the *BypassNestedModerationEnabled* parameter of the moderated distribution group to `$true`. For more parameter and syntax information, see Set-DistributionGroup.

Bypassing Moderation

Messages from moderators are delivered to the moderated recipient immediately, bypassing the approval process. By definition, a moderator has the authority to determine what messages are appropriate for a moderated recipient.

Moderation is also bypassed for owners of distribution groups and dynamic distribution groups. The owner of a distribution group can be responsible for managing the distribution group membership, but may not be able to moderate messages sent to it. For example, the account provisioning staff may be the owners of a distribution group called All Employees, but only specific people in human resources may have moderator rights for the same distribution group.

1.7.1.26 Understanding the Pickup and Replay Directories

Understanding the Pickup and Replay Directories

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

By default, the Pickup and Replay directories exist on every computer running Microsoft Exchange Server 2010 that has the Hub Transport server role or the Edge Transport server role installed. Correctly formatted e-mail message files that you copy to the Pickup or Replay directories are submitted for delivery. The Pickup directory is used by administrators for mail flow testing, or by applications that must create and submit their own messages. The Replay directory receives messages from foreign gateway servers and can also be used to resubmit messages that administrators export from the queues of Exchange 2010 servers.

Looking for management tasks related to Pickup and Relay directories? See Managing Connectors.

Contents

Anatomy of an E-Mail Message File

A standard SMTP e-mail message consists of a *message envelope* and message content. The message envelope contains information required for transmitting and delivering the message. The message content contains message header fields (collectively called the *message header*) and the message body. The message envelope is described in RFC 2821, and the message header is described in RFC 2822.

When a sender composes an e-mail message and submits it for delivery, the message contains the basic information required to comply with SMTP standards, such as a sender, a recipient, the date and time that the message was composed, an optional subject line, and an optional message body. This information is contained in the message itself and, by definition, is contained in the message header.

The sender's messaging server generates a message envelope for the message by using the sender and recipient information found in the message header and transmits the message to the Internet for delivery to the recipient's messaging server. Recipients never see the message envelope, because it's generated by the message transmission process and isn't actually part of the message.

Each server involved in the transmission of the message may insert message header fields related to the server's role in delivering the message or other application-specific message header fields into the message header. When the recipient opens the message by using an e-mail client, the e-mail client displays some of the more relevant information from the message header, such as the sender, the recipients, and the subject together with the message body.

Return to top

How the Pickup Directory Processes Messages

A correctly formatted .eml message file copied to the Pickup directory is processed for submission in the following steps:

1. The Pickup directory is checked for new message files every five seconds. You can't modify this polling interval. You can adjust the rate of message file processing by using the *PickupDirectoryMaxMessagesPerMinute* parameter on the **Set-TransportServer** cmdlet. The default value is 100 messages per minute. Files that can't be opened are left in the Pickup directory and are reevaluated at the next poll.

2. Limits put on message files in the Pickup directory, such as the maximum header size and the maximum number of recipients, are checked. By default, the maximum header size is 64 kilobytes (KB), and the maximum number of recipients is 100. You change these limits by using the **Set-TransportServer** cmdlet.
3. The file is renamed from *<filename>*.eml to *<filename>*.tmp. If the *<filename>*.tmp file already exists, the file is renamed as *<filename><datetime>*.tmp. If the file renaming fails, an event log error is generated, and the pickup process proceeds to the next file.
4. After the .tmp file is successfully converted into an e-mail message, a **delete on close** command is issued to the .tmp file. The .tmp file appears to remain in the Pickup directory, but the file can't be opened.
5. After the message is successfully queued for delivery, a **close** command is issued, and the .tmp file is deleted from the Pickup directory. If the deletion fails, an event log error is generated. If the Microsoft Exchange Transport service is restarted when there are .tmp files in the Pickup directory; all .tmp files are renamed as .eml files and are reprocessed. This could lead to duplicate message transmission.

Requirements for Message Files in the Pickup Directory

A message file copied to the Pickup directory must meet the following requirements for successful delivery:

- The message file must be a text file that complies with the basic SMTP message format. MIME message header fields and content are supported.
- The message file must have an .eml file name extension.
- At least one e-mail address must exist in the Sender or From message header fields in the message header. If a single e-mail address exists in both the Sender and From fields, the e-mail address in the From field is used as the originator of the message in the message envelope.
- Only one e-mail address can exist in the Sender field. Multiple e-mail addresses aren't allowed. The Sender field is optional if only one e-mail address exists in the From field.
- Multiple e-mail addresses are allowed in the From field, but a single e-mail address must also exist in the Sender field. The address in the Sender field is then used as the originator of the message in the message envelope.
- At least one e-mail address must exist in the To, Cc, or Bcc fields.
- A blank line must exist between the message header and the message body.

This example shows a plain text message that uses acceptable formatting for the Pickup directory.

```
To: mary@contoso.com
From: bob@fabrikam.com
Subject: Message subject
This is the body of the message.
```

MIME content is also supported in Pickup directory message files. MIME defines a broad range of message content that includes languages that can't be represented in 7-bit ASCII text, HTML, and other multimedia content. A complete description of MIME and its requirements is beyond the scope of this topic. This example shows a simple MIME message that uses acceptable formatting for the Pickup directory.

```
To: mary@contoso.com
From: bob@fabrikam.com
Subject: Message subject
MIME-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
<HTML><BODY>
<TABLE>
<TR><TD>cell 1</TD><TD>cell 2</TD></TR>
<TR><TD>cell 3</TD><TD>cell 4</TD></TR>
```

```
</TABLE>
</BODY></HTML>
```

Modifications to the Message Header That Are Made to Message Files in the Pickup Directory

The Pickup directory removes any of the following message header fields from the message header:

- `Received`
- `Resent-*`
- `Bcc`

Note:

Any e-mail addresses found in the optional Bcc message header fields in the message header are correctly processed. After the Bcc recipients are promoted to invisible message envelope recipients, they are removed from the message header to protect their identity. If a message contains only Bcc recipients, the value of **Undisclosed Recipients** is added to the To field in the message header.

The Pickup directory adds its own Received header field to a message as part of the message submission process. The Received header field is applied in the following format.

```
Received: from localhost by Pickup with Microsoft SMTP Server id <ExchangeServerV
```

The Pickup directory modifies the following message header fields if they're missing or malformed:

- **Message-Id** If the Message-Id field is missing or empty, the Pickup directory adds a Message-Id field by using the format *<GUID>*@*<defaultdomain>*.
- **Date** If the Date field is missing or malformed, the Pickup directory adds the date and time of message processing by the Pickup directory.

Failures in Pickup Directory Message Processing

A message file copied to the Pickup directory may not be successfully queued for delivery. The following categories of message submission failure can occur:

- **Delivery failures** A correctly formatted message file together with a valid sender that can't be successfully submitted for delivery by the Pickup directory generates a non-delivery report (NDR). Malformed content or Pickup directory message restriction violations could also cause the Pickup directory to generate an NDR. When an NDR is generated during Pickup directory message processing, the original message file is attached to the NDR message, and the message file is deleted from the Pickup directory.

  Note:

  A correctly formatted message submitted by the Pickup directory may later experience a delivery failure and be returned to the sender with an NDR. This kind of failure may be caused by transmission issues unrelated to the Pickup directory, such as messaging server failures or routing failures along the delivery path of the message.

- **Badmail** A message classified as *badmail* has serious problems that prevent the Pickup directory from submitting the message for delivery. The other condition that causes badmail is when the message is formatted correctly, but the recipients aren't valid, and an NDR message can't be sent to the sender because the sender isn't valid.
  Message files determined to be badmail are left in the Pickup directory and are renamed from *<filename>*.eml to *<filename>*.bad. If the *<filename>*.bad file already exists, the file is renamed to *<filename><datetime>*.bad. If badmail exists in the Pickup directory, an event log error is generated, but the same badmail messages don't generate repeated event log errors.

  Note:

Always compose and save message files in a different location before you copy them into the Pickup directory for delivery. The Pickup directory polls for new messages every five seconds. Therefore, if you try to compose and save the message files in the Pickup directory itself, the Pickup directory may try to process the message files before you finish composing them.

Return to top

How the Replay Directory Processes Messages

A correctly formatted .eml message file copied to the Replay directory is processed for submission in the following steps:

1. The Replay directory is checked for new message files every five seconds. You can't modify this polling interval. You can adjust the rate of message file processing by using the *PickupDirectoryMaxMessagesPerMinute* parameter on the **Set-TransportServer** cmdlet. The default value is 100 messages per minute. Files that can't be opened are left in the Replay directory and are reevaluated at the next poll.
2. The file is renamed from *<filename>*.eml to *<filename>*.tmp. If the *<filename>*.tmp file already exists, the file is renamed as *<filename><datetime>*.tmp. If the file renaming fails, an event log error is generated, and the Replay process proceeds to the next file.
3. After the .tmp file is successfully converted into an e-mail message, a **delete on close** command is issued to the .tmp file. The .tmp file appears to remain in the Replay directory, but the file can't be opened.
4. After the message is successfully queued for delivery, a **close** command is issued, and the .tmp file is deleted from the Replay directory. If the deletion fails, an event log error is generated. If the Microsoft Exchange Transport service is restarted when there are .tmp files in the Replay directory, all .tmp files are renamed as .eml files and are reprocessed. This could lead to duplicate message transmission.

Requirements for Message Files in the Replay Directory

The Replay directory is used to resubmit exported Exchange messages and to receive messages from foreign gateway servers. These messages are already formatted for the Replay directory. There is little or no need for an administrator or other application to compose and submit new message files by using the Replay directory. The Pickup directory should be used to create and submit new message files.

The Replay directory messages make extensive use of *X-Headers*. X-Headers are user-defined, unofficial message header fields that exist in the message header. X-Headers aren't specifically mentioned in RFC 2822, but the use of an undefined message header field starting with "X-" has become an accepted way to add unofficial message header fields to a message. The Exchange 2010-specific X-Headers used in the message files in the Replay directory can actually set delivery information that normally exists in the message envelope. This feature is required to preserve original message information when you use the Replay directory to process exported messages from another Exchange server.

A message file copied to the Replay directory must meet the following requirements for successful delivery:

- The message file must be a text file that complies with the basic SMTP message format. MIME message header fields and content are supported.
- The message file must have an .eml file name extension.
- X-Headers must occur before all regular header fields.
- A blank line must exist between the header fields and the message body.

The X-Headers described in the following list are required by messages in the Replay directory:

- **X-Sender** This X-Header replaces the From message header field requirement in a typical SMTP message. One X-Sender field that contains one e-mail address must exist. The Replay directory ignores the From message header field if it's present, although the recipient's e-mail client displays the value of the From message header field as the sender of the message. Other parameters usually exist in the X-Sender field, as shown in the following example.

```
X-Sender: <bob@fabrikam.com> BODY=7bit RET=HDRS ENVID=12345ABCD auth=<s
```

Note:

These parameters are message envelope values that are ordinarily generated by the sending server. You may see parameters similar to this in exported message files.
RET specifies whether the whole message or only the headers should be returned to the sender if the message can't be delivered. RET can have a value of HDRS or FULL. ENVID is a message envelope identifier. BODY specifies the text encoding of the message. auth specifies an authentication mechanism to the messaging server as described in RFC 2554.

- **X-Receiver** This X-Header replaces the To message header field requirement in a typical SMTP message. At least one X-Receiver field that contains one e-mail address must exist. Multiple X-Receiver fields are allowed for multiple recipients. The Replay directory ignores the To message header fields if they're present, although the recipient's e-mail client displays the values of the To message header fields as the recipients of the message. Other optional parameters may exist in the X-Receiver fields, as shown in the following example.

```
X-Receiver: <mary@contoso.com> NOTIFY=NEVER ORcpt=mary@contoso.com
```

Note:

These parameters are message envelope values that are ordinarily generated by the sending server. You may see parameters similar to this in exported message files. These parameters are related to delivery status notification (DSN) messages as described in RFC 1891.
NOTIFY can have a value of NEVER, DELAY, or FAILURE. ORcpt preserves the original recipient of the message.

The X-Headers described in the following list are optional for message files in the Replay directory:

- **X-CreatedBy** Used for header firewall functionality. If this X-Header exists, it must not be blank. If the X-CreatedBy field doesn't exist, it's added with a value of Unspecified. Typically, the value of this field is MSExchange14, but it also may contain the non-SMTP address space type set on a Send connector, such as Notes.
- **X-EndOfInjectedXHeaders** Size in bytes of all the X-Headers present. This X-Header may be used as a marker to indicate the last X-Header before the regular message header fields start.
- **X-ExtendedMessageProps** Extended message properties for the message.
- **X-HeloDomain** HELO/EHLO domain string presented during the initial SMTP protocol conversation.
- **X-LegacyExch50** Used to preserve custom properties generated by Exchange Server 2003 if Exchange 2003 servers are present.
- **X-Source** Used by Queue Viewer under the **MessageSourceName** column. If

the value of this X-Header isn't specified, the value of `Replay` is used. Other possible values for this X-Header are `Smtp Receive Connector` and `Smtp Send Connector`.

- **X-SourceIPAddress** IP address of the sending server. This field is 0.0.0.0 if no IP address is specified.

This example shows a plain text message that uses acceptable formatting for the Replay directory.

```
X-Receiver: <mary@contoso.com> NOTIFY=NEVER ORcpt=mary@contoso.com
X-Sender: <bob@fabrikam.com> BODY=7bit ENVID=12345AB auth=<someAuth>
Subject: Optional message subject
This is the body of the message.
```

MIME content is also supported in Replay directory message files. MIME defines a broad range of message content that includes languages that can't be represented in 7-bit ASCII text, HTML, and other multimedia content. A complete description of MIME and its requirements is beyond the scope of this topic. This example shows a simple MIME message that uses acceptable formatting for the Replay directory.

```
X-Receiver: <mary@contoso.com> NOTIFY=NEVER ORcpt=mary@contoso.com
X-Sender: <bob@fabrikam.com> BODY=7bit ENVID=12345ABCD auth=<someAuth>
To: mary@contoso.com
From: bob@fabrikam.com
Subject: Optional message subject
MIME-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
<HTML><BODY>
<TABLE>
<TR><TD>cell 1</TD><TD>cell 2</TD></TR>
<TR><TD>cell 3</TD><TD>cell 4</TD></TR>
</TABLE>
</BODY></HTML>
```

Modifications to the Message Header That Are Made to Message Files in the Replay Directory

The Replay directory deletes the Bcc message header field from the message file.

The Replay directory adds its own Received message header field to a message as part of the message submission process. The Received message header field is applied in the following format.

```
Received: from <ReceivingServerName> by Replay with <ExchangeServerVersion><DateT
```

The Replay directory modifies the following message header fields in the message header:

- **Message-ID** If this message header field is missing or empty, the Replay directory adds a Message-ID message header field by using the format *<GUID>*@*<defaultdomain>*.
- **Date** If this message header field is missing or malformed, the Replay directory adds the Date message header field using the date and time of message processing by the Replay directory.

Failures in Replay Directory Message Processing

Any problems converting a message file into an e-mail message causes the Replay directory to consider the message undeliverable (badmail). A badmail message file has serious problems, such as a missing sender, missing recipients, or formatting problems. Message files determined to be badmail are left in the Replay directory and are renamed from *<filename>*.eml to *<filename>*.bad. If the *<filename>*.bad file already exists, the file is renamed to *<filename><datetime>*.bad. If badmail exists in the Replay directory, an event log error is generated, but the same badmail messages don't generate repeated event log errors.

Return to top

Security Considerations for the Pickup and Replay Directories

The following list describes security concerns that are common to the Pickup directory and the Replay directory:

- Any security checks configured on a Receive connector, such as anti-spam, antivirus, sender filtering, or recipient filtering actions, aren't performed on messages submitted through the Pickup directory or the Replay directory.
- A compromised Pickup directory or Replay directory can act as an open relay. This enables messages to be resubmitted or *relayed* by using a different server to mask the true source of the messages.

The following list describes additional security concerns that apply to the Replay directory:

- The X-Headers used by the Replay directory allow for the manual creation of the message envelope. The information in the X-Sender and X-Receiver fields can be completely different from the To or From message header fields displayed by e-mail clients. Such an impersonation of a sender and a domain is frequently called *spoofing*. A *spoofed mail* is an e-mail message that has a sending address that was modified to appear as if it originates from a sender other than the actual sender of the message.
- If the X-CreatedBy field has the value of `MSExchange14`, the destination is considered trustworthy, and a header firewall isn't applied. A header firewall is a way for Exchange to preserve X-Headers in messages transmitted between trusted Exchange 2010 servers or to remove potentially revealing X-Headers from messages transmitted to untrusted destinations outside the Exchange organization. These X-Headers can be used to share Exchange 2010 information such as spam confidence level (SCL), message signing, or encryption between authorized Exchange 2010 servers. Revealing this information to unauthorized sources could pose a potential security risk.

Tighter security should be applied to the Replay directory because of the additional security risks associated with the Replay directory. Users or applications that must generate and submit messages can be granted access to the Pickup directory, but they shouldn't require access to the Replay directory.

Both the Pickup directory and the Replay directory are enabled by default on all Hub Transport servers and Edge Transport servers. If the Pickup directory or the Replay directory isn't required on a specific Hub Transport server or Edge Transport server in your organization, you can disable the Pickup directory or the Replay directory on that server. For more information, see the following topics:

- Configure the Pickup Directory
- Configure the Replay Directory

Return to top

Permissions for the Pickup and Replay Directories

The following permissions are required on the Pickup and Replay directories:

- Administrator: Full Control
- System: Full Control
- Network Service: Read, Write, and Delete Subfolders and Files

By default, the Microsoft Exchange Transport service uses the security credentials of the Network Service user account to manage the location and permissions of the Pickup and Replay directories. The Network Service account requires these permissions on the Pickup directory so that .eml files can be opened, renamed to .tmp and deleted, or renamed to .bad if the message is classified as badmail.

You can move the location of these directories by using the *PickupDirectoryPath* and *ReplayDirectoryPath* parameters on the **Set-TransportServer** cmdlet. Successfully changing the location of the Pickup directory depends on the rights granted to the Network Service account at the new directory locations, and whether the new directories already exist. If the directory doesn't exist, and the Network Service account has the rights required to create folders and apply permissions at the new location, the directory is created, and the correct permissions are applied to it. If the new directory already exists, the existing folder permissions aren't checked. Whenever you move the directory locations by using the *PickupDirectoryPath* or *ReplayDirectoryPath* parameter with the **Set-TransportServer** cmdlet, always verify that the new directory exists and that the new directory has the correct permissions applied to it.

Return to top

1.7.1.27 Understanding Priority Queuing

Understanding Priority Queuing

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-25*

Priority queuing is a feature of Microsoft Exchange Server 2010 that enables the sender-defined priority of a message to influence the processing of the message by a server running Exchange that has the Hub Transport server role installed.

The message priority is assigned by the sender in Microsoft Outlook when the sender creates and sends the message. The sender can set any of the following message priority values in Outlook:

- Low importance
- Normal importance
- High importance

The default priority for a message created in Outlook or Microsoft Office Outlook Web App is Normal priority. The message priority is stored in the `X-Priority` header field in the message header.

Every message sent or received in an Exchange 2010 organization must be categorized on a Hub Transport server before it can be routed and delivered. The categorizer on a Hub Transport server picks up one message at a time from the Submission queue and performs recipient resolution, routing resolution, and content conversion on the message before putting the message in a delivery queue. For more information, see Understanding Transport Pipeline.

Delivery queues are dynamically created based on the destination of a message. Mailbox delivery queues are created for messages destined for Mailbox servers that exist in the same Active Directory site as the Hub Transport server. Remote delivery queues are created for messages destined for Mailbox servers that exist in a different Active Directory site than the Hub Transport server, and for remote domains. For more information, see

Understanding Transport Queues.

All messages that have the same destination are put in the same delivery queue. Priority queuing affects the transmission of messages from a delivery queue to the destination messaging server. When priority queuing is enabled, High priority messages are transmitted to their destinations before Normal priority messages, and Normal priority messages are transmitted to their destinations before Low priority messages. The prioritized delivery of messages based on the message priority can help you define specific service level agreement (SLA) requirements for message delivery times.

Options for Configuring Priority Queuing

All configuration options for priority queuing are available in the EdgeTransport.exe.config application configuration file located in the C:\Program Files\Microsoft\Exchange Server \V14\Bin directory. For more information about the EdgeTransport.exe.config file, see Understanding the EdgeTransport.exe.Config File. Many configuration options available are unrelated to priority queuing. Any configuration options that don't involve back pressure are outside the scope of this topic.

Enabling or Disabling Priority Queuing

The *PriorityQueuingEnable* parameter enables or disables priority queuing on a Hub Transport server. The default value is `False`. To enable priority queuing, set the *PriorityQueuingEnable* parameter value to `True` in the EdgeTransport.exe.config file and restart the Microsoft Exchange Transport service.

Configuring the Maximum Size of a High Priority Message

The *MaxHighPriorityMessageSize* parameter controls the maximum allowed size of a High priority message. The default value is 250 kilobytes (KB). If a High priority message is larger than the value of the *MaxHighPriorityMessageSize* parameter, the message is automatically downgraded from High priority to Normal priority.

When you enter a value, qualify the value with one of the following units:

- KB (kilobytes)
- MB (megabytes)
- GB (gigabytes)

The value of the *MaxHighPriorityMessageSize* parameter should be significantly less than the value of the *MaxMessageSize* parameter on the **Set-TransportConfig** cmdlet. The default value of the *MaxMessageSize* parameter is 10 MB. A smaller value in the *MaxHighPriorityMessageSize* parameter helps ensure consistent and predictable delivery times for High priority messages.

Configuring the Delay Notification Time-Out Based on the Message Priority

After each message delivery failure, the Hub Transport server generates a delay delivery status notification (DSN) message and queues it for delivery to the sender of the undeliverable message. This delay DSN message is sent only after a specified delay notification time-out interval, and only if the failed message wasn't successfully delivered during that time. This delay prevents the sending of unnecessary delay DSN messages that may be caused by temporary message transmission failures.

The following table shows the delay DSN notification time-out options based on the message priority.

Delay DSN notification time-out options based on the message priority

Parameter name	Default value

LowPriorityDelayNotificationTimeout	8:00:00 (8 hours)
NormalPriorityDelayNotificationTimeout	4:00:00 (4 hours)
HighPriorityDelayNotificationTimeout	00:30:00 (30 minutes)

To specify a value for a delay notification time-out, enter the value as a time span: *dd.hh:mm:ss*, where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. If the value is less than 1 day, you can omit the day part of the time span.

Configuring the Message Expiration Time-Out Based on the Message Priority

The *message expiration time-out* specifies the maximum length of time that a Hub Transport server tries to deliver a failed message. If the message can't be successfully delivered before the expiration time-out interval has passed, a non-delivery report (NDR) that contains the original message or the message headers is delivered to the sender.

The following table shows the message expiration time-out options based on the message priority.

Message expiration time-out options based on the message priority

Parameter name	Default value
LowPriorityMessageExpirationTimeout	2.00:00:00 (2 days)
NormalPriorityMessageExpirationTimeout	2.00:00:00 (2 days)
HighPriorityMessageExpirationTimeout	8:00:00 (8 hours)

To specify a value for a message expiration time-out, enter the value as a time span: *dd.hh:mm:ss*, where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. If the value is less than 1 day, you can omit the day part of the time span.

Configuring the Maximum Number of Connections Per Domain Based on the Message Priority

The maximum number of connections per domain specifies the maximum number of connections that a Hub Transport server can have open to any single remote domain. The outgoing connections to remote domains occur by using the remote delivery queues and Send connectors that exist on the Hub Transport server.

The following table shows the maximum number of connections per domain options based on the message priority.

Maximum number of connections per domain options based on the message priority

Parameter name	Default value
MaxPerDomainLowPriorityConnections	2
MaxPerDomainNormalPriorityConnections	15
MaxPerDomainHighPriorityConnections	3

The sum of the *MaxPerDomainLowPriorityConnections* parameter, the *MaxPerDomainNormalPriorityConnections* parameter, and the *MaxPerDomainNormalPriorityConnections* parameter should be less than or equal to the value of the *MaxPerDomainOutboundConnections* parameter on the **Set-TransportServer**

cmdlet. The default value of the *MaxPerDomainOutboundConnections* parameter is 20.

How Priority Queuing Affects Other Message Limits on Hub Transport Servers

All messages that pass through a Hub Transport server are subject to a variety of message retry, resubmit, and expiration limits. For more information, see Understanding Transport Queues.

Some message limits available in the **Set-TransportServer** cmdlet have corresponding priority queuing message limits available in the EdgeTransport.exe.config configuration file. The following table shows these corresponding message limits.

Message limits in the Set-TransportServer cmdlet that correspond to priority queuing message limits in the EdgeTransport.exe.config configuration file

Source	Parameter	Default value
Set-TransportServer	*DelayNotificationTimeOut*	4:00:00 (4 hours)
EdgeTransport.exe.config	*NormalPriorityDelayNotificationTimeout*	4:00:00 (4 hours)
Set-TransportServer	*MessageExpirationTimeOut*	2.00:00:00 (2 days)
EdgeTransport.exe.config	*NormalPriorityMessageExpirationTimeout*	2.00:00:00 (2 days)

When priority queuing is disabled, all the priority queuing message limits that exist in the EdgeTransport.exe.config configuration file are ignored. All the message limits on the **Set-TransportServer** cmdlet apply to all messages that travel through the Hub Transport server.

When priority queuing is enabled, the priority queuing message limits in the EdgeTransport.exe.config configuration file override the corresponding message limits in the **Set-TransportServer** cmdlet. All other message limits in the **Set-TransportServer** cmdlet still apply to Low priority, Normal priority, and High priority messages that travel through the Hub Transport server.

User Settings for Priority Queuing

The **Set-Mailbox** cmdlet in the Exchange Management Shell has the *DowngradeHighPriorityMessagesEnabled* parameter. The default value is `False`. When this parameter is set to `True`, any High priority messages sent from the mailbox are automatically downgraded to Normal priority. For more information, see Set-Mailbox.

1.7.1.28 Understanding Receive Connectors

Understanding Receive Connectors

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Receive connectors are configured on computers that are running Microsoft Exchange Server 2010 and that have the Hub Transport server role or Edge Transport server role installed. Receive connectors represent a logical gateway through which all inbound messages are received. This topic provides an overview of Receive connectors and how the configuration of Receive connectors affects individual message processing.

Overview of Receive Connectors

Exchange 2010 transport servers require Receive connectors to receive messages from the Internet, from e-mail clients, and from other e-mail servers. A Receive connector controls inbound connections to the Exchange organization. By default, the Receive connectors that are required for internal mail flow are automatically created when the Hub Transport server role is installed. The Receive connector that's capable of receiving mail from the Internet and from Hub Transport servers is automatically created when the Edge Transport server role is installed. However, end-to-end mail flow is possible only after the Edge Transport server has been subscribed to the Active Directory site by using the Edge Subscription process. Other scenarios, such as an Internet-facing Hub Transport server or an unsubscribed Edge Transport server, require manual connector configuration to establish end-to-end mail flow.

In Exchange 2010, the Receive connector is a *receive listener*. This means that the connector is listening for inbound connections that match the settings of the Receive connector. A Receive connector listens for connections that are received through a particular local IP address and port, and from a specified IP address range. You create Receive connectors when you want to control which servers receive messages from a particular IP address or IP address range, and when you want to configure special connector properties for messages that are received from a particular IP address, such as a larger message size, more recipients per message, or more inbound connections.

Receive connectors are scoped to a single server and determine how that specific server listens for connections. When you create a Receive connector on a Hub Transport server, the Receive connector is stored in Active Directory as a child object of the server on which it's created. When you create a Receive connector on an Edge Transport server, the Receive connector is stored in Active Directory Lightweight Directory Services (AD LDS).

If you need additional Receive connectors for specific scenarios, you can create them by using the Exchange Management Console (EMC) or the Exchange Management Shell. Each Receive connector must use a unique combination of IP address bindings, port number assignments, and the remote IP address ranges from which mail will be accepted by this connector.

Default Receive Connectors Created During Setup

Certain Receive connectors are created by default when you install a Hub Transport or Edge Transport server role.

Default Receive Connectors Created on a Hub Transport Server

When you install the Hub Transport server role, two Receive connectors are created. No additional Receive connectors are needed for typical operation, and in most cases the default Receive connectors don't require a configuration change. The usage type and configuration of these connectors are described in the following table.

Default Receive connector configuration on Hub Transport servers

Connector name and usage type	Configuration

Client Servername This Receive connector accepts SMTP connections from all non-MAPI clients, such as POP and IMAP.	• Status: Enabled. • Protocol logging level: None. • Connector fully qualified domain name (FQDN): *Servername.forestroot.extension* • Bindings: All available IP addresses. The server accepts mail received through any network adapter on the Hub Transport server. • Port: 587. This is the default port for receiving messages from all non-MAPI clients for SMTP relay. • Remote server IP address range: 0.0.0.0–255.255.255.255 IPv4 and 0000:0000:0000:0000:0000:0000:0.0.0.0–ffff:ffff:ffff:ffff:ffff:ffff:255.255.255.255 IPv6. The Hub Transport server accepts mail that's sent from any IP address. • Available authentication methods: Transport Layer Security (TLS), Basic authentication, Exchange Server authentication, Integrated Windows authentication. • Permission groups: Exchange users.
Default Servername This Receive connector accepts connections from other Hub Transport servers and any Edge Transport servers you have.	• Status: Enabled. • Protocol logging level: None. • Connector FQDN: *Servername.forestroot.extension* • Local server Receive connector bindings: All available IP addresses. The server accepts mail received through any network adapter on the Hub Transport server. • Port: 25. • Remote server IP address range: 0.0.0.0–255.255.255.255 IPv4 and 0000:0000:0000:0000:0000:0000:0.0.0.0–ffff:ffff:ffff:ffff:ffff:ffff:255.255.255.255 IPv6.. The Hub Transport server accepts mail that's sent from any IP address. • Available authentication methods: TLS, Basic authentication, Integrated Windows authentication. • Permission groups: Exchange users, Exchange servers, Legacy Exchange servers.

Note:

Any Receive connector that's responsible for accepting connections from Edge Transport servers or other Hub Transport servers must have the Exchange Server authentication method assigned to it. The Exchange Server authentication method is the default authentication method when you create a Receive connector that has the Internal usage type.

Default Receive Connector Created on an Edge Transport Server

During installation, one Receive connector is created. This Receive connector is configured

to accept SMTP communications from all IP address ranges and is bound to all IP addresses of the local server. It's configured to have the Internet usage type, and therefore, the connector accepts anonymous connections. In a typical installation, no additional Receive connectors are required. If you use EdgeSync, you don't need to make any configuration changes because the Edge Subscription process automatically configures permissions and authentication mechanisms. Anonymous sessions and authenticated sessions are granted different permission sets.

If you don't use EdgeSync, we recommend that you modify the settings of this Receive connector and create an additional Receive connector of the Internal usage type. To complete Receive connector configuration, follow these steps:

1. **Modify the settings of the default Receive connector** Set the local network bindings to the IP address of only the Internet-facing network adapter.
2. **Create a Receive connector** Select Internal as the connector usage type. Set the local network bindings to the IP address of only the organization-facing network adapter. Configure the remote network settings to receive mail from the remote IP addresses that are assigned to the Hub Transport servers.

   Note:

   Any Receive connector that's responsible for accepting connections from Edge Transport servers or other Hub Transport servers must have the Exchange Server authentication method assigned to it. The Exchange Server authentication method is the default authentication method when you create a Receive connector that has the Internal usage type.

3. **Determine whether Basic authentication is desired** If you want to support Basic authentication, create a local user account and grant the necessary permissions by using the Add-ADPermission cmdlet.

For more information, see Configure Mail Flow Between an Edge Transport Server and Hub Transport Servers Without Using EdgeSync.

Receive Connector Usage Types

The usage type determines the default security settings for the connector.

The security settings for a Receive connector specify the permissions that are granted to sessions that connect to the Receive connector and the supported authentication mechanisms.

When you use the EMC to configure a Receive connector, the New SMTP Receive Connector wizard prompts you to select the usage type for the connector. You can use two different methods to specify the usage type:

- Use the *Usage* parameter with the desired value, such as *Usage* `Custom`. There are other required parameters based on the usage type that you specify. If you don't specify the required parameters in the **New-ReceiveConnector** command, the command will fail.
- Use the switch parameter for the desired usage type, such as *Custom*. There are other required parameters based on the usage type that you specify. If you don't specify the required parameters in the **New-ReceiveConnector** command, you're prompted for the missing parameter values so the command can continue.

Permission Groups

A permission group is a predefined set of permissions that's granted to well-known security principals and assigned to a Receive connector. Security principals include users, computers, and security groups. A security principal is identified by a security identifier (SID). Permission groups are only available for Receive connectors. The use of permission groups simplifies the configuration of permissions on Receive connectors. The

PermissionGroups property defines the groups or roles that can submit messages to the Receive connector and the permissions that are assigned to those groups. The set of permission groups is predefined in Exchange 2010. This means that you can't create additional permission groups. Also, you can't modify the permission group members or the associated permissions.

The following table lists the available permission groups and identifies the security principals and the permissions that are granted when that permission group is configured for a Receive connector.

Receive connector permission groups

Permission group name	Associated security principals (SIDs)	Permissions granted
Anonymous	Anonymous user account	• Ms-Exch-SMTP-Submit • Ms-Exch-SMTP-Accept-Any-Sender • Ms-Exch-SMTP-Accept-Authoritative-Domain-Sender • Ms-Exch-Accept-Headers-Routing
ExchangeUsers	Authenticated user accounts	• Ms-Exch-SMTP-Submit • Ms-Exch-SMTP-Accept-Any-Recipient • Ms-Exch-Bypass-Anti-Spam • Ms-Exch-Accept-Headers-Routing
ExchangeServers	• Hub Transport servers • Edge Transport servers • Exchange Servers (Hub Transport server only) • Externally Secured servers	• Ms-Exch-SMTP-Submit • Ms-Exch-SMTP-Accept-Any-Sender • Ms-Exch-SMTP-Accept-Any-Recipient • Ms-Exch-Accept-Authoritative-Domain-Sender • Ms-Exch-Bypass-Anti-Spam • Ms-Exch-SMTP-Accept-Authentication-Flag • Ms-Exch-Bypass-Message-Size-Limit • Ms-Exch-Accept-Headers-Routing • Ms-Exch-Accept-Exch50 • Ms-Exch-Accept-Headers-Organization **Note:** This permission isn't granted to Externally Secured servers. • Ms-Exch-Accept-Headers-Forest **Note:** This permission isn't

		granted to Externally Secured servers.
ExchangeLegacyServers	Exchange Legacy Interop security group	• Ms-Exch-SMTP-Submit • Ms-Exch-SMTP-Accept-Any-Sender • Ms-Exch-SMTP-Accept-Any-Recipient • Ms-Exch-Accept-Authoritative-Domain-Sender • Ms-Exch-Bypass-Anti-Spam • Ms-Exch-SMTP-Accept-Authentication-Flag • Ms-Exch-Bypass-Message-Size-Limit • Ms-Exch-Accept-Headers-Routing • Ms-Exch-Accept-Exch50
Partner	Partner Server account	• Ms-Exch-SMTP-Submit • Ms-Exch-Accept-Headers-Routing

Receive Connector Usage Types

The usage type determines the default permission groups that are assigned to the Receive connector and the default authentication mechanisms that are available for session authentication. A Receive connector always responds to a request from a sender to use TLS. The following table describes the available usage types and default settings.

Receive connector usage types

Usage type	Default permission groups	Default authentication mechanism
Client (unavailable on Edge Transport servers)	ExchangeUsers	TLS Basic authentication plus TLS Integrated Windows authentication
Custom	None	None
Internal	ExchangeServers ExchangeLegacyServers (This permission group is unavailable on Edge Transport servers.)	Exchange Server authentication
Internet	AnonymousUsers Partner	None or Externally Secured
Partner	Partner	Not applicable. This usage type is selected when you establish mutual TLS with a remote domain.

The Receive connector permissions and authentication mechanisms are discussed later in this topic.

Receive Connector Usage Scenarios

Each usage type is appropriate for a specific connection scenario. Select the usage type that has the default settings most applicable to the configuration that you want. You can modify permissions by using the **Add-ADPermission** and **Remove-ADPermission** cmdlets. For more information, see the following topics:

- Add-ADPermission
- Remove-ADPermission

The following table lists common connection scenarios and the usage type for each scenario.

Receive Connector usage scenarios

Connector scenario	Usage type	Comment
Edge Transport server receiving e-mail from the Internet	Internet	A Receive connector that's configured to accept e-mail from all domains is created automatically when the Edge Transport server role is installed.
Hub Transport server receiving e-mail from the Internet	Internet	This isn't a recommended configuration. For more information, see Configure Internet Mail Flow Directly Through a Hub Transport Server.
Edge Transport server receiving e-mail from an Exchange Server 2003 bridgehead server	Internal	In this scenario, the Exchange 2003 bridgehead server is configured to use the Edge Transport server as a smart host for a Send connector.
Hub Transport server receiving e-mail submissions from a client application that uses POP3 or IMAP4	Client	This Receive connector is automatically created on every Hub Transport server when the role is installed. By default, this Receive connector is configured to receive e-mail through TCP port 587.
Hub Transport server receiving e-mail from a Hub Transport server	Internal	You don't have to configure Receive connectors between Hub Transport servers within the same organization. This usage type can be used to configure a cross-forest Receive connector.
Hub Transport server receiving e-mail from an Exchange 2003 bridgehead server in the same forest	Internal	This is an optional configuration. Transport between Exchange 2010 and earlier versions of Exchange is accomplished through two-way routing group connectors. If you create SMTP connectors to Exchange 2003 routing groups, a routing group connector must also exist. For more information, see Create Additional Routing Group Connectors from Exchange 2010 to Exchange 2003.
Edge Transport server	Internal	A Receive connector that's configured

receiving e-mail from a Hub Transport server		to accept e-mail from all domains is created automatically when the Edge Transport server role is installed. You can create another connector and configure it to receive e-mail only from the Exchange organization.
Cross-forest Receive connector for a Hub Transport server in one forest receiving e-mail from a Hub Transport server in a second forest	Custom	For detailed configuration steps, see Configure Cross-Forest Connectors.
Cross-forest Receive connector for a Hub Transport server in one forest receiving e-mail from an Exchange 2003 bridgehead server in a second forest	Custom	For detailed configuration steps, see Configure Cross-Forest Connectors.
Hub Transport server receiving e-mail from a third-party message transfer agent (MTA)	Internal	Specify the IP address range from which messages will be accepted and set the authentication mechanism to either Basic authentication or Externally Secured.
Edge Transport server receiving e-mail from a third-party MTA	Custom	Use the **Add-ADPermission** cmdlet to set the extended rights. Specify the IP address range from which messages will be accepted and set the authentication mechanism to Basic authentication. You can also select the Internal usage type and set Externally Secured as the authentication method. No additional permissions configuration is required if you select this option.
Edge Transport server receiving e-mail from an external relay domain	Custom	The Edge Transport server can accept e-mail from an external relay domain and then relay to the destination recipient domain. Specify the IP address range from which messages will be accepted, set the appropriate authentication mechanism, and use the **Add-ADPermission** cmdlet to set the extended rights.
Edge Transport server receiving e-mail from a domain to which you have established mutual TLS authentication	Partner	Mutual TLS authentication functions correctly only if the following conditions are true: • The value of the *DomainSecureEnabled* parameter is set to `$true`. • The value of the *AuthMechanism* parameter contains `TLS` and doesn't contain `External`.

		• The *TLSReceiveDomainSecureList* parameter in the Transport configuration contains at least one domain that's serviced by this Receive connector. The wildcard character (*) isn't supported in domains that are configured for mutual TLS authentication. The same domain must also be defined on the corresponding Send connector, and in the value of the *TLSSendDomainSecureList* parameter in the Transport configuration. For more information, see Set-ReceiveConnector.
Edge Transport server receiving connections from Microsoft Exchange Hosted Services server	Custom	The Exchange Hosted Services server can act as an externally authoritative server. To use the Externally Secured authentication mechanism, use the **Set-ReceiveConnector** cmdlet to set the *PermissionGroup* parameter to `ExchangeServers`.
Hub Transport server receiving connections from an Exchange Hosted Services server	Custom	The Exchange Hosted Services server can act as an externally authoritative server. To use the Externally Secured authentication mechanism, use the **Set-ReceiveConnector** cmdlet to set the *PermissionGroup* parameter to `ExchangeServers`.

Receive Connector Permissions

Receive connector permissions are assigned to security principals when you specify the permission groups for the connector. When a security principal establishes a session with a Receive connector, the Receive connector permissions determine whether the session is accepted and how the received messages are processed. The following table describes the permissions that can be assigned on a Receive connector to security principals. You can set Receive connector permissions by using the EMC or by using the *PermissionGroups* parameter with the **Set-ReceiveConnector** cmdlet in the Shell. To modify the default permissions for a Receive connector, you can also use the **Add-ADPermission** cmdlet.

Receive connector permissions

Receive connector permission	Description
ms-Exch-SMTP-Submit	The session must be granted this permission or it will be unable to submit messages to this Receive connector. If a session doesn't have this permission, the MAIL FROM and AUTH commands will fail.

ms-Exch-SMTP-Accept-Any-Recipient	This permission allows the session to relay messages through this connector. If this permission isn't granted, only messages that are addressed to recipients in accepted domains are accepted by this connector.
ms-Exch-SMTP-Accept-Any-Sender	This permission allows the session to bypass the sender address spoofing check.
ms-Exch-SMTP-Accept-Authoritative-Domain-Sender	This permission allows senders that have e-mail addresses in authoritative domains to establish a session to this Receive connector.
ms-Exch-SMTP-Accept-Authentication-Flag	This permission allows Exchange 2003 servers to submit messages from internal senders. Exchange 2010 will recognize the messages as being internal. The sender can declare the message as trusted. Messages that enter your Exchange system through anonymous submissions will be relayed through your Exchange organization with this flag in an untrusted state.
ms-Exch-Accept-Headers-Routing	This permission allows the session to submit a message that has all received headers intact. If this permission isn't granted, the server will strip all received headers.
ms-Exch-Accept-Headers-Organization	This permission allows the session to submit a message that has all organization headers intact. Organization headers all start with **X-MS-Exchange-Organization-**. If this permission isn't granted, the receiving server will strip all organization headers.
ms-Exch-Accept-Headers-Forest	This permission allows the session to submit a message that has all forest headers intact. Forest headers all start with **X-MS-Exchange-Forest-**. If this permission isn't granted, the receiving server will strip all forest headers.
ms-Exch-Accept-Exch50	This permission allows the session to submit a message that contains the XEXCH50 command. This command is needed for interoperability with Exchange 2003. The XEXCH50 command provides data such as the spam confidence level (SCL) for the message.
ms-Exch-Bypass-Message-Size-Limit	This permission allows the session to submit a message that exceeds the message size restriction configured for the connector.
Ms-Exch-Bypass-Anti-Spam	This permission allows the session to bypass anti-spam filtering.

Local Network Settings

In the EMC, you use the local network settings for a Receive connector to specify the IP address and port through which the transport server accepts connections. In the Shell, use the *Bindings* parameter to specify the local IP address and port of the transport server through which the Receive connector accepts connections. These settings bind the Receive connector to a particular network adapter and TCP port on the transport server.

By default, a Receive connector is configured to use all available network adapters and TCP port 25. If a transport server has multiple network adapters, you may want a Receive connector to be bound to a particular network adapter, or to accept connections through an alternative port. For example, you may want to configure one Receive connector on the Edge Transport server to accept anonymous connections through the external network adapter. A second Receive connector can be configured to accept connections from only Hub Transport servers through the internal network adapter.

Note:

If you choose to bind a Receive connector to a specific local IP address, that IP address must be valid for the Hub Transport server or Edge Transport server on which the Receive connector is located. If you specify an invalid local IP address, the Microsoft Exchange Transport service may fail to start when the service is restarted. Instead of binding the Receive connector to a specific IP address, you can bind the Receive connector to all available IP addresses on the Hub Transport server or Edge Transport server.

Specify the IP address of the network adapter when you configure Receive connector bindings. If the Receive connector is configured to accept connections through a port other than the default, the sending client or server must be configured to send to that port and any firewalls between the message sender and the receiving server must allow network traffic through that port.

The **Local Network Settings** page of the New SMTP Receive Connector wizard in the EMC includes an option to **Specify the FQDN this connector will provide in response to HELO or EHLO**. In the Shell, this property is set by using the *Fqdn* parameter with the **Set-ReceiveConnector** cmdlet. After an SMTP session is established, an SMTP protocol conversation starts between a sending e-mail server and a receiving e-mail server. The sending e-mail server or client sends the EHLO or HELO SMTP command and its FQDN to the receiving server. In response, the receiving server sends a success code and provides its own FQDN. In Exchange 2010, you can customize the FQDN that's provided by the receiving server if you configure this property on a Receive connector. The FQDN value is displayed to connected messaging servers whenever a destination server name is required, as in the following examples:

- In the default SMTP banner of the Receive connector
- In the most recent `Received:` header field in the incoming message when the message enters the Hub Transport server or Edge Transport server
- During TLS authentication

Note:

Don’t modify the FQDN value on the default Receive connector named Default *<Server Name>* that's automatically created on Hub Transport servers. If you have multiple Hub Transport servers in your Exchange organization and you change the FQDN value on the Default *<Server Name>* Receive connector, internal mail flow between Hub Transport servers will fail.

Remote Network Settings

In the EMC, you use the remote network settings for a Receive connector to specify the IP address ranges from which this Receive connector accepts connections. In the Shell, you use the *RemoteIPRanges* parameter to specify the IP address ranges from which this Receive connector accepts connections. By default, Receive connectors are created on Hub Transport servers and Edge Transport servers that allow connections from 0.0.0.0–255.255.255.255, or from every IP address.

Note:
In Exchange 2010 , the IPv6 address range 0000:0000:0000:0000:0000:0000:0.0.0.0–ffff:ffff:ffff:ffff:ffff:ffff:255.255.255.255 also exists in the default Receive connectors on a Hub Transport server.

If you're configuring a Receive connector for a specific scenario, set the remote network settings to only the IP addresses of the servers that should be allowed the permissions and configuration settings for the Receive connector. Multiple Receive connectors can have overlapping remote IP address ranges as long as one range is completely overlapped by another. When remote IP address ranges overlap, the remote IP address range that has the most specific match to the connecting server's IP address is used.

The IP address or IP address range for the remote servers from which the Receive connector will accept inbound connections is entered in one of the following formats:

- **IP address** 192.168.1.1
- **IP address range** 192.168.1.10-192.168.1.20
- **IP address together with subnet mask** 192.168.1.0(255.255.255.0)
- **IP address together with subnet mask by using Classless Interdomain Routing (CIDR) notation** 192.168.1.0/24

Receive Connector Authentication Settings

In the EMC, you use the authentication settings for a Receive connector to specify the authentication mechanisms that are supported by the Exchange 2010 transport server. In the Shell, you use the *AuthMechanisms* parameter to specify the supported authentication mechanisms. You can configure more than one authentication mechanism for a Receive connector. For the authentication mechanisms that are automatically configured for each usage type, see the table labeled "Receive connector usage types" earlier in this topic. The following table lists the available authentication mechanisms for a Receive connector.

Receive connector authentication mechanisms

Authentication mechanism	Description
None	No authentication.
TLS	Advertise STARTTLS. Requires availability of a server certificate to offer TLS.
Integrated	NTLM and Kerberos (Integrated Windows authentication).
BasicAuth	Basic authentication. Requires an authenticated logon.
BasicAuthRequireTLS	Basic authentication over TLS. Requires a server certificate.
ExchangeServer	Exchange Server authentication (Generic Security Services application programming interface (GSSAPI) and Mutual GSSAPI).
ExternalAuthoritative	The connection is considered externally secured by using a security mechanism that's external to Exchange. The connection may be an Internet Protocol security (IPsec) association or a virtual private network (VPN). Alternatively, the servers may reside

	in a trusted physically controlled network. The `ExternalAuthoritative` authentication method requires the `ExchangeServers` permission group. This combination of authentication method and security group permits the resolution of anonymous sender e-mail addresses for messages that are received through this connector. This replaces the **Resolve anonymous senders** function in Exchange Server 2003.

Additional Receive Connector Properties

The property configuration for a Receive connector defines how e-mail is received through that connector. Not all properties are available in the EMC. For more information about the properties that can be configured by using the Shell, see Set-ReceiveConnector.

Using a Receive Connector for Anonymous Relay

Anonymous relay on Internet SMTP messaging servers is a serious security deficiency that could be exploited by unsolicited commercial e-mail senders, or spammers, to hide the source of their messages. Therefore, restrictions are placed on Internet-facing messaging servers to prevent relaying to unauthorized destinations.

In Exchange 2010, relaying is typically handled by using accepted domains. Accepted domains are configured on the Edge Transport server or Hub Transport server. The accepted domains are additionally classified as internal relay domains or external relay domains. For more information about accepted domains, see Understanding Accepted Domains.

You can also restrict anonymous relay based on the source of the incoming messages. This method is useful when an unauthenticated application or messaging server must use a Hub Transport server or an Edge Transport server as a relay server.

When you create the Receive connector that's configured to allow anonymous relay, you should place the following restrictions on the Receive connector:

- **Local network settings** Restrict the Receive connector to listen only on the appropriate network adapter on the Hub Transport server or Edge Transport server.
- **Remote network settings** Restrict the Receive connector to accept connections only from the specified server or servers. This restriction is necessary, because the Receive connector is configured to accept relay from anonymous users. Restricting the source servers by IP address is the only measure of protection that's allowed on this Receive connector.

To grant the relay permission to anonymous users on the Receive connector, you can use either of the strategies described later in this topic. Each strategy has advantages and disadvantages. For step by step instructions for both approaches, see Allow Anonymous Relay on a Receive Connector.

Granting Relay Permission to Anonymous Connections

This strategy involves the following tasks:

- Creating a Receive connector with the usage type set to `Custom`.
- Adding the Anonymous permission group to the Receive connector.

- Assigning the relay permission to the Anonymous Logon security principal on the Receive connector.

The Anonymous permission group grants the following permissions to the Anonymous Logon security principal on the Receive connector:

- Ms-Exch-Accept-Headers-Routing
- Ms-Exch-SMTP-Accept-Any-Sender
- Ms-Exch-SMTP-Accept-Authoritative-Domain-Sender
- Ms-Exch-SMTP-Submit

However, to allow anonymous relay on this Receive connector, you must also grant the following permission to the Anonymous Logon security principal on the Receive connector:

- Ms-Exch-SMTP-Accept-Any-Recipient

The advantage of this strategy is that it grants the minimum required permissions to relay to the specified remote IP addresses.

The disadvantages of this strategy are as follows:

- Additional configuration steps are required to grant the necessary permissions.
- The messages that originate from the specified IP addresses are treated as anonymous messages. Therefore, the messages don't bypass anti-spam checks, don't bypass message size limit checks, and anonymous senders can't be resolved. The process of resolving anonymous senders forces an attempted match between the anonymous sender's e-mail address and the corresponding display name in the global address list (GAL).

Configuring the Receive Connector as Externally Secured

This strategy involves the following tasks:

- Creating a Receive connector with the usage type set to `Custom`.
- Adding the ExchangeServers permission group to the Receive connector.
- Adding the `ExternalAuthoritative` authentication mechanism to the Receive connector.

The ExchangeServers permission group is required when you select the `ExternalAuthoritative` authentication mechanism. This combination of authentication method and permission group grants the following permissions to any incoming connection that's permitted on the Receive connector:

- Ms-Exch-Accept-Headers-Routing
- Ms-Exch-SMTP-Accept-Any-Sender
- Ms-Exch-SMTP-Accept-Authoritative-Domain-Sender
- Ms-Exch-SMTP-Submit
- Ms-Exch-Accept-Exch50
- Ms-Exch-Bypass-Anti-Spam
- Ms-Exch-Bypass-Message-Size-Limit
- Ms-Exch-SMTP-Accept-Any-Recipient
- Ms-Exch-SMTP-Accept-Authentication-Flag

The advantages of this strategy are as follows:

- Ease of configuration
- The messages that originate from the specified IP addresses are treated as authenticated messages. The messages bypass anti-spam checks, bypass message size limit checks, and can resolve anonymous senders.

The disadvantage of this strategy is that the remote IP addresses are considered completely trustworthy. The permissions that are granted to the remote IP addresses allow the remote messaging server to submit messages as if they originated from internal senders within your Exchange organization.

New Features in Exchange 2010 Service Pack 1

In Service Pack 1 (SP1) for Exchange Server 2010, new functionality was added to Receive connectors. This section provides an overview of these new features.

Bare Line Feed Control

When a mail server establishes an SMTP session, it issues SMTP commands to send messages. After specifying the sender and recipient information, the sending server transmits the contents of the message using the DATA command. The content that is transmitted after issuing the DATA command is known as the data stream. The data stream is terminated by a special sequence of characters: a carriage return line feed (CRLF), followed by a period, followed by another CRLF.

Line feed (LF) characters that aren't immediately preceded by carriage return (CR) characters are known as bare line feeds. Bare line feeds aren't allowed in SMTP communications. Although it may be possible for a message containing a bare line feed to be delivered successfully, such messages don't adhere to the SMTP protocol standards and may cause problems with messaging servers.

In Exchange 2010 SP1, you can configure your Receive connectors to reject any messages that contain bare line feeds in their data stream. This behavior is controlled by the *BareLineFeedRejectionEnabled* parameter of the **Set-ReceiveConnector** cmdlet. By default, this setting is disabled to maintain backwards compatibility. For more information about configuring this parameter, see Set-ReceiveConnector.

Extended Protection Capability

Windows offers channel binding to protect NTLM authentication over encrypted channels from authentication relay attacks. In Exchange 2010, all services provided by Exchange have been updated to support Extended Protection for Authentication. To support this feature in Transport, the Receive connectors have been updated. You can allow, require, or disable Extended Protection for Authentication on your Receive connectors.

You can use the *ExtendedProtectionPolicy* and *ExtendedProtectionTlsTerminatedAtProxy* parameters of the **Set-ReceiveConnector** cmdlet to control how your Transport servers handle extended protection. You can configure a Receive connector to allow or require extended protection. When you configure a Receive connector to require extended protection, any incoming connections from hosts that don't support extended protection will be rejected. To maintain backwards compatibility, the extended protection is disabled by default. For more information about configuring extended protection on your Receive connectors, see Set-ReceiveConnector.

To learn more about extended protection, see the following resources:

- Microsoft Knowledge Base article 973811, Microsoft Security Advisory: Extended protection for authentication
- MSDN Library topic, Integrated Windows Authentication with Extended Protection

1.7.1.29 Understanding Recipient Resolution

Understanding Recipient Resolution

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-25*

Recipient resolution is the process of expanding and resolving all the recipients in a message. The act of resolving the recipients matches a recipient to the corresponding Active Directory object in the Microsoft Exchange organization. The act of expanding the recipients expands all distribution groups into a list of individual recipients. Recipient resolution allows message limits and alternative recipients to be applied correctly to each recipient.

In a Microsoft Exchange Server 2010 organization, recipient resolution is performed by the categorizer on a server that has the Hub Transport server role installed. Categorization on each message happens after a newly arrived message is put in the Submission queue. Recipient resolution, in addition to content conversion and routing, is performed on the message before the message is put in a delivery queue. The categorizer performs recipient resolution before routing. The component of the categorizer that's responsible for recipient resolution is frequently called the *resolver*.

Contents

Top-Level Resolution

Top-level resolution is the first stage of recipient resolution. Top-level resolution associates each recipient in an incoming message to a matching recipient object in Active Directory. During top-level resolution, the categorizer creates a list that contains the sender and the initial, unexpanded recipient e-mail addresses that exist within the message. The categorizer then uses that list of e-mail addresses to query Active Directory to find any mail-enabled objects that have matching e-mail address attributes. When a match is found, the properties of matching Active Directory objects are cached for later use. Any sender message restrictions are also enforced.

Recipient E-mail Addresses

Top-level resolution begins with a message and the initial, unexpanded list of recipients from the *message envelope*. The message envelope contains the commands that are used to transmit messages among SMTP messaging servers. The sender's e-mail address is contained in the MAIL FROM: command. Each recipient's e-mail address is contained in a separate RCPT TO: command. The envelope sender and envelope recipients are typically created from the sender and recipients in the To:, From:, Cc:, and Bcc: header fields in the message header. However, this isn't always true. The To:, From:, Cc:, and Bcc: header fields in a message are easily forged and may not match the actual sender or recipient e-mail addresses that were used to transmit the message.

Encapsulated E-mail Addresses

Standard SMTP e-mail addresses follow the specifications of RFC 2821 and RFC 2822, such as chris@contoso.com, for example. However, an e-mail address can also be a non-SMTP e-mail address that's encapsulated inside a valid SMTP address. Exchange 2010 supports encapsulated addresses that use the Internet Mail Connector Encapsulated Address (IMCEA) encapsulation method.

This encapsulation method requires the encoding of any characters that are invalid in SMTP e-mail addresses. Alphanumeric characters, the equal sign (=) and the hyphen (-) don't require encoding. Other characters use the following encoding syntax:

- A forward slash (/) is replaced by an underscore (_).
- Other US-ASCII characters are replaced by a plus sign (+) and the two digits of its ASCII value are written in hexadecimal. For example, the space character has the encoded value +20.

The IMCEA encapsulation method uses the following syntax: `IMCEA<Type>-<address>@<domain>`

The placeholder <*Type*> identifies the type of non-SMTP address, for example EX, X400, or FAX.

Note:
Although SMTP and X500 are theoretically valid values for <*Type*>, Exchange 2010 recipient resolution rejects any IMCEA-encoded addresses that use either of these types.

The placeholder <*address*> is the encoded original address. The placeholder <*domain*> represents the SMTP domain that's used to encapsulate the non-SMTP address, for example, contoso.com

With the IMCEA encapsulation method, addresses are unencapsulated only when the domain matches the default authoritative domain in the Exchange organization. For more information about accepted domains, see Understanding Accepted Domains.

The maximum length for an SMTP e-mail address in Exchange 2010 is 571 characters. This limit includes the following:

- 315 characters for the name part of the address
- 255 characters for the domain name
- The at sign (@) character that separates the name part of the address from the domain name

Currently, Exchange 2010 doesn't support messages that are encoded with the IMCEA encapsulation method when the name part of the address exceeds 315 characters.

Address Resolution

For each message, the sender e-mail address and all recipient e-mail addresses are added to a list that's used to query Active Directory. Any encapsulated addresses are unencapsulated before they're added to the list of e-mail addresses. The Active Directory query is performed on up to 20 e-mail addresses at a time. If the Active Directory query encounters any transient errors, the message is returned to the Submission queue and deferred for the time that's specified by the *ResolverRetryInterval* parameter in the EdgeTransport.exe.config application configuration file. The default value is 30 minutes.

The following table describes the recipient objects that are found in Active Directory. For more information about Exchange 2010 recipient types, see Understanding Recipients.

Recipient objects in Active Directory

Active Directory recipient type	Description
DistributionGroup	Any mail-enabled group object. The distribution group object types are as follows: • **MailUniversalDistributionGroup** A

	universal distribution group object • **MailUniversalSecurityGroup** A universal security group (USG) object that has an e-mail address • **MailNonUniversalGroup** A local security group object or global security group object that has an e-mail address
DynamicDistributionGroup	An object that has the Active Directory class **msExchDynamicDistributionList**. For more information, see Create a Dynamic Distribution Group.
Mailbox	A user object that has an e-mail address and a defined *Database* parameter
MailUser	A user object that has an e-mail address without a defined *Database* parameter. For more information, see Create a Mail User.
MailContact	A contact object that has an e-mail address. Typically, a mail contact is used for recipients outside the Exchange organization. A mail contact is also used in cross-forest Exchange environments. For more information, see Create a Mail Contact.
MailPublicFolder	A public folder object that has an e-mail address.
MicrosoftExchangeRecipient	An object that has the Active Directory class **msExchExchangeServerRecipient**. For more information about the Exchange recipient object, see Understanding the Microsoft Exchange Recipient.
PublicDatabase	An object that has the Active Directory class **msExchPublicMDB**.
SystemAttendantMailbox	An object that has the Active Directory class **exchangeAdminService**. There should be only one system attendant mailbox in the Exchange 2010 organization.
SystemMailbox	A user object that has an e-mail address and that's located in the Microsoft Exchange System Objects container. There should be one system mailbox for each mailbox database in the Exchange 2010 organization.

An object that contains missing or malformed critical properties is classified by the Active Directory query as an invalid object. For example, a dynamic distribution group object without an e-mail address is considered invalid. Messages that are sent to recipients that are classified as invalid objects generate a non-delivery report (NDR).

For each e-mail address, a single initial query is performed for all possible recipient properties, such as the recipient identifiers, recipient type, message limits, e-mail addresses, and alternative recipients. The applicable properties for the recipient are cached for later use. Recipient resolution classifies the recipients based on similarities in how the recipients are resolved, and the similarity of the applicable recipient properties.

The LDAP filter that's used for address resolution is described as follows:

- For the EX e-mail address type, the LDAP filter is based on the recipient **legacyExchangeDN** Active Directory attribute or the recipient **proxyAddresses** Active Directory attribute. The **legacyExchangeDN** Active Directory attribute takes precedence.
- For all other e-mail addresses types, the recipient **proxyAddresses** Active Directory attribute is used as the LDAP filter.

If the e-mail address that's used in the message doesn't match the primary SMTP address of the corresponding Active Directory object, the categorizer rewrites the e-mail address in the message to match the primary SMTP address. The original e-mail address is saved in the *ORCPT*= parameter in the RCPT TO: command in the message envelope.

Sender Message Restrictions

The size that's used for the sender message size restriction is the value of the `X-MS-Exchange-Organization-OriginalSize:` header field in the message header. Exchange 2010 uses this header field to record the original message size of the message when it entered the Exchange 2010 organization. Whenever the message is checked against the specified message size limits, the lower value of the current message size or the original message size header is used. The size of the message can change because of content conversion, encoding, and agent processing. If this header field doesn't exist, it's created by using the current message size value. If the message is too large, an NDR is generated and additional message processing is stopped.

The sender recipient limit is only enforced on the first Hub Transport server that processes the message. The original, unexpanded message envelope recipient count is compared to the sender recipient limit. The original, unexpanded message envelope recipient count is used to avoid the partial message delivery problems that occur in Microsoft Exchange Server 2003 when nested distribution lists used remote expansion servers.

The message sender and all recipients are marked as resolved by stamping an extended property in the message. This extended property allows the message to bypass top-level resolution if the message must go through recipient resolution again. A message may have to go through recipient resolution again because the Microsoft Exchange Transport service restarted.

Return to top

Expansion

Expansion occurs after top-level resolution. Expansion completely expands nested levels of recipients into individual recipients. Expansion may require multiple trips through the expansion process to expand all recipients. Not all recipients have to be expanded. However, all recipients must go through the expansion process. The expansion process also enforces recipient message restrictions for all kinds of recipients.

The following list describes the kinds of recipients that require expansion:

- **Distribution groups and dynamic distribution groups** Distribution groups are expanded based on the **memberOf** Active Directory property. Dynamic distribution groups are expanded by using the Active Directory query definition. If the *ExpansionServer* parameter is set on the group, the group isn't expanded by the current server. The distribution group is routed to the specified server for expansion.

Note:

If you select a specific Hub Transport server in your organization as the expansion server, the distribution group usage becomes dependent on the availability of the expansion server. If the expansion server is unavailable, any messages that are sent to the distribution group can't be delivered. If you plan to use specific expansion servers for your distribution groups, to

reduce the risk of service interruption, you should consider implementing high availability solutions for these servers.

- **Alternative recipients** The *ForwardingAddress* parameter may be set on mailboxes and mail-enabled public folders. The *ForwardingAddress* parameter redirects all messages to the specified alternative recipient. This is known as a *forwarded recipient*. When an alternative delivery address is specified in the *ForwardingAddress* parameter and the *DeliverToMailboxAndForward* parameter is set to `$true`, the message is delivered to the original recipient and the alternative recipient. This is known as *delivered and forwarded recipient*.
- **Contact chains** A *contact chain* is a mail user or mail contact that has the *ExternalEmailAddress* parameter set to the e-mail address of another recipient in the Exchange organization.

Detection of Recipient Loops

As the distribution groups, alternative recipients, and contacts chains are expanded, the categorizer checks for *recipient loops*. A recipient loop is a recipient configuration problem that causes message delivery to the same recipients in an endless circle. The following list describes the different types of recipient loops:

- **Harmless recipient loop** A harmless recipient loop results in successful message delivery. The following list describes two scenarios when harmless recipient loops occur:
  - When two distribution groups contain one another as members.
  - When mailboxes or mail-enabled public folders are set to deliver and forward to one another. This happens when the *DeliverToMailboxAndForward* parameter of both recipients is set to `$true` and the *ForwardingAddress* parameter is set to one another.

  When a harmless recipient loop is detected, the message is delivered to the recipient, but no additional attempts are made to deliver the message to the same recipient.
- **Broken recipient loop** A broken recipient loop can't result in successful message delivery. An example of a broken recipient loop is when mailboxes or mail-enabled public folders have the *ForwardingAddress* parameter set to one another. When the categorizer detects a broken recipient loop, expansion activity for the current recipient stops, and an NDR is generated for the recipient.

Detection of recipient loops doesn't prevent duplicate message delivery. For example, Distribution Group C will experience duplicate message delivery if the following conditions are true:

- Distribution Group B and Distribution Group C are members of Distribution Group A.
- Distribution Group C is also a member of Distribution Group B.

Delivery Report Redirection for Distribution Groups

When a distribution group is expanded, the message type is checked to determine whether it's a delivery report message. If the message is a delivery report, the redirection settings of the distribution group are checked to determine whether redirection of the delivery report is required. You may want to suppress the delivery reports because the delivery reports may disclose unwanted information about the distribution group and its membership.

The following list describes the delivery report redirection settings that are available for distribution groups and dynamic distribution groups:

- **ReportToManagerEnabled** This parameter enables delivery reports to be sent to the distribution group manager. Valid values are `$true` or `$false`. The default value is `$false`. For a distribution group, the manager is controlled by the *ManagedBy* parameter in the **Set-Group** cmdlet. For a dynamic distribution group, the manager is controlled by the *ManagedBy* parameter in the **Set-**

DynamicDistributionGroup cmdlet.

- **ReportToOriginatorEnabled** This parameter enables delivery reports to be sent to the sender of e-mail messages that are sent to this distribution group. Valid values are `$true` or `$false`. The default value is `$true`.

Note:

The values of the *ReportToManagerEnabled* parameter and *ReportToOriginatorEnabled* parameter can't both be `$true`. If one parameter is set to `$true`, the other must be set to `$false`. The values of both parameters can be `$false`. This suppresses all redirection of all delivery report messages.

The following list describes the available delivery report messages:

- **Delivery receipt (DR)** This report confirms that a message was delivered to its intended recipient.
- **Delivery status notification (DSN)** This report describes the result of an attempt to deliver a message. For more information about DSN messages, see Managing Delivery Status Notifications.
- **Message disposition notification (MDN)** This report describes the status of a message after it has been successfully delivered to a recipient. A read notification (RN) and a non-read notification (NRN) are both examples of an MDN message. MDN messages are defined in RFC 2298 and are controlled by the `Disposition-Notification-To:` header field in the message header. MDN settings that use the `Disposition-Notification-To:` header field are compatible with many different message servers. MDN settings can also be defined by using MAPI properties in Microsoft Outlook and Exchange.
- **Non-delivery report (NDR)** This report indicates to the message sender that the message couldn't be delivered to the specified recipients.
- **Non-read notification (NRN)** This report indicates that a message was deleted before it was read.
- **Out of office (OOF)** This report indicates that the recipient won't respond to e-mail messages. The acronym OOF dates back to the original Microsoft messaging system where the corresponding notification was named "out of facility."
- **Read notification (RN)** This report indicates that a message was read.
- **Recall Report** This report indicates the status of a recall request for a specific recipient. A recall request is when a sender tries to recall a sent message by using Outlook.

When a delivery report message is sent to a distribution group, the following settings cause the report message to be deleted:

- Report redirection isn't set. Alternatively, report redirection is set to the message sender.
- Report redirection is set to the distribution group manager, and the delivery report message isn't an NDR.

When a delivery report message is sent to a distribution group, the following setting causes the delivery report message to be delivered to the distribution group manager:

- Report redirection is set to the distribution group manager, and the report message is an NDR.

When a message that isn't a delivery report message is sent to a distribution group, the message is delivered to the distribution group members. The report request settings are summarized in the following list:

- If report redirection is set to the message sender, the report request settings aren't modified.
- If report redirection isn't set, all report request settings are suppressed. The *NOTIFY=NEVER* parameter is added to RCPT TO: for each recipient in the message envelope.

- If report redirection is set to the distribution group manager, all report request settings are suppressed except NDR messages that are sent to the distribution group manager.

Message Restrictions on Recipients

The expansion process also enforces any message restrictions that are configured for recipients. These restrictions may be configured individually for each recipient or organizationally for all Hub Transport servers in the Exchange organization. The following table describes the message restrictions that are configured for recipients.

Message restrictions on recipients

Source	Parameter	Description
Set-DistributionGroup **Set-DynamicDistributionGroup** **Set-Mailbox** **Set-MailContact** **Set-MailPublicFolder** **Set-MailUser** **Set-TransportConfig**	*MaxReceiveSize*	The *MaxReceiveSize* parameter specifies the size that's used for message restrictions that are configured for recipients is the value of the `X-MS-Exchange-Organization-OriginalSize:` header field in the message header. Exchange 2010 uses this header field to record the original message size of the message when it entered the Exchange 2010 organization. Whenever the message is checked against the specified message size limits, the lower value of the current message size or the original message size header is used. The size of the message can change because of content conversion, encoding, and agent processing. If this header field doesn't exist, it's created by using the current message size value. If the message is too large, an NDR is generated and additional message processing is stopped.
Set-DistributionGroup **Set-DynamicDistributionGroup** **Set-Mailbox** **Set-MailContact** **Set-MailPublicFolder** **Set-MailUser**	*RequireSenderAuthenticationEnabled*	The *RequireSenderAuthenticationEnabled* parameter requires that all messages that are sent to the recipient come from authenticated senders. When the value of this parameter is set to `$true`, messages from unauthenticated senders are rejected. All senders who send messages to the System and System Attendant mailboxes must be

		authenticated.
Set-DistributionGroup **Set-DynamicDistributionGroup** **Set-Mailbox** **Set-MailContact** **Set-MailPublicFolder** **Set-MailUser**	*AcceptMessagesOnlyFrom* *AcceptMessagesOnlyFromDLMembers* *RejectMessagesFrom* *RejectMessagesFromDLMembers*	The *AcceptMessagesOnlyFrom* parameter specifies the senders who can send e-mail messages to the recipient. The *AcceptMessagesOnlyFromDLMembers* parameter specifies the distribution groups that can send e-mail messages to the recipient. The *RejectMessagesFrom* parameter specifies the senders that can't send e-mail messages to this recipient. The *RejectMessagesFromDLMembers* parameter specifies the distribution groups that can't send e-mail messages to the distribution group. The categorizer checks the recipient permission in two passes. The first pass determines whether the sender is present in the *AcceptOnlyMessagesFrom* or *RejectMessagesFrom* parameter. If the sender isn't found in either parameter, the recipients in the *AcceptMessagesOnlyFromDLMembers* and *RejectMessagesFromDLMembers* parameters are fully expanded. This complete expansion of distribution groups may take some time. We recommend that you minimize the depth of nested distribution groups in the *AcceptMessagesOnlyFromDLMembers* parameter and the *RejectMessagesFromDLMembers* parameters.

Certain types of messages that are sent by authenticated senders are exempt from restrictions. The following list describes the messages that are exempt from recipient restrictions:

- **All messages that are sent by the Microsoft Exchange recipient** These messages include DSN messages, journal reports, quota messages, and other system-generated messages that are sent to internal message senders. For more information about the Microsoft Exchange recipient, see Understanding

the Microsoft Exchange Recipient.

- **Public folder replication messages** These messages are sent by a public database sender.
- **All messages that are sent by the external postmaster address** These messages include DSN messages and other system-generated messages that are sent to external message senders. For more information about the external postmaster address, see Configure the External Postmaster Address.

Certain types of messages are blocked when they are sent from the Exchange organization to external domains. The settings are controlled by the following parameters in the **Set-RemoteDomain** cmdlet:

- *AllowedOOFType*
- *AutoForwardEnabled*
- *AutoReplyEnabled*
- *DeliveryReportEnabled*
- *NDREnabled*

For more information, see Understanding Remote Domains.

Return to top

Bifurcation and Controlling Recipient Expansion

Because the complete list of message recipients is expanded and resolved by recipient resolution, there are occasions when different copies of the same message must be created. These occasions are described by the following scenarios:

- **When message recipients require different message settings** Message properties such as read receipts may have to be enabled for some recipients and blocked for other recipients. Creating a new version of the message that has slightly different properties than the original message is called *bifurcation*.
- **To limit the number of envelope recipients in a single message** The recipient expansion process can generate thousands of individual recipients when large distribution groups are expanded. In Exchange 2010, instead of creating a single copy of the message that has thousands of envelope recipients, multiple copies of the same message that have a limited number of envelope recipients are created.

Bifurcation

Recipient resolution bifurcates a message if the following conditions are true:

- When the message sender in MAIL FROM:, in the message envelope, is updated. An example is when the *ReportToManagerEnabled* parameter on a distribution group has a value of `$true`.
- When auto-response messages, such as DSNs, OOF messages, and recall reports must be suppressed.
- When alternative recipients are expanded.
- When a `Resent-From:` header field must be added to the message header. Resent header fields are informational header fields that can be used to determine whether a message has been forwarded by a user. Resent header fields are used so that the message appears to the recipient as if it was sent directly by the original sender. The recipient can view the message header to discover who forwarded the message. Resent header fields are defined in section 3.6.6 of RFC 2822.
- When the history of the expansion of the distribution group must be transmitted.

Controlling Recipient Expansion

When the number of expanded recipients is too large, the categorizer splits the message into multiple copies. This is performed to reduce system resource use during message expansion. The maximum number of envelope recipients in a message is controlled by the *ExpansionSizeLimit* parameter in the EdgeTransport.exe.config application configuration file. The default value is 1000.

Caution:

We recommend that you don't modify the value of the *ExpansionSizeLimit* parameter on an Exchange transport server in a production environment.

Return to top

Recipient Resolution Diagnostics

Reporting and diagnostic information for recipient resolution is provided by performance counters, message tracking log entries, and recipient resolution logging. These sources can help you identify and diagnose problems with recipient resolution.

Recipient Resolution Performance Counters

The following table describes the performance counters that are available for recipient resolution.

Recipient resolution performance counters

Counter name	Display name	Description
AmbiguousRecipientsTotal	Ambiguous Recipients	This is the total number of ambiguous recipients that were detected during recipient resolution. Ambiguous recipients are different recipients that have matching **legacyExchangeDN** Active Directory attributes or matching **proxyAddresses** Active Directory attributes.
AmbiguousSendersTotal	Ambiguous Senders	This is the number of ambiguous senders that were detected during recipient resolution. Ambiguous senders are different senders that have matching **legacyExchangeDN** Active Directory attributes or matching **proxyAddresses** Active Directory attributes.
FailedRecipientsTotal	Failed Recipients	This is the number of failed recipients that were detected during recipient resolution.
LoopRecipientsTotal	Loop Recipients	This is the number of recipients that failed recipient resolution because of recipient loops.
MessagesChippedTotal	Messages Chipped	This is the total number of copies of the same message that were created during

		recipient resolution to control the number of envelope recipients in a single message. In Exchange 2010, this process is referred to as *chipping*.
MessagesCreatedTotal	Messages Created	This is the number of messages that were created during recipient resolution.
MessagesRetriedTotal	Messages Retried	This is the number of messages that were scheduled for retry during recipient resolution.
UnresolvedOrgRecipientsTotal	Unresolved Org Recipients	This is the number of unresolved recipients from an authoritative domain that were detected during recipient resolution.
UnresolvedOrgSendersTotal	Unresolved Org Senders	This is the number of unresolved senders from an authoritative domain that were detected during recipient resolution.

Recipient Resolution Events That Are Written in the Message Tracking Log

The following table describes the recipient resolution events that are written in the message tracking log.

Recipient resolution events in the message tracking log

Message tracking event	Description
EXPAND	This event indicates that a distribution group was expanded.
REDIRECT	This event indicates that a message sent to a mailbox recipient or a mail-enabled public folder recipient was redirected to an alternative recipient as specified by the *ForwardingAddress* parameter.
RESOLVE	This event indicates that a recipient e-mail address was changed to the primary SMTP e-mail address of the corresponding Active Directory recipient object.
TRANSFER	This event indicates that message bifurcation or chipping occurred.

For more information about message tracking, see Understanding Message Tracking.

Recipient Resolution Logging

Recipient resolution logging is controlled by the *ResolverLogLevel* parameter in the EdgeTransport.exe.config application configuration file. The valid values for this parameter are `Disabled`, `Enabled`, and `FullContent`. The default value is `Disabled`. When the *ResolverLogLevel* parameter is set to `Enabled`, only message envelope data is logged.

When the *ResolverLogLevel* parameter is set to `FullContent`, message envelope data and message header data is logged.

Return to top

1.7.1.30 Understanding Remote Domains

Understanding Remote Domains

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can create remote domain entries to define the settings for message transfer between the Microsoft Exchange Server 2010 organization and domains outside your Active Directory forest. When you create a remote domain entry, you control the types of messages that are sent to that domain. You can also apply message format policies and acceptable character sets for messages that are sent from users in your organization to the remote domain. The settings for remote domains are global configuration settings for the Exchange organization.

The remote domain settings are applied to messages during categorization. When recipient resolution occurs, the recipient domain is matched against the configured remote domains. If a remote domain configuration blocks a specific message type from being sent to recipients in that domain, the message is deleted. If you specify a particular message format for the remote domain, the message headers and content are modified. Information about the remote domain configuration is stored in Active Directory. The settings apply to all messages that are processed by the Exchange organization.

Note:

If you configure message settings per user, the per-user settings override the organizational configuration.

By default, there's a single remote domain entry. The domain address space is configured as an asterisk (*). This represents all domains. If you don't create additional remote domain entries, all messages that are sent to all recipients in all remote domains have the same settings applied to them.

When you configure remote domains, you can prevent certain types of messages from being sent to that domain. These message types include out-of-office messages, auto-reply messages, non-delivery reports (NDRs), and meeting forward notifications. If you have a multiple forest environment, you may want to allow the sending of those types of messages to those domains. However, if you have identified a domain from which spam originates, you may want to block sending of those types of messages to those remote domains.

Message Format

You can specify the message format and the character set to use for e-mail messages that are sent to remote domains. These settings can be useful to make sure that e-mail sent by senders in your domain to the remote domain is compatible with the receiving e-mail system. For example, if you know that the remote domain's messaging system is Exchange, you can specify to always use Exchange rich text format (RTF). For more information, see Understanding Content Conversion.

Automatic Replies Settings

Automatic replies, formerly known as out-of-office replies, have changed substantially starting with Exchange Server 2007. In Exchange 2010 and Exchange 2007, users can specify different automatic replies for internal and external recipients. Furthermore, the types of automatic replies available in your organization also depend on the Microsoft Outlook version in use.

In Exchange 2010, there are three types of automatic replies:

- **External** Supported by Exchange 2010 and Exchange 2007. Can only be set by Outlook 2010 or Office Outlook 2007, or using Microsoft Office Outlook Web App.
- **Internal** Supported by Exchange 2010 and Exchange 2007. Can only be set by Outlook 2010 or Outlook 2007, or using Outlook Web App.
- **Legacy** Supported by Exchange 2010, Exchange 2007, and Exchange Server 2003. Can be set by Office Outlook 2003 or earlier.

The following table describes various client and server combinations and the types of automatic replies that can be used in each scenario.

Client and server support for automatic replies

Client version	Exchange version	Automatic replies supported
Outlook 2010 or Outlook 2007	Exchange 2010 Exchange 2007	Internal, External
Outlook Web App	Exchange 2010 Exchange 2007	Internal, External
Outlook 2003	Exchange 2010 Exchange 2007	Legacy
Outlook 2010, Outlook 2007, or Outlook 2003	Exchange 2003	Legacy
Outlook Web Access	Exchange 2003	Legacy

For a remote domain, you can specify one of the following options for sending automatic replies:

- **Allow none** If you select this option, no automatic replies are sent to recipients in the remote domain.
- **Allow external out-of-office messages only** If you select this option, only External automatic replies are sent to the remote domain.
- **Allow external out-of-office messages and legacy out-of-office messages (configured by using Outlook 2003 or earlier clients, or configured on Exchange 2003 mailboxes)** If you select this option, both External and Legacy automatic replies are sent to the remote domain.
- **Allow internal out-of-office messages, and legacy out-of-office messages (configured by using Outlook 2003 or earlier clients, or configured on Exchange 2003 mailboxes)** If you select this option, both Internal and Legacy automatic replies are sent to the remote domain.

Controlling NDR Information

As mentioned at the beginning of this topic, you can prevent NDRs from being sent to a remote domain. By blocking NDRs to a remote domain, you can prevent the information contained within the NDR message from leaving your organization, thereby limiting the knowledge a malicious user can obtain about your organization. However, this also

prevents legitimate senders from receiving NDRs, resulting in confusion and lost productivity.

Exchange 2010 SP1 provides you with more granular control over the contents of an NDR destined for a remote domain. With Exchange 2010 SP1, you can now allow NDRs to a remote domain, while stripping any diagnostic information. This way, you can still prevent information about your Exchange deployment from leaving your organization while at the same time providing NDR notifications to external senders.

This feature is controlled with the new *NDRDiagnosticInfoEnabled* parameter of the **Set-RemoteDomain** cmdlet. Because this setting is configurable for each remote domain, you can have different settings based on your needs. For example, you can choose to remove the NDR diagnostic information for the default remote domain, but allow full NDR diagnostic information for the remote domains that represent your partners.

For more information about this new settings, see Set-RemoteDomain.

Remote Domains in Cross-Premises Deployments

Exchange 2010 SP1 supports cross-premises deployments where your Exchange organization is split between your on-premises servers and a cloud-based service such as Microsoft Office 365. In this deployment scenario, a remote domain object represents the part of your organization that exists in the cloud-based service. This remote domain is different from all the other remote domains you may have because it's considered an internal remote domain.

You can use either the Shell or the EMC to designate a remote domain as your Office 365 deployment. For detailed steps, see Configure Remote Domain Properties.

1.7.1.31 Understanding Send Connectors

Understanding Send Connectors

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Send connectors are configured on computers that are running Microsoft Exchange Server 2010 and that have the Hub Transport server role or Edge Transport server role installed. The Send Connector represents a logical gateway through which outbound messages are sent. This topic provides an overview of Send connectors and explains how the configuration of Send connectors affects the processing of individual messages.

Overview of Send Connectors

Exchange 2010 transport servers require Send connectors to deliver messages to the next hop on the way to their destination. A Send connector controls outbound connections from the sending server to the receiving server or destination e-mail system. By default, no explicit Send connectors are created when the Hub Transport server role or the Edge Transport server role is installed. However, implicit and invisible Send connectors that are automatically computed based on the Active Directory site topology are used to route messages internally between Hub Transport servers. End-to-end mail flow is only possible after the Edge Transport server has been subscribed to the Active Directory site

by using the Edge Subscription process. Other scenarios, such as an Internet-facing Hub Transport server or an unsubscribed Edge Transport server, require manual configuration of connectors to establish end-to-end mail flow. For more information, see Transport Server Post-Deployment Tasks.

Send connectors that are created on Hub Transport servers are stored in Active Directory and are available to all Hub Transport servers in the organization. If a Send connector is configured to send messages to an external domain, any Hub Transport server in the organization will route a message for that domain to a source server for that connector to be relayed to the destination domain.

The Send connector that's used to route messages to a recipient is selected during the routing resolution phase of message categorization. For more information, see Understanding Message Routing.

Selecting the Usage Type for a Send Connector

When you use the Exchange Management Console (EMC) to create a Send connector, the New SMTP Send Connector wizard prompts you to select a usage type for the connector. The usage type determines the default permission sets that are assigned on the connector and grants those permissions to trusted security principals. Security principals include users, computers, and security groups. A security principal is identified by a security identifier (SID).

You can also specify a usage type when you create a Send connector by using the **New-SendConnector** cmdlet in the Exchange Management Shell. However, the *Usage* parameter isn't required. If you don't specify a usage type when you run the **New-SendConnector** cmdlet, the default usage type is set to Custom. The following table describes the Send connector usage types and their default settings.

Send connector usage types

Type	Default permissions	SID that's granted the default permissions	Default smart host authentication mechanism
Custom	None	None	None
Internal	• ms-Exch-Send-Headers-Organization • ms-Exch-SMTP-Send-Exch50 • ms-Exch-Send-Headers-Routing • ms-Exch-Send-Headers-Forest	• Hub Transport servers • Edge Transport servers • Exchange Servers (on Hub Transport servers only) • Externally Secured servers • Exchange Legacy Interop universal security group • Exchange Server 2003 and Exchange 2000 Server bridgehead servers	Exchange Server Authentication

Internet	Ms-Exch-Send-Headers-Routing	Anonymous User Account	None
Partner	Ms-Exch-Send-Headers-Routing	Partner Servers	Not applicable. This usage type is selected when you establish mutual Transport Layer Security (TLS) authentication with a remote domain.

Note:
If Domain Name System (DNS) resolution delivery is selected for a Send connector instead of a smart host, no smart host authentication mechanism is configured.

The Send connector permissions and smart host authentication mechanisms are discussed in detail later in this topic.

Send Connector Usage Scenarios

Each usage type is appropriate for a specific connection scenario. Select the usage type that has the default settings most applicable to the configuration that you want. You can modify permissions by using the **Add-ADPermission** and **Remove-ADPermission** cmdlets. For more information, see the following topics:

- Add-ADPermission
- Remove-ADPermission

The following table lists common connection scenarios and the usage type for each scenario.

Connector usage scenarios

Connector scenario	Usage type	Comment
Edge Transport server that sends e-mail to the Internet	Internet	A Send connector that's configured to send e-mail to all domains is created automatically when the Edge Transport server is subscribed to the Exchange organization.
Hub Transport server that sends e-mail to the Internet	Internet	This isn't a recommended configuration.
A subscribed Edge Transport server that sends e-mail to a Hub Transport server	Internal	This connector is automatically created by the Edge Subscription process.
Edge Transport server that sends e-mail to an Exchange 2003 bridgehead server	Internal	The Exchange 2003 bridgehead server is configured as a smart host for the Send connector.
Edge Transport server that sends e-mail to a	Custom	When the Edge Subscription process isn't used, a manual connector must

Hub Transport server		be created. Use the **Add-ADPermission** cmdlet to set the extended rights. Set the authentication mechanism as Basic authentication or Externally Secured.
Cross-forest Send connector for a Hub Transport server in one forest that sends e-mail to an Exchange 2010 or Exchange 2007 Hub Transport server in a second forest	Custom	For detailed configuration steps, see Configure Cross-Forest Connectors.
Cross-forest Send connector for a Hub Transport server in one forest that sends e-mail to an Exchange 2003 bridgehead server in a second forest	Custom	For detailed configuration steps, see Configure Cross-Forest Connectors.
Hub Transport server that sends e-mail to a third-party smart host	Custom	Use the **Add-ADPermission** cmdlet to set the extended rights. Route all messages to a smart host and set the authentication mechanism to either Basic authentication or Externally Secured.
Edge Transport server that sends e-mail to a third-party smart host	Custom	Use the **Add-ADPermission** cmdlet to set the extended rights. Route all messages to a smart host and set the authentication mechanism to either Basic authentication or Externally Secured.
Edge Transport server that sends e-mail to an external relay domain	Custom	The Edge Transport server can accept e-mail for an external relay domain and then relay the messages to the authoritative e-mail system for that domain. Route all messages to a smart host, set the appropriate authentication mechanism, and use the **Add-ADPermission** cmdlet to set the extended rights.
Edge Transport server that sends e-mail to a domain to which you have established mutual TLS authentication	Partner	Mutual TLS authentication functions correctly only if the following conditions are true: • The value of the *DomainSecureEnabled* parameter must be `$true`. • The value of the *DNSRoutingEnabled* parameter must be `$true`. • The value of the *IgnoreStartTLS* parameter must be `$false`.

		For more information, see Set-SendConnector.

Send Connector Permissions

You assign Send connector permissions to a security principal. When a security principal establishes a session with a Send connector, the Send connector permissions determine the types of header information that can be sent with the e-mail message. If an e-mail message includes header information that isn't allowed by the Send connector permissions, those headers are stripped from the message when it's sent. The following table describes the permissions that can be assigned on a Send connector to security principals. You can't set Send connector permissions by using the EMC. To modify the default permissions for a Send connector, you must use the **Add-ADPermission** cmdlet in the Shell.

Send connector permissions

Send connector permission	Description
ms-Exch-Send-Exch50	This permission allows the session to send a message that contains the EXCH50 command. If this permission isn't granted, and a message is sent that contains the EXCH50 command, the server sends the message, but doesn't include the EXCH50 command.
Ms-Exch-Send-Headers-Routing	This permission allows the session to send a message that has all received headers intact. If this permission isn't granted, the server removes all received headers.
Ms-Exch-Send-Headers-Organization	This permission allows the session to send a message that has all organization headers intact. Organization headers all start with **X-MS-Exchange-Organization-**. If this permission isn't granted, the sending server removes all organization headers.
Ms-Exch-Send-Headers-Forest	This permission allows the session to send a message that has all forest headers intact. Forest headers all start with **X-MS-Exchange-Forest-**. If this permission isn't granted, the sending server removes all forest headers.

Address Spaces and Connector Scope

The address space for a Send connector specifies the recipient domains to which the Send connector will route e-mail. You can specify SMTP address spaces or non-SMTP address spaces on Send connectors that are configured on Hub Transport servers. You can only specify SMTP address spaces on Send connectors that are configured on Edge Transport servers. If you use a non-SMTP address space type, you must use a smart host to route e-mail.

Note:
Although you can configure non-SMTP address spaces on a Send connector on a Hub Transport server, the Send connector uses SMTP as the transport mechanism to send

messages to other messaging servers. Delivery Agent connectors and foreign connectors on Hub Transport servers are used to send messages to non-SMTP local messaging servers, such as third-party fax gateway servers. For more information, see Understanding Delivery Agents and Understanding Foreign Connectors.

The following table lists valid entries for the SMTP address space of a Send connector.

Valid entries for the SMTP address space of a Send connector

Address space entry	Send connector routes mail to:
*	All domains that don't have an explicit address space entry on another Send connector entry or that aren't an included subdomain of an address space on another Send connector.
Contoso.com	All recipients with e-mail addresses in the Contoso.com domain.
*.Contoso.com	All recipients with e-mail addresses in the Contoso.com domain or any subdomain of Contoso.com. In the EMC, select **Include all subdomains** to set this configuration.
--	This address space is only used on Send connectors configured on Edge Transport servers for sending messages to the Hub Transport servers. When you use this address space, all messages addressed to your accepted domains are routed through this connector.

During routing resolution, a Send connector, to which e-mail is routed for delivery to the destination address space, is selected. The Send connector whose address space most closely matches the recipient's e-mail address is selected. For example, an e-mail message addressed to Recipient@marketing.contoso.com would be routed through the connector that's configured to use the *.Contoso.com address space. When you configure a Send connector for a particular address space, e-mail sent to that address space is always routed through that connector. Also, the configuration settings for that connector are always applied to e-mail sent to that address space.

You can use the scope of a Send connector to control the visibility of the Send connector within the Exchange organization. By default, all Send connectors that you create are usable by all the Hub Transport servers in the Exchange organization. However, you can limit the scope of any Send connector so that it's only usable by other Hub Transport servers that exist in the same Active Directory site.

In Exchange 2010, the complete syntax for specifying an address space is as follows:

<AddressSpaceType>:*<AddressSpace>*;*<AddressSpaceCost>*

You can use the following methods to specify the scope of the Send connector:

- In the EMC, use the **Scoped Send connector** property in the **Address Space** page of the New SMTP Send Connector wizard, or in the **Address Space** tab in the properties of an existing Send connector.
  When **Scoped Send connector** is selected, the connector can only be used by Hub Transport servers in the same Active Directory site. When **Scoped Send connector** isn't selected, the connector can be used by all Hub Transport servers in the Exchange organization.

- In the Shell, use the *IsScopedConnector* parameter in the **New-SendConnector** cmdlet or the **Set-SendConnector** cmdlet.
  When the value of this parameter is `$true`, the connector can only be used by Hub Transport servers in the same Active Directory site. When the value of this parameter is `$false`, the connector can be used by all Hub Transport servers in the Exchange organization.

Network Settings

You can set Send connectors so that they deliver e-mail by using DNS address resolution or by routing the e-mail to a smart host.

Using DNS to Route E-Mail

When the Send connector is set to use DNS MX resource records to route mail automatically, the DNS client on the source server must be able to resolve public DNS records. By default, the DNS server that's configured on the source server's internal network adapter is used for name resolution. You can configure a specific DNS server to use for internal and external DNS lookups by using the EMC to modify the DNS settings on the Exchange server properties. You can also use the Shell to configure the parameters in the **Set-TransportServer** cmdlet.

If you configure a specific DNS server on the transport server to use for external DNS lookups, you must select **Use the external DNS lookup settings on the transport server** on the **Network Settings** page of the New SMTP Send Connector wizard or, in the Shell, on the **Set-TransportServer** cmdlet, set the *UseExternalDNSServersEnabled* parameter to `$true`. The *DnsRoutingEnabled* parameter on the Send connector must also be set to `$true`.

For more information, see the following topics:

- Configure Edge Transport Server Properties
- Configure Hub Transport Server Properties
- Set-TransportServer

Using a Smart Host to Route E-Mail

If you select the Internal usage type for the Send connector, you must specify a smart host. When you route mail through a smart host, the smart host handles delivery to the next hop in the delivery destination. You can use an IP address or the fully qualified domain name (FQDN) of the smart host to specify the smart host identity. The smart host identity can be the FQDN of a smart host server, an MX record, or an A (address) resource record. If you configure an FQDN as the smart host identity, the source server for the Send connector must be able to use DNS name resolution to locate the smart host server.

The smart host for a Send connector with the Internet usage type may be a server that's hosted by your Internet service provider. The smart host for a Send Connector with the Custom or Internal usage types may be another e-mail server in your organization or an e-mail server in a remote domain.

Smart Host Security Settings

When you route mail through a smart host, you must specify how the source server will authenticate to the smart host computer. You can't require security settings for a Send connector unless a smart host destination is specified. For example, an Internet-facing connector can't be set to require TLS.

The following table lists the smart host authentication mechanism that you can configure for a Send connector.

Smart host authentication mechanisms

Security setting	Description

None	Anonymous access is allowed.
Basic authentication	Basic authentication requires that you provide a user name and password. Basic authentication sends credentials in clear text. All smart hosts with which this Send connector is authenticating must accept the same user name and password.
Basic authentication over TLS	Select TLS to encrypt the transmission of the credentials. The receiving server must have a server certificate. The exact FQDN of the smart host, MX record, or A record that's defined on the Send connector as the smart host identity must also exist in the server certificate. The Send connector will attempt to establish the TLS session by sending the STARTTLS verb to the destination server and will only perform Basic authentication after the TLS session has been established. A client certificate is also required to support mutual TLS authentication.
Exchange Server authentication	Exchange Server authentication (Generic Security Services application programming interface (GSSAPI) and Mutual GSSAPI)
Externally Secured (for example, with IPsec)	The network connection is secured using a method that's external to the Exchange server.

Source Server

You must select at least one source server for a Send connector. The source server is the transport server to which messages are routed for delivery through the selected Send connector. You can set more than one source server on a Send connector that's configured for the Exchange organization. When you specify more than one source server, you provide load balancing and redundancy if a server fails. The source servers associated with Send connectors that are configured for the Exchange organization can be Hub Transport servers or subscribed Edge Transport servers.

FQDN

The **General** tab of the Send connector properties in the EMC includes the option **Specify the FQDN this connector will provide in response to HELO or EHLO**. In the Shell, this property is set by using the *Fqdn* parameter with the **Set-SendConnector** cmdlet. After an SMTP session is established, an SMTP protocol conversation starts between a sending e-mail server and a receiving e-mail server. The sending e-mail server or client sends the EHLO or HELO SMTP command and its FQDN to the receiving server. In response, the receiving server sends a success code and provides its own FQDN. In Exchange 2010, you can customize the FQDN that's provided by the sending server if you configure this property on a Send connector. The value of the *Fqdn* parameter is displayed to connected messaging servers whenever a source server name is required, as in the following examples:

- In the most recent Received: header field of the message that's added to the message by the next hop messaging server after the message leaves the Hub Transport server or Edge Transport server
- During TLS authentication

If the Send connector is configured on a Hub Transport server that also has the Mailbox server role installed, any value that you specify for the *Fqdn* parameter isn't used. Instead, the FQDN of the server that's displayed by using the **Get-ExchangeServer** cmdlet is always used.

For servers that have both the Hub Transport server role and the Mailbox server role installed, the only way to remove the server name from the Received: headers of the outgoing message is to use the **Remove-ADPermission** cmdlet to remove the Ms-Exch-Send-Headers-Routing permission from the security principals that use the connector. This action will remove all the Received: headers from the message as the message leaves the Hub Transport server. We recommend that you don't remove the Received: headers for internal messages, because the Received: headers are used for maximum hop count calculations. For more information about the **Remove-ADPermission** cmdlet and the **Get-ExchangeServer** cmdlet, see the following topics:

- Remove-ADPermission
- Get-ExchangeServer

New Features in Exchange 2010 Service Pack 1

In Service Pack 1 (SP1) for Exchange Server 2010, new functionality was added to Send connectors. This section provides an overview of these new features.

Support for Downgrading Connection Failures

You may have dedicated Send connectors that are responsible for transmitting messages over well-defined communication channels that are expected to always be available, such as a Send connector dedicated to send messages to Microsoft Office 365 or to one of your partners over a private channel. On such connections, many of the typical errors that are possible on ordinary destinations on the Internet aren't expected. In this scenario, you may want to treat any communication errors as transient as opposed to issuing non-delivery reports (NDRs). With Exchange 2010 SP1, you can configure a Send connector to downgrade authentication and name resolution errors, which would normally result in an NDR, to transient errors. In these cases, Exchange will attempt delivery again instead of issuing an NDR.

Downgrading connection failures over reliable connections give you an opportunity to troubleshoot and resolve problems without impacting your users.

Important:

This feature should only be enabled for Send connectors that transmit messages over well-defined and reliable networks. You shouldn't enable this feature for your Send connectors to the Internet.

To configure this feature, you use the *ErrorPolicies* parameter of the **Set-SendConnector** cmdlet. You can choose to downgrade authentication failures, DNS failures or both for any Send connector. For more information about configuring this property, see Set-SendConnector.

Support for TLS Domain Validation

Exchange 2010 SP1 provides support for domain validation for outbound TLS connections. Domain validation is an additional security feature that reduces the risk of malicious users impersonating a receiving server. When you enable domain validation on a Send connector, the Transport server performs the following security checks on the outbound connection:

- The communication channel is encrypted using TLS.
- The certificate of the receiving server is validated and revocation list checks are performed.
- The Transport server verifies that the FQDN on the certificate of the receiving

server matches the domain configured in the Send connector properties.

When you enable domain validation on a Send connector, you also have to specify the domain name to validate against. Both of these properties are configurable using the *TlsAuthLevel* and *TlsDomain* parameters of the **Set-SendConnector** cmdlet. For more information about configuring this feature, see Set-SendConnector.

1.7.1.32 Understanding Shadow Redundancy

Understanding Shadow Redundancy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-19*

High availability strategies for Exchange have focused on the availability and recoverability of data stored in mailbox databases. When you implement a highly available solution for your Mailbox servers, the e-mail messages won't be lost, and they can easily be recovered after a failure, after they arrive in a mailbox.

However, these strategies didn't extend to messages while they're in transit. If a Hub Transport server fails while processing messages and can't be recovered, data loss could occur. As the volume of messages processed by Hub Transport servers increases, potential data loss becomes an increasing concern for administrators.

Microsoft Exchange Server 2007 introduced the transport dumpster feature for the Hub Transport server role. An Exchange 2007 Hub Transport server maintains a queue of messages delivered recently to recipients whose mailboxes are on a clustered mailbox server. When a failover is experienced, the clustered mailbox server automatically requests every Hub Transport server in the Active Directory site to resubmit mail from the transport dumpster queue. This prevents mail from being lost during the time taken for the cluster to fail over. While this does provide a basic level of transport redundancy, it's only available for message delivery in a cluster continuous replication (CCR) environment and doesn't address potential message loss when messages are in transit between Hub Transport and Edge Transport servers.

Exchange Server 2010 introduces the *shadow redundancy* feature to provide redundancy for messages for the entire time they're in transit. The solution involves a technique similar to the transport dumpster. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all of the next hops for that message have completed delivery. If any of the next hops fail before reporting back successful delivery, the message is resubmitted for delivery to that next hop.

Shadow redundancy provides the following benefits:

- It eliminates the reliance on the state of any specific Hub Transport or Edge Transport server. As long as redundant message paths exist in your routing topology, any transport server becomes disposable.
- If a transport server fails, you can remove it from production without emptying its queues or losing messages.
- If you want to upgrade a Hub Transport or Edge Transport server, you can bring that server offline at any time without the risk of losing messages.
- It eliminates the need for storage hardware redundancy for transport servers.
- It consumes less bandwidth than creating duplicate copies of messages on multiple servers. The only additional network traffic generated with shadow

redundancy is the exchange of *discard status* between transport servers. Discard status is the information each transport server maintains. It indicates when a message is ready to be discarded from the transport database.
- It provides resilience and simplifies recovery from a transport server failure.

Shadow redundancy is implemented by extending the SMTP service. The service extensions allow SMTP hosts to negotiate shadow redundancy support and exchange discard status for shadow messages.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Shadow Redundancy Components

The following table provides descriptions of all the components of shadow redundancy.

Shadow redundancy components

Component	Description
Primary message	The original message submitted to transport for delivery.
Shadow message	The copy of a message that a transport server retains until it confirms that all the next hops for that message have successfully delivered it.
Primary server	The transport server that's currently processing a message.
Shadow server	The transport server that holds shadow copies of a message after delivering the message to the primary server.
Shadow queue	The queue that a transport server uses to store shadow messages. A transport server will have separate shadow queues for each hop to which it delivered the primary message.
Discard status	The information a transport server maintains for shadow messages that indicate when a message is ready to be discarded.
Discard notification	The response a shadow server receives from a primary server indicating a message is ready to be discarded.
Shadow Redundancy Manager	The transport component that manages shadow redundancy.
Heartbeat	The process of transport servers verifying the availability of each other.

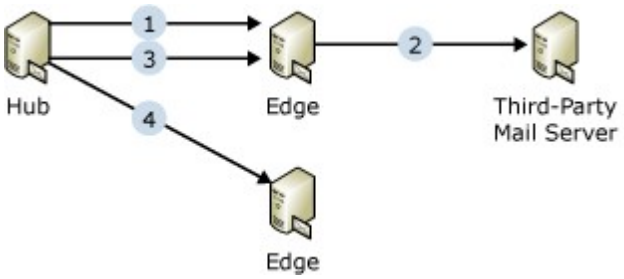
Return to top

Shadow Redundancy Message Flow

To illustrate the mail flow with shadow redundancy enabled, consider the simple scenario

where a Hub Transport server sends a message to a third-party mail server via an Edge Transport server in the perimeter network.

Message flow with shadow redundancy



In this scenario, the message flow goes through following stages:

1. The Hub Transport server delivers a message to the Edge Transport server.
   - 1.a. The Hub Transport server opens an SMTP session with the Edge Transport server.
   - 1.b. The Edge Transport server advertises shadow redundancy support.
   - 1.c. The Hub Transport server notifies the Edge Transport server to track discard status.
   - 1.d. The Hub Transport server submits the message to the Edge Transport server.
   - 1.e. The Edge Transport server acknowledges the receipt of the message and records the Hub Transport server identity for sending discard information for the message.
   - 1.f. The Hub Transport server moves the message to the shadow queue for the Edge Transport server and marks the Edge Transport server as the primary server. The Hub Transport server becomes the shadow server.
2. The Edge Transport server delivers the message to the next hop.
   - 2.a. The Edge Transport server submits the message to a third-party mail server.
   - 2.b. The third-party mail server acknowledges the receipt of the message.
   - 2.c. The Edge Transport server updates the discard status for the message as delivery complete.
3. The Hub Transport server queries the Edge Transport server for discard status (success case).
   - 3.a. At the end of each SMTP session with the Edge Transport server, the Hub Transport server queries the Edge Transport server for discard status on messages previously submitted. If the Hub Transport server hasn't opened any SMTP sessions with the Edge Transport server after the initial message submission, it will open an SMTP session with the Edge Transport server just to query for the discard status after a specific amount of time.
   - 3.b. The Edge Transport server checks the local discard status and sends back the list of messages that have been delivered, and removes the discard information.
   - 3.c. The Hub Transport server deletes the list of messages from its shadow queue.
4. The Hub Transport server queries the Edge Transport server for the discard status and resubmits the message (failure case).
   - 4.a. If the Hub Transport server can't contact the Edge Transport server, the Hub Transport server resumes the primary server role and resubmits the messages in the shadow queue.
   - 4.b. Resubmitted messages are delivered to another Edge Transport server and the workflow starts from stage 1.

Note:

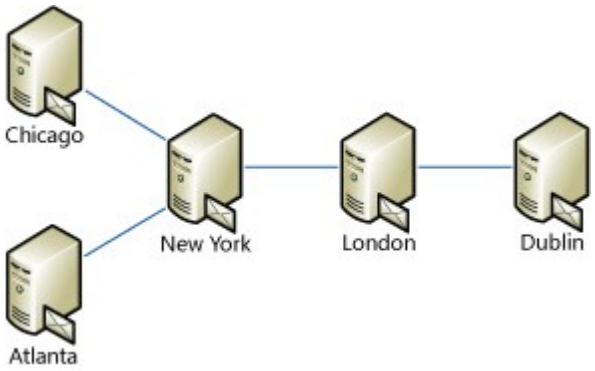
If there are no alternative routes available for a shadow message (such as the second Edge Transport server shown in

the preceding figure), it won't be resubmitted, but remain in the shadow queue.

For more information about message flow in various different scenarios, see Shadow Redundancy Mail Flow Scenarios.

Multiple Hop Scenario

If a message travels through multiple servers that support shadow redundancy, the shadow messages are retained on a server only until the next server in the message path confirms delivery. To illustrate how this works, consider an organization that has five Active Directory sites with Hub Transport servers installed. The sites are connected to each other as shown in the following figure. The organization has New York and London sites configured as hub sites, so the messages from Chicago or Atlanta need to go through Hub Transport servers in the New York and London sites to get to the Dublin site.



Assume that a message is sent by a user in the Chicago site to a user in the Dublin site. This message will need to travel through the New York and London sites to get to Dublin. In this case, the following occurs:

1. The Hub Transport server in Chicago will send the message to the Hub Transport server in New York, and it will retain a shadow copy of the message.
2. The New York Hub Transport server will send the message to the Hub Transport server in London and queue a discard status for the Chicago hub.
3. The Chicago hub queries the New York hub for discard status and receives the discard notification for the message. At this time, it can remove the shadow message from its database. Whether the message was delivered from London to Dublin doesn't have an impact on when the Chicago server deletes the shadow message.

Shadow Redundancy Protection when Hub Transport and Mailbox Server Roles Coexist with DAGs

When using database availability groups (DAGs), the messages that are already committed to mailbox databases are protected with the DAG architecture. For any message delivered to a mailbox database that's part of a DAG, the shadow copy for that message is retained in the transport dumpster until that message is replicated to all DAG members. Similarly, any message submitted to Hub Transport servers from a DAG member has two copies, one in the Hub Transport server queue waiting for delivery, and a shadow copy in the sender's Sent Items folder. This approach is a key component of shadow redundancy.

However, when the Hub Transport and Mailbox server roles coexist on the same server, and you have mailbox databases that are part of a DAG, Hub Transport servers may have to route a message through an extra hop to avoid having the primary message and the shadow message on the same server hardware. Specifically, the Hub Transport server role attempts to avoid the following two scenarios because a failure of a single server

may result in the loss of both the primary and shadow messages:

- **During message delivery, where the active mailbox database of the message recipient and the transport dumpster containing the shadow copy of the message are on the same server** To avoid this scenario, the Hub Transport server routes the message through another Hub Transport server within the site to ensure that the shadow message ends up on different server hardware. However, if no other Hub Transport servers are available, it delivers the message directly.
- **During message submission, where the transport queue holding the primary message and the shadow message in the Sent Items folder of the sender are on the same server** To avoid this scenario, the store driver prefers other Hub Transport servers in the site for message submission. However, if no other Hub Transport servers are available in the site, it submits the message to the local Hub Transport server.

For more information about Hub Transport and Mailbox server role coexistence when using DAGs, see Hub Transport and Mailbox Server Roles Coexistence When Using DAGs.

Interoperability

Whether shadow redundancy will be used or not is decided while establishing a new SMTP connection. If both servers in an SMTP connection support shadow redundancy, the workflow mentioned previously is used. However, there will be situations where Exchange 2010 transport servers exchange messages with mail servers that don't support shadow redundancy. These could be third-party mail servers, earlier versions of Exchange, or an Exchange 2010 organization that hasn't enabled shadow redundancy.

When an Exchange 2010 transport server that supports shadow redundancy establishes a connection with a server that doesn't support shadow redundancy, the following events take place:

1. Exchange establishes an SMTP connection to the target server.
2. The target server doesn't advertise shadow redundancy support.
3. Because the target server doesn't support redundancy, Exchange will perform the following for each message:
   3.a. Deliver the message to the target server.
   3.b. Shadow Redundancy Manager will mark that the message is delivered to the next hop.
   3.c. Delete the message after it's delivered to all of the next hops.

When a server that doesn't support shadow redundancy establishes a connection with an Exchange 2010 server, the following events take place:

1. The sending server establishes an SMTP connection with Exchange.
2. Exchange advertises shadow redundancy support.
3. The sending server doesn't support shadow redundancy and therefore it won't use it. It will deliver messages to the Exchange server.
4. For each message Exchange receives, it will do the following:
   4.a. Deliver the message to the next hop, or make a shadow copy of it.
   4.b. Send acknowledgement to the sending server.

Delayed Acknowledgement

The main principle behind shadow redundancy is maintaining a copy of the message on the previous hop until the server verifies that it has successfully delivered it to all the next hops. This isn't possible when an Exchange 2010 transport server is receiving a message from a mail server that doesn't support shadow redundancy. This mail server can be an Exchange server running an older version of Exchange, a standard SMTP client, or a non-Exchange mail server on the Internet. In this case, Exchange attempts to achieve shadow redundancy by delaying the acknowledgement to the mail server until it verifies that the message has been successfully delivered to all the next hops internally. This way, if the Exchange 2010 server fails, the sending mail server will assume that the message was never delivered to Exchange and will attempt delivery again.

However, the delivery of the message to the next hops may take a long time due to the complexity of your routing infrastructure, or failure of one of the next hops. In this case, to prevent the SMTP session from timing out, the Exchange 2010 transport server will send an acknowledgement to the sending mail server. In this case, the mail redundancy isn't guaranteed, but it's a best effort. For example, a message may be lost in the following scenario: An Internet mail server transmits a message to an Edge Transport server. The Edge Transport server can't communicate with the Hub Transport server due to a network problem and acknowledges the receipt of the message to the Internet mail server. The Edge Transport server then fails and can't be recovered before the network problem is resolved. At this point, the message is lost.

The delayed acknowledgement time-out value is controlled by the *MaxAcknowledgementDelay* attribute of each Receive connector. The default value is 30 seconds. To learn more about configuring this attribute, see Configure Shadow Redundancy.

Bypassing Delayed Acknowledgement

There are cases where it's unlikely a message will be delivered before the delayed acknowledgement time-out is reached. In these cases, the transport server uses one of the following methods to handle messages:

- **Skipping delayed acknowledgement** By default, the transport server skips the delayed acknowledgement to maintain SMTP receive throughput. In essence, the transport server issues an acknowledgment before the time-out is reached.
- **Shadow redundancy promotion** In Microsoft Exchange Server 2010 Service Pack 1 (SP1), instead of skipping the delayed acknowledgement, the transport server can be configured to relay the message to any other transport server in the site. This effectively inserts the message into the shadow redundancy pipeline, thereby protecting the message. This process is called *shadow redundancy promotion*. This approach minimizes the number of unprotected messages in the organization when compared to the skipping delayed acknowledgement method. By default, this feature is disabled. To enable shadow redundancy promotion, an administrator must edit the Edgetransport.exe.config file, change the **shadowredundancypromotionenabled** key to **true**, save the changes to the file, and then restart the Microsoft Exchange Transport service (MSExchangeTransport.exe). For more information about how to do this, see the "Enable Shadow Redundancy Promotion" section in the Configure Shadow Redundancy topic.

The following table lists different scenarios ion which a transport server bypasses delayed acknowledgement, and describes how an Exchange 2010 server handles that scenario.

Scenario	Exchange 2010 default behavior (skipping delayed acknowledgement)	Exchange 2010 SP1 with shadow redundancy promotion enabled
The target queue for the message is either in suspended or retry state.	The receiving transport server skips the delayed acknowledgement.	The receiving transport server immediately uses shadow redundancy promotion.
The target queue enters retry state after the message is added to it.	The receiving transport server skips the delayed acknowledgement for subsequent messages until the target queue returns to ready state.	The receiving transport server uses shadow redundancy promotion for subsequent messages until the target queue returns to ready state.
An administrator suspends	If the administrator suspends	If the administrator suspends

either the target queue or the message.	the target queue, the receiving transport server skips the delayed acknowledgement until the target queue returns to ready state. If the administrator suspends the message, the receiving transport server handles subsequent messages normally.	the target queue, the receiving transport server uses shadow redundancy promotion until the target queue returns to ready state. If the administrator suspends the message, the receiving transport server handles subsequent messages normally.
The target queue for the message has more than 100 messages.	The receiving transport server skips the delayed acknowledgement until the target queue size falls below 100.	If the target queue has any messages in it, the receiving transport server uses shadow redundancy promotion for subsequent messages until the queue clears.

Return to top

Shadow Redundancy Manager

Shadow Redundancy Manager is the core component of an Exchange 2010 transport server that's responsible for managing shadow redundancy.

Shadow Redundancy Manager is responsible for maintaining the following information for all the primary messages that a server is currently processing:

- The shadow server for each primary message being processed.
- The discard status to be sent to shadow servers.

Shadow Redundancy Manager is responsible for the following for all the shadow messages that a server has in its shadow queues:

- Maintaining the list of primary servers for each shadow message.
- Checking the availability of each primary server for which a shadow message is queued.
- Processing discard notifications from primary servers.
- Removing the shadow messages from the database after all expected discard notifications are received.
- Deciding when the shadow server should take ownership of shadow messages, becoming a primary server.

In addition, Shadow Redundancy Manager is also responsible for managing performance counters related to shadow redundancy.

Heartbeat

Shadow Redundancy Manager uses heartbeat to determine the availability of the servers for which shadow messages are queued. During the SMTP session between two servers that both support shadow redundancy, the server that initiates the connection queries the target server for discard status of messages previously submitted to that server. The initiating server accomplishes this by issuing an XQUERYDISCARD command. In response, the target server returns the discard notifications. This exchange between the two servers is used as the heartbeat for shadow redundancy.

There is a time-out value for the heartbeat. If no connections are established to a server for which Shadow Redundancy Manager is maintaining a shadow queue for that duration, the server will attempt to establish an SMTP connection with the primary server

specifically to query the discard status and reset the timer. The time-out value is controlled by the *ShadowHeartbeatTimeoutInterval* parameter of the **Set-TransportConfig** cmdlet. The default value for this parameter is 300 seconds in the release to manufacture (RTM) version of Exchange 2010, and 900 seconds in Exchange 2010 SP1.

If the server can't establish a connection to a primary server when the time-out value is reached, it will reset the timer and try again. If the time-out value is reached twelve times in a row (three times in a row in Exchange 2010 RTM), the server will conclude that the primary server has failed and will assume ownership of the shadow messages and begin to generate discard notifications for them to send to the primary server that failed. The number of time-outs a server will wait before deciding a primary server has failed is controlled by the *ShadowHeartbeatRetryCount* parameter of the **Set-TransportConfig** cmdlet.

To learn more about configuring the shadow redundancy heartbeat, see Configure Shadow Redundancy.

Return to top

Message Processing After an Outage

Shadow redundancy minimizes message loss due to server outages. When a transport server comes back online after an outage, there are two scenarios:

- **The server comes back online with a new transport database** In this scenario, the transport database is unrecoverable due to data corruption or hardware failure. In this case, because the transport server will have a new database ID, it will be recognized as a new route by the other transport servers in the organization. This also applies to the situation where a server couldn't be recovered, and a new server was provisioned as a replacement.
- **The server comes back online with the same transport database** In this scenario, the particular transport server didn't fail, but was offline for an extended period of time. For example, a network card failure, or a long maintenance on the server would cause this scenario.

The following table summarizes how transport reacts to these two scenarios when shadow redundancy is enabled. For clarity, assume that the server that had an outage is named Hub01.

Message processing in recovery scenarios

Recovery scenario	Actions taken for messages that have alternative routes	Actions taken for messages with no alternative routes
Hub01 comes back online with a new database.	When Hub01 becomes unavailable, each server that has shadow messages queued for Hub01 will assume ownership of those messages and resubmit them. The messages then get delivered to their destinations using alternative routes. The total delay for messages is equal to the product of the heartbeat time-out interval and the heartbeat retry count configured in your	These messages remain in the shadow queue on each server that has shadow messages queued for Hub01. When Hub01 comes back online with a new database ID, the shadow servers detect that it's a new database and resubmit the messages that are in the shadow queue to Hub01. This is equivalent to suddenly discovering an alternative route for these messages. The total delay for the

	organization.	messages depends on the duration of the outage.
Hub01 comes back online with the same database.	Hub01 will deliver the messages in its queues. This will result in duplicate delivery of these messages. Exchange mailbox users won't see duplicate messages due to duplicate message detection. However, recipients on foreign systems may receive duplicate copies. The total delay for messages is equal to the product of the heartbeat time-out interval and the heartbeat retry count configured in your organization.	Hub 01 will deliver the messages in its queues and then send discard notifications to the shadow servers. The total delay for the messages depends on the duration of the outage.

Return to top

Extended Rights Required for Shadow Redundancy

Exchange 2010 introduces the following two extended rights, which are required for shadow redundancy:

- ms-Exch-SMTP-Accept-XSHADOW
- ms-Exch-SMTP-Send-XSHADOW

When an SMTP connection is established to an Exchange 2010 transport server, it will advertise shadow redundancy support if the ms-Exch-SMTP-Accept-XSHADOW extended right exists on the Receive connector being used. In addition, the authentication mechanism on the Receive connector should be either Exchange Server authentication or Externally Secured.

When an Exchange 2010 transport server establishes an SMTP connection to another server that advertises shadow redundancy support, it will issue an XSHADOW command only if the session has been granted the ms-Exch-SMTP-Send-XSHADOW extended right.

By default, these extended rights are granted to the Exchange Servers group on all internal Send connectors and Receive connectors.

Note:

Shadow redundancy can be enabled or disabled for the entire organization using the *ShadowRedundancyEnabled* parameter of the **Set-TransportConfig** cmdlet. This setting overrides the extended rights described in this section. If shadow redundancy is disabled for the organization, Exchange will never advertise shadow redundancy support or issue XSHADOW commands even if the necessary extended rights are granted to the SMTP session.

Return to top

1.7.1.32.1 Shadow Redundancy Mail Flow Scenarios

Shadow Redundancy Mail Flow Scenarios

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

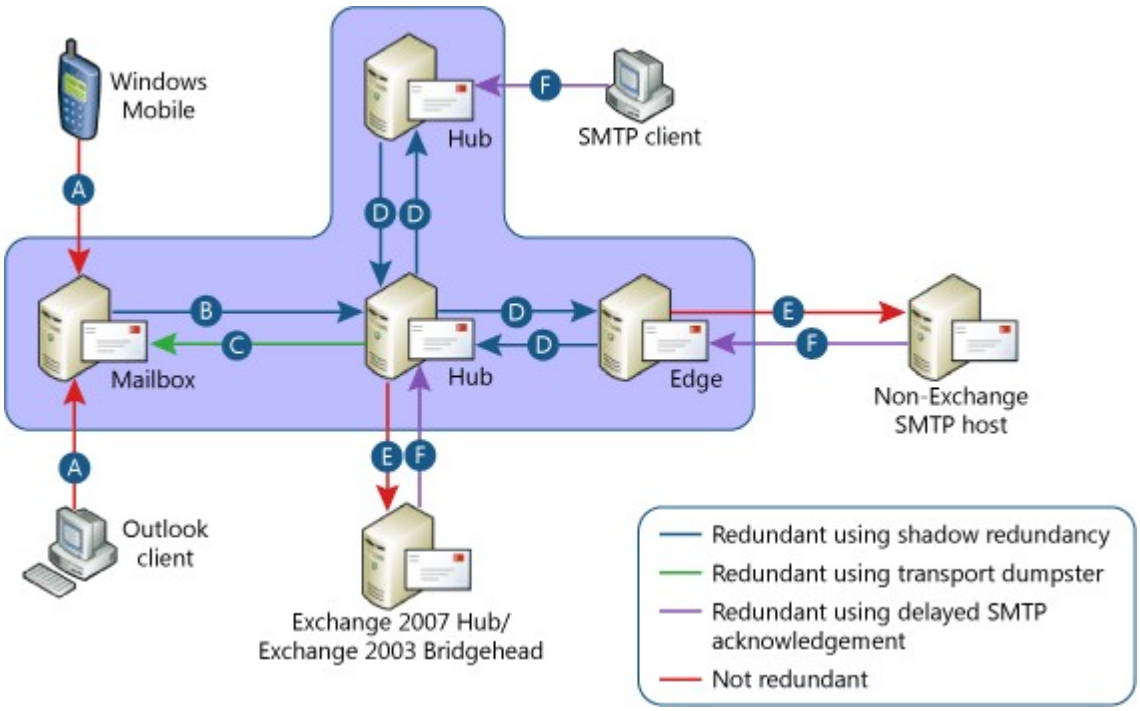
Topic Last Modified: *2010-06-07*

The shadow redundancy feature in Microsoft Exchange Server 2010 provides redundancy for messages for the entire time they're in transit. The general message flow is explained in Understanding Shadow Redundancy. This topic explains in detail what happens for each specific message flow scenario that can involve Exchange.

Mail Flow Scenarios

The following figure shows each possible redundancy scenario in an Exchange organization and how message redundancy is achieved in each scenario. The shaded area shows where shadow redundancy is in effect. Exchange 2010 shadow redundancy prevents data loss while messages are in transit within the shaded area.

Note:
Client Access servers are omitted from the figure for simplicity.



As can be seen from the preceding figure, all mail flow paths possible in an Exchange organization fit into one of the following scenarios:

A. MAPI/Windows Mobile Client Submission

B. Mail Flow from Mailbox Server to Hub Transport Server

C. Message Delivery from Hub Transport Server to Mailbox Server

D. Mail Flow Between Exchange 2010 Transport Servers

E. Mail Flow from Exchange 2010 Transport Servers to Mail Servers That Don't Support Shadow Redundancy

F. Mail Flow from Mail Servers That Don't Support Shadow Redundancy to Exchange 2010 Transport Servers

The following sections explain what happens for each mail flow scenario.

A. MAPI/Windows Mobile Client Submission

Message submissions from MAPI or Windows Mobile clients aren't redundant. After the message is successfully stored on the Mailbox server, Exchange high availability features can take effect and help prevent data loss. This scenario provides a complete picture of message flow, from beginning to end.

Return to the list of mail flow scenarios

B. Mail Flow from Mailbox Server to Hub Transport Server

The following actions take place when an Exchange 2010 Mailbox server submits messages to an Exchange 2010 Hub Transport server.

Important:

Exchange 2010 Mailbox servers can't communicate with transport servers running previous versions of Exchange. Therefore, this topic only discusses mail flow from an Exchange 2010 Mailbox server to an Exchange 2010 Hub Transport server.

1. The mail submission service notifies the Hub Transport server that there is a new message.
2. The Hub Transport server picks up the message from the Outbox of the mailbox submitting the message and stores it in its database.
3. If the message has recipients on Mailbox servers that are in the same Active Directory site, the Hub Transport server delivers the message to the destination mailboxes, following the steps listed in scenario C. For all other recipients, the Hub Transport server delivers the message to the next hop.
4. After delivery to the next hop is complete, the Hub Transport server notifies the Mailbox server that it has finished processing the message and assumed ownership of the message. After this notification, the message is deleted from the Outbox.
5. If none of the other hops for the message support shadow redundancy, the Hub Transport server deletes the message. Otherwise, it converts the message to a shadow message by storing it in the shadow queues for the hops to which it delivered the message.

Return to the list of mail flow scenarios

C. Message Delivery from Hub Transport Server to Mailbox Server

The following actions take place when an Exchange 2010 Hub Transport server delivers messages to an Exchange 2010 Mailbox server.

Important:

Exchange 2010 Hub Transport servers can't communicate with Mailbox servers running previous versions of Exchange. Therefore, this topic only discusses mail flow from an Exchange 2010 Hub Transport server to an Exchange 2010 Mailbox server.

1. The Hub Transport server delivers the message to the destination mailboxes.
2. After the message is delivered to all the destination mailboxes, the Hub Transport server adds the message to the transport dumpster.
3. The Hub Transport server queues discard notifications to the hop from which it has received the message. These discard notifications are created when

the hop queries the Hub Transport server.
4. The previous hop deletes the corresponding shadow message.

Return to the list of mail flow scenarios

D. Mail Flow between Exchange 2010 Transport Servers

The mail flow process is identical for all message exchanges between transport servers running Exchange 2010, whether it's between two Hub Transport servers or between a Hub Transport server and an Edge Transport server. The following actions take place when a message is transferred from one Exchange 2010 transport server to another. For clarity purposes, assume that the server that's sending the message is called Hub01 and the server that's receiving the message is called Edge01.

1. Hub01 establishes an SMTP connection to Edge01.
2. Edge01 advertises shadow redundancy support.
3. Hub01 requests shadow redundancy in the SMTP session by issuing an **XSHADOW** command. The process is similar to establishing Transport Layer Security (TLS) on an SMTP session.
4. For each message that Hub01 needs to send to Edge01:
   4.a. Hub01 transmits the message to Edge01.
   4.b. Edge01 marks the message as shadowed by Hub01.
   4.c. Hub01 marks Edge01 as the primary server and adds it to its shadow queue for Edge01.
   4.d. Hub01 prepares discard notifications for the message to be sent to the hop from which it received the message.
5. Hub01 queries Edge01 for discard status of messages it has previously submitted to Edge01.
6. Edge01 sends all discard notifications that it has prepared for Hub01. These could be for messages that are sent in the same SMTP session or for those that were sent during previous SMTP sessions.
7. Hub01 deletes all shadow messages for which Edge01 has sent a discard notification.

Return to the list of mail flow scenarios

E. Mail Flow from Exchange 2010 Transport Servers to Mail Servers That Don't Support Shadow Redundancy

Neither Exchange Server 2007 transport servers nor Exchange Server 2003 bridgehead servers support shadow redundancy. Therefore, if you have a coexistence scenario with previous versions of Exchange, Exchange 2010 redundancy features can guarantee message delivery only until the legacy Exchange hop, and not all the way to its destination. The same applies to the scenario where Exchange 2010 Edge Transport servers send messages to non-Exchange mail servers.

The following actions take place when an Exchange 2010 Hub Transport server sends a message to an Exchange transport server running a previous version of Exchange, or an Exchange 2010 Edge Transport server sends a message to a non-Exchange mail server. For clarity, assume that an Exchange 2010 Hub Transport server called Hub01 is sending a message to an older Exchange transport server called Legacy01.

1. Hub01 establishes an SMTP connection to Legacy01.
2. Legacy01 doesn't advertise shadow redundancy support.
3. Because Legacy01 didn't advertise shadow redundancy, Hub01 doesn't initiate shadow redundancy on the SMTP session.
4. Hub01 delivers the message to Legacy01.
5. Hub01 deletes the message.
6. Hub01 prepares discard notifications for the hop from which it received the message.

Return to the list of mail flow scenarios

F. Mail Flow from Mail Servers That Don't Support Shadow

Redundancy to Exchange 2010 Transport Servers

There are four entry points to an Exchange organization where a mail server that doesn't support shadow redundancy may establish an SMTP connection to an Exchange 2010 transport server and send messages.

- An Exchange 2010 Unified Messaging (UM) server connecting to an Exchange 2010 Hub Transport server.
- An Exchange transport server that's running Exchange 2007 or Exchange 2003 connecting to an Exchange 2010 Hub Transport server.
- A non-Exchange mail server on the Internet connecting to an Exchange 2010 Edge Transport server.
- A non-Exchange mail server in the organization, such as a UNIX server, or an SMTP client that's submitting messages to an Exchange 2010 Hub Transport server.

In this scenario, Exchange 2010 achieves shadow redundancy using a feature called *delayed acknowledgement*. When an Exchange 2010 transport server receives a message from a mail server that doesn't support shadow redundancy, it delays sending an acknowledgement to the sending mail server until it has confirmed that the message has been successfully delivered to its destination. For more information about delayed acknowledgement, see Understanding Shadow Redundancy.

To illustrate this scenario, assume that an Exchange 2010 Edge Transport server called Edge01 is receiving a message from a non-Exchange mail server on the Internet called Internet01. In this example, the following actions take place:

1. Internet01 establishes an SMTP connection to Edge01.
2. Edge01 advertises shadow redundancy support.
3. Because Internet01 doesn't support shadow redundancy, it simply sends the message to Edge01.
4. Edge01 marks the message as a delayed acknowledgement message.
5. Edge01 delivers the message to the next hops using the steps outlined in scenario D.
6. Edge01 queries the next hops for the discard status of the message.
7. After Edge01 receives discard notifications from all of the next hops, it sends the acknowledgement to Internet01.
8. Edge01 deletes the message from its database.

Note:
If Edge01 can't verify successful delivery of the message to all of the next hops within 30 seconds, it will time out and send an acknowledgement to Internet01. This time-out value is controlled by the value of the *MaxAcknowledgementDelay* attribute of the Receive connector.

Return to the list of mail flow scenarios

1.7.1.32.2 Hub Transport and Mailbox Server Roles Coexistence When Using DAGs

Hub Transport and Mailbox Server Roles Coexistence When Using DAGs

Transport > Understanding Transport > Understanding Shadow Redundancy >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-19*

Microsoft Exchange Server 2007 doesn't support Hub Transport and Mailbox server roles on the same server hardware when high availability features such as single copy cluster

(SCC) or cluster continuous replication (CCR) are used. A minimum high availability deployment in Exchange 2007 requires four servers: two nodes for mailbox high availability and two Hub Transport servers for message transfer redundancy.

To reduce the number of servers required to provide a high availability solution, Exchange Server 2010 supports Hub Transport and Mailbox server roles on the same server hardware when using database availability groups (DAGs). Exchange 2010 provides a feature called *shadow redundancy*, which protects against data loss while messages are in transit. When used together, DAGs and shadow redundancy offer a highly resilient messaging infrastructure.

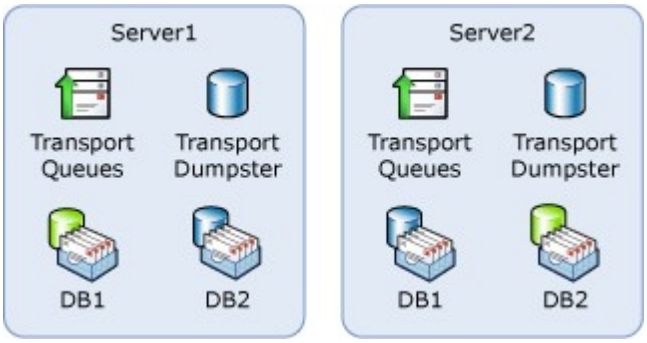
This topic focuses on how the Exchange 2010 Hub Transport server role behaves when deployed on the same server hardware as a Mailbox server that participates in a DAG. To learn more about DAGs, see Understanding Database Availability Groups.

Message Submission and Delivery

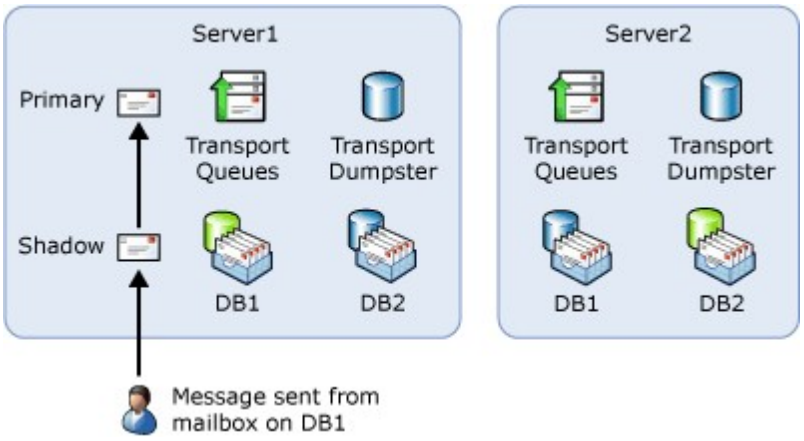
Shadow redundancy prevents data loss while messages are in transit by keeping a duplicate copy of the message along the message path. If a message is lost in transit due to a failure, the shadow copy of the message is resubmitted by the Transport component. For detailed information about how shadow redundancy is implemented, see Understanding Shadow Redundancy.

Mailbox servers are involved during initial message submission, when a user clicks **Send**, and during final delivery, when the message is saved to the Inbox of the recipient. When a message is submitted to Transport, the primary copy of that message is in the queues of the Hub Transport server to which the message was submitted. The shadow copy of that message is the item stored in the Sent Items folder of the sender. When a message is delivered, the primary copy is in the recipient's Inbox and the shadow copy of the message is stored in the transport dumpster.

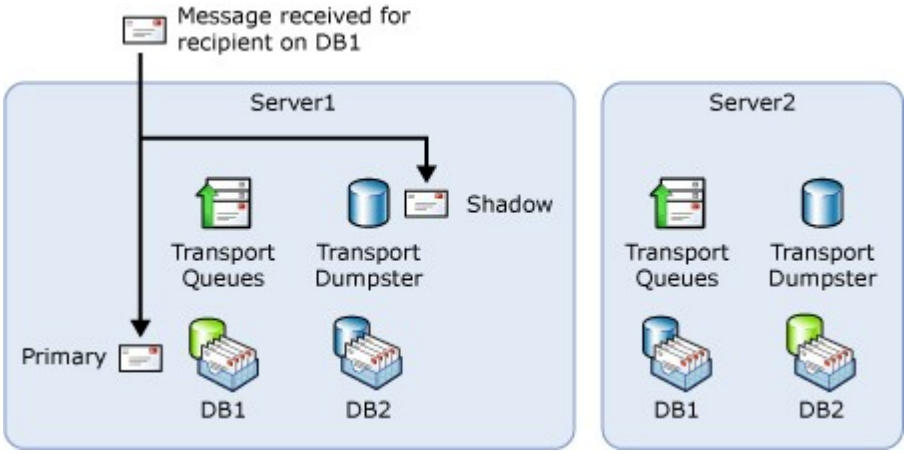
In a high availability scenario where Hub Transport and Mailbox server roles coexist on the same server hardware, it's crucial to try to avoid having both copies of a message reside on the same server. Consider the deployment scenario shown in the following figure. The topology consists of two Exchange servers participating in a DAG with the Hub Transport server role installed. The databases DB1 and DB2 are part of the DAG. Active databases are shown in green, and passive databases are shown in blue.



In this topology, assume that a user whose mailbox is on DB1 sends a message. If that message is submitted to the Hub Transport server role on Server1, both the primary and shadow messages will be physically stored on Server1. The primary messages will be in the Hub Transport server queues, and the shadow messages will be in the Sent Items folder of the sender, as shown in the following figure.



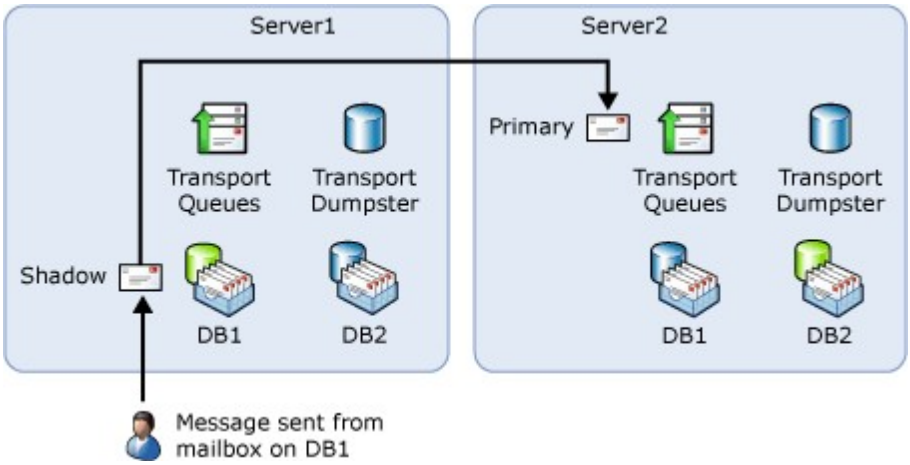
Similarly, if the Hub Transport server role on Server1 receives a message destined to a user on DB1, the message is delivered directly, and both the primary and shadow messages will be physically stored on Server1. The primary messages will be in the Inbox of the recipient, and the shadow messages will be in the transport dumpster, as shown in the following figure. If a server failure occurs at either of those instances, there's a chance that the message can be lost.



To avoid these scenarios where message loss can occur, Exchange attempts to submit or deliver messages over a route that ensures that the primary and shadow copies of messages are stored on different physical servers. The modified message submission and delivery behaviors are discussed in the following section.

Message Submission Behavior

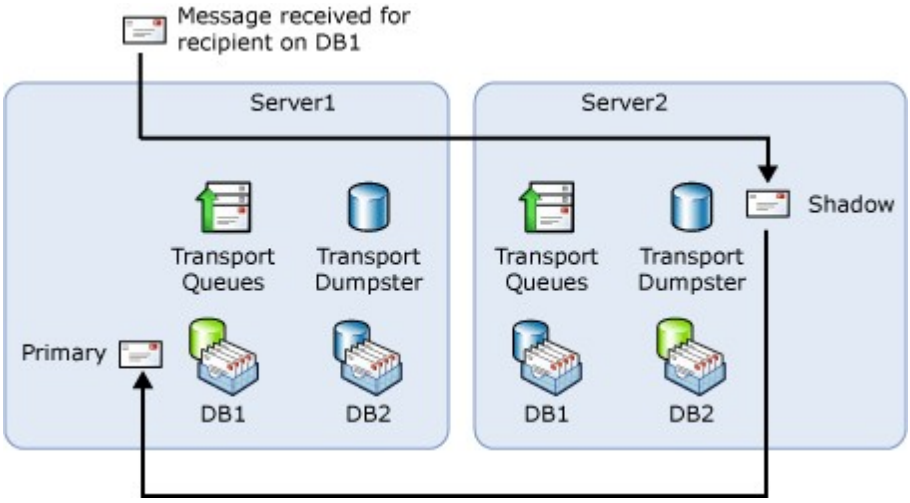
When a user whose mailbox is in a database that's a member of a DAG sends a message, the mail submission service gives preference to remote Hub Transport servers if it detects that the Hub Transport server is also installed on the local server. As shown in the figure "Two server high availability topology with Hub Transport and Mailbox server roles", if a user whose mailbox is on DB1 sends a message, the mail submission service will attempt to use the Hub Transport server installed on Server2 for message submission. The following figure shows this preferred message submission path.



In the case where no other Hub Transport servers are available in the site (for example, if Server2 is unavailable due to scheduled maintenance), the message submission service will fall back to submitting the message to the local Hub Transport server. Even though this is an undesirable submission path for redundancy, Exchange won't delay delivery of messages. This fallback submission path is desirable for availability and low delivery latency.

Message Delivery Behavior

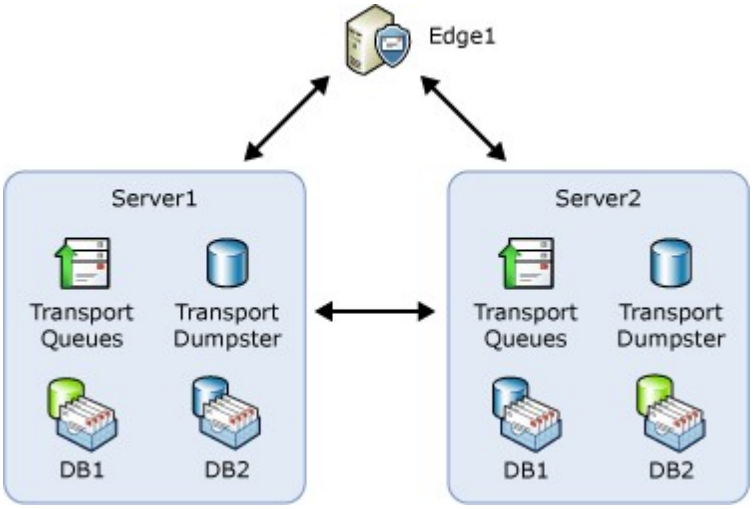
The message routing and delivery behavior doesn’t change in most cases. For example, if Server1 shown in the figure "Two server high availability topology with Hub Transport and Mailbox server roles" receives a message for a recipient on DB2, it will deliver the message normally because that database is active on a different server. The only scenario when a Hub Transport server will process an incoming message differently is when the target mailbox is on a database that's part of a DAG and is also active on the local server. Because a direct delivery in this situation would result in both the delivered message and the copy in the transport dumpster being on the same server, the Hub Transport server will instead reroute this message to another Hub Transport server within the same site. The following figure shows the message delivery path in this scenario.



In the case where no other Hub Transport servers are available in the site, the Hub Transport server will fall back to local delivery even though it's an undesirable delivery path for redundancy. Again, this fallback delivery path is desirable for availability and low delivery latency.

Message Flow Scenarios

This section explains in detail what happens in various message flow scenarios when Hub Transport and Mailbox server roles coexist on the same server. The topology shown in the following figure is used to illustrate various possible message flow scenarios.



The following table shows how the Hub Transport server role on Server1 processes messages in various scenarios. In all of these cases, Server1 is considered the entry point.

Sender location	Recipient location	Normal message path	High availability scenarios
DB1, active on Server1	DB1, active on Server1	1. Submission service on Server1 submits a message to the Hub Transport server role on Server2. 2. Hub Transport server role on Server2 delivers the message to DB1 on Server1 and adds the message to the transport dumpster on Server2.	• If Server1 fails before the message submission completes, the message in the sender's Outbox may be lost. • If Server2 fails before the message submission completes, the message is submitted to the Hub Transport server role on Server1. • If Server1 fails after the message submission to the Hub Transport server role on Server2 completes, DB1 will become active on

			Server2. The message will be queued on Server2 until DB1 is mounted, and then the Hub Transport server role delivers the message locally. • If Server2 fails after the message submission to Hub Transport server role on Server2 completes, the shadow message in DB1 is resubmitted to the Hub Transport server role on Server1, which delivers the message locally. • If Server1 fails after the message delivery is completed, DB1 will become active on Server2. If the delivered message hasn't yet been committed to the database, it's redelivered from the transport dumpster on Server2.
DB1, active on Server1	DB2, active on Server2	1. Submission service on Server1 submits the message to the Hub Transport server role on Server2. 2. Hub Transport server role on Server2 reroutes the message to the Hub Transport server role on Server1. 3. Hub Transport server role on Server1 delivers	• Any server failures prior to the completion of message submission are handled in the same manner as described in the previous row. • If Server1 fails after the message submission to the Hub Transport server role on Server2

		the message to DB2 on Server2 and adds the message to the transport dumpster on Server1.	completes, the Hub Transport server role on Server2 will deliver the message locally. • If Server2 fails after the message submission to the Hub Transport server role on Server2 completes, DB2 will become active on Server1. After the Hub Transport server role on Server1 detects that the Hub Transport server role on Server2 is unavailable, it will resubmit the shadow message. After DB2 is mounted on Server1, the message will be delivered locally. • If Server1 fails after the message is rerouted to Server1 for delivery, the Hub Transport server role on Server2 will resubmit the shadow message after it detects the Hub Transport server role on Server1 is unavailable. It will then deliver the message locally. • If Server2 fails after the message is rerouted to Server1 for delivery, DB2 will become active on Server1. The message will remain queued

			on Server1 until DB2 is mounted on Server1 and then it's delivered locally. • If Server2 fails after the message delivery is completed, DB2 will become active on Server1. If the delivered message hasn't yet been committed to the database, it's redelivered from the transport dumpster on Server1.
External	DB1, active on Server1	1. Hub Transport server role on Server1 reroutes the message to the Hub Transport server role on Server2. 2. Hub Transport server role on Server2 delivers the message to DB1 on Server1 and adds the message to the transport dumpster on Server2.	• If Server1 fails before it completes receiving the message from Edge1, Edge1 will attempt delivery to the Hub Transport server role on Server2. • If Server1 fails after it completes receiving the message from Edge1, Edge1 will resubmit the message to the Hub Transport server role on Server2 after it detects that the Hub Transport server role on Server1 is unavailable. The Hub Transport server role on Server2 will then deliver the message locally after DB1 is mounted on Server2. • All other failure scenarios are

			handled in the same manner as described in the first row.
External	DB2, active on Server2	1. Hub Transport server role on Server1 delivers the message to DB2 on Server2, and adds the message to the transport dumpster on Server1.	• If Server1 fails before it completes receiving the message from Edge1, Edge1 will attempt delivery to the Hub Transport server role on Server2. • If Server1 fails after it completes receiving the message from Edge1, but before delivering to DB2 on Server2, Edge1 will resubmit the shadow message to the Hub Transport server role on Server2. This is because Server1 won't send an acknowledgement to Edge1 until it successfully delivers the message to DB2. Because Edge1 hasn't received an acknowledgement, it will resubmit the message after it detects that Server1 is unavailable. • If Server2 fails after message delivery is completed, DB2 will become active on Server1. If the delivered message hasn't yet been committed to the database, it's redelivered from

			the transport dumpster on Server1.

The preceding table focuses on the minimum scenario where there are only two Hub Transport servers in a site that both coexist with Mailbox server roles that participate in DAGs. In more complex deployments where additional dedicated Hub Transport servers are available, those servers are also used when making routing decisions. However, if you have a large enough deployment where you can employ dedicated Hub Transport servers, it's a best practice to not install the Hub Transport server role on Mailbox servers that participate in a DAG.

1.7.1.33 Understanding TLS Certificates

Understanding TLS Certificates

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-04*

In cryptographic terms, the certificate and related private keys that are generated by the **New-ExchangeCertificate** cmdlet are TLS keys. The **New-ExchangeCertificate** cmdlet lets you specify metadata about the certificate so that different services can use the same certificate and private key. Before you create certificates or certificate requests for Exchange services that use TLS, you should understand the metadata that are used by the certificates for SSL and TLS services. This metadata is referred to as "fields" in the resulting certificate.

To view the fields of computer certificates on a specific computer, you can use the **Get-ExchangeCertificate** cmdlet in the Exchange Management Shell. Alternatively, you can use the Certificate Manager snap-in in the Microsoft Management Console (MMC).

Looking for management tasks related to TLS certificates? See Certificates.

Contents

Fields Used by Certificates for TLS Services

If you're using the **New-ExchangeCertificate** cmdlet to generate a certificate request from a third-party or other public key infrastructure (PKI) certification authority (CA), make sure that you validate which certificate fields and certificate format are required by the CA.

This section explains the most important certificate fields and provides some best practices for generating certificates and certificate requests.

Subject Name

The Subject Name of a TLS certificate is the field that is used by DNS-aware services. The Subject Name field binds a certificate to a particular server or domain name.

A subject name is an X.500 distinguished name that consists of one or more relative distinguished names, also known as RDN. The following table lists the frequently used relative distinguished names for identifying organizations or server entities.

Name	Abbreviation	Type	Max Size	Frequency Max.\Recommended in certificate\request	Order in subject
Country/Region	**C**	ASCII	2	1\1	1
Domain Component	**DC**	ASCII	255	Many	1
State or Province	**S**	Unicode	128	1	2
Locality	**L**	Unicode	128	1	3
Organization	**O**	Unicode	64	1\1	4
Organizational Unit	**OU**	Unicode	64	Many\Many	5
Common Name	**CN**	Unicode	64	Many\1	6

The Country/Region codes are the ISO 3166-1 codes. For more information, see English country names and code elements.

Domain Component and Country/Region are by convention mutually exclusive. It's a best practice to reference the name by Country/Region or reference the name by Domain Name System (DNS) name. Also, be aware that the maximum size of the Domain Component (255 characters) is the total of all Domain Component values.

Important:

Although certificates can have more than one common name field, some services are implemented on the assumption that there is only one common name. Therefore, multiple common names can cause interoperability issues. We recommend that the certificate or certificate request that you create contains only one common name.

Specifying Relative Distinguished Names

When creating certificate requests using the **New-ExchangeCertificate** cmdlet, subject names are represented as a single parameter that consists of a series of comma-separated names. Each name is identified by the abbreviation for the relative distinguished name. For example, the following subject name represents Country/Region = US, Organization = Contoso Corp, and Common Name = mail1.contoso.com:

```
-SubjectName "C=US o=contoso corp, CN=mail1.contoso.com"
```

Other examples of subject names that can represent the same server include the following examples:

```
-SubjectName  "O=contoso corp, CN=mail1.contoso.com"
-SubjectName "DC=contoso, DC=com, CN=mail1.contoso.com"
-SubjectName "DC= contoso, DC=com, O=contoso corp, CN=mail1.contoso.com"
```

If you have a registered DNS name that you use to send SMTP mail, it's a best practice to use the domain component convention and the DNS name for the certificate name, such as DC=contoso, DC=com, CN=mail1.contoso.com.

However, when you generate a certificate request for a CA provider, you must understand the Subject Name field requirements of the CA and your unique PKI needs. In some cases, you may have to use the Country/Region code ("C"). If that's the case, you must register your relative distinguished name with an X.500 registration authority.

International Subject Names

For subject names that contain non-ASCII characters, you can enter the *SubjectName* parameter as a distinguished name enclosed in quotation marks, as follows:

-*SubjectName* "C=ES,O=Diversión de Bicicleta,CN=mail1. DiversiondeBicicleta.com"

Subject Names and Domain Names

By convention, a common name can contain a fully qualified domain name (FQDN). Although this practice is widespread, be aware of the following two issues with this approach.

First, the maximum size of the Common Name field is 64 characters. This is fewer characters than the maximum size of a FQDN. Therefore, for FQDNs that are more than 64 characters, you must put the domain name in the Subject Alternative Name. The *DomainName* parameter is the parameter that maps to the Subject Alternative Name on the resulting certificate.

Second, the FQDN is restricted to a subset of the ASCII character set. However, the common name (CN) supports Unicode. Therefore, you can create a valid certificate with a CN that seems like a DNS name but is an invalid DNS name. Software that is looking for a FQDN in a certificate CN will not return the correct result if the CN contains non-ASCII characters. For example, if you create a certificate with a Subject Name where CN=mail.mïcrosoft.com, the name would be ignored as a FQDN because the name contains a Unicode character (the ï character with the diacritic (x00ef)). To the eye, the Unicode CN can be easily be mistaken for a FQDN because of the small difference between the ï character with the diacritic (x00ef) and the ASCII i (x0069). The Exchange certificate task doesn't require or enforce that the subject CN be a valid FQDN. By default, this means that the cmdlet includes the FQDN of the server as the default CN.

Certificate Domain Names

For TLS, certificates must contain DNS names because the TLS relies on DNS resolution. Clients verify the DNS name of the server to which they are connecting with the DNS name that they expect to be connecting to. This is true for Web browsers that connect to a Web site over HTTPS and for SMTP servers that transmit e-mail over the Internet or intranet.

A single server may support multiple DNS names for the following reasons:

- A SMTP server supports multiple accepted domains
- A client can access an e-mail server by the server name, by the domain name, by a FQDN local name, or by a load-balanced name.

When a TLS connection is established, if the client finds the name that it is looking for, the client ignores the other names in the certificate. Multiple domain and server names can be added to the Subject Alternative Name field of a TLS certificate. You can create a certificate that contains multiple Subject Alternative Names by using the *DomainName* parameter of the **New-ExchangeCertificate** cmdlet. The *DomainName* parameter is multivalued so that it can accept multiple names.

X.509 certificates can contain zero, one, or more DNS names in the Subject Alternative Name (SubjectAltName) certificate extension. DNS names in the SubjectAltName extension

exactly match the restrictions of a DNS name. They must not exceed 255 characters and must consist of A-Z, a-z, 0-9 and a dash (-).

Name Matching Logic for the Domain Security Feature

The certificate name matching logic for the Domain Security feature checks whether a domain name in the received certificate matches the domain name when it sends mail to that domain. For example, consider the FQDN of the recipient domain woodgrovebank.com. The certificate name matching logic searches through all DNS names in the certificates, and as long as one DNS name matches, the certificate is verified as a match for the specified domain.

In this example, the certificate name matching logic accepts a certificate with an exact domain match, such as woodgrovebank.com. It also supports using wildcard character domain names in certificates so that a certificate with a DNS name of *.woodgrovebank.com is accepted as a match. For more information about wildcard character domain names, see "Wildcard Character Domain Names" later in this topic.

The certificate name matching logic also searches DNS one node deep. Therefore, mail1.woodgrovebank.com is also accepted as a match for woodgrovebank.com. However, DNS names more than two nodes deep aren't accepted. Therefore, mail1.us.woodgrovebank.com, for example, would not be accepted as a match for woodgrovebank.com.

Best Practices for Domain Names for Internet SMTP

When you create a certificate or a certificate request for an Edge Transport server performing SMTP TLS over the Internet, the set of domain names that you should include in the request are as follows:

- **The fully qualified Internet domain name of the server** This may be different from the internal FQDN that is used between Edge Transport servers and Hub Transport servers and should match the A record that is published on the Internet (public) DNS server. This name should be entered as a CN in the *SubjectName* parameter of the **New-ExchangeCertificate** cmdlet.
- **All the accepted domain names of the organization** Use the *IncludeAcceptedDomains* parameter of the **New-ExchangeCertificate** cmdlet to populate the Subject Alternative Name for the resulting certificate.
- **The FQDN for the connector if it isn't covered by either of the previous items** Use the *DomainName* parameter of the **New-ExchangeCertificate** cmdlet to populate the Subject Alternative Name for the resulting certificate.

Wildcard Character Domain Names

Wildcard character domain names are a special type of domain name that represents multiple sub-domains. Wildcard character domain names can simplify certificates because a single wildcard domain name represents all the sub-domains for that domain. They are represented by an asterisk character (*) at the DNS node. For example, ***.contoso.com** represents **contoso.com** and all the sub-domains for **contoso.com**. When you use a wildcard character to create a certificate or a certificate request for all accepted domains, you can simplify the request significantly.

Certificate Selection

Exchange follows different certificate selection processes depending on the type of SMTP connection.

When Hub Transport servers are communicating with each other or with the Edge Transport servers in your organization, anonymous TLS certificates are used. For more information, see Selection of Inbound Anonymous TLS Certificates and Selection of Outbound Anonymous TLS Certificates.

When an SMTP host or client connects to the Edge or Hub Transport servers, then the STARTTLS certificate selection process is used. For more information, see Selection of Inbound STARTTLS Certificates.

Creating TLS Certificates

Exchange 2010 creates a self-signed certificate during installation that uses all the server and domain names that are known to Exchange at the time of installation. You can clone this certificate to use it on additional servers. You can also replace this certificate with certificates that are issued by a third-party CA. The following topics provide step-by-step instructions for each task.

- Generate Request for Third-Party Certificate Services
- Install Certificates Issued for Certificate Requests
- Clone an Existing Certificate

References

For more information about cryptography and certificate technologies and concepts, see the following publications:

- Windows Server 2008 PKI and Certificate Security
- Housley, Russ and Tim Polk. *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*. New York: John Wiley & Son, Inc., 2001.
- Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition. New York: John Wiley & Son, Inc., 1996.

1.7.1.33.1 TLS Functionality and Related Terminology in Exchange 2010

TLS Functionality and Related Terminology in Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-25*

Microsoft Exchange Server 2010 provides administrative functionality and other enhancements that improve the overall management of Transport Layer Security (TLS). As you work with this functionality, you need to learn about some TLS-related features and functionality. Some terms and concepts apply to more than one TLS-related feature. In this topic, a brief explanation of each feature is provided, which is intended to help you understand some differences and general terminology related to TLS and the Domain Security feature set:

- **Transport Layer Security** TLS is a standard protocol that's used to provide secure Web communications on the Internet or intranets. It enables clients to authenticate servers or, optionally, servers to authenticate clients. It also provides a secure channel by encrypting communications. TLS is the latest version of the Secure Sockets Layer (SSL) protocol.
- **Mutual TLS** Mutual TLS authentication differs from TLS as TLS is usually deployed. Typically, when TLS is deployed, it's used only to provide confidentiality in the form of encryption. No authentication occurs between the sender and receiver. In addition to this kind of deployment, sometimes when TLS is deployed, only the receiving server is authenticated. This deployment of TLS is typical of the HTTP implementation of TLS. This implementation, where

only the receiving server is authenticated, is SSL.
With mutual TLS authentication, each server verifies the identity of the other server by validating a certificate that's provided by that other server. In this scenario, where messages are received from external domains over verified connections in an Exchange 2010 environment, Microsoft Outlook displays a Domain Secured icon.

- **Domain Security** Domain Security is the set of features, such as certificate management, connector functionality, and Outlook client behavior that enables mutual TLS as a manageable and useful technology.
- **Opportunistic TLS** In earlier versions of Exchange, you had to configure TLS manually. In addition, you had to install a valid certificate, suitable for TLS usage, on the server running Exchange. In Exchange 2010, Setup creates a self-signed certificate. By default, TLS is enabled. This enables any sending system to encrypt the inbound SMTP session to Exchange. By default, Exchange 2010 also attempts TLS for all remote connections.
- **Direct trust** By default, all traffic between Edge Transport servers and Hub Transport servers is authenticated and encrypted. Again, the underlying mechanism for authentication and encryption is mutual TLS. Instead of using X.509 validation, Exchange 2010 uses direct trust to authenticate the certificates. Direct trust means that the presence of the certificate in Active Directory or Active Directory Lightweight Directory Services (AD LDS) validates the certificate. Active Directory is considered a trusted storage mechanism. When direct trust is used, it doesn't matter if the certificate is self-signed or signed by a certification authority. When you subscribe an Edge Transport server to the Exchange organization, the Edge Subscription publishes the Edge Transport server certificate in Active Directory for the Hub Transport servers to validate. The Microsoft Exchange EdgeSync service updates AD LDS with the set of Hub Transport server certificates for the Edge Transport server to validate.

1.7.1.33.2 Selection of Inbound Anonymous TLS Certificates

Selection of Inbound Anonymous TLS Certificates

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-23*

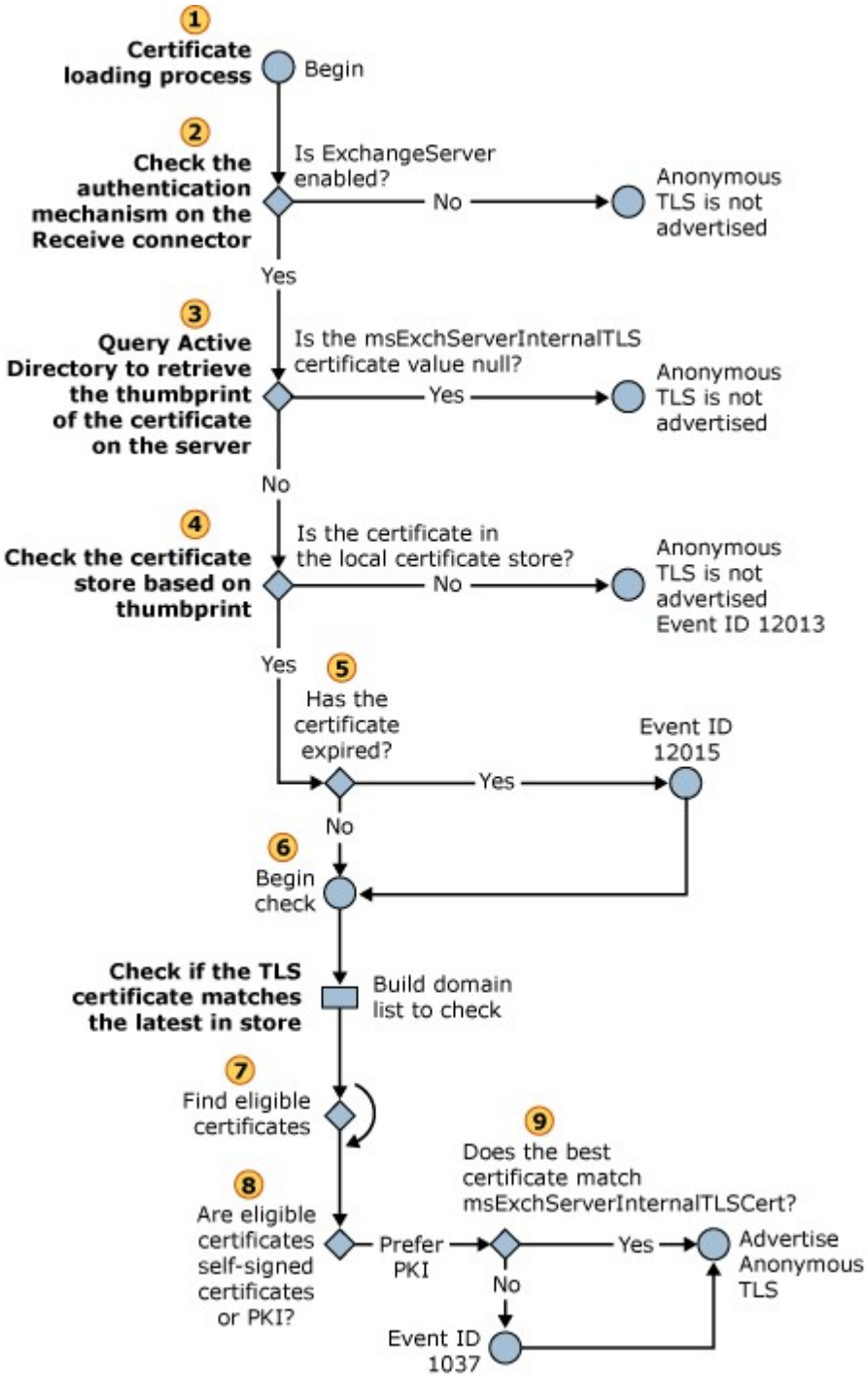
The selection of an inbound anonymous Transport Layer Security (TLS) certificate occurs in the following scenarios:

- SMTP sessions between Edge Transport servers and Hub Transport servers for authentication
- SMTP sessions between Hub Transport servers for encryption only by using public keys

For communication between Hub Transport servers, anonymous TLS and the public keys from certificates are used to encrypt the session. Kerberos is used for authentication. When an SMTP session is established, the receiving server initiates a certificate selection process to determine which certificate to use in the TLS negotiation. The sending server also performs a certificate selection process. For more information about that process, see Selection of Outbound Anonymous TLS Certificates.

This topic describes the selection process for inbound anonymous TLS certificates. All the

steps are performed on the receiving server. The following figure shows the steps of this process.



1. When the SMTP session is established, Microsoft Exchange calls a process to load the certificates.
2. In the load certificate function, the Receive connector to which the session is connected is checked to see whether the **AuthMechanism** property is set to a value of ExchangeServer. You can set the **AuthMechanism** property on the Receive connector by using the Set-ReceiveConnector cmdlet. You can

also set the **AuthMechanism** property to ExchangeServer by selecting **Exchange Server authentication** on the **Authentication** tab of a specific Receive connector.
If ExchangeServer isn't enabled as an authentication mechanism, the server doesn't advertise X-ANONYMOUSTLS to the sending server in the SMTP session and no certificate is loaded. If ExchangeServer is enabled as an authentication mechanism, the certificate selection process continues to the next step.

3. Microsoft Exchange queries Active Directory to retrieve the thumbprint of the certificate on the server. The **msExchServerInternalTLSCert** attribute on the server object stores the certificate thumbprint.
   If the **msExchServerInternalTLSCert** attribute can't be read or if the value is null, Microsoft Exchange doesn't advertise X-ANONYMOUSTLS and no certificate is loaded.

   Note:
   If the **msExchServerInternalTLSCert** attribute can't be read or if the value is null during startup of the Microsoft Exchange Transport service, instead of during the SMTP session, Event ID 12012 is logged in the Application log.

4. If a thumbprint is found, the certificate selection process searches the local computer certificate store for a certificate that matches the thumbprint. If the certificate isn't found, the server doesn't advertise X-ANONYMOUSTLS, no certificate is loaded, and Event ID 12013 is logged in the Application log.
5. After a certificate is loaded from the certificate store, it's checked to see whether it has expired. The *Valid to* field on the certificate is compared to the current date and time. If the certificate has expired, Event ID 12015 is logged in the Application log. In this case, the certificate selection process doesn't fail and continues with the remaining checks.
6. The certificate is checked to see whether it's the latest in the local computer's certificate store. As part of this check, a domain list is built for potential certificate domains. The domain list is based on the following computer configuration:
   - Fully qualified domain name (FQDN), such as mail.contoso.com
   - Host name, such as EdgeServer01
   - Physical FQDN, such as EdgeServer01.contoso.com
   - Physical host name, such as EdgeServer01

   Note:
   If the server is configured as a cluster or for a computer that's running Microsoft Windows Load Balancing, the following registry key is checked instead of the DnsFullyQualifiedDomainName setting: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WLBS\Parameters\Interface\{GUID}\ClusterName**

7. After the domain list is built, the certificate selection process checks to find all certificates in the certificate store that have a matching FQDN. From this list, the certificate selection process identifies a list of eligible certificates. Eligible certificates must meet the following criteria:
   - The certificate is an X.509 version 3 or a later version certificate.
   - The certificate has an associated private key.
   - The Subject or Subject Alternate Name fields contain the FQDN that was retrieved in step 6.
   - The certificate is enabled for Secure Sockets Layer (SSL)/TLS use. Specifically, the SMTP service has been enabled for this certificate by using the Enable-ExchangeCertificate cmdlet.
8. From the eligible certificates, the best certificate is selected based on the following sequence:
   - Sort eligible certificates by most recent *Valid from* date. *Valid from* is a Version 1 field on the certificate.

- The first valid public key infrastructure (PKI) certificate that's found in this list is used.
- If no valid PKI certificates are found, the first self-signed certificate is used.

9. After the best certificate has been determined, another check is made to determine whether its thumbprint matches the certificate that's stored in the **msExchServerInternalTLSCert** attribute. If the certificate matches, the certificate is used for X-ANONYMOUSTLS. If it doesn't match, Event ID 1037 is logged in the Application log. However, this doesn't cause X-ANONYMOUSTLS to fail.

1.7.1.33.3 Selection of Inbound STARTTLS Certificates

Selection of Inbound STARTTLS Certificates

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

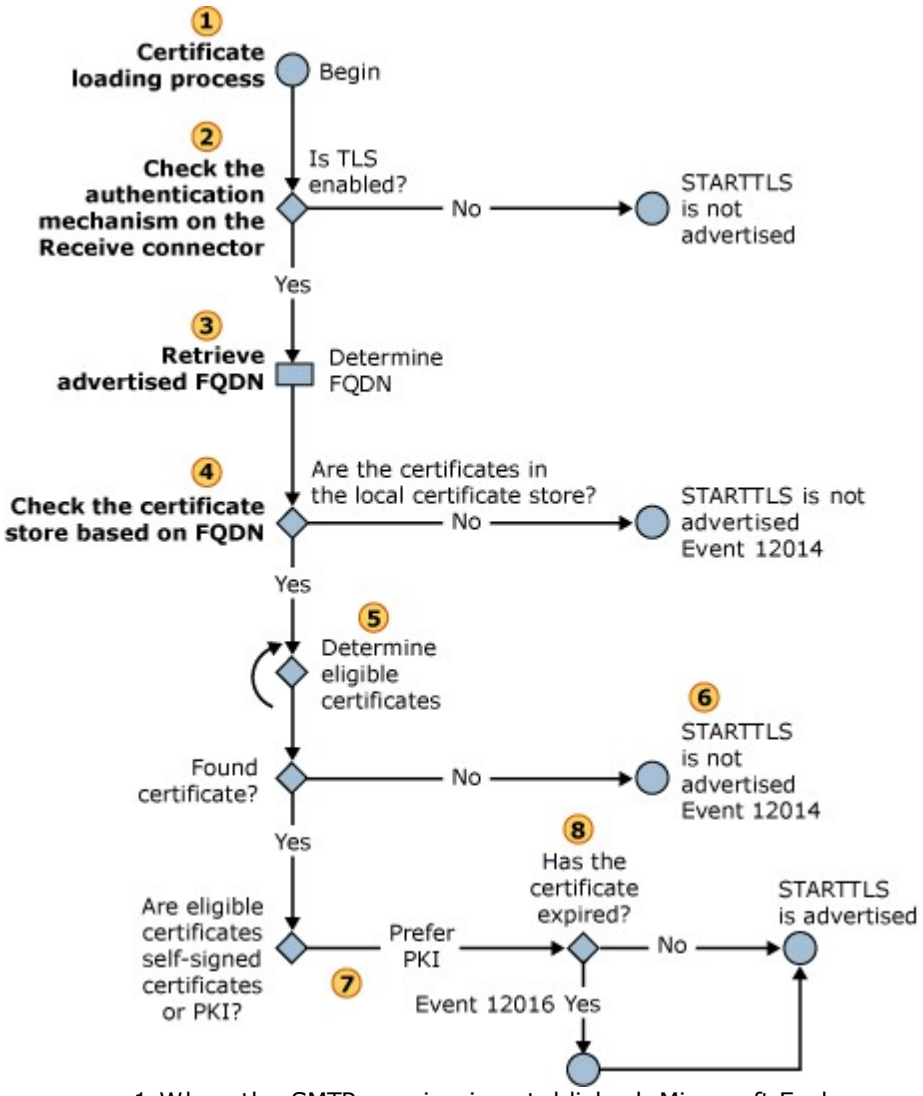
Topic Last Modified: *2011-04-27*

The selection of an inbound STARTTLS certificate occurs in the following scenarios:

- SMTP hosts request Transport Layer Security (TLS) with Edge Transport servers. The host that requests TLS with the Edge Transport server may be any other SMTP host. This also describes the Domain Security scenario. For more information about Domain Security, see Understanding Domain Security.
- SMTP clients, such as Microsoft Outlook Express, request TLS with Hub Transport servers.
- Internet-facing Hub Transport servers request TLS with an Edge Transport server.

When an SMTP session is established, the receiving server initiates a certificate selection process to determine which certificate to use in the TLS negotiation. The sending server also performs a certificate selection process. For more information about that process, see Selection of Outbound Anonymous TLS Certificates.

This topic describes the certificate selection process for inbound STARTTLS. All the steps described in this topic are performed on the receiving server. The following figure shows the steps of this process.



1. When the SMTP session is established, Microsoft Exchange calls a process to load the certificates.
2. In the load certificate function, the Receive connector to which the session is connected is checked to see whether the **AuthMechanism** property is set to a value of TLS. You can set the **AuthMechanism** property on the Receive connector by using the Set-ReceiveConnector cmdlet. You can also set the **AuthMechanism** property to TLS by selecting **Transport Security Layer (TLS)** on the **Authentication** tab of a specific Receive connector.
   If TLS isn't enabled as an authentication mechanism, the server doesn't advertise X-STARTTLS as an option to the sending server and no certificate is loaded. If TLS is enabled as an authentication mechanism, the certificate selection process continues to the next step.
3. The certificate selection process retrieves the fully qualified domain name (FQDN) value from the Receive connector configuration. If the FQDN value on the Receive connector is `null`, the server's physical FQDN is retrieved.
4. The certificate selection process searches the local computer certificate store for certificates that match the FQDN. If a certificate isn't found, the server doesn't advertise X-STARTTLS, no certificate is loaded, and Event ID 12014 is logged in the Application log.
5. The certificate selection process searches for all certificates in the certificate store that have a matching FQDN. From this list, the certificate selection process identifies a list of eligible certificates. Eligible certificates must meet

the following criteria:
- The certificate is an X.509 version 3 or a later version certificate.
- The certificate has an associated private key.
- The Subject or Subject Alternate Name fields contain the FQDN that was retrieved in step 3.
- The certificate is enabled for SSL/TLS use. Specifically, the SMTP service has been enabled for this certificate by using the Enable-ExchangeCertificate cmdlet.

6. If no eligible certificates are found after these checks, the server doesn't advertise X-STARTTLS, no certificate is loaded, and Event ID 12014 is logged in the Application log.
7. From the eligible certificates, the best certificate is selected based on the following sequence:
   - Sort eligible certificates by most recent *Valid from* date. *Valid from* is a Version 1 field on the certificate.
   - The first valid public key infrastructure (PKI) certificate that's found in this list is used.
   - If no valid PKI certificates are found, the first self-signed certificate is used.
8. The certificate is checked to see whether it has expired. The *Valid to* field in the certificate properties is compared to the current date and time. If the certificate hasn't expired, STARTTLS is advertised. If the certificate has expired, Event ID 12016 is logged in the Application log, but STARTTLS is still advertised.

1.7.1.33.4 Selection of Outbound Anonymous TLS Certificates

Selection of Outbound Anonymous TLS Certificates

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

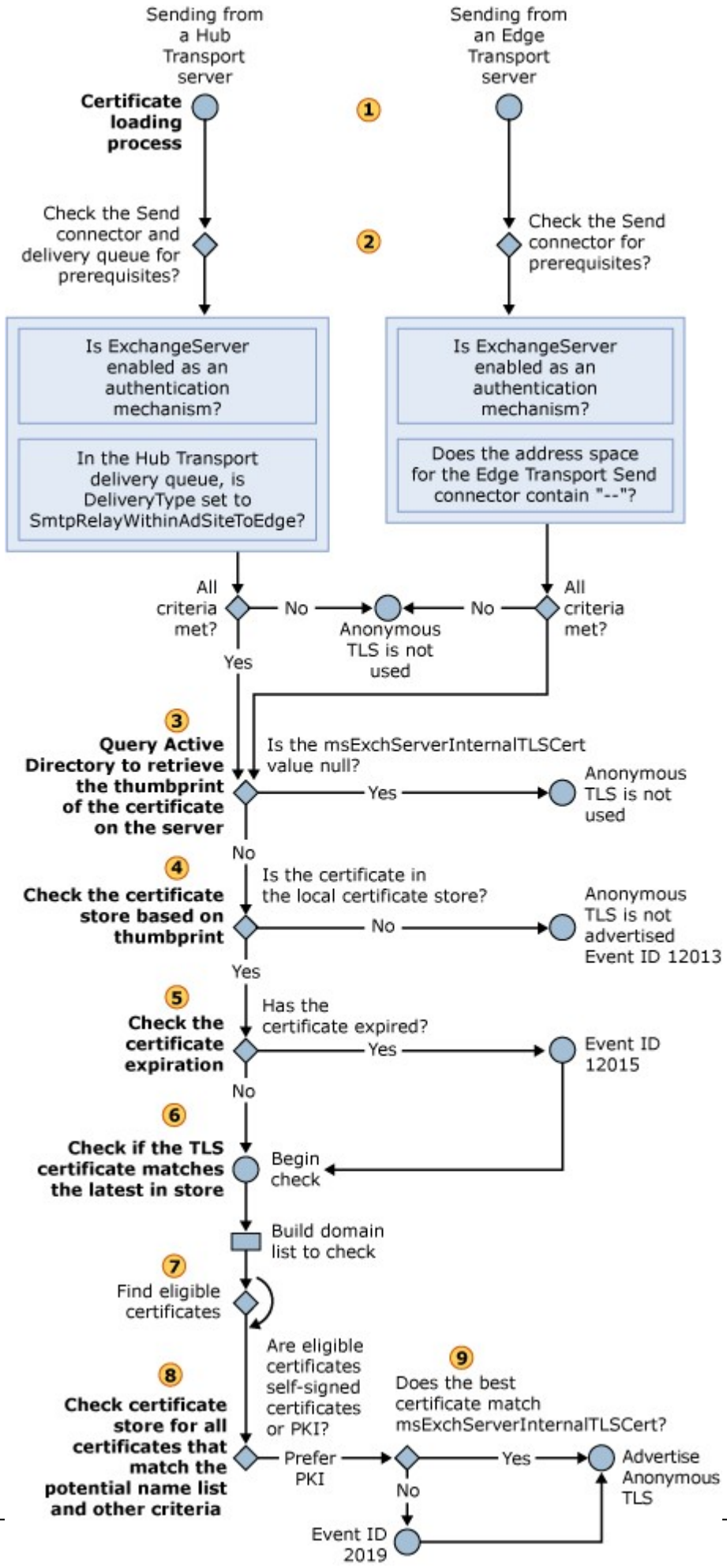
This topic describes the selection process for outbound anonymous Transport Layer Security (TLS) certificates in Microsoft Exchange Server 2010. The selection of an outbound anonymous TLS certificate occurs in the following scenarios:
- SMTP sessions between Edge Transport servers and Hub Transport servers for authentication
- SMTP sessions between Hub Transport servers for encryption only by using public keys

For communication between Hub Transport servers, anonymous TLS and the public keys from certificates are used to encrypt the session. When an SMTP session is established, the receiving server initiates a certificate selection process to determine which certificate to use in the TLS negotiation. The receiving server also performs a certificate selection process. For more information about that process, see Selection of Inbound Anonymous TLS Certificates.

Sending from a Hub Transport Server or an Edge Transport Server

All the steps for the selection of an outbound anonymous TLS certificate are performed on

the sending server. The following figure shows the steps of this process.


Sending from a Hub Transport server
Sending from an Edge Transport server
Certificate loading process
1
Check the Send connector and delivery queue for prerequisites?
2
Check the Send connector for prerequisites?
Is ExchangeServer enabled as an authentication mechanism?
In the Hub Transport delivery queue, is DeliveryType set to SmtpRelayWithinAdSiteToEdge?
Is ExchangeServer enabled as an authentication mechanism?
Does the address space for the Edge Transport Send connector contain "--"?
All criteria met?
No
Anonymous TLS is not used
No
All criteria met?
Yes
3
Query Active Directory to retrieve the thumbprint of the certificate on the server
Is the msExchServerInternalTLSCert value null?
Yes
Anonymous TLS is not used
No
4
Check the certificate store based on thumbprint
Is the certificate in the local certificate store?
No
Anonymous TLS is not advertised Event ID 12013
Yes
5
Check the certificate expiration
Has the certificate expired?
Yes
Event ID 12015
No
6
Check if the TLS certificate matches the latest in store
Begin check
Build domain list to check
7
Find eligible certificates
Are eligible certificates self-signed certificates or PKI?
9
Does the best certificate match msExchServerInternalTLSCert?
8
Check certificate store for all certificates that match the potential name list and other criteria
Prefer PKI
Yes
Advertise Anonymous TLS
No
Event ID 2019

1. When the SMTP session is established from a Hub Transport server or Edge Transport server, Microsoft Exchange calls a process to load the certificates.

   Note:
   During the initial loading of the certificate, the outbound certificate selection process is different for the Edge Transport server role and the Hub Transport server role. The figure shows the starting point for each server role.

2. The certificate loading process depends on whether the SMTP session is initiated from a Hub Transport server or an Edge Transport server.
   On a Hub Transport server The following checks are made:
   2.a. The Send connector to which the session is connected is checked to see whether the **SmartHostAuthMechanism** property is configured for `ExchangeServer`. You can set the **SmartHostAuthMechanism** property on the Send connector by using the **Set-SendConnector** cmdlet. You can also set the **SmartHostAuthMechanism** property to `ExchangeServer` by selecting **Exchange Server Authentication** on the **Configure Smart Host Authentication Settings** page of a specific Send connector. To open the **Configure Smart Host Authentication Settings** page, click **Change** on the **Network** tab of the Send connector properties page.
   2.b. The **DeliveryType** property of the message is checked to determine whether it's set to a value of `SmtpRelayWithinAdSitetoEdge`. You can view the **DeliveryType** property by running the **Get-Queue** cmdlet with the format list argument (| `Format-List`).
   Both of the following conditions must be met. If `ExchangeServer` isn't enabled as an authentication mechanism or if the **DeliveryType** property isn't set to `SmtpRelayWithinAdSitetoEdge`, the sending Hub Transport server doesn't use anonymous TLS and no certificate is loaded. If both conditions are met, the certificate selection process continues to step 3.
   On an Edge Transport server The following checks are made:
   2.c. The Send connector to which the session is connected is checked to see whether the **SmartHostAuthMechanism** property is configured for `ExchangeServer`. As noted earlier in this topic, you can set the **SmartHostAuthMechanism** property on the Send connector by using the **Set-SendConnector** cmdlet. You can also set the **SmartHostAuthMechanism** property to `ExchangeServer` by selecting **Exchange Server Authentication** on the **Configure Smart Host Authentication Settings** page of a specific Send connector. To open the **Configure Smart Host Authentication Settings** page, click **Change** on the **Network** tab of the Send connector properties page.
   2.d. The Send connector to which the session is connected is checked to determine whether the **SmartHost** address space property contains "- -".
   Both of the following conditions must be met. If `ExchangeServer` isn't enabled as an authentication mechanism or the address space doesn't contain "- -", the sending Edge Transport server doesn't use anonymous TLS and no certificate is loaded. If both conditions are met, the certificate selection process continues to step 3.
3. Microsoft Exchange queries Active Directory to retrieve the thumbprint of the certificate on the server. The **msExchServerInternalTLSCert** attribute on the server object stores the certificate thumbprint.
   If the **msExchServerInternalTLSCert** attribute can't be read or if the value is `null`, Microsoft Exchange doesn't advertise X-ANONYMOUSTLS in the SMTP session and no certificate is loaded.

   Note:
   If the **msExchServerInternalTLSCert** attribute can't be read or if the value is `null` during startup of the Microsoft Exchange Transport service, instead of during the SMTP session, Event ID 12012 is logged in the Application log.

4. If a thumbprint is found, the certificate selection process searches the local computer certificate store for a certificate that matches the thumbprint. If the certificate isn't found, the server doesn't advertise X-ANONYMOUSTLS, no certificate is loaded, and Event ID 12013 is logged in the Application log.
5. After a certificate is loaded from the certificate store, it's checked to see whether it has expired. The *Valid to* field on the certificate is compared to the current date and time. If the certificate has expired, Event ID 12015 is logged in the Application log. In this case, the certificate selection process doesn't fail and continues with the remaining checks.
6. The certificate is checked to see whether it's the latest in the local computer's certificate store. As part of this check, a domain list is built for potential certificate domains. The domain list is based on the following computer configuration:
   6.a. Fully qualified domain name (FQDN), such as mail.contoso.com
   6.b. Host name, such as EdgeServer01
   6.c. Physical FQDN, such as EdgeServer01.contoso.com
   6.d. Physical host name, such as EdgeServer01

   Note:
   If the server is running Microsoft Windows Load Balancing, the following registry key is checked instead of the DnsFullyQualifiedDomainName setting: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WLBS\Parameters\Interface\{GUID}\ClusterName**
7. After the domain list is built, the certificate selection process performs a search to find all certificates in the certificate store that have a matching FQDN. From this list, the certificate selection process identifies a list of eligible certificates. Eligible certificates must meet the following criteria:
   7.a. The certificate is an X.509 version 3 or a later version certificate.
   7.b. The certificate has an associated private key.
   7.c. The Subject or Subject Alternate Name fields contain the FQDN that was retrieved in step 6.
   7.d. The certificate is enabled for Secure Sockets Layer (SSL)/TLS use. Specifically, the SMTP service has been enabled for this certificate by using the Enable-ExchangeCertificate cmdlet.
8. From the eligible certificates, the best certificate is selected based on the following sequence:
   8.a. Sort eligible certificates by most recent *Valid from* date. *Valid from* is a Version 1 field on the certificate.
   8.b. The first valid public key infrastructure (PKI) certificate that's found in this list is used.
   8.c. If no valid PKI certificates are found, the first self-signed certificate is used.
9. After the best certificate has been determined, another check is made to determine whether its thumbprint matches the certificate that's stored in the **msExchServerInternalTLSCert** attribute. If the certificate matches, the certificate is used for X-ANONYMOUSTLS. If it doesn't match, Event ID 1037 is logged in the Application log. However, this doesn't cause X-ANONYMOUSTLS to fail.

1.7.1.33.5 Disabling TLS Between Active Directory Sites to Support WAN Optimization

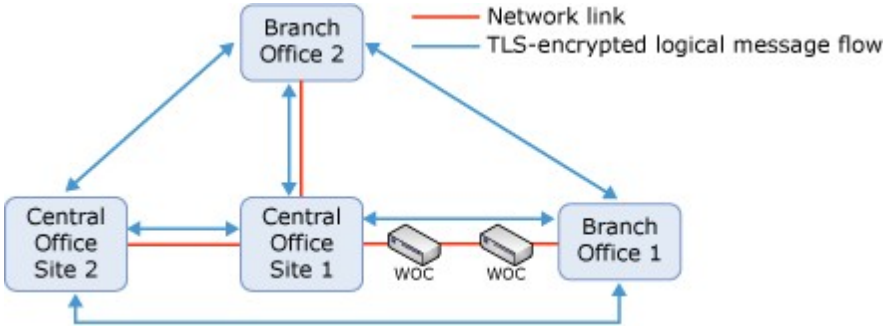
Disabling TLS Between Active Directory Sites to Support WAN Optimization

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

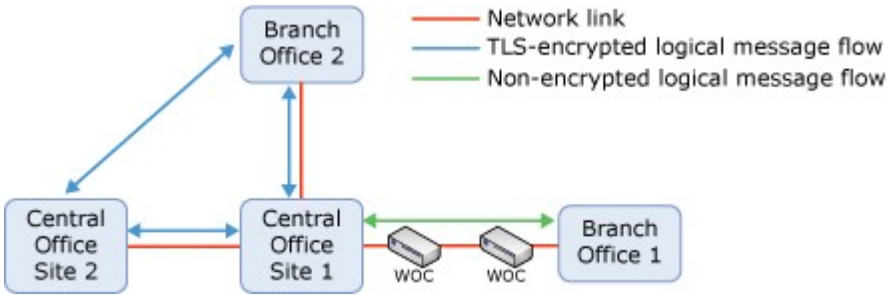
Topic Last Modified: *2009-12-01*

In Microsoft Exchange Server 2007, Transport Layer Security (TLS) encryption is mandatory for all SMTP communication between Hub Transport servers. This increases overall security of hub-to-hub communications. However, in certain topologies where WAN Optimization Controller (WOC) devices are used, the TLS encryption of SMTP traffic may be undesirable. Exchange Server 2010 supports disabling TLS for hub-to-hub communications for these specific scenarios.

Consider the topology shown in the following figure. The assumption for this four-site topology is that the two central office sites and Branch Office 2 are well-connected, whereas the connection between Central Office Site 1 and Branch Office 1 is over a WAN link. The company has installed WOC devices on this link to compress and optimize traffic over the WAN.



In this topology, because Exchange 2010 uses TLS encryption for communication between Hub Transport servers, the SMTP traffic that goes over the WAN link can't be compressed. Ideally, all SMTP traffic that goes over the WAN link should be unencrypted SMTP, while retaining TLS security within well-connected sites. Exchange 2010 gives you the option to disable TLS encryption for traffic between sites by configuring Receive connectors. Using this ability in Exchange 2010, you can configure an exception to the SMTP traffic between Central Office Site 1 and Branch Office 1, as shown in the following figure.



The recommended configuration is to limit the non-encrypted SMTP traffic to only those messages that pass over the WAN link. Therefore, the intrasite hub-to-hub traffic in all sites, and the cross-site hub-to-hub communications that don't involve Branch Office 1 should all be TLS encrypted.

To achieve this end result, you need to do the following, in the specified order, on every Hub Transport server in the sites that contain the WOC devices (Central Office Site 1 and Branch Office 1 in the sample topology):

1. Enable downgraded Exchange Server authentication.
2. Create a Receive connector to handle the traffic over the connection that has WOC devices.

3. Configure the remote IP address range property of the new Receive connector to the IP address ranges of the Hub Transport servers in the remote site.
4. Disable TLS on the new Receive connector.

In addition, you need to do the following to ensure all SMTP traffic over the WAN is handled by the new Receive connectors you created:

- Configure the sites that will participate in the non-TLS communication as hub sites to force all message flow through the new Receive connectors (Central Office Site 1 and Branch Office Site 1 in the sample topology).
- Verify that the IP site link costs are configured in a way that ensures the least cost routing path to your remote site (Branch Office 1 in the sample topology) goes through the network link that has the WOC devices.

The following sections provide an overview of each of these steps. For step-by-step instructions on how to configure your Hub Transport servers to disable TLS, see Suppress Anonymous TLS Connections.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Downgrading Authentication over TLS-Disabled Connections

Kerberos authentication is used with TLS encryption in Exchange. When you disable TLS on hub-to-hub communications, you need to perform another form of authentication. When Exchange 2010 communicates with other servers running Exchange that don't support X-ANONYMOUSTLS, such as the Exchange Server 2003 servers, it falls back to using GSSAPI (Generic Security Services Application Programming Interface) authentication. All communications between Exchange 2010 Hub Transport servers use X-ANONYMOUSTLS. By configuring your Hub Transport server to use downgraded Exchange Server authentication, you are in effect enabling it to use GSSAPI when communicating with other Exchange 2010 Hub Transport servers.

Return to top

Creating and Configuring Receive Connectors

You need to create Receive connectors that will solely be responsible for handling the non-TLS encrypted traffic. Using separate Receive connectors for this purpose ensures that all traffic that doesn't pass through the WAN link remains protected by TLS encryption.

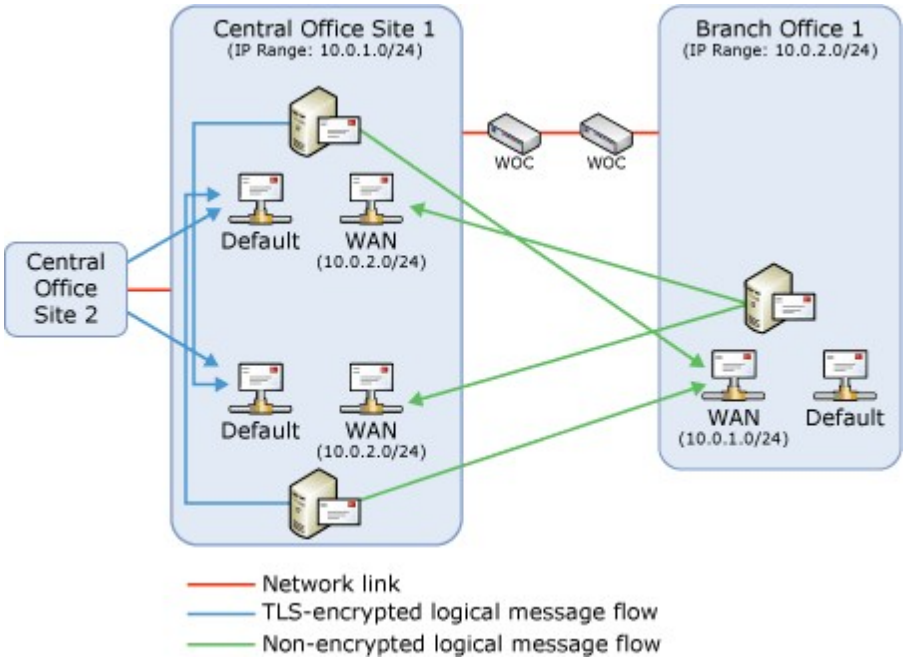
To restrict the new Receive connectors to only the traffic over the WAN, you need to

configure the remote IP address range property. Exchange always uses the connector with the most specific remote IP address range. Therefore, these new connectors will be preferred over the default Receive connector configured to receive messages from anywhere.

Going back to the sample topology, assume that the class C subnet 10.0.1.0/24 is used for the Central Office Site 1 and 10.0.2.0/24 is used for the Branch Office 1. To prepare for disabling TLS between these two sites, you need to:

1. Create a Receive connector (called WAN) on each Hub Transport server in Central Office Site 1 and Branch Office 1.
2. Configure the remote IP address range of 10.0.2.0/24 on each new Receive connector in Central Office Site 1.
3. Configure the remote IP address range of 10.0.1.0/24 on each new Receive connector in Branch Office 1.
4. Disable TLS on all of the new Receive connectors.

The end result is shown in the following figure (with the remote IP address range property of the WAN Receive connectors shown in parentheses). Only a single Hub Transport server is shown in Branch Office 1, and Branch Office 2 is omitted for clarity purposes.



Return to top

Creating Hub Sites

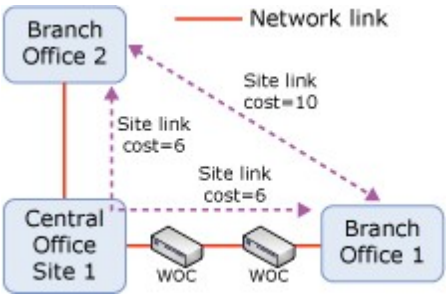
By default, an Exchange 2010 Hub Transport server will attempt a direct connection to the Hub Transport server closest to the final destination of a specific message. In the sample topology, if a user in Branch Office 2 sends a message to a user in Branch Office 1, the Hub Transport server in Branch Office 2 will connect to the Hub Transport server in Branch Office 1 directly to deliver that message. That connection will be encrypted and therefore not desirable in the specific topology. To have such messages pass through the Hub Transport servers on Central Office Site 1, thereby ensuring they aren't encrypted while in transit over the WAN link, Central Office Site 1 and Branch Office 1 need to be configured as hub sites. In short, any site where you have a Hub Transport server with a Receive

connector with TLS disabled needs to be configured as a hub site, so you can force servers in other sites to route traffic through that site. For more information about hub sites, see "Implementing Hub Sites" in Understanding Message Routing.

Return to top

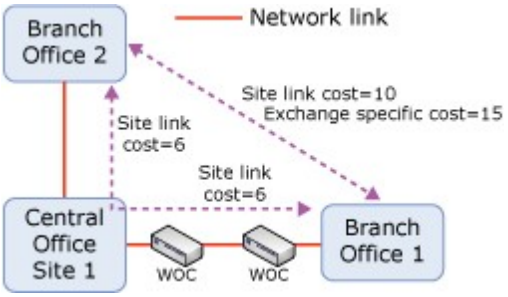
Configuring Site Link Costs

Configuring hub sites alone isn't sufficient to ensure that all traffic is unencrypted over the WAN link. This is because Exchange will route messages through hub sites only if the hub site lies within the least cost routing path. For example, assume that the IP site link costs for our sample topology are configured in Active Directory as shown in the following figure (Central Office Site 2 is omitted for clarity).



In this case, the path from Branch Office 2 to Branch Office 1 that goes through the hub site has a total cost of 12 (6+6), whereas the cost of the direct path is 10. Therefore, none of the messages from Branch Office 2 to Branch Office 1 will go through Central Office Site 1 and therefore all of that traffic will still be TLS encrypted.

To avoid this issue, you need to designate an Exchange-specific cost that is higher than 12 for the IP site link between Branch Office 2 and Branch Office 1, as shown in the following figure. This will ensure that all messages go through the unencrypted channel between Central Office Site 1 and Branch Office 1.



For more information about configuring Exchange-specific IP site link costs, see "Controlling IP Site Link Costs" in Understanding Message Routing.

Return to top

1.7.1.34 Understanding Transport Agents

Understanding Transport Agents

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-15*

Transport agents let you install custom software, created by Microsoft, by third-party vendors, or by your organization, on a computer that is running Microsoft Exchange Server 2010. This software can then process e-mail messages that pass through the transport pipeline on a Hub Transport server or Edge Transport server. Custom transport agents provide additional functionality to Exchange 2010, such as anti-spam or antivirus programs or any transport function that your organization may require.

Transport agents are typically installed automatically as part of applications that are designed to function together with Exchange 2010. However, there may be instances where organizations want to develop their own transport agents to manage mail that flows through their Exchange 2010 organization.

Caution:
Transport agents have full access to all e-mail messages that they encounter. Exchange puts no restrictions on a transport agent's behavior. Transport agents that are unstable or contain security flaws may affect the stability and security of Exchange. Therefore, you must only install transport agents that you fully trust and that have been fully tested in a test environment.

Looking for management tasks related to managing transport agents? See Managing Transport Agents.

Contents

Transport Agents and SMTP Events

Transport agents that are written for Exchange 2010 use SMTP events. These events are triggered as messages move through the transport pipeline. SMTP events give transport agents access to messages at specific points during the SMTP conversation and during routing of messages through the organization. The following tables list the SMTP events that provide access to messages in the transport pipeline.

SMTP Receive events

Sequence	SMTP event	Description
1	**OnConnect**	This event is triggered upon initial connection from a remote SMTP host.

2	**OnEhloCommand**	This event is triggered when the EHLO SMTP verb is issued by the remote SMTP host.
3	**OnHeloCommand**	This event is triggered when the HELO SMTP verb is issued by the remote SMTP host.
4	**OnAuthCommand**	This event is triggered when the AUTH SMTP verb is issued by the remote SMTP host.
5	**OnEndOfAuthentication**	This event is triggered when the remote SMTP host has completed authentication.
6	**OnMailCommand**	This event is triggered when the MAIL FROM SMTP verb is issued by the remote SMTP host.
7	**OnRcptToCommand**	This event is triggered when the RCPT TO SMTP verb is issued by the remote SMTP host.
8	**OnDataCommand**	This event is triggered when the DATA SMTP verb is issued by the remote SMTP host.
9	**OnEndOfHeaders**	This event is triggered when the remote SMTP host as completed submitting the e-mail message headers.
10	**OnEndOfData**	This event is triggered when the remote SMTP host issues <CRLF>, which indicates the end of data.
**	**OnHelpCommand**	This event is triggered when the HELP SMTP verb is issued by the remote SMTP host. This event can occur at any time after the **OnConnect** SMTP event and before the **OnDisconnect** SMTP event.
**	**OnNoopCommand**	This event is triggered when the NOOP SMTP verb is issued by the remote SMTP host. This event can occur at any time after the **OnConnect** SMTP event and before the **OnDisconnect** SMTP event.
**	**OnReject**	This event is triggered when the receiving SMTP host issues a temporary or permanent delivery status notification (DSN) code to the

		sending SMTP host. This event can occur at any time after the **OnConnect** SMTP event and before the **OnDisconnect** SMTP event.
**	**OnRsetCommand**	This event is triggered when the RSET SMTP verb is issued by the sending SMTP host. This event can occur at any time after the **OnConnect** SMTP event and before the **OnDisconnect** SMTP event.
11	**OnDisconnect**	This event is triggered upon disconnection of the SMTP conversation by either a receiving or sending SMTP host.

Categorizer events

Sequence	Categorizer event	Description
1	**OnSubmittedMessage**	This event is triggered upon submission of a message into the Submission queues on the receiving SMTP host. All messages encounter this event whether they arrived via SMTP submission, MAPI submission, or the Pickup or Replay directories.
2	**OnResolvedMessage**	This event is triggered after all the recipients have been resolved, but before the next hop has been determined for each recipient. The **OnResolvedMessage** routing event enables subsequent events to override the default routing behavior by using the per-recipient **SetRoutingOverride** method.
3	**OnRoutedMessage**	This event is triggered after messages have been categorized, distribution lists have been expanded, and recipients have been resolved.
4	**OnCategorizedMessage**	This event is triggered when the Categorizer completes processing the message.

Transport agents can be registered on any of the SMTP events that are listed in the preceding tables. However, the intended action of the transport agent usually dictates which SMTP events it will run on.

Consider anti-spam agents as an example. For these agents, the most important consideration, other than the validity of the message contents, is the point at which a valid spam message is identified and rejected. The sooner a message that has been confirmed to be spam is rejected, the lower the cost to your organization. All the SMTP events that are triggered before the **OnEndOfData** SMTP event do not require that a non-delivery receipt (NDR) be generated by the receiving SMTP host. An NDR isn't generated because the full message contents aren't delivered before the **OnEndOfData** SMTP event is reached. Therefore, the sending SMTP host is still responsible for the final delivery of the message. If delivery to the receiving SMTP host fails before the **OnEndOfData** SMTP event, the sending SMTP host must generate the NDR to the message sender. After the **OnEndOfData** SMTP event is reached, the receiving SMTP host has accepted the full contents of the message. This means that the SMTP host now has the responsibility to successfully deliver the message and generate and send an NDR to the message sender. Therefore, it's critical that an anti-spam agent register itself on the SMTP events before the **OnEndOfData** SMTP event is reached to reduce the chance that the receiving SMTP host will store the message contents and have to generate an NDR to the message sender.

However, for antivirus agents, the most important consideration is to make sure that every message is scanned. Agents that must see every message must be configured on the **OnSubmittedMessage** SMTP event. Every message that flows through the transport pipeline encounters the **OnSubmittedMessage** SMTP event because it occurs after all the possible submission entry points, such as SMTP submission from remote hosts, MAPI submission from computers that are running the Mailbox server role, the Pickup directory that is used by custom applications, or the Replay directory used by third-party e-mail applications.

Return to top

Prioritization of Transport Agents

Exchange 2010 lets you specify the priority of transport agents that are included with Exchange and that are added by custom applications. If you specify the priority of a transport agent, you can control which agents act on a message first. Transport agents can be assigned a priority of 1 or higher. Transport agents with a priority closer to 1 are applied to messages first. However, the priority that you assign to a transport agent is only one factor that is used to determine the order in which transport agents are applied to messages. The second factor that is used to determine the priority of transport agents is where the SMTP event that has a registered transport agent fits within the sequence of SMTP events.

As shown in the tables earlier in this topic, SMTP events have a specific sequence in which they are applied to messages that flow through the transport pipeline. Because transport agents are registered to specific SMTP events, the priority only comes into play for agents that are registered to the same SMTP event.

For example, you may have transport agents configured as follows:

- Transport agent **AgentA** with a priority of 1 registered to the **OnEndofHeaders** SMTP event
- Transport agent **AgentB** with a priority of 4 registered to the **OnMailCommand** SMTP event

When you view the list of registered agents by using the **Get-TransportAgent** cmdlet, transport agent **AgentA** is listed with a higher priority than transport agent **AgentB**. However, when a message flows through the transport pipeline, transport agent **AgentB** will be applied to the message before transport agent **AgentA** because the **OnMailCommand** SMTP event encounters the message before the **OnEndOfHeaders** SMTP event.

Return to top

Built-In Transport Agents

Exchange 2010 includes several default transport agents that enable it to provide features such as transport rules and journaling. By default, the transport agents listed in the following tables are installed on Hub Transport servers and Edge Transport servers. The following tables also provide links to topics that contain more information about each agent.

Hub Transport server transport agents

Agent Name	Priority	SMTP events	Related topic
Transport Rule agent	1	**OnRoutedMessage**	Understanding Transport Rules
RMS Decryption agent	The priority of this agent isn't user-configurable.	**OnSubmittedMessage**	Understanding Information Rights Management
Journal Report Decryption agent	The priority of this agent isn't user-configurable.	**OncCategorizedMessage**	Understanding Journaling
RMS Encryption agent	The priority of this agent isn't user-configurable.	**OnRoutedMessage**	Understanding Information Rights Management
Prelicensing agent	The priority of this agent isn't user-configurable.	**OnRoutedMessage**	Understanding Information Rights Management
Journaling agent	The priority of this agent isn't user-configurable.	**OnSubmittedMessage, OnRoutedMessage**	Understanding Journaling

Edge Transport server transport agents

Agent name	Priority	SMTP events	Related topic
Connection Filtering agent	1	**OnConnectEvent**, **OnMailCommand**, **OnRcptComand**, **OnEndOfHeaders**	Understanding Connection Filtering
Address Rewriting Inbound agent	2	**OnRcptCommand**, **OnEndOfHeaders**	Understanding Address Rewriting
Edge Rule agent	3	**OnEndOfData**	Understanding Transport Rules
Content Filter agent	4	**OnEndOfData**	Understanding Content Filtering
Sender ID agent	5	**OnEndOfHeaders**	Understanding Sender ID
Sender Filter agent	6	**OnMailCommand**, **OnEndOfHeaders**	Understanding Sender Filtering
Recipient Filter agent	7	**OnRcptCommand**	Understanding

			Recipient Filtering
Protocol Analysis agent	8	**OnEndOfHeaders**, **OnEndOfData**, **OnReject**, **OnRsetCommand**, **OnDisconnectEvent**	Understanding Protocol Logging
Attachment Filtering agent	9	**OnEndOfData**	Understanding Attachment Filtering
Address Rewriting Outbound agent	10	**OnRcptCommand**, **OnEndOfHeaders**	Understanding Address Rewriting

Return to top

Troubleshooting Transport Agents

With transport agents, Exchange helps you control the flow of e-mail messages through your organization. This capability enables you to match your Exchange infrastructure to your organization's requirements instead of forcing your organization to match your e-mail infrastructure. As you customize your environment, the complexity of that environment increases. To help you troubleshoot issues that may occur and to help you verify that the changes that you make are applied to messages in the manner you expect, Exchange provides the following features:

- **Get-TransportPipeline cmdlet** The **Get-TransportPipeline** cmdlet shows all the enabled transport agents, and the SMTP events on which they are registered, that have encountered messages in the transport pipeline between the time when the Microsoft Transport service was started and the time when the cmdlet was run. For more information, see View Transport Agents in the Transport Pipeline.

  Note:
  The information that is displayed by the **Get-TransportPipeline** cmdlet is generated only after a message has been sent through the transport pipeline. Also, only the transport agents that encountered the message are displayed.

- **Pipeline Tracing** Pipeline tracing enables you to create an exact snapshot of a whole message before and after it encounters each transport agent. Pipeline tracing enables you to determine which transport agent may have generated unexpected results or to verify that the transport agent behaves as expected.

1.7.1.35 Understanding Transport Database Configuration Options

Understanding Transport Database Configuration Options

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-26*

Servers that have the Microsoft Exchange Server 2010 Hub Transport server role or the

Edge Transport server role installed use Extensible Storage Engine (ESE) database technology for certain transport server components. Formerly known as JET, ESE is a method that defines a low-level API to the underlying database structures in Exchange 2010. ESE is used for the following transport components:

- **Message queue database** A *queue* is a temporary holding location for messages waiting to enter the next stage of processing. Each queue represents a logical set of messages that a transport server processes in a specific order. For more information, see Understanding Transport Queues.
- **IP filter database** The IP filter database stores the IP Allow lists and IP Block lists that are part of connection filtering. For more information, see Understanding Connection Filtering.

The message queue database and the IP filter database are separate ESE databases. These databases don't share any resources. However, you can configure ESE database configuration options on the Hub Transport server or Edge Transport server that apply to all the ESE databases that exist on the server.

Overview of ESE Databases

ESE databases use log files to accept, track, and maintain data. To enhance performance, all transactions are written first to log files and memory, and then to the database file. The checkpoint file tracks the transaction log entries that have been committed to the database. During an ordinary shutdown of the Microsoft Exchange Transport service, uncommitted database changes found in the transaction logs are always committed to the database.

Circular logging is used for the message queue database and the IP filter database. This means that the history of committed transactions found in the transaction logs isn't maintained. Any transaction logs older than the current checkpoint are immediately and automatically deleted. Therefore, the transaction logs can't be replayed for message queue database recovery or IP filter database recovery from backup.

Understanding Storage Configuration

For best practice guidance about the storage configuration of ESE databases, see Understanding Storage Configuration.

Configuring Shared ESE Database Options on Transport Servers

The shared ESE database configuration options are available in the EdgeTransport.exe.config application configuration file located in the C:\Program Files\Microsoft\Exchange Server\V14\Bin directory. The EdgeTransport.exe.config file is an XML application configuration file associated with the EdgeTransport.exe file. EdgeTransport.exe and MSExchangeTransport.exe are the executable files used by the Microsoft Exchange Transport service. This service runs on every Hub Transport server or Edge Transport server. Changes saved to the EdgeTransport.exe.config file are applied after the Microsoft Exchange Transport service is restarted. If a configuration option is missing or is present and contains the default value, the default value is enforced.

This example shows the typical structure of the EdgeTransport.exe.config file.

```
<configuration>
   <runtime>
      <gcServer enabled="true" />
   </runtime>
```

```
   <appSettings>
      <add key="Configuration Option" value="Value" />
      ...
   </appSettings>
</configuration>
```

You can add new configuration options or modify existing configuration options in the <appSettings> section. Many configuration options are unrelated to the shared ESE database options. Any configuration options that don't involve the shared ESE database options are outside the scope of this topic.

Note:

The parameter names in the <add key=../> section are case sensitive.

For information about the message queue database parameters available in the EdgeTransport.exe.config file, see Understanding Transport Queues.

The following table shows the shared ESE database configuration options available in the EdgeTransport.exe.config file.

Shared ESE database configuration options

Parameter name	Description
DatabaseCacheFlushStart	This parameter enables the removal of cached database transactions from memory when the cache is overused. The value of this parameter represents the percentage of the cache that's unused. When the free database cache resources drop under the specified percentage, a background process writes the cached database transactions to the transaction log. The default value is 3.
DatabaseCacheFlushStop	This parameter suspends the removal of cached database transactions from memory when the cache utilization level returns to normal. The value of this parameter represents the percentage of the cache that's unused. When the free database cache resources increase to more than the specified percentage, the background process that writes the cached database transactions to the transaction log is suspended. The default value is 5.
DatabaseCheckPointDepthMax	This parameter controls the total allowed size of all uncommitted transaction logs that exist on the hard disk drive. The default value is **512MB**. Setting the value of the *DatabaseCheckPointDepthMax* parameter too low can cause significant performance issues because uncommitted transactions are forcibly committed to the database instead of being written to transaction logs. We recommend that you don't modify the default value of the *DatabaseCheckPointDepthMax* parameter.
DatabaseMaxCacheSize	This parameter specifies the maximum size of the database cache in memory. The

	default value is **1GB**.

Remember that the message queue database and the IP filter database are isolated from one another. The ESE database files don't share database files, transaction logs, or caches. The shared configuration options apply to each database and its supporting infrastructure. For example, when you set the *DatabaseMaxCacheSize* parameter, you are also setting the maximum cache size for the message queue database and the IP filter database.

1.7.1.36 Understanding Transport Logs

Understanding Transport Logs

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-09*

Transport logs are generated by Hub Transport and Edge Transport servers and they provide information about the functioning of your transport pipeline. Transport servers can generate agent, connectivity, message tracking, protocol, and routing table logs. The following topics provide detailed information about each of these logs.

Understanding Agent Logging

Understanding Connectivity Logging

Understanding Message Tracking

Understanding Protocol Logging

Understanding Routing Table Logging

1.7.1.36.1 Understanding Agent Logging

Understanding Agent Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-17*

Agent logs record the actions performed on a message by specific anti-spam agents installed and configured on a computer running Microsoft Exchange Server 2010 that has the Edge Transport server role or the Hub Transport server role installed. Only the following agents can write information to the agent log:

- Connection Filter agent
- Content Filter agent
- Edge Rules agent
- Recipient Filter agent
- Sender Filter agent
- Sender ID agent

The information written to the agent log depends on the agent, the SMTP event, and the action performed on the message.

The only configurable option for agent logging is the *AgentLogEnabled* parameter in the EdgeTransport.exe.config application configuration file. By default, agent logging is enabled on Hub Transport servers or Edge Transport servers. The other agent log values that aren't configurable are described in the following list:

- Path where the agent logs are stored is C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\AgentLog.
- Maximum size for the individual agent log files is 10 megabytes (MB).
- Maximum size for the directory that contains the agent log files is 250 MB.
- Maximum age for the agent log files is 30 days.

The Exchange 2010 server uses circular logging to limit the agent logs based on file size and file age to help control the hard disk space used by the log files.

Note:
If you want to keep the agent log files longer than allowed by file age or directory size values that you can't configure, you can create a scheduled task that periodically moves the unused agent log files to a different location.

Note:
By default, the transport logging process has a logging level value of 0 (Lowest). If you want Exchange to write an event log entry when circular logging removes a log file, you must change the logging level value of the transport logging process to 5 (Maximum) or 7 (Expert).

Contents

Looking for management tasks related to agent logging? See Managing Transport Servers.

Overview of Transport Agents

Agents can only act upon messages at specific points in the SMTP command sequence used to transport the messages through a Hub Transport server or Edge Transport server. These access points in the SMTP command sequence are called *SMTP events*. Each agent has a priority value that can be assigned. However, the SMTP events must always occur in a specific order. Therefore, the agent priority depends on the SMTP event. If two agents can act on a message during the same SMTP event, the agent that has the highest priority will act on the message first.

The following table lists the SMTP events in order of occurrence and the agents that write information to the agent log in order of priority from highest to lowest for each SMTP event.

SMTP events in order of occurrence and the agents that write

information to the agent log in order of priority for each SMTP event

SMTP event	Agent
OnConnect	Connection Filter agent
OnMailCommand	Connection Filter agent Sender Filter agent
OnRcptCommand	Connection Filter agent Recipient Filter agent
OnEndOfHeaders	Connection Filter agent Sender ID agent Sender Filter agent
OnEndOfData	Edge Rules agent Content Filter agent

For more information about agents, SMTP events, and agent priority, see Understanding Transport Agents.

Return to top

Structure of the Agent Log Files

The agent logs exist in C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\AgentLog.

The naming convention for the agent log files is AGENTLOG*yyyymmdd-nnnn*.log. The placeholders represent the following information:

- The placeholder *yyyymmdd* is the Coordinated Universal Time (UTC) date that the log file was created. The placeholder *yyyy* = year, *mm* = month, and *dd* = day.
- The placeholder *nnnn* is an instance number that starts at the value of 1 for each day.

Information is written to the log file until the file size reaches 10 MB. Then, a new log file that has an incremented instance number is opened. This process is repeated throughout the day. Circular logging deletes the oldest log files when the agent log directory reaches 250 MB, or when a log file is 30 days old.

The agent log files are text files that contain data in the comma-separated value file (CSV) format. Each agent log file has a header that contains the following information:

- **#Software** Name of the software that created the agent log file. Typically, the value is Microsoft Exchange Server.
- **#Version** Version number of the software that created the agent log file. Currently, the value is 8.0.0.0.
- **#Log-Type** Log type value, which is Agent Log.
- **#Date** UTC date-time when the log file was created. The UTC date-time is represented in the ISO 8601 date-time format: *yyyy-mm-ddThh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu, which is another way to denote UTC.

- **#Fields** Comma delimited field names used in the agent log files.

Return to top

Information Written to the Agent Log

The agent log stores each agent transaction on a single line in the log. The information stored on each line is organized by fields. These fields are separated by commas. The field name is generally descriptive enough to determine the type of information it contains. However, some of the fields may be blank. Or the type of information stored in the field may change based on the agent or the action performed on the message by the agent. The following table describes the fields used to classify each agent transaction.

Fields used to classify each agent transaction

Field name	Description
Timestamp	UTC date-time of the agent event. This is represented in the ISO 8601 format. The value is formatted as *yyyy-mm-ddThh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu, which is another way to denote UTC.
SessionId	Unique SMTP session identifier. This identifier is represented as a 16-digit hexadecimal number.
LocalEndpoint	Local IP address and port number that accepted the message. SMTP sessions typically use port 25.
RemoteEndpoint	IP address and port number of the previous SMTP server that connected to this server to deliver the message. In an Edge Transport server and Hub Transport server topology, the value of **RemoteEndpoint** in the agent log on the Hub Transport server will be the IP address of the Edge Transport server. Even though the message is transmitted by SMTP, the port number used by the sending server will be a random number larger than 1,024.
EnteredOrgFromIP	IP address of the remote SMTP server that first connected to the Exchange organization to deliver the message. On an Edge Transport server, the value of **RemoteEndpoint** and **EnteredOrgFromIP** are the same. Anti-spam agents use the IP address in **EnteredOrgFromIP** to examine a message.
MessageId	Value of the `MessageID` header field. If this value is blank, the Exchange 2010 transport server assigns an arbitrary value, but only if the message is accepted. After assigned, the value of `MessageID` is constant for the lifetime of the message.
P1FromAddress	Sender e-mail address specified in `MAIL FROM` in the message envelope. This value is used to transport the message between SMTP messaging servers. This value serves as a comparison to the

	value of **P2FromAddresses** to determine whether the sender address in the message header is forged.
P2FromAddresses	Sender e-mail address specified in the `From` header field or in the `Sender` header field in the message header.
Recipient	E-mail address of the recipients. Although the original message may contain multiple recipients, only one recipient is displayed per line in the agent log.
NumRecipients	Total number of recipients in the original message.
Agent	Name of the agent that took the action. The possible values are as follows: • Connection Filter agent • Content Filter agent • Edge Rules agent • Recipient Filter agent • Sender Filter agent • Sender ID agent
Event	SMTP event where the action was taken by the agent. The value of **Event** depends on the agent. The SMTP events available to each agent are described in the first table earlier in this topic. The possible values for **Event** are as follows: • OnConnect • OnEndOfHeaders • OnEndOfData • OnMailCommand • OnRcptCommand
Action	Action performed on the message by the agent. The possible values for **Action** are as follows: • AcceptMessage • DeleteMessage • DeleteRecipients • Disconnect • QuarantineMessage • QuarantineRecipients • RejectAuthentication • RejectCommand • RejectConnection • RejectMessage • RejectRecipients
SmtpResponse	Enhanced SMTP response as defined in RFC 2034.
Reason	Reason for the action supplied by the agent.
ReasonData	Descriptive details for the action supplied by the agent.

Return to top

Searching the Agent Logs

You can use the **Get-AgentLog** cmdlet in the Exchange Management Shell and the Get-AntiSpamFilteringReport script to search the agent logs. For more information, see Get-AgentLog.

Return to top

Enable or Disable Agent Logging

By default, agent logging is enabled on a Hub Transport server or an Edge Transport server. Agent logging is enabled or disabled by modifying the EdgeTransport.exe.config file located in C:\Program Files\Microsoft\Exchange Server\V14\Bin. For more information, see Understanding the EdgeTransport.exe.Config File. EdgeTransport.exe and MSExchangeTransport.exe are the executable files used by the Microsoft Exchange Transport service.

Many available configuration options are unrelated to agent logging. Any configuration options that don't involve agent logging are outside the scope of this topic.

1. Open the following file by using Notepad: C:\Program Files\Microsoft\Exchange Server\V14\Bin\EdgeTransport.exe.config
2. Modify the following line in the <appSettings> section.

```
<add key="AgentLogEnabled" value="<TRUE | FALSE>" />
```

This example disables agent logging by modifying the *AgentLogEnabled* parameter.

```
<add key="AgentLogEnabled" value="FALSE" />
```

3. Save and close the EdgeTransport.exe.config file.
4. Restart the Microsoft Exchange Transport service.

Return to top

1.7.1.36.2 Understanding Connectivity Logging

Understanding Connectivity Logging

Transport > Understanding Transport > Understanding Transport Logs >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-18*

Connectivity logging records the connection activity of the outbound message delivery queues that exist on computers running Microsoft Exchange Server 2010 that have the Hub Transport server role or the Edge Transport server role installed. The connectivity log tracks the connection activity from the sending queue to the destination Mailbox server, smart host, or domain. It isn't intended to track the transmission of individual e-mail messages. The following list describes the type of information recorded in the connectivity log:

- Source queue, which can be the remote delivery queue or mailbox delivery queue
- Destination Mailbox server, smart host, or domain
- Domain Name System (DNS) resolution information
- Detailed information about connection failures
- Number of messages and bytes transmitted

You use the **Set-TransportServer** cmdlet in the Exchange Management Shell to perform all connectivity log configuration tasks. The following options are available for the

connectivity logs on an Edge Transport server or Hub Transport server:

- Enable or disable connectivity logging. The default is disabled.
- Specify the location of the connectivity log files.
- Specify a maximum size for the individual connectivity log files. The default size is 10 megabytes (MB).
- Specify a maximum size for the directory that contains connectivity log files. The default size is 250 MB.
- Specify a maximum age for the connectivity log files. The default age is 30 days.

By default, the Exchange 2010 server uses circular logging to limit the connectivity logs based on file size and file age to help control the hard disk space used by the connectivity log files.

Looking for management tasks related to connectivity logging? See Managing Transport Servers.

Structure of the Connectivity Log Files

By default, the connectivity log files exist in C:\Program Files\Microsoft\Exchange Server \V14\TransportRoles\Logs\Connectivity.

The naming convention for the connectivity log files is CONNECTLOG*yyyymmdd-nnnn*.log. The placeholders represent the following information:

- The placeholder *yyyymmdd* is the Coordinated Universal Time (UTC) date that the log file was created. The placeholder *yyyy* = year, *mm* = month, and *dd* = day.
- The placeholder *nnnn* is an instance number that starts at the value of 1 for each day.

Information is written to the log file until the file size reaches its maximum specified value, and a new log file that has an incremented instance number is opened. This process is repeated throughout the day. Circular logging deletes the oldest log files when the connectivity log directory reaches its maximum specified size, or when a log file reaches its maximum specified age.

The connectivity log files are text files that contain data in the comma-separated value file (CSV) format. Each connectivity log file has a header that contains the following information:

- **#Software** Name of the software that created the connectivity log file. Typically, the value is Microsoft Exchange Server.
- **#Version** Version number of the software that created the connectivity log file. Currently, the value is 8.0.0.0.
- **#Log-Type** Log type value, which is Transport Connectivity Log.
- **#Date** UTC date-time when the log file was created. The UTC date-time is represented in the ISO 8601 date-time format: *yyyy-mm-ddThh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu, which is another way to denote UTC.
- **#Fields** Comma delimited field names used in the connectivity log files.

Information Written to the Connectivity Log

The connectivity log stores each outbound queue connection event on a single line in the connectivity log. The information stored on each line is organized by fields. These fields are separated by commas. The following table describes the fields used to classify each

outgoing queue event.

Fields used to classify each connection event

Field name	Description
date-time	UTC date-time of the connection event, which is represented in the ISO 8601 format. The value is formatted as *yyyy-mm-ddThh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu, which is another way to denote UTC.
session	GUID that's unique for each SMTP session but is the same for each event associated with that SMTP session. For MAPI sessions, the session field is blank.
source	Value of SMTP for connections from the remote delivery queue, or the value of MAPI for connections from the mailbox delivery queue.
Destination	Name of the destination Mailbox server, smart host, or domain.
direction	Single character that represents the start, middle, or end of the connection. The possible values for the direction field are as follows: • **+** Connect • **-** Disconnect • **>** Send
description	Text information associated with the connection event. The following values are examples of values for the description field: • Number and size of messages that were transmitted • DNS MX resource record resolution information for destination domains • DNS resolution information for destination Mailbox servers • Connection establishment messages • Connection failure messages

When an outbound delivery queue establishes a connection to a destination Mailbox server, smart host, or domain, the queue may be prepared to send one message or several messages. The connection and message transmission processes generate multiple events written on multiple lines in the connectivity log. Simultaneous connections to different destinations create connectivity log entries related to different destinations that are interlaced. However, you can use the date-time, session, source, and direction fields to arrange the connectivity log entries for each separate connection from start to finish.

1.7.1.36.3 Understanding Message Tracking

Understanding Message Tracking

Transport > Understanding Transport > Understanding Transport Logs >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-07-01*

A message tracking log is a detailed log of all message activity as messages are transferred to and from a computer that is running Microsoft Exchange Server 2010 and that has the Hub Transport server role, the Mailbox server role, or the Edge Transport server role installed. Exchange servers that have the Client Access server role or Unified Messaging server role installed don't have message tracking logs. You use message tracking logs for message forensics, mail flow analysis, reporting, and troubleshooting.

You can use the **Set-TransportServer** cmdlet for all message tracking configuration tasks on a Hub Transport server or Edge Transport server. You can use the **Set-MailboxServer** cmdlet for all message tracking configuration tasks on a Mailbox server. For servers that have the Hub Transport server role and the Mailbox server role installed, you can use the **Set-TransportServer** cmdlet or the **Set-MailboxServer** cmdlet. You can use these cmdlets to make the following message tracking configuration changes:

- **Enable or disable message tracking**: The default is enabled.
- **Specify the location of the message tracking log files**
- **Specify a maximum size for the individual message tracking log files**: The default is 10 MB.
- **Specify a maximum size for the directory that contains the message tracking log files**: The default is 1000 MB.
- **Specify maximum age for the message tracking log files**: The default is 30 days.
- **Enable or disable message subject logging in the message tracking logs** The default is enabled.

Note:

You can also use the Exchange Management Console on a Hub Transport server or Edge Transport server to enable or disable message tracking, and to specify the location of the message tracking log files.

Exchange 2010 uses log rotation to limit the message tracking logs based on both file size and age. This helps limit the hard disk space that is used by the log files.

Structure of the Message Tracking Log Files

By default, the message tracking log files exist in C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking.

The naming convention for log files in the message tracking log directory depends on the server role that is installed. On a Hub Transport server or an Edge Transport server, the log files are named MSGTRK*yyyymmdd-nnnn*.log. On a Mailbox server, the log files are named MSGTRKM*yyyymmdd-nnnn*.log. When the Hub Transport server role and Mailbox server role are installed on the same server, separate log files that use these different name prefixes are created in the message tracking log directory.

The placeholders in the log file names represent the following information:

- The placeholder *yyyymmdd* is the coordinated universal time (UTC) date on which the log file was created. *yyyy* = year, *mm* = month, and *dd* = day.
- The placeholder *nnnn* is an instance number that starts at the value of 1 daily for each message tracking log file name prefix.

Information is written to each log file until the file size reaches its maximum specified value for each log file. Then, a new log file that has an incremented instance number is

opened. This process is repeated throughout the day. The log file rotation functionality deletes the oldest log files when either of the following conditions is true:

- A log file reaches its maximum specified age.
- The message tracking log directory reaches its maximum specified size.

Important:

The maximum size of the message tracking log directory is calculated as the total size of all log files that have the same name prefix. Other files that do not follow the name prefix convention are not counted in the total directory size calculation. Renaming old log files or copying other files into the message tracking log directory could cause the directory to exceed its specified maximum size. When the Hub Transport server role and the Mailbox server role are installed on the same server, the maximum size of the message tracking log directory is not the specified maximum size, because the message tracking log files that are generated by the different server roles have different name prefixes. When the Hub Transport server role and the Mailbox server role are installed on the same server, the maximum size of the message tracking log directory is two times the specified value.

The message tracking log files are text files that contain data in the comma-separated value (CSV) format. Each message tracking log file has a header that contains the following information:

- **#Software:** The name of the software that created the message tracking log file. Typically, the value is Microsoft Exchange Server.
- **#Version:** The version number of the software that created the message tracking log file. Currently, the value is 14.0.0.0.
- **#Log-Type:** The value of this field is Message Tracking Log.
- **#Date:** The UTC date-time when the log file was created. The UTC date-time is represented in the ISO 8601 date-time format: *yyyy-mm-ddThh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu, which is another way to denote UTC.
- **#Fields:** The comma-delimited field names that are used in the message tracking log files. The following fields are listed:

Information that is Written to the Message Tracking Log

The message tracking log stores each message event on a single line in the log. The events types that are used to classify each message event are explained in Table 1.

Table 1 Event Types that are Used to Classify Each Message Event

Event name	Description
BADMAIL	A message was submitted by the Pickup directory or the Replay directory that cannot be delivered or returned.
DELIVER	A message was delivered to a mailbox.
DEFER	Message delivery was delayed.
DSN	A delivery status notification (DSN) was generated.
DUPLICATEDELIVER	A duplicate message was delivered to the recipient. Duplication may occur if a recipient is a member of two distribution groups.

	Duplicate messages are detected and removed by the information store.
EXPAND	A distribution group was expanded.
FAIL	Message delivery failed.
POISONMESSAGE	A message is put in the poison message queue or removed from the poison message queue.
RECEIVE	A message was received and committed to the database. The RECEIVE event can be SMTP receive (Source: SMTP) or mail submitted by STOREDRIVER (Source: STOREDRIVER). SMTP RECEIVE can be from any source that submits a message by using SMTP. For example, it can be a Hub Transport server role, an Edge Transport server role, a third-party message transfer agent (MTA), or a POP/IMAP client. STOREDRIVER RECEIVE is logged by the EdgeTransport.exe process, and is the event that corresponds to a STOREDRIVER SUBMIT event. STOREDRIVER SUBMIT is logged by the Mail Submission process. These events can be on the same server if both server roles are installed locally, or they can be on different servers. **Note:** EdgeTransport.exe and MSExchangeTransport.exe are the executable files that are used by the Microsoft Exchange Transport service. This service runs on every Hub Transport server or Edge Transport server.
REDIRECT	A message was redirected to an alternative recipient after an Active Directory directory service lookup.
RESOLVE	A message's recipients were resolved to a different e-mail address after an Active Directory lookup.
SEND	A message was sent by Simple Mail Transfer Protocol (SMTP) to a different server.
SUBMIT	A SUBMIT event is logged by the Mail Submission service on an Exchange 2007 computer that is running the Mailbox server role. The SUBMIT event is logged when the service has successfully notified a Hub Transport server that a message is awaiting submission in the mailbox store. The SourceContext property provides the Messaging Database (MDB) GUID, Mailbox

	GUID, Event sequence number, Message class, Creation time stamp of the client submission to store, and Client type. The Client type can be User (Outlook direct MAPI), RPCHTTP (Outlook Anywhere), Outlook Web Access, Exchange Web Services (EWS), Exchange ActiveSync, Assistants, or Transport. The message tracking logs that are generated by the Mailbox server role contain only SUBMIT events.
TRANSFER	Recipients were moved to a forked message because of content conversion, message recipient limits, or agents.

The message event information that is stored on each line is organized by fields. These fields are separated by commas. The field name is generally descriptive enough to determine the type of information that it contains. However, some fields may be blank, or the type of information that is stored in the field may change based on the message event type as described in Table 1. General descriptions of the fields that are used to classify each message tracking event are explained in Table 2.

Table 2 Fields that are Used to Classify Each Message Tracking Event

Field name	Description
date-time	The UTC date-time of the message tracking event, which is represented in the ISO 8601 format. The value is formatted as *yyyy-mm-ddThh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu, which is another way to denote UTC.
client-ip	The TCP/IP address of the messaging server or messaging client that submitted the message.
client-hostname	The name of the messaging server or messaging client that submitted the message.
server-ip	The TCP/IP address of the source or destination Exchange server.
server-hostname	The name of the destination server.
source-context	Extra information associated with the source field.
connector-id	The name of source or destination Send connector or Receive connector.
source	The Exchange transport component responsible for the message tracking event. The possible values for this field are as follows: • ADMIN for Replay directory submission • AGENT • DSN • GATEWAY for Foreign connector submission • PICKUP

	• ROUTING • SMTP • STOREDRIVER for MAPI submission
event-id	The message event type. These events are described fully in Table 1 earlier in this topic. The possible values are BADMAIL, DEFER, DELIVER, DSN, EXPAND, FAIL, POISONMESSAGE, RECEIVE, REDIRECT, RESOLVE, SEND, SUBMIT, and TRANSFER.
internal-message-id	A message identifier that is assigned by Exchange 2010 server that is currently processing the message. A specific message's value of internal-message-id is different in the message tracking log of every Exchange 2010 server that is involved in the delivery of the message.
message-id	The value of the `Message-Id:` field found in the message's header fields. If the `Message-Id:` header field does not exist or is blank, an arbitrary value is assigned. This value is constant for the lifetime of the message.
recipient-address	The e-mail addresses of the message's recipients. Multiple e-mail addresses are separated by the semicolon character (;).
recipient-status	This field is populated for a SEND event or a FAIL event.
total-bytes	The size of the message that includes attachments, in bytes.
recipient-count	The number of recipients in the message.
related-recipient-address	This field is used with EXPAND, REDIRECT, and RESOLVE events to display other recipient e-mail addresses associated with the message.
reference	This field contains additional information for specific types of events: **DSN** The Reference field contains the Internet-Message-Id of the message that caused the DSN. **SEND** The Reference field contains the Internet-Message-Id of any delivery status notification (DSN) messages. **TRANSFER** The Reference field contains the Internal-Message-Id of the message that is being forked. For all other types of events, the Reference field is blank.
message-subject	The message's subject found in the `Subject:` header field. The tracking of message subjects is controlled by the

	MessageTrackingLogSubjectLoggingEnabled parameter in the **Set-TransportServer** cmdlet for Hub Transport servers and Edge Transport servers, or in the **Set-MailboxServer** cmdlet for Mailbox servers. By default, message subject tracking is enabled. Message subject logging can be disabled by setting the value of the *MessageTrackingLogSubjectLoggingEnabled* parameter to `$false`.
sender-address	The e-mail address specified in the `Sender:` header field, or the `From:` header field if `Sender:` is not present.
return-path	The return e-mail address specified by `MAIL FROM:` in the message envelope. Although this field is never empty, it can have the null sender address value represented as <>.
message-info	This field contains the message origination date-time for DELIVER and SEND events. The origination date-time is the time that the message first enters the Exchange organization. The value is formatted as *yyyy-mm-ddThh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu, which is another way to denote UTC.

You can use the **Get-MessageTrackingLog** cmdlet in the Exchange Management Shell or the Message Tracking tool in the Exchange Management Console to search for messages by using specific message criteria.

Security Concerns for the Message Tracking Log

No message content is stored in the message tracking log. By default, the subject line of an e-mail message is stored in the message tracking log. You may want to disable message subject logging to comply with increased security or privacy requirements. Before you enable or disable message subject logging, make sure that you verify your organization's policy about revealing subject line information.

For More Information

For more information, see the following topics:

Configure Message Tracking

Search Message Tracking Logs

Understanding Protocol Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-23*

Protocol logging records the SMTP conversations that occur between e-mail servers as part of message delivery. These SMTP conversations occur on Send connectors and Receive connectors configured on servers running Microsoft Exchange Server 2010 that have the Hub Transport server role or the Edge Transport server role installed. You can use protocol logging to diagnose mail flow problems.

By default, protocol logging is disabled on all Send connectors and Receive connectors. Protocol logging is enabled or disabled on a per-connector basis. Other protocol logging options are set on a per-connector type basis for the whole server. All the Receive connectors on a Hub Transport server or an Edge Transport server share the same protocol log files and protocol log options. These protocol log files and protocol log options are separate from the Send connector protocol log files and protocol log options on the same server.

The following options are available for the protocol logs of all Send connectors or all Receive connectors on an Edge Transport server or a Hub Transport server:

- Specify the location of the Send connector or the Receive connector protocol log files.
- Specify a maximum size for the Send connector or the Receive connector protocol log files. The default size is 10 megabytes (MB).
- Specify a maximum size for the directory that contains the Send connector or Receive connector protocol log files. The default size is 250 MB.
- Specify a maximum age for the Send connector or Receive connector protocol log files. The default age is 30 days.

By default, the Exchange 2010 server uses circular logging to limit the protocol logs based on file size and file age to help control the hard disk space used by the log files.

A special Send connector named the intra-organization Send connector exists on every Hub Transport server. This connector is implicitly created, invisible, and requires no management. The intra-organization Send connector is used to relay messages to the following destinations:

- To other Hub Transport servers in the Exchange organization, including Exchange 2007 Hub Transport servers
- To Exchange Server 2003 servers in the Exchange organization
- To Edge Transport servers in the Exchange organization

By default, protocol logging for the intra-organization Send connector is disabled. You can enable or disable protocol logging for the intra-organization Send connector by using the *IntraOrgConnectorProtocolLoggingLevel* parameter on the **Set-TransportServer** cmdlet. If you enable protocol logging for the intra-organization Send connector, logging occurs in the Send connector protocol logs configured on the Hub Transport server.

Looking for management tasks related to protocol logging? See Managing Transport Servers.

Structure of the Protocol Log Files

By default, the protocol log files exist in the following locations:

- **Receive connector protocol log files** C:\Program Files\Microsoft\Exchange

Server\V14\TransportRoles\Logs\ProtocolLog\SmtpReceive
- **Send connector protocol log files** C:\Program Files\Microsoft\Exchange Server\V14TransportRoles\Logs\ProtocolLog\SmtpSend

The naming convention for log files in each protocol log directory is *prefixyyyymmdd-nnnn*.log. The placeholders represent the following information:
- The placeholder *prefix* is SEND for Send connectors or RECV for Receive connectors.
- The placeholder *yyyymmdd* is the Coordinated Universal Time (UTC) date on which the log file was created. The placeholder *yyyy* = year, *mm* = month, and *dd* = day.
- The placeholder *nnnn* is an instance number that starts at the value of 1 for each day.

Information is written to the log file until the file size reaches its maximum specified value, and a new log file that has an incremented instance number is opened. This process is repeated throughout the day. Circular logging deletes the oldest log files when the protocol log directory reaches its maximum specified size, or when a log file reaches its maximum specified age.

The protocol log files are text files that contain data in the comma-separated value file (CSV) format. Each protocol log file has a header that contains the following information:
- **#Software** Name of the software that created the protocol log file. Typically, the value is Microsoft Exchange Server.
- **#Version** Version number of the software that created the protocol log file. Currently, the value is 14.0.0.0.
- **#Log-Type** Log type value of this field, which is either SMTP Receive Protocol Log or SMTP Send Protocol Log.
- **#Date** UTC date-time when the log file was created. The UTC date-time is represented in the ISO 8601 date-time format: *yyyy-mm-ddThh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu, which is another way to denote UTC.
- **#Fields** Comma-delimited field names used in the protocol log files.

Information Written to the Protocol Log

The protocol log stores each SMTP protocol event on a single line in the protocol log. The information stored on each line is organized by fields. These fields are separated by commas. The following table describes the fields used to classify each protocol.

Fields used to classify each protocol event

Field name	Description
date-time	UTC date-time of the protocol event, which is represented in the ISO 8601 format. The value is formatted as *yyyy-mm-ddThh:mm:ss.fffZ*, where *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute, *ss* = second, *fff* = fractions of a second, and *Z* signifies Zulu, which is another way to denote UTC.
connector-id	Distinguished name (DN) of the connector associated with the SMTP event.
session-id	GUID that's unique for each SMTP session but is the same for each event associated with that SMTP session.
sequence-number	Counter that starts at 0 and is incremented for

	each event in the same SMTP session.
local-endpoint	Local endpoint of an SMTP session. This consists of an IP address and TCP port number formatted as *<IP address>:<port>*.
remote-endpoint	Remote endpoint of an SMTP session. This consists of an IP address and TCP port number formatted as *<IP address>:<port>*.
event	Single character that represents the protocol event. The possible values for the event are as follows: • + Connect • - Disconnect • > Send • < Receive • * Information
data	Text information associated with the SMTP event.
context	Additional contextual information that may be associated with the SMTP event.

A single SMTP conversation that represents the sending or receiving of a single e-mail message generates multiple SMTP events. These SMTP events cause multiple lines to be written to the protocol log. Multiple SMTP conversations that represent the sending or receiving of multiple e-mail messages can occur at the same time. This creates protocol log entries from different SMTP conversations that are interspersed. You can use the session-id and sequence-number fields to sort the protocol log entries by SMTP conversation.

1.7.1.36.5 Understanding Routing Table Logging

Understanding Routing Table Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-17*

Routing table logging periodically records a snapshot of the routing table that's used by the computer that's running Microsoft Exchange Server 2010 that has the Hub Transport server role or Edge Transport server role installed. The routing table is used to route messages to their destinations. The routing table log is recorded in these cases:

- After a fixed time interval.
- After the Microsoft Exchange Transport service is started.
- After a routing configuration change is detected.

The routing table log can be used to help troubleshoot mail flow and routing issues.

You can control the automatic routing table recalculation interval in the EdgeTransport.exe.config application configuration file. This value controls how frequently the routing table is automatically recalculated and how frequently the routing table is logged. However, regular routing table updates may cause the routing table to be recalculated and logged earlier than the specified automatic recalculation interval as explained later in this topic.

You use the **Set-TransportServer** cmdlet to perform all other routing table log configuration tasks. The following options are available for the routing table logs on an Edge Transport server or Hub Transport server:

- Specify the location of the routing table log files.
- Specify a maximum size for the directory that contains routing table log files. The default size is 50 megabytes (MB).
- Specify a maximum age for the routing table log files. The default age is seven days.

By default, the Exchange 2010 server uses circular logging to limit the connectivity logs based on file size and file age to help control the hard disk space that's used by the log files.

In Exchange 2010, you can use the Routing Log Viewer in the Exchange Management Console to view and search the routing table logs. For more information, see Using the Routing Log Viewer.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Structure of the Routing Table Log Files

By default, the routing table log files exist in C:\Program Files\Microsoft\Exchange Server \V14\TransportRoles\Logs\Routing.

The naming convention for the routing table log files is RoutingConfig#1@*UTCcreationdate-time*.xml. For example, depending on your regional date-time format settings, the routing table log files may be named RoutingConfig#1@*mm_dd_yyyy hh_mm_ss*.xml. The placeholders represent the following information: *yyyy* = year, *mm* = month, *dd* = day, *hh* = hour, *mm* = minute and *ss* = second. The date-time is always represented in Coordinated Universal Time (UTC).

The routing table log is a complete snapshot of the routing table that's stored in memory. The routing table is written to the routing table log when the following events occur:

- A routing configuration change is detected. An example of a configuration change is adding or removing a Send connector in the Exchange organization or a Receive connector on the local server. A regular routing configuration change occurs when the Hub Transport server or Edge Transport server renews its Kerberos token with an Active Directory domain controller. The renewal of the Kerberos token causes a recalculation of the routing table and the creation of a new routing table log. The Kerberos token is renewed every six hours.
- The time interval specified by the *RoutingConfigReloadInterval* parameter in the EdgeTransport.exe.config has passed. This value specifies how frequently the routing table is automatically recalculated and logged if no routing configuration changes are detected. The default value is 12 hours.
- The Microsoft Exchange Transport service is started.

Circular logging deletes the oldest log files when the routing table log directory reaches its maximum specified size, or when a log file reaches its maximum specified age.

The routing table log files are text files that contain data in XML format. The routing table log files contain a large amount of information. However, the actual file size depends on the size and complexity of the Exchange organization.

Information Written to the Routing Table

Log

The routing table log is composed of several sections. Each section identifies a particular element of the Exchange organization, such as connectors, address spaces, or Active Directory sites. The information that's defined in one section is connected to the information that's defined in another section to build a complete routing table for the whole Exchange organization. For large Exchange organizations, the amount of information in the routing table log can be very large. The following table provides a description for each section of the routing table log.

Sections of the routing table log

Section	Description
RoutingTables ID	This section contains basic information about the routing table, such as the following information: • The routing table creation date-time in UTC. • On Hub Transport servers, the ExchangeTopology ID, ADSiteRelayMap ID, and RoutingGroupRelayMap ID that are being used by the routing table. • On Hub Transport servers, the identity of every Mailbox server, Hub Transport server, Edge Transport server, and legacy Exchange server in the Exchange organization. Each identity maps to a ServerRoute ID. • The ConnectorRouting ID for all Send connectors, Receive connectors that are linked to Send connectors on the local server, foreign connectors, and legacy gateway connectors in the Exchange organization. Legacy gateway connectors exist on the server that's running Exchange Server 2003. Legacy gateway connectors send messages to other messaging servers, such as Lotus Notes or GroupWise.
ExchangeTopology ID	This section contains all the Exchange servers, Active Directory sites, and Active Directory site links that exist in the Exchange organization.
TopologyServer ID	This section contains details about every Exchange server in the Exchange organization.
TopologySite ID	This section contains details about every Active Directory site in the Exchange organization.
TopologySiteLink ID	This section contains details about the IP site links that exist in the Exchange organization.
ADSiteRelayMap ID	This section links an ADTopologyPath ID to each remote Active Directory site that contains an Exchange 2010 Hub Transport server.
ADTopologyPath ID	This section contains details about the least cost routing path from the current Active Directory site to any remote Active Directory site.

TargetSite ID	This section contains the names of all remote Active Directory sites that exist in the Active Directory forest, and a list of Hub Transport servers that exist in each remote Active Directory site.
RoutingGroupRelayMap ID	This section maintains the interrelationship between a routing group, the RgTopologySite ID, the RgTopologyPath ID, and the RgConnectorRoute ID.
RgTopologySite ID	This section contains details about each routing group that exists in the Exchange organization.
RgTopologyLink ID	This section contains details about routing group connectors and SMTP connectors with connected routing groups.
RgTopologyPath ID	This section contains details about remote routing groups and is used to link remote routing groups to a routing group connector or an SMTP connector that contains connected routing groups.
RgConnectorRoute ID	This section contains the route to the first hop routing group that can be used to route mail to a remote routing group.
ServerRoute ID	This section lists every Hub Transport server, Edge Transport server, Mailbox server, and legacy Exchange server object in the Exchange organization, and associates a route to that server.
ConnectorRouting ID	This section contains routes to all Send connectors, foreign connectors, and legacy gateway connectors. It also contains a mapping of Receive connectors on the local server that are linked to Send connectors on the local server. When a Receive connector is linked to a Send connector, all messages that arrive on the linked Receive connector are immediately forwarded out through the corresponding Send connector.
ConnectorRoute ID	This section lists all the Send connectors, foreign connectors, and legacy gateway connectors in the Exchange organization, and associates a route to the connector.
SmtpSendConnectorConfig ID	This section contains details about every Send connector that exists in the Exchange organization.
AddressSpace ID	This section lists all the address spaces that are configured on every Send connector, foreign connector, or legacy gateway connector in the Exchange organization.
LegacyGatewayConnector ID	This section lists details about every legacy gateway connector that exists in the Exchange organization. Legacy gateway connectors exist on servers that are running Exchange 2003.

ForeignConnector ID	This section contains details about every foreign connector that exists in the Exchange organization. Foreign connectors are homed on Exchange 2010 Hub Transport servers and use a Drop directory to send messages to non-SMTP messaging servers.
AddressTypeRouting ID	This section maps an address type to an SmtpConnectorIndex ID.
SmtpConnectorIndex ID	This section contains the SMTPIndexNode ID of the root index that's supported by this SMTPConnectorIndex ID.
X400ConnectorIndex ID	This section contains the X400IndexNode ID of the root index that's supported by this X400ConnectorIndex ID.
GenericConnectorIndex ID	This section contains the IndexEntry ID of the root index that's supported by this GenericConnectorIndex ID.
SMTPIndexNode ID	This section contains the SMTPIndexNode ID, which represents a part of an SMTP address space. The values of the index nodes are combined to form the complete SMTP address space. For example, the domain exchange.contoso.com has the following four index nodes: • The root SMTP index node • The com SMTP index node • The contoso SMTP index node • The exchange SMTP index node
X400IndexNode ID	This section contains the X400IndexNode ID, which represents a part of an X.400 address space. The values of the index nodes are combined to form the complete X.400 address space.
IndexEntry ID	This section contains the IndexEntry ID, which represents a part of a non-SMTP address space, such as Lotus Notes or fax. The values of the index entries are combined to form the complete non-SMTP address space.
ConnectorRouteWithCost ID	This section links an address space cost to a connector route.

1.7.1.37 Understanding Transport Pipeline

Understanding Transport Pipeline

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

In Microsoft Exchange Server 2010, the transport pipeline is a collection of Exchange 2010 server roles, connections, components, and queues that work together to route all messages to the categorizer on a Hub Transport server inside the organization.

Messages from outside the organization enter the transport pipeline through a Receive connector on an Edge Transport server and are then routed to a Hub Transport server inside the organization. Messages inside the organization enter the transport pipeline on a Hub Transport server in one of the following ways:

- Through a Receive connector
- From the Pickup directory or the Replay directory
- By direct placement in the Submission queue by the store driver
- Through agent submission

Every message that's sent or received by an Exchange 2010 client must be categorized on a Hub Transport server before it can be routed and delivered. After a message has been categorized, it's put in a delivery queue for delivery to a mailbox in the same Active Directory site as the Hub Transport server on which the message was categorized or for routing to a recipient in a different Active Directory site or forest, or to a recipient outside the organization.

The Exchange 2010 transport pipeline consists of the following components and processes:

- **SMTP Receive** When messages are received at the Edge Transport server, anti-spam and antivirus agents filter connections and message contents, and help identify the sender and the recipient of a message while the message is being accepted into the organization. When messages are received at a Hub Transport server, transport rules are applied and, if anti-spam and antivirus agents are configured, these agents provide an additional layer of anti-spam and antivirus protection.
  The SMTP session has a series of events that work together in a specific order to validate the contents of a message before it's accepted into the organization. After a message has passed completely through SMTP Receive and isn't rejected by receive events or by an anti-spam and antivirus agent, it's put in the Submission queue.
- **Submission** Submission is the process of putting messages into the Submission queue. The categorizer picks up one message at a time for categorization. There are four types of submission:
  - SMTP submission through a Receive connector.
  - Submission through the Pickup directory or the Replay directory. These directories exist on the Hub Transport server or Edge Transport server. Correctly formatted message files that are copied into the Pickup directory or the Replay directory are put directly into the Submission queue.
  - Submission by the store driver, which picks up messages from a sender’s Outbox as they're sent.
  - Submission by an agent.

  On the Edge Transport server, submission is generally only through the Receive connector. On the Hub Transport server, submission can occur through a Receive connector, Pickup directory, Replay directory, or store driver.
- **Categorizer** The categorizer picks up one message at a time from the Submission queue. On the Edge Transport server, categorization is a short process in which the message is put directly in the delivery queue. From the delivery queue, the message is routed to a computer that's running a Hub Transport server role in the organization.
  On the Hub Transport server, the categorizer completes the following steps:
  - Recipient resolution, which includes top-level addressing, expansion, and bifurcation
  - Routing resolution
  - Content conversion

  Additionally, mail flow rules that are defined by the organization are applied. After messages have been categorized, they're put into a delivery queue. A mailbox delivery queue delivers the message to a local mailbox by using the store driver. A remote delivery queue delivers the message to a remote

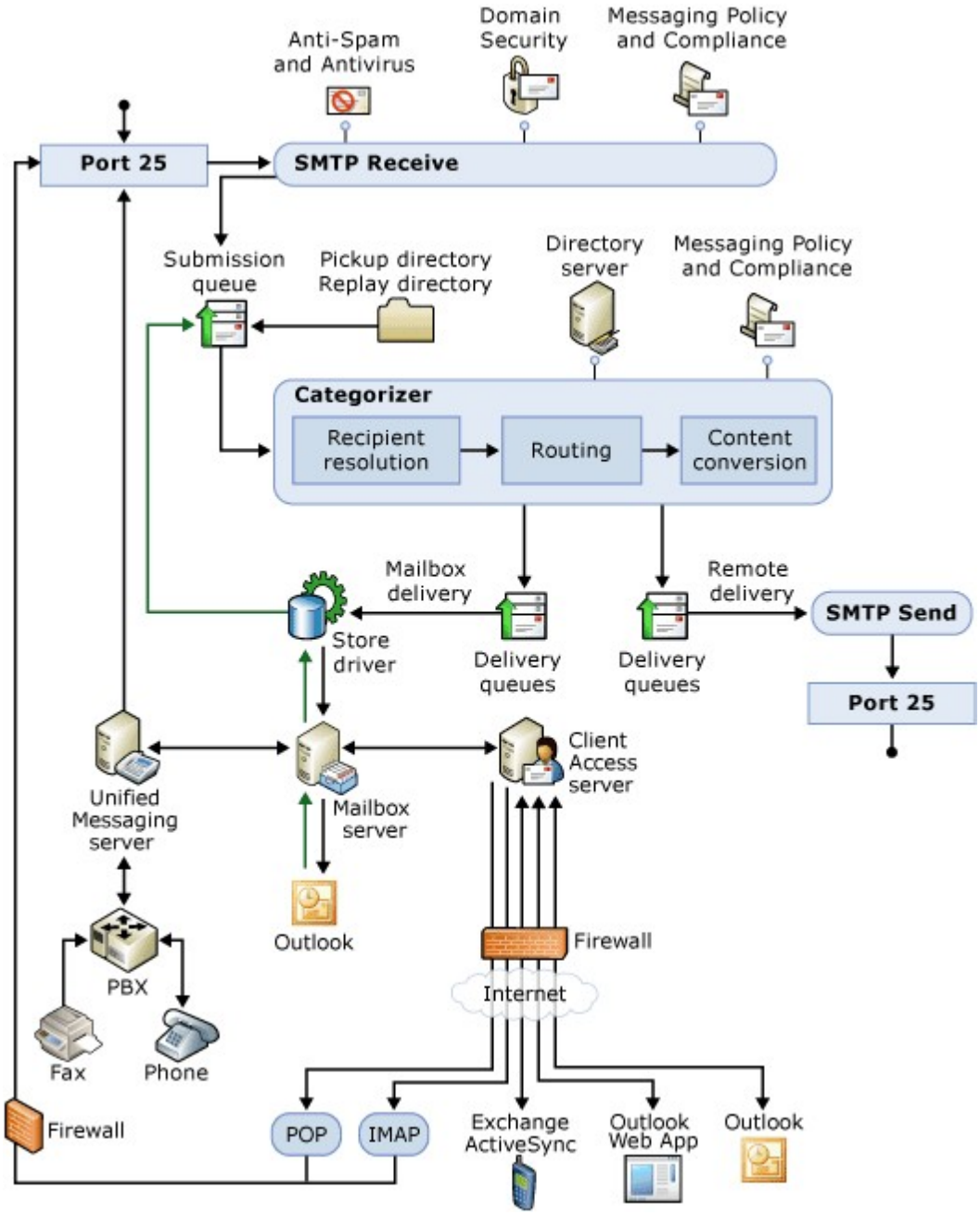
recipient through a Send connector.

- **Local Delivery** Only messages that are sent to a recipient with a mailbox in the same Active Directory site as the Hub Transport server on which categorization occurred are delivered locally. In this case, local delivery means delivery in the same Active Directory site. All messages delivered locally are picked up from a delivery queue by the store driver and put in the recipient's inbox on a Mailbox server.
- **SMTP Send** Messages that are sent to recipients in Active Directory sites that differ from the computer that's running a Hub Transport server role on which categorization occurred are delivered remotely or outside the organization. All messages that are sent to a different Active Directory site, to a mailbox that resides on a computer that's running an earlier version of Exchange, or to a mailbox that resides in a different Active Directory forest must be routed through a Send connector to a Hub Transport server that can deliver the message to the intended recipient. All messages that require delivery through the Internet must be routed through a Send connector to an Edge Transport server that can send messages to the Internet for delivery outside the organization.
- **Client Access and Unified Messaging Scenarios** Several client access scenarios and Unified Messaging scenarios don't interact directly with the transport pipeline. Users of Microsoft Outlook 2007, Outlook 2003, Outlook Web App, Outlook Voice Access, and Exchange ActiveSync interact directly with the Client Access server role, Unified Messaging server role, and Mailbox server role to access their mailbox. In each case, when mail is sent, the message is put in the sender's Outbox directly on the Mailbox server by Outlook or the Client Access server on behalf of the sender.

  Note:
  Outlook Voice Access requires interaction with the Client Access server and with the Mailbox server through the Unified Messaging server.

  After the message is put in the sender's Outbox, the store driver is alerted by the Microsoft Exchange Mail Submission service, which retrieves the message from the sender's Outbox, and then puts it into the Submission queue on a Hub Transport server in the same Active Directory site as the mailbox from which the message was retrieved.

The following figure shows the relationships among the components in the Exchange 2010 transport pipeline.



Looking for management tasks related to managing transport servers? See Managing Transport Servers.

1.7.1.38 Understanding Transport Policy and Compliance Agents

Understanding Transport Policy and Compliance Agents

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Many organizations are obligated by legal, regulatory, or business process requirements to process, filter, modify, and store e-mail messages transferred to and from the organization and the Internet, in addition to internal communications between individuals in the organization. The transport policy and compliance infrastructure of Microsoft Exchange Server 2010 provides a set of rules that govern how e-mail messages are stored and processed based on a set of requirements. The following important features help you comply with these legal, regulatory, and business process requirements more easily:

- **Transport rules agents** There are two transport rules agents in Exchange 2010. The Transport Rule agent runs on Hub Transport servers and helps you meet regulatory and corporate policy requirements. The Edge Rule agent runs on the Edge Transport server and helps you protect your organization from unsolicited commercial e-mail (spam) and viruses. For more information about transport rules agents and specific scenarios where they might be used, see the following topics:
  - Understanding Transport Rules
  - Understanding How Transport Rules Are Applied
  - Understanding Ethical Walls
- **Journaling agent** The Journaling agent helps you configure how Exchange enforces e-mail retention policies on messages sent or received by departments or individuals in your organization, to and from recipients outside your organization, or both.

  Important:
  In Exchange 2010, the Journaling agent is a built-in agent. Built-in agents aren't included in the list of agents returned by the **Get-TranpsortAgent** cmdlet. For more details, see Understanding Transport Agents.

  For more information about the Journaling agent, journal reports, and journaling in a mixed Exchange Server 2003 and Exchange Server 2007 organization or in a mixed Exchange 2010 and Exchange Server 2007 organization, see the following topics:
  - Understanding Journaling
  - Understanding Journal Reports
  - Protecting Journal Reports
  - Understanding How to Manage Journal Reports
  - Understanding Journaling in a Mixed Exchange 2003 and Exchange 2010 Environment
  - Export and Import Exchange 2007 Journal Rules
- **Information Rights Management (IRM) agents** There are three IRM agents in Exchange 2010. The Encryption agent IRM-protects messages flagged by the Transport Rule agent on Hub Transport servers. The Pre-licensing agent inserts a use license in messages that are IRM-protected by using the organization's Active Directory Rights Management Services (AD RMS) cluster. The Decryption agent decrypts IRM-protected messages to allow other transport agents access to message content, and for including a plaintext copy of the message in journal reports for archival and discovery.
  For more information about IRM agents, see the following topics:
  - Understanding Information Rights Management
  - Understanding Transport Protection Rules
  - Understanding Transport Decryption
  - Understanding Journal Report Decryption

Using Exchange Hosted Services

Policy and compliance features are enhanced by or are also available as services from Microsoft Exchange Hosted Services.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

1.7.1.39 Understanding Transport Queues

Understanding Transport Queues

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

This topic provides an overview of queues in Microsoft Exchange Server 2010 and the queue management tasks that administrators can perform.

Looking for management tasks related to managing transport servers? See Managing Transport Servers.

Contents

Overview

A *queue* is a temporary holding location for messages that are waiting to enter the next stage of processing. Each queue represents a logical set of messages that a transport server processes in a specific order.

The Exchange Management Shell and Queue Viewer support two types of interaction with queues. You can use these interfaces to view the status and contents of queues and detailed message properties. You can also use these interfaces to perform actions that modify queues or the messages in the queues.

Exchange 2010 uses an Extensible Storage Engine (ESE) database for queue storage. Formerly known as JET, ESE is a method that defines a low-level API to the underlying database structures in Exchange.

Messages that come from and go to the Internet are queued at the computers that have the Edge Transport server role installed. Messages in transit within the Exchange 2010 organization are queued at the computers that have the Hub Transport server role installed.

Types of Queues

The routing of a message determines the type of queue in which a message is stored. The following types of queues are used in Exchange 2010:

- **Submission queue** A persistent queue that's used by the categorizer to gather all messages that have to be resolved, routed, and processed by transport agents. The *categorizer* is a component of Exchange transport that processes all inbound messages and determines what to do with the messages based on information about the intended recipients. In Exchange 2010, the Edge Transport server uses the categorizer to route the message to the appropriate destination. The Hub Transport server uses the categorizer to expand distribution lists and to identify alternative recipients and forwarding addresses. After the categorizer retrieves full information about recipients, it uses that information to apply policies, route the message, and perform content conversion.
  All messages that are received by a transport server enter processing in the Submission queue. Messages are submitted through a Receive connector, the Pickup directory, or the store driver. The categorizer retrieves messages from this queue and, among other things, determines the location of the recipient and the route to that location. After categorization, the message is moved to a delivery queue or to the unreachable queue. Each Exchange 2010 transport server has only one Submission queue. Messages that are in the Submission queue can't be in other queues at the same time.
- **Mailbox delivery queue** The mailbox delivery queues hold messages that are being delivered to a Mailbox server by using encrypted Exchange RPC. Mailbox delivery queues exist on Hub Transport servers only. Mailbox delivery queues hold messages that are being delivered to mailbox recipients whose mailbox data is stored on a Mailbox server that's located in the same site as the Hub Transport server. More than one mailbox delivery queue can exist on a Hub Transport server. The next hop for a mailbox delivery queue is the distinguished name of the mailbox store.
- **Remote delivery queue** Remote delivery queues hold messages that are being delivered to a remote server by using SMTP. Remote delivery queues can exist on both Hub Transport servers and Edge Transport servers, and more than one remote delivery queue can exist on each server. Each remote delivery queue contains messages that are being routed to recipients that have the same delivery destination. On an Edge Transport server, these destinations are external SMTP domains or SMTP connectors. On a Hub Transport server, these destinations are outside the Active Directory site in which the Hub Transport server is located. Remote delivery queues are dynamically created when they're required and are automatically deleted from the server when they no longer hold messages and the configurable expiration time has passed. By default, a remote delivery queue is deleted three minutes after the last message has left the queue. The next hop for a remote delivery queue is an SMTP domain name, a smart host name or IP address, or an Active Directory site name.
- **Poison message queue** The poison message queue is a special queue that's used to isolate messages that are detected to be potentially harmful to the Exchange 2010 system after a server failure. Messages that contain errors that are potentially fatal to the Exchange system are delivered to the poison message queue. This queue is typically empty, and if no poison messages exist, the queue doesn't appear in the queue viewing interfaces. The poison message queue is always in a ready state. By default, all messages in this queue are suspended. The messages can be deleted if they're considered to be harmful to the system. If the event that caused the message to enter the

poison message queue is determined to be unrelated to the message, delivery of the message can be resumed. When delivery is resumed, the message enters the Submission queue.

- **Unreachable queue** Each transport server can have only one Unreachable queue. The Unreachable queue contains messages that can't be routed to their destinations. Typically, an unreachable destination is caused by configuration changes that have modified the routing path for delivery. Regardless of destination, all messages that have unreachable recipients reside in this queue.

The following table lists the queues that exist on a Hub Transport server or Edge Transport server and their characteristics.

Queues that exist on a Hub Transport server or Edge Transport server

Queue name	Server role	Number of queues on the server
Mailbox delivery queue	Hub Transport	One queue for every unique destination Mailbox server
Poison message queue	Edge Transport Hub Transport	1
Remote delivery queue	Edge Transport Hub Transport	Edge Transport: One queue for every unique destination SMTP domain or smart host Hub Transport: One queue for every unique remote Active Directory site
Submission queue	Edge Transport Hub Transport	1
Unreachable queue	Edge Transport Hub Transport	1

When a message is received by transport, a transport mail item is created and saved to the database. A unique identifier is assigned to the transport mail item when it enters the database. If a message, or transport mail item, is being routed to more than one recipient, the item can have more than one destination. Each destination represents a separate routing solution for the transport mail item, and each routing solution causes a routed mail item to be created.

The routed mail item is a reference to the transport mail item and is the unit of operation for queuing actions. If a transport mail item has more than one routing solution, more than one routed mail item references the same transport mail item. A message that's being sent to recipients in two different domains appears as two distinct messages in the delivery queues, even if only one transport mail item is in the database.

About the Poison Message Queue and the Unreachable Queue

The categorizer sends messages to the Unreachable queue when there's no known route to their destinations. Typically, an unreachable destination is caused by a configuration error that affects the delivery path. For example, the messages will be sent to the Unreachable queue if the following conditions are true:

- There are messages in the remote delivery queue named Contoso.com.

- You delete the Send connector that's used to reach the Contoso.com domain.

By default, the messages in the Unreachable queue have the status of Ready. Messages in the Unreachable queue are never automatically resubmitted. Messages remain in the Unreachable queue until they're manually resubmitted by an administrator, removed by an administrator, or the value specified in the *MessageExpirationTimeOut* parameter passes.

The poison message queue contains messages that are determined to be potentially harmful to the Exchange 2010 server after a server failure. The messages may be genuinely harmful in their content and format. Alternatively, they may be the results of a poorly written agent that has caused the Exchange server to fail when it processed the supposedly bad messages. All messages in the poison message queue are in a permanently suspended state. The poison message queue can't be resubmitted with the **Retry-Queue** cmdlet with the *Resubmit* parameter. To resubmit the messages in the poison message queue, you can use Queue Viewer or the **Resume-Message** cmdlet to resume the messages. The messages in the poison message queue are never automatically resumed or expired. Messages remain in the poison message queue until they're manually resumed or removed by an administrator.

Return to top

Queue Database Files

All the different queues are stored in a single ESE database. By default, this queue database is located at C:\Program Files\Microsoft\Exchange Server\TransportRoles\data\Queue.

Like any ESE database, the queue database uses log files to accept, track, and maintain data. To enhance performance, all message transactions are written first to log files and memory, and then to the database file. The checkpoint file tracks the transaction log entries that have been committed to the database. During an ordinary shutdown of the Microsoft Exchange Transport service, uncommitted database changes that are found in the transaction logs are always committed to the database.

Circular logging is used for the queue database. This means that the history of committed transactions that are found in the transaction logs isn't maintained. Any transaction logs that are older than the current checkpoint are immediately and automatically deleted. Therefore, the transaction logs can't be replayed for queue database recovery from backup.

The following table lists the files that constitute the queue database.

Files that constitute the queue database

File	Description
Mail.que	This queue database file stores all the queued messages.
Tmp.edb	This temporary database file is used to verify the queue database schema on startup.
Trn*.log	This transaction log records all changes to the queue database. Changes to the database are first written to the transaction log and then committed to the database. Trn.log is the current active transaction log file. Trntmp.log is the next provisioned

	transaction log file that's created in advance. If the existing Trn.log transaction log file reaches its maximum size, Trn.log is renamed to Trn*nnnn*.log, where *nnnn* is a sequence number. Trntmp.log is then renamed Trn.log and becomes the current active transaction log file.
Trn.chk	This checkpoint file tracks the transaction log entries that have been committed to the database. This file is always in the same location as the mail.que file.
Trnres00001.jrs Trnres00002.jrs	These reserve transaction log files act as placeholders. They're only used when the hard disk that contains the transaction log runs out of space to stop the queue database cleanly.

Options for Configuring the Queue Database

You can't use the Exchange Management Console (EMC) or the Shell to configure the queue database. You configure the queue database by modifying the EdgeTransport.exe.config file. The EdgeTransport.exe.config file is an XML application configuration file that's associated with the EdgeTransport.exe file.

For more information about the EdgeTransport.exe.config file, see Understanding the EdgeTransport.exe.Config File.

The <appSettings> section of the EdgeTransport.exe.config file is where you can add new configuration options or modify existing configuration options. Many configuration options that are completely unrelated to the queue database are also available. However they're outside the scope of this topic and won't be discussed.

The configuration options for the queue database that are available in the EdgeTransport.exe.config file are described in the following table.

Message queue database configuration options that are available in the EdgeTransport.exe.config file

Parameter name	Description
QueueDatabaseBatchSize	This parameter specifies the number of database I/O operations that can be grouped together before they're executed. The default value is 40.
QueueDatabaseBatchTimeout	This parameter specifies the maximum time in milliseconds that the database will wait for multiple database I/O operations to group before it executes them. The database I/O operations are executed without waiting for any more if the following conditions are true: • The number of database I/O operations that's specified by the *QueueDatabaseBatchSize* parameter hasn't been reached. • The time specified by the *QueueDatabaseBatchTimeout* parameter has passed. The default value is 100.

QueueDatabaseMaxConnections	This parameter specifies the number of ESE database connections that can be open. The default value is 4.
QueueDatabaseLoggingBufferSize	This parameter specifies the memory that's used to cache the transaction records before they're written to the transaction log file. The default value is 5242880 bytes.
QueueDatabaseLoggingFileSize	This parameter specifies the maximum size of a transaction log file. When the maximum log file size is reached, a new log file is opened. The default value is 5242880 bytes.
QueueDatabaseLoggingPath	This parameter specifies the default directory for the queue database log files. The default value is C:\Program Files\Microsoft\Exchange Server \TransportRoles\data\Queue. Before you change the queue database logging directory, make sure that the new directory exists. Also make sure that the following file permissions are applied to it: Network Service: Full Control; System: Full Control; Administrators: Full Control.
QueueDatabaseMaxBackgroundCleanup Tasks	This parameter specifies the maximum number of background cleanup work items that can be queued to the database engine thread pool at any time. The default value is 32.
QueueDatabaseOnlineDefragEnabled	The parameter enables or disables scheduled online defragmentation of the mail queue database. The default value is `$true`.
QueueDatabaseOnlineDefragSchedule	This parameter specifies the time of day in 24 hour format to start the online defragmentation of the mail queue database. To specify a value, enter the value as a time: *hh:mm:ss*, where *h* = hours, *m* = minutes, and *s* = seconds. The default value is `1:00:00`, which is 01:00 or 1:00 A.M.
QueueDatabaseOnlineDefragTimeToRun	This parameter specifies the time that span the online defragmentation task is allowed to run. Even if the defragmentation task doesn't finish in the time specified, the queue database is left in a consistent state. To specify a value, enter the value as a time span: *hh:mm:ss*, where *h* = hours, *m* = minutes, and *s* = seconds. The default value is `3:00:00`.
QueueDatabasePath	This parameter specifies the default directory for the queue database files. The default value is C:\Program Files\Microsoft\Exchange Server \TransportRoles\data\Queue. Before you change the queue database directory, make sure that the new directory exists. Also make sure that the following file permissions are applied to it: Network Service: Full Control; System: Full Control; Administrators: Full Control.

Return to top

Queue Management

When you experience a mail flow problem or an influx of spam, you can perform operations that modify the status of queues and messages that are located in queues. You can perform an action on a single object, or you can perform a bulk action on more than one selected object. Use the Queue Viewer graphical user interface and commands in the Shell in Exchange 2010 to retrieve information about messages and delivery queues. After you retrieve this information, you can select the queues and messages that you want to manage.

You use Queue Viewer or commands in the Shell to create filter criteria to identify the queues and messages that you want to manage. The filter criteria are based on the following attributes:

- Queue state
- Queue properties
- Message state
- Message properties

For more information about how to filter queues, see Filter Queues. For more information about how to filter messages, see Filter Messages in Queues.

Queue Management Tasks

You use Queue Viewer or commands in the Shell to view information about queues and messages. You can also use these tools to perform the following actions:

- **Suspend queue** This action temporarily prevents delivery of messages that are currently in the queue. The queue continues to accept new messages, but no messages leave the queue. For more information, see Suspend Queues.
- **Resume queue** This action reverses the effect of the suspend queue action and enables delivery of queued messages to resume. For more information, see Resume Queues.
- **Retry queue** When a connection to the next hop for a queue fails, a retry timer is set. The retry timer schedules subsequent connection tries. The retry queue action overrides the next scheduled connection attempt and tries to connect to the next hop immediately. If no connection is made, the next retry time is reset. For more information, see Retry Queues.
  You can also use the **Retry-Queue** cmdlet together with the *Resubmit* parameter to cause the messages in the queue to be resubmitted to the Submission queue and to go back through the categorization process. You can manually resubmit messages that have the following status:
  - Mailbox delivery queues or remote delivery queues that have the status of Retry. The messages in the queues must not be in the Suspended state.
  - Messages in the Unreachable queue that aren't in the Suspended state.
  - Messages in the poison message queue.

  For more information, see Resubmit Messages in Queues.
- **Suspend message** This action temporarily prevents delivery of a message. You can use the suspend message action to prevent delivery of a message to all the recipients in a specific queue or to all recipients in all queues. For more information, see Suspend Messages.
- **Resume message** This action reverses the effect of the suspend message action and enables delivery of queued messages to resume. You can use the resume message action to resume delivery of a message to all the recipients in a specific queue or to all recipients in all queues. You can also use this action to resubmit messages in the poison message queue. For more information, see Resume Messages.
- **Remove message** This action permanently prevents delivery of a message. You can use the remove message action to prevent delivery of a message to any recipients in a specified queue or to all recipients in all queues. You can also configure the remove message action to send a non-delivery report (NDR)

to the sender when the message is removed. For more information, see Remove Messages from Queues.

- **Export message** This action copies a message to the file path that you specify. The messages aren't deleted from the queue, but a copy of the message is saved to a file location. This enables administrators or officials in an organization to later examine the messages. Before you export a message, you must suspend the message in the queue so that typical delivery doesn't continue during the export process. The export format is compatible with e-mail applications such as Microsoft Office Outlook. Save the message in .eml format to make sure that the operating system associates the file with an e-mail application. For more information, see Export Messages from Queues.

Queue Filtering Scenarios

Filtering generates different views of the queues. You use the queue properties as filter options. By specifying filter criteria, you can quickly locate queues and take action on them. The following scenarios are examples of how you can use queue filtering to manage message flow:

- You receive a message from the Microsoft System Center Operations Manager that indicates that a queue length has exceeded the established threshold. You want to investigate whether a server-wide mail flow problem exists.
  You can create a filter to view all the queues that have a message count that exceeds what you consider typical. If a mail flow problem is indicated, you can select all the queues in the filter results and suspend the queues while you continue to investigate.
- You suspend several queues to investigate the cause of mail flow problems. You determine that the problem was caused by an incorrect connector configuration and is now fixed.
  You can create a filter to view all the queues that have a status of Suspended, and then select all the queues in the filter results and resume the queues.

Queue Properties to Use When Filtering Queues

You can use the queue properties to create a filter and locate queues that meet specified criteria. The following table lists the queue properties by which you can filter and the valid values for those properties.

Queue properties

Queue Viewer queue property	Shell queue property	Property type	Value
Delivery Type	DeliveryType	Enumeration	This value is determined by the next hop selection. The next hop selection identifies where messages are queued for delivery. To use the delivery type property in a filter, you must use the constant values that are assigned to each type. The delivery type can be one of the following values: • **DNSConnectorDelivery** The messages are queued for delivery to an external recipient by using an SMTP connector that's located on the local server and that's configured to use Domain Name

			System (DNS) for routing resolution. • **NonSmtpGatewayDelivery** The messages are queued for delivery to an external recipient by using a non-SMTP connector on the local server. • **SmartHostConnectorDelivery** The messages are queued for delivery to an external recipient by using an SMTP connector that's located on the local server and that's configured to use a smart host for routing resolution. • **SmtpRelayWithinAdSitetoEdge** The messages are queued for delivery to an external recipient by using an SMTP connector that's located on an Edge Transport server that's subscribed to the local Active Directory site. • **MapiDelivery** The messages are queued for delivery to recipients that have mailboxes that are located on a Mailbox server that's located in the local Active Directory site. • **SmtpRelayWithinAdSite** The messages are queued for delivery to a Hub Transport server that's located in the same Active Directory site as the local server. The destination server can be the source server for an SMTP connector, the source server of a routing group

			connector, or an expansion server. • **SmtpRelaytoRemoteAdSite** The messages are queued for delivery to a server that's located in a remote Active Directory site. The destination server can be the source server for a connector that's configured to transport messages for external recipients, an expansion server, or a Hub Transport server that delivers messages addressed to mailbox recipients that are located in the remote Active Directory site. • **SmtpRelaytoTiRg** The messages are queued for delivery to an Exchange Server 2003 routing group. The destination server can be the source server for a connector that's configured to transport messages for external recipients, an expansion server, or an Exchange 2003 bridgehead server that delivers messages addressed to mailbox recipients that are located in the routing group. • **Undefined** The messages are located in the Submission queue, and the next hop destination hasn't yet been resolved. • **Unreachable** The messages are located in the

			Unreachable queue, and a route to the recipient couldn't be established.
Identity	Identity	QueueIdentity	This value specifies the identity of the queue. Enter the queue identity in the form of *Server\destination*, where *destination* is a remote domain, Mailbox server, persistent queue name, or the integer that identifies this queue in the queuing database.
Last Error	LastError	String	This value specifies a text string of the last error that was recorded for a queue.
Last Retry Time	LastRetryTime	DateTime	This value specifies the time of the last connection attempt for a queue that has a status of Retry.
Message Count	MessageCount	Ulong	This value is expressed as an integer that represents the number of items in the queue.
Next Hop Connector	NextHopConnector	GUID	This value is expressed as a system GUID and is the GUID of the connector that was used to create the queue.
Next Hop Domain	NextHopDomain	String	This value specifies the next destination of a delivery queue. The next hop domain can be expressed as follows: • Remote SMTP domain name • Exchange server name • Connector name • Routing group • Active Directory site name • Mailbox server fully qualified domain name (FQDN)
Next Retry Time	NextRetryTime	DateTime	This value specifies the time of the next connection attempt for a queue that has a status of Retry.
Status	Status	Enumeration	This value specifies the current queue status. A queue can have one of the following status values: • Active • Suspended • Ready • Retry

Operators to Use When Filtering Queues

When you create a queue filter, you must include an operator for the property value to match. The following table shows the comparison operators that you can use in a filter expression and how each operator functions.

Filter expression operators

Operator	Shell value	Function	Shell code example
Equals	-eq	This operator is used to specify that the results must exactly match the property value that's supplied in the expression.	To display a list of all queues that have a status of Retry: `Get-Queue -Filter {status -eq "retry"}`
Does Not Equal	-ne	This operator is used to specify that the results shouldn't match the property value that's supplied in the expression.	To display a list of all queues that don't have a status of Active: `Get-Queue -Filter {status -ne "active"}`
Greater Than	-gt	This operator is used with properties where the value is expressed as an integer. The filter results only include queues where the value of the specified property is greater than the value that's supplied in the expression.	To display a list of queues that currently contain more than 1,000 messages: `Get-Queue -Filter {messagecount -gt 1000}`
Greater Than or Equals	-ge	This operator is used with properties where the value is expressed as an integer. The filter results only include queues where the value of the specified property is greater than or equal to the value that's supplied in the expression.	To display a list of queues that currently contain 1,000 or more messages: `Get-Queue -Filter {messagecount -ge 1000}`
Less Than	-lt	This operator is used with properties where the value is expressed as an integer. The filter results only include queues where the value of the specified property is less than the value that's	To display a list of queues that currently contain less than 1,000 messages: `Get-Queue -Filter {messagecount -lt 1000}`

		supplied in the expression.	
Less Than or Equals	-le	This operator is used with properties where the value is expressed as an integer. The filter results only include queues where the value of the specified property is less than or equal to the value supplied in the expression.	To display a list of queues that currently contain 1,000 or fewer messages: `Get-Queue -Filter {messagecount -le 1000}`
Contains	-like	This operator is used with properties where the value is expressed as a text string. The filter results only include queues where the value of the specified property contains the text string that's supplied in the expression. You can include the wildcard character (*) in a **-like** expression that's applied to a text string field, but not with a field that has the enumeration type.	To display a list of delivery queues that have a destination to any SMTP domain that ends in Contoso.com: `Get-Queue -Filter {identity -like "*Contoso.com"}`

You can specify multiple expressions in your queue filter by using the **-and** operator in the Shell or by adding multiple expressions in Queue Viewer. Queues must meet all criteria to be included in the result set. For example, the results of the following command will display a list of queues that have a destination to any SMTP domain name that ends in Contoso.com and that currently contain more than 500 messages.

```
Get-Queue -Filter {Identity -like "*Contoso.com*" -and MessageCount -gt 500}
```

Message Filtering Scenarios

Filtering generates different views of the messages in queues. By specifying filter criteria, you can quickly locate messages and take action on them. When an e-mail message is sent to multiple recipients, the message may be located in multiple queues. When you filter by message properties, you can locate messages across all queues. The following scenarios are examples of how you might use message filtering to manage mail flow:

- The Submission queue on the computer that has the Edge Transport server role installed has a high volume of messages that are queued for delivery. Many of the messages have the same subject. Therefore, you suspect that spam is being sent to your organization. You can create a filter to view all the messages that meet the subject criteria. If you determine that the messages are spam, you can select them all and delete them from the delivery queue without sending an NDR.
- A user reports that mail flow is slow. You examine the queues and see that many messages that have random subjects appear to be coming from a single

domain. You can create a filter to view all the queued messages from that domain. If you determine that the messages are spam, you can select them all and delete them from the queues without sending an NDR.

Message Properties to Use When Filtering Messages

You can use message properties to create a filter and locate messages that meet specified criteria. The following table lists the message properties by which you can filter and the values that are associated with those properties.

Message properties

Queue Viewer message property	Shell message property	Property type	Value
Date Received	DateReceived	DateTime	This value specifies the time stamp when the message was received by the server that holds the queue in which the message is located.
Expiration Time	ExpirationTime	DateTime	This value specifies the time stamp when the message will expire and be deleted from the queue if the message can't be delivered.
From Address	FromAddress	SMTP Address	This value specifies the SMTP address of the sender of the message.
Identity	Identity	Integer	This value is an integer that represents a particular message. The message identity is assigned by the queuing database when the message is received for processing. You can include an optional server and queue identity to identify a unique instance of the message. This value can be expressed as follows: • *Server**QueueId**MessageId* • *Server*\Poison*MessageId* • *MessageId* • *Server**MessageId*
Internet Message ID	InternetMessageId	String	This value specifies the value of the `Message-ID:` message header field that's located in the message header. The value of this property is expressed as a GUID followed by the SMTP address of the sending server, as in this example: 67D754D6103DC4FB3BA6BC7205DACABA61231@exchange.contoso.com

Last Error	LastError	String	This value specifies a text string of the last error that was recorded for a message.
Message Source Name	MessageSourceName	String	This value specifies a text string of the name of the component that submitted this message to the queue.
Queue ID	Queue	QueueIdentity	The value of this property specifies the identity of the queue that holds the message. Enter the queue identity in the form of *Server\destination*, where *destination* is a remote domain, Mailbox server, persistent queue name, or the queuing database identifier. The database identifier is represented as an integer and can be determined by viewing the message properties.
Retry Count	RetryCount	Integer	This value specifies the number of times that delivery of a message to a destination was tried.
SCL	SCL	Integer	The value of the spam confidence level (SCL) property specifies the SCL of the message. Valid SCL entries are integers from 0 through 9. An empty SCL property value indicates that the message hasn't been processed by the Content Filter agent.
Size (KB)	Size	ByteQuantifiedSize	This value specifies the size of the message.
Source IP	SourceIP	IP Address	This value specifies the IP address of the external server that submitted the message to the Exchange organization.
Status	Status	Enumeration	This value specifies the current message status. A message can have one of the following status values: • **Active** If the message is in a delivery queue, the message is being delivered to its destination. If the message is in the Submission queue, the message is being processed by the categorizer.

			• **Suspended** The message was suspended by the administrator. • **PendingRemove** The message was deleted by the administrator, but was already in delivery. The message will be deleted if the delivery ends in an error that causes the message to reenter the queue. Otherwise, delivery will continue. • **PendingSuspend** The message was suspended by the administrator, but was already in delivery. The message will be suspended if the delivery ends in an error that causes the message to reenter the queue. Otherwise, delivery will continue. • **Ready** The message is waiting in the queue and is ready to be processed. • **Retry** The last connection attempt for the queue in which this message is located failed. The message is waiting for the next queue retry.
Subject	Subject	String	This value specifies the subject of a message that's expressed as a text string.

Operators to Use When Filtering Messages

When you create a message filter, you must include an operator for the property value to match. The following table shows the comparison operators that you can use in a filter expression and how each operator functions.

Filter expression operators

Operator	Shell value	Function	Shell code example
Equals	-eq	This operator is used to specify that the	To display a list of all messages that have

		results must exactly match the property value that's supplied in the expression.	a status of Retry: `Get-Message -Filter {status -eq "retry"}`
Does Not Equal	-ne	This operator is used to specify that the results shouldn't match the property value that's supplied in the expression.	To display a list of all messages that don't have a status of Active: `Get-Message -Filter {status -ne "active"}`
Greater Than	-gt	This operator is used with properties where the value is expressed as an integer. The filter results only include messages where the value of the specified property is greater than the value that's supplied in the expression.	To display a list of messages that currently have a retry count that's more than 3: `Get-Message -Filter {retrycount -gt 3}`
Greater Than or Equals	-ge	This operator is used with properties where the value is expressed as an integer. The filter results only include messages where the value of the specified property is greater than or equal to the value that's supplied in the expression.	To display a list of messages that currently have a retry count that's 3 or more: `Get-Message -Filter {retrycount -ge 3}`
Less Than	-lt	This operator is used with properties where the value is expressed as an integer. The filter results only include messages where the value of the specified property is less than the value that's supplied in the expression.	To display a list of messages that have an SCL that's less than 6: `Get-Message -Filter {SCL -lt 6}`
Less Than or Equals	-le	This operator is used with properties where the value is expressed as an integer. The filter results only include messages where the	To display a list of messages that have an SCL that's 6 or less: `Get-Message -Filter {SCL -le`

		value of the specified property is less than or equal to the value that's supplied in the expression.	6}
Contains	-like	This operator is used with properties where the value is expressed as a text string. The filter results only include messages where the value of the specified property contains the text string that's supplied in the expression. You can include the wildcard character (*) in a **-like** statement that's applied to a text string field, but not a field that has the enumeration type.	To display a list of messages that have a subject that contains the text "payday loan": `Get-Messages -Filter {subject -like "*payday loan*"}`

You can specify a filter that evaluates multiple expressions by using the **-and** comparison operator in the Shell or by adding multiple expressions in Queue Viewer. To be included in the result set, messages must meet all conditions of the filter. For example, the results of the following command will display a list of messages that are sent from any e-mail address that has a domain name that ends in Contoso.com and that have an SCL that's greater than 5.

```
Get-Message -Filter {FromAddress -like "*Contoso.com*" -and SCL -gt 5}
```

Return to top

Message Retry, Resubmit, and Expiration Intervals

Messages that can't be successfully delivered are subject to various retry, resubmit, and expiration deadlines based on the message's source and destination. *Retry* is a renewed connection attempt with the destination domain, smart host, or Mailbox server. *Resubmit* is the act of sending messages back to the Submission queue for the categorizer to reprocess. The message is said to time-out or *expire* after all delivery efforts have failed over a specified period of time. After a message expires, the sender is notified of the delivery failure. Then the message is deleted from the queue.

In all three cases of retry, resubmit, or expire, you can manually intervene before the automatic actions are performed on the messages.

Configuration Options for Message Retry

When a transport server can't connect to the next hop, the queue is put in a status of Retry. Connection attempts continue until the queue expires or a connection is made.

Configuration Options for Automatic Message Retry

The configuration options that are available for message retry intervals are described in the following table.

Configuration options that are available for message retry intervals

Parameter name	Default value	Where to configure	Description
QueueGlitchRetryCount	4	EdgeTransport.exe.config	This parameter specifies the number of connection attempts that are immediately tried when a transport server has trouble connecting with the destination server. Such connection problems are typically caused by very brief network outages. Typically, you don't have to modify this parameter unless the network is unreliable and continues to experience many accidentally dropped connections.
QueueGlitchRetryInterval	1 minute	EdgeTransport.exe.config	This parameter controls the connection interval between each connection attempt that's specified by the *QueueGlitchRetryCount* parameter. Typically, you don't have to modify this parameter unless the network is unreliable and continues to experience many accidentally dropped connections.
TransientFailureRetryCount	6	**Set-TransportServer** cmdlet or transport server properties in the EMC	This parameter specifies the number of connection attempts that are tried after the connection

			attempts that are controlled by the *QueueGlitchRetryCount* and *QueueGlitchRetryInterval* parameters have failed. Connection problems that exhaust the *QueueGlitchRetryCount* and *QueueGlitchRetryInterval* parameters can be caused by such things as server restarts or cached DNS lookup failures.
TransientFailureRetryInterval	• Hub Transport server: 5 minutes • Edge Transport server: 10 minutes	**Set-TransportServer** cmdlet or transport server properties in the EMC	This parameter controls the connection interval between each connection attempt that's specified by the *TransientFailureRetryCount* parameter.
OutboundConnectionFailureRetryInterval	• Hub Transport server: 10 minutes • Edge Transport Server: 30 minutes	**Set-TransportServer** cmdlet or transport server properties in the EMC	This parameter specifies the retry interval for outbound connection attempts that have previously failed. The previously failed connection attempts are controlled by the *TransientFailureRetryCount* and *TransientFailureRetryInterval* parameters.
MessageRetryInterval	1 minute	**Set-TransportServer** cmdlet	This parameter specifies the retry interval for individual messages that have a status of Retry. We recommend that you don't modify the default value unless Microsoft

			Customer Service and Support advises you to do this.
MailboxDeliveryQueueRetryInterval	5 minutes	EdgeTransport.exe.config	This parameter controls the retry interval for mailbox delivery queues between Hub transport servers.

The <appSettings> section of the EdgeTransport.exe.config file is where you can add new configuration options or modify existing configuration options. There are many configuration options available that are completely unrelated to the message retry, resubmit, and expiration intervals. Any configuration options that don't involve these intervals are outside the scope of this topic.

For more information about the EdgeTransport.exe.config file, see Understanding the EdgeTransport.exe.Config File.

For more information, see Configure Message Retry, Resubmit, and Expiration Intervals.

Configuration Options for Manual Message Retry

When a mailbox delivery queue or a remote delivery queue is in the status of Retry, you can manually force an immediate connection attempt by using Queue Viewer in the EMC or the **Retry-Queue** cmdlet in the Shell. The manual retry attempt overrides the next scheduled retry time. If the connection isn't successful, the retry interval timer is reset. The delivery queue must be in a status of Retry for this action to have any effect.

For more information, see Retry Queues.

Configuration Options for Delay DSN Messages

After each message delivery failure, the Edge Transport server or the Hub Transport server generates a delay delivery status notification (DSN) message and queues it for delivery to the sender of the undeliverable message. This delay DSN message is sent only after a specified delay notification time-out interval, and only if the failed message wasn't successfully delivered during that time. By default, the delay notification time-out interval is 4 hours. This delay prevents the sending of unnecessary delay DSN messages that may be caused by temporary message transmission failures. The sending of delay DSN notification messages can be selectively enabled or disabled for messages that originate inside or outside the Exchange organization.

The configuration options that are available for delay DSN notification messages are described in the following table.

Configuration options that are available for delay DSN notification messages

Parameter name	Default value	Location	Description
DelayNotificationTimeOut	4 hours	**Set-TransportServer**	This parameter specifies how long the server waits before it sends a delay DSN message to the message's sender. The value of this parameter should

			always be greater than the value of the *TransientFailureRetryCount* parameter multiplied by the value of the *TransientFailureRetryInterval* parameter.
ExternalDelayDSNEnabled	`$true`	**Set-TransportConfig**	This parameter specifies whether delay DSN messages can be sent to message senders who are outside the Exchange organization.
InternalDelayDSNEnabled	`$true`	**Set-TransportConfig**	This parameter specifies whether delay DSN messages can be sent to message senders who are inside the Exchange organization.

For more information, see Configure Message Retry, Resubmit, and Expiration Intervals.

Configuration Options for Message Resubmission

Message resubmission sends undelivered messages back to the Submission queue to be reprocessed by the categorizer.

Automatic Message Resubmission

Undelivered messages are automatically resubmitted if the delivery queue is in the status of Retry and has been unable to successfully deliver any messages for a specified period of time. That period of time is controlled by the *MaxIdTimeBeforeResubmit* parameter in the EdgeTransport.exe.config application configuration file. By default, the value of the *MaxIdTimeBeforeResubmit* parameter is 12 hours. Only messages in mailbox delivery queues or remote delivery queues are candidates for automatic resubmission.

For more information, see Configure Message Retry, Resubmit, and Expiration Intervals.

Manual Message Resubmission

You can manually resubmit messages that have the following status on a Hub Transport server or an Edge Transport server:

- Mailbox delivery queues or remote delivery queues that have the status of Retry. The messages in the queues must not be in the Suspended state.
- Messages that are in the Unreachable queue and aren't in the Suspended state.
- Messages that are in the poison message queue.

For more information about the poison message queue and the Unreachable queue, see "About the Poison Message Queue and the Unreachable Queue" earlier in this topic.

If you want to manually resubmit messages that are located in the mailbox delivery queues, the remote delivery queues, or the Unreachable queue without waiting for the time that's specified by the *MaxIdleTimeBeforeResubmit* parameter to pass, you must use the **Retry-Queue** cmdlet with the *Resubmit* parameter. To manually resubmit messages that are located in the poison message queue, you can use Queue Viewer or the

Resume-Message cmdlet to resume the message.

For more information, see the following topics:

- Resubmit Messages in Queues
- Resume Messages

Another way that you can manually resubmit messages is to suspend the messages, export the messages to text files that have the .eml file name extension, and then copy the .eml files to the Replay directory on any Hub Transport server or Edge Transport server. This resubmission method works for messages that are located in the mailbox delivery queues, remote delivery queues, or the Unreachable queue. Messages that are located in the poison message queue are already in the Suspended state. Messages that are located in the Submission queue can't be suspended or exported.

Note:

When you export messages from a queue, you don't remove the messages from the queue. After you export the messages and successfully resubmit them by using the Replay directory, you should remove the suspended messages to avoid duplicate message delivery.

For more information, see Export Messages from Queues and Resubmit Messages in Queues.

Configuration Options for Message Expiration

The *message expiration time-out interval* specifies the maximum length of time that an Edge Transport server or a Hub Transport server tries to deliver a failed message. If the message can't be successfully delivered before the expiration time-out interval has passed, an NDR that contains the original message or the message headers is delivered to the sender.

Automatic Message Expiration

The message expiration time-out interval is controlled by the *MessageExpirationTimeOut* parameter in the **Set-TransportServer** cmdlet or in the transport server properties in the EMC. By default, the value of the *MessageExpirationTimeOut* parameter is 2 days.

For more information, see the following topics:

- Configure Message Retry, Resubmit, and Expiration Intervals
- Set-TransportServer

Manual Message Expiration

Although you can't manually force messages to expire, you can manually remove messages from any queue, except the Submission queue, with or without an NDR.

For more information, see Remove Messages from Queues.

Return to top

1.7.1.40 Understanding Transport in a Hybrid Deployment

Understanding Transport in a Hybrid Deployment

Exchange Server 2010 > Transport > Understanding Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-16*

Service Pack 2 (SP2) for Microsoft Exchange Server 2010 gives you the ability to host some of your Exchange users in an Exchange Online organization hosted in Microsoft Office 365 for enterprises while maintaining a seamless messaging experience for all your users. This topic provides an overview of how Transport servers are used in this scenario.

A hybrid deployment requires at least one server running Exchange Server 2010 SP2 in your organization. If you're currently running a previous version of Exchange, you must add one or more Exchange 2010 SP2 servers to act as gateways to the Exchange Online organization. By doing so, you can enable a hybrid deployment without having to upgrade your entire existing deployment. These Exchange 2010 servers are known as the *hybrid servers*.

Your organization must contain one or more hybrid servers with the Hub Transport and Client Access server roles installed. The Mailbox server role is also required for Exchange Server 2003 organizations that need to support the exchange of free/busy information between your on-premises Exchange 2003 mailboxes and Exchange Online mailboxes. Adding this hybrid server to your organization is equivalent to introducing your first Exchange 2010 server to your deployment. To learn more about hybrid deployments, see Understanding Hybrid Deployments with Exchange 2010 SP3.

Contents

Mail Flow

Mail flow between your on-premises deployment and your Exchange Online organization is secured and protected by Transport Layer Security (TLS). The TLS endpoint in your on-premises organization must be an Exchange 2010 SP2 Hub Transport or Edge Transport server running Exchange 2010 SP1 or SP2.

Your on-premises organization and Exchange Online organization send messages directly to each other through a secure channel. To enable this mail flow, a dedicated hybrid Send connector is automatically created by the Manage Hybrid Configuration wizard. Only a Hub Transport server running on Exchange 2010 SP2 or Edge Transport source server(s) running on Exchange 2010 SP1 or Exchange 2010 SP2 can be selected for this Send connector. If you're running Exchange 2010 SP2 in your organization, any Hub Transport or Edge Transport server can act as the gateway to your Exchange Online organization. If you're running older versions of Exchange, you must deploy hybrid Hub Transport or Edge Transport servers to route messages between your two organizations.

In a hybrid deployment, each organization treats the other one as an internal organization. There is practically no difference between a user hosted on your on-premises servers and an Exchange Online user when Exchange is processing messages. Anti-spam filters are also bypassed for messages between the two organizations.

Secured and Authenticated Mail Flow

Even though messages between the on-premises and Exchange Online organizations go through a logical tunnel, they're still transferred over the Internet and therefore must be protected against malicious users. Exchange 2010 provides the following protection measures:

- **Channel privacy** Unauthorized parties can't access any captured packets.
- **Receiver authentication** Senders are protected from unauthorized parties impersonating valid receivers.

- **Sender authentication** Receivers are protected from unauthorized parties impersonating valid senders.

Channel Privacy

To protect both the on-premises and cloud-based organizations, Exchange 2010 forces TLS using Secure Sockets Layer (SSL) certificates provided by a trusted third-party Certificate Authority (CA). Self-signed certificates are not supported for channel privacy in a hybrid deployment. All messages sent through the TLS-protected channel are encrypted.

The sending and receiving servers examine the certificate configured on the other server. The subject name, or one of the subject alternative names (SANs), configured on the certificates must match the fully qualified domain name (FQDN) that an administrator has explicitly specified on the other server. For example, if the Exchange Online organization is configured to accept and secure messages sent from the mail.contoso.com FQDN, the sending on-premises hybrid servers must have an SSL certificate with mail.contoso.com in either the subject name or SAN. If this requirement isn't met, the connection is refused.

Receiver Authentication

In addition to the regular certificate checks performed during TLS, the Send connectors that participate in hybrid deployment mail flow also perform domain validation. Domain validation is an additional security feature that reduces the risk of malicious users impersonating a receiving server. When domain validation is enabled on a Send connector, the Transport server performs the following security checks on the outbound connection:

- The communication channel is encrypted using TLS.
- The certificate of the receiving server is validated, and revocation list checks are performed.
- The Transport server verifies that the FQDN on the certificate of the receiving server matches the domain configured in the Send connector properties.

Sender Authentication

To prevent a malicious user from impersonating a valid sender, each message is authenticated to verify that it was submitted by the specified sender. Inside an Exchange organization, sender authentication is verified by using custom message headers added by Exchange servers. For messages that are sent between the on-premises and Exchange Online organizations, these header values are encrypted at the source and then decrypted and verified at the destination. While in transit, these headers can’t be decrypted by any third party that might capture the message.

Mail To and From the Internet

Recipients in the on-premises and Exchange Online organizations typically have the same reply address, such as @contoso.com. Because they have the same reply address, all messages to recipients in both organizations must follow the same inbound route. All inbound messages can be delivered either to the on-premises organization or to the Exchange Online organization. Where you decide to route inbound messages depends on where the majority of your mailboxes are located, whether you have a Microsoft Forefront Online for Protection (FOPE), and other factors.

Messages sent from recipients in the on-premises and Exchange Online organizations can either follow the same or different routes to the Internet. Messages sent from on-premises recipients are always sent directly to the Internet. Messages sent from Exchange Online recipients can either be sent directly to the Internet or routed through your on-premises organization first. You may want to route Exchange Online messages through your on-premises organization if you want to apply compliance policies to them first.

There are many considerations that you need to think about when planning transport for your hybrid deployment, such as whether you use FOPE to protect your on-premises

organization, whether you have an Edge Transport server configured, and how you want to route inbound and outbound Internet mail. For detailed information about these considerations and help on deciding which options are best for your organization, see Understanding Transport Options in Exchange 2003 Hybrid Deployments.

Transport Features

This section discusses how various Transport features are used in a hybrid deployment. The information here assumes that you're running Exchange 2010 for your on-premises deployment because some of the features described here don't apply to earlier versions of Exchange. To learn more, see the following topics:

- Upgrade from Exchange 2007 Transport
- Upgrade from Exchange 2003 Transport

Note:
The features discussed in this section are only available in a hybrid deployment.

Transport Rules and Journaling

Transport Rules and Journaling rules aren't synchronized between your on-premises deployment and your Exchange Online organization. Therefore, you must ensure that you keep any rules that you have implemented consistent in both organizations.

Delivery Reports

Users can track messages they've sent and received in a hybrid deployment as long as delivery reports are enabled for the corresponding organizational relationships for both the on-premises and Exchange Online organizations. By default, this feature is enabled in a hybrid deployment. However, keep in mind that if you have older versions of Exchange in your on-premises deployment, the delivery reports will not show the final delivery to recipients hosted on the legacy servers, but rather that the message was transferred to the legacy Exchange system. This isn't a limitation of the hybrid deployment; it's because of changes in the message tracking implementation in Exchange 2010. For more information, see the "Message Tracking Across Versions" section in Upgrade from Exchange 2007 Transport.

MailTips

MailTips are designed to work seamlessly in a hybrid deployment. If an on-premises user addresses a message to a recipient in your Exchange Online organization, your local Client Access servers contact the Client Access servers in the Exchange Online organization and requests MailTips data for the message. Upon this request, the Client Access servers in the Exchange Online organization processes the MailTips request, evaluates the message for any MailTips, and returns all applicable MailTips to your on-premises Client Access servers. The process is the same when a user in your Exchange Online organization addresses a message to an on-premises recipient.

In a hybrid deployment, keep in mind the following differences regarding MailTips:

- The External Recipients MailTip is evaluated only in the local organization. This is because the Exchange Online organization can't determine which recipients would be considered external for an on-premises user.
- Number of external recipients in a group MailTip is only evaluated for the local groups using the local Group Metrics data for the same reason.
- The Oversize Message MailTip is evaluated both locally and in the remote organization. Therefore, it's important to make sure that the message size restrictions for your on-premises organization match those configured for your Exchange Online organization to avoid an inconsistent experience for your users.
- All objects in the remote organization are represented as mail-enabled objects in the local organization. For example, a mailbox in your Exchange Online organization is represented as a mail user in your on-premises organization.

Because all objects can have Custom MailTips, you potentially can configure two different Custom MailTips for the same recipient. In this case, only the local Custom MailTip will be shown. On-premises users will see the Custom MailTip configured for the on-premises object, and cloud-based users will see the Custom MailTip configured for the Exchange Online object.

- It's also possible to have a mismatching configuration for moderated recipients or restricted recipients. For example, an on-premises mailbox may be restricted, but the corresponding mail user in your Exchange Online organization may not be restricted. In this scenario, the Restricted Recipient MailTip will be shown even for an Exchange Online user. The Moderated Recipient MailTip functions in a similar fashion.

MailTips are configured to work in a hybrid deployment by default. However, it's possible to customize the way MailTips are handled if you want different experiences for your on-premises and Exchange Online users. For more information, see the "MailTips Architecture" section in Understanding MailTips and "Use the Shell to configure MailTips for organizational relationships" section in Configure Organizational Settings for MailTips.

Message Moderation

Hybrid deployment message moderation functionality relies on the following requirements:

- Synchronization of moderation attributes of mail-enabled objects.
- At least one arbitration mailbox created in your on-premises organization.
- At least one arbitration mailbox created in your Exchange Online organization.
- Preservation of the headers and TNEF format between the two organizations.

When you configure a hybrid deployment with Office 365, all the requirements above are met. You don't need to do anything additional for message moderation to work.

Edge Transport in a Hybrid Deployment

Mail flow in a hybrid deployment requires an Exchange 2010 SP2 server as the TLS endpoint for your on-premises deployment. This is typically an Exchange 2010 SP2 Hub Transport server in your on-premises organization. However, if you don't want to expose your internal Hub Transport server directly to the Internet, you can use an Exchange 2010 SP2 Edge Transport server as the TLS endpoint. If you use an Edge Transport server, that server will handle mail between your on-premises organization and the Exchange Online organization on behalf of the Hub Transport server. You can also elect to use an Edge Transport server for handling mail sent to and from Internet recipients for your on-premises organization.

To learn more about Edge Transport servers in your hybrid deployment, see:

- Understanding Edge Transport Servers in Exchange 2003 Hybrid Deployments

If you're using Exchange 2007 Edge Transport servers in your organization, they must be upgraded to Exchange 2010 SP2 if you plan to use them in a hybrid deployment.

1.7.2 Managing Transport Servers

Managing Transport Servers

Exchange Server 2010 > Transport >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-09*

1.7.2.1 Change the Method for 7-bit Transfer Encoding

Change the Method for 7-bit Transfer Encoding

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Microsoft Exchange Server 2010, the 7-bit transfer encoding method for MIME format is fixed to quoted-printable (QP) encoding. You can change the transfer encoding method by editing the EdgeTransport.exe.config file. Use Microsoft Windows Explorer to change the method for transfer encoding on the Microsoft Exchange Server 2010-based computer running the Hub Transport server role.

Looking for other management tasks related to managing transport servers? Check out Managing Transport Servers.

Use Windows Explorer and Notepad to change the method for transfer encoding

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

1. On the Exchange 2010-based server running the Hub Transport server role, start Windows Explorer.
2. Locate the following folder, in which *<drive>* represents the actual installation drive: **<drive>:\Program Files\Microsoft\Exchange Server\V14\Bin**.
3. Make a backup copy of the EdgeTransport.exe.config file, and name the backup file copy **EdgeTransport.exe.config.old**.
4. Start Notepad, and then open the **EdgeTransport.exe.config** file.
5. Locate the following line between the <appsettings> tag and the </appsettings> tag.

   ```
   <add key="ByteEncoderTypeFor7BitCharsets" value="1" />
   ```

   If this line doesn't exist in this location, insert the line between the <appsettings> tag and the </appsettings> tag.
6. Change the value described in the line to an appropriate value from the table in "Values to Change the Method for Transfer Encoding" later in this topic. This value controls the MIME encoding behavior.
7. Save the changes, and then exit Notepad.
8. Start the Microsoft Exchange Transport service.

Values to Change the Method for Transfer Encoding

The following table lists the values that you can use to change the method for transfer encoding. This table also describes the behavior of the value.

Value	Behavior
0	Always use default 7-bit transfer encoding for HTML and for plain text.
1	Always use QP encoding for HTML and for plain text.
2	Always use Base64 encoding for HTML and for plain text.
5	Use QP encoding for HTML and for plain text unless line wrapping is enabled in plain text. If line wrapping is enabled, use 7-bit encoding for plain text.
6	Use Base64 encoding for HTML and for plain text, unless line wrapping is enabled in plain text. If line wrapping is enabled in plain text, use Base64 encoding for HTML, and use 7-bit encoding for plain text.
13	Always use QP encoding for HTML. Always use 7-bit encoding for plain text.
14	Always use Base64 encoding for HTML. Always use 7-bit encoding for plain text.

1.7.2.2 Configure Edge Transport Server Properties

Configure Edge Transport Server Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The property configuration of a transport server running Microsoft Exchange Server 2010 determines how that server processes messages. The transport server settings that you configure on an Edge Transport server apply only to that specific server.

Looking for other management tasks related to configuring Edge Transport server properties? Check out Managing Transport Servers.

What Do You Want to Do?

- Use the EMC to configure the properties of an Edge Transport server
- Use the Shell to configure the properties of an Edge Transport server

Use the EMC to configure the properties of an Edge Transport server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, right-click the Edge Transport server you want to configure, and then select **Properties**.
3. On the **General** tab, you can view general information about the server:
   - **Version** This field displays the version of Exchange installed on the server.
   - **Edition** This field displays the Exchange Server edition. The edition is either Standard Edition or Enterprise Edition.
   - **Role(s)** This field displays the Exchange server roles installed on the server.
   - **Product ID** This field displays the product ID for the Exchange server. If you haven't yet entered the product key for the server, the product ID displayed is **Unlicensed**. To license an unlicensed version of Exchange, see Enter Product Key.
   - **Modified** This field displays the last date and time that a configuration change was made on this server.
4. On the **System Settings** tab, view the domain controller servers and global catalog servers. You can also enable an error reporting feature:
   - **Domain controller servers being used by Exchange** This read-only box displays a list of domain controller servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.
   - **Global catalog servers being used by Exchange** This read-only box displays a list of global catalog servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.
   - **Automatically send fatal service error report to Microsoft** Select this

check box if you want to enable the error reporting feature and automatically send an error report to Microsoft in the event of a fatal error.
If you enable the error reporting feature, information about fatal service errors is sent to Microsoft over encrypted channels. The information is used to improve Microsoft products. When this feature is enabled and the issue reported has a known solution, the server receives feedback from Microsoft. This feedback contains a link to information that may help resolve the problem.

5. On the **Customer Feedback Options** tab, you can enroll the selected server into the Customer Experience Improvement Program. For more information, see Opt-in or Opt-out of the Customer Experience Improvement Program.

6. Use the **External DNS Lookups** tab to specify whether to use the DNS servers that are configured on a network adapter installed on this server or to use specific DNS servers when resolving the addresses of mail servers for external mail delivery. External DNS servers are used by Send connectors that are configured to use the external DNS lookup configuration on the transport server. When messages are routed to these Send connectors, the external DNS lookup settings that are configured for the source servers are used to resolve IP addresses for the delivery destination.
   You can choose one of the following options:
   - **Use network card DNS settings** To select an installed network adapter from the list, select **Use network card DNS settings**, and then select a network adapter from the drop-down list. The server then uses the DNS servers configured on that network adapter. The default setting is **All Available IPv4**. If you select this setting, the server uses the DNS servers configured on all the adapters on that server.
   - **Use these DNS servers** To have the server select from a list of manually entered DNS servers to query when resolving a remote server, select **Use these DNS servers**. To add a server to the list, type the IP address of the external DNS server, and then click **Add**. To change the IP address of a previously added DNS server, select that server, and then click **Edit**. To remove a previously added DNS server, select that server, and then click  .

7. Use the **Internal DNS Lookups** tab to specify whether to use the DNS servers that are configured on a network adapter installed on this server or to use specific DNS servers when resolving the addresses of mail servers for internal mail delivery. Internal DNS servers are used to resolve IP addresses for servers inside your organization.
   You can choose one of the following options:
   - **Use network card DNS settings** To select an installed network adapter from the list, select **Use network card DNS settings**, and then select a network adapter from the drop-down list. The server then uses the DNS servers configured on that network adapter. The default setting is **All Available IPv4**. If you select this setting, the server uses the DNS servers configured on all the adapters on that server.
   - **Use these DNS servers** To have the server select from a list of manually entered DNS servers to query when it's resolving an internal server, select **Use these DNS servers**. To add a server to the list, type the IP address of the internal DNS server, and then click **Add**. To change the IP address of a previously added DNS server, select that server, and then click **Edit**. To remove a previously added DNS server, select that server, and then click  .

8. Use the **Limits** tab to specify the number of times that the server retries message delivery, to set notification for undelivered messages, and to specify connection restrictions.

- **Outbound connection failure retry interval (minutes)** Select this option to specify the retry interval for subsequent connection attempts to a remote server where earlier connection attempts as specified by the transient failure retry attempts and the transient failure retry interval have failed. The valid input range is 1 minute to 28800 minutes (20 days). We recommend that you don't modify the default value unless Microsoft Customer Service and Support has advised you to do this. The default value is 30 minutes.
- **Transient failure retry interval (seconds)** Select this option to specify the interval between each connection attempt specified by the **Transient failure retry attempts** option. The valid input range is 1 second to 43200 seconds (12 hours). The default value is 600 seconds (10 minutes).
- **Transient failure retry attempts** Select this option to specify the maximum number of times that a server immediately retries when it encounters a connection failure with a remote server. The default value is 6. The valid input range is 0 to 15. When this parameter is set to 0, the server doesn't immediately try to reconnect.
- **Maximum time since submission (days)** Select this option to specify the expiration time-out for a particular message. If a message remains in the queue for longer than this period of time, the message is returned to the sender as a hard failure. The default value is 2 days. The valid input range is 1 day to 90 days.
- **Notify sender when message is delayed more than (hours)** Select this option to specify how long the server waits before it generates a delivery status notification (DSN) that notifies the sender of a delivery delay. The default value is 4 hours. The valid input range is 1 hour to 720 hours (30 days).
- **Maximum concurrent outbound connections** Select this option to specify the maximum number of outgoing connections that can be open at a time. If the connection limit is reached, the server doesn't initiate new connections until the number of current connections decreases. The default value is 1000. The valid input range is 1 to 2147483647. To disable this restriction, clear the check box next to **Maximum concurrent outbound connections**.
- **Maximum concurrent outbound connections per domain** Select this option to specify the maximum number of concurrent connections to any single domain. The default value is 20. The valid input range is 1 to 2147483647. To disable this restriction, clear the check box next to **Maximum concurrent outbound connections per domain**.

9. Use the **Log Settings** tab to enable or disable message tracking, enable or disable connectivity logging, and to view or change the path for the message tracking logs, connectivity logs, Send connector protocol logs, and Receive connector protocol logs. On the **Log Settings** tab, you can view or set the following options:
   - **Enable message tracking log** By default, message tracking is enabled on Hub Transport and Edge Transport servers. To disable message tracking, clear the check box next to **Enable message tracking log**. To enable message tracking, select the check box next to **Enable message tracking log**.
   - **Message tracking log path** This field displays the current location of the message tracking logs. By default, the message tracking logs are stored at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking. To change the location of the message tracking logs, type the path to the new log location. Before you can change the path, message tracking must be enabled.
   - **Enable connectivity log** By default, connectivity logging is disabled on Hub Transport and Edge Transport servers. To enable connectivity logging, select the check box next to **Enable connectivity log**. To disable connectivity logging, clear the check box next to **Enable connectivity log**.

- **Connectivity log path** This field displays the current location of the connectivity logs. By default, the connectivity logs are stored at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Connectivity. To change the location of the connectivity logs, type the path to the new log location. Before you can change the path, connectivity logging must be enabled.
- **Send protocol log path** This field displays the current location of the Send connector protocol logs. By default, the Send connector protocol logs are stored at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\ProtocolLog\SmtpSend. All the Send connectors that are configured on the Edge Transport server share the same protocol logs. By default, protocol logging is disabled on all Send connectors.

  To change the location of the Send connector protocol logs, type the path to the new log location.
- **Receive protocol log path** This field displays the current location of the Receive connector protocol logs. By default, the Receive connector protocol logs are stored at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\ProtocolLog\SmtpReceive. All the Receive connectors that are configured on the Edge Transport server share the same protocol logs. By default, protocol logging is disabled on all Receive connectors.

  To change the location of the Receive connector protocol logs, type the path to the new log location.

Use the Shell to configure the properties of an Edge Transport server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

You use the **Set-TransportServer** cmdlet to configure the properties of an Edge Transport server. Although the EMC allows you to configure the most commonly used properties of an Edge Transport server, the **Set-TransportServer** cmdlet allows you to configure all the properties of an Edge Transport server. The following examples demonstrate how you can use the Shell to configure the most common properties of an Edge Transport server. For more information about the possible configuration options, see Managing Transport Servers.

This example configures an Edge Transport server to use a specific list of DNS servers for external DNS lookups instead of the DNS servers configured on the adapters installed on that server.

```
Set-TransportServer Edge01 -ExternalDNSAdapterEnabled $false -ExternalDNSServers
```

This example enables connectivity logging on the Edge Transport server and configures it to store the connectivity log files in the C:\SMTP Logs folder.

```
Set-TransportServer Edge01 -ConnectivityLogEnabled $true -ConnectivityLogPath "C:
```

For detailed syntax and parameter information, see Set-TransportServer.

1.7.2.3 Configure Edge Transport Server Using Cloned Configuration

Configure Edge Transport Server Using Cloned Configuration

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the provided Shell scripts to duplicate the configuration of a computer that has the Microsoft Exchange Server 2010 Edge Transport server role installed. This process is referred to as *cloned configuration*. *Cloned configuration* is the practice of deploying new Edge Transport servers based on the configuration information from a previously configured source server. The configuration information from the previously configured source server is copied and exported to an XML file, which is then imported to the target server.

Edge Transport server configuration information is stored in Active Directory Lightweight Directory Services (AD LDS) and isn't replicated among multiple Edge Transport servers. By using cloned configuration, you can make sure that every Edge Transport server that's deployed in the perimeter network is operating by using the same configuration.

Important:

Cloned configuration doesn't duplicate the Edge Subscription settings of a server. The certificates used by the Microsoft Exchange EdgeSync service aren't cloned. You must run the EdgeSync process separately for each Edge Transport server. The Microsoft Exchange EdgeSync service overwrites any settings included in both cloned configuration information and in EdgeSync replication information.

Included with the Edge Transport server installation are two Shell scripts that you use to perform the following cloned configuration tasks:

- **ExportEdgeConfig.ps1** This script exports all user-configured settings and data from an Edge Transport server and stores that data in an XML file.
- **ImportEdgeConfig.ps1** During the validate configuration step, the ImportEdgeConfig.ps1 script checks the XML file to see whether the server-specific export settings are valid for the target server. If settings have to be modified, the script writes the invalid settings to an answer file that you modify to specify the target server information that's used during the import configuration step. During the import configuration step, the script imports all user-configured settings and data that's stored in the intermediate XML file that was created by the ExportEdgeConfig.ps1 script.

These scripts are located in the \scripts folder in your Exchange installation folder. The default location for this folder is C:\Program Files\Microsoft\Exchange Server\Scripts.

Looking for other management tasks related to managing transport servers? Check out Managing Transport Servers.

Prerequisites

- Understand what configuration data is cloned and the parameters that can be used with the cloned configuration scripts. For more information, see Understanding Edge Transport Server Cloned Configuration.
- The Edge Transport server role is installed and configured on the source server.
- The Edge Transport server role is installed on the target server.

Note:

If any Send connectors are configured to use credentials, the password is

written to the intermediate XML file as an encrypted string. You can use the *-key* parameter with the ImportEdgeConfig.ps1 and ExportEdgeConfig.ps1 scripts to specify the 32-byte string to use for password encryption and decryption. If you don't use the *-key* parameter, a default encryption key is used.

Use the Shell to clone a source server by using the Shell scripts

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

1. Copy the ExportEdgeConfig.ps1 script to the root folder of your user profile on the source server.
2. On the source server, export the server configuration data by using the ExportEdgeConfig.ps1 script. Run the following command in the Shell. In the command, replace *C:\CloneConfigData.xml* with the full path of the XML file to be created by the ExportEdgeConfig.ps1 script.

   ```
   ./ExportEdgeConfig -CloneConfigData:"C:\CloneConfigData.xml"
   ```

   The confirmation message, "Edge configuration data is exported successfully to: *C:\CloneConfigData.xml*," appears.
3. Copy the output file to the target server.

Use the Shell scripts to validate a configuration file and create an answer file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

1. Copy the ImportEdgeConfig.ps1 script to the root folder of your user profile on the target server.
2. On the target server, validate the configuration file by using the ImportEdgeConfig.ps1 script. Run the following command in the Shell. In the command, replace C*:\CloneConfigData.xml* with the full path of the XML file that was created by the ExportEdgeConfig.ps1 script. Replace *C:\CloneConfigAnswer.xml* with the full path of the answer file that will be used by the ImportEdgeConfig.ps1 script to configure server-specific settings.

   ```
   ./ImportEdgeConfig -CloneConfigData:"C:\CloneConfigData.xml" -IsImport
   ```

   The confirmation message, "Answer file is successfully created," appears.
3. Open the answer file and modify any settings that are invalid for the target server. If no modifications are required, the answer file will have no entries. Save your changes.

Use the Shell scripts to import a configuration file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

Import the server configuration data by using the ImportEdgeConfig.ps1 script. Run the following command in the Shell. In the command, replace *C:\CloneConfigData.xml* with the full path of the XML file that was created by the ExportEdgeConfig.ps1 script. Replace *C:\CloneConfigAnswer.xml* with the full path of the answer file that was created by the ImportEdgeConfig.ps1 script.

```
./ImportEdgeConfig -CloneConfigData:"C:\CloneConfigData.xml" -IsImport $true -Clo
```

The confirmation message, "Importing Edge configuration information succeeded," appears.

1.7.2.4 Configure Hub Transport Server Properties

Configure Hub Transport Server Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The property configuration of a transport server running Microsoft Exchange Server 2010 determines how that server processes messages. The transport server settings that you configure on a Hub Transport server apply only to that specific server.

Looking for other management tasks related to configuring Hub Transport server properties? Check out Managing Transport Servers.

What Do You Want to Do?

- Use the EMC to configure the properties of a Hub Transport server
- Use the Shell to configure the properties of a Hub Transport server

Use the EMC to configure the properties of a Hub Transport server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Hub Transport**.
2. In the result pane, right-click the Hub Transport server you want to configure, and then select **Properties**.
3. On the **General** tab, you can view general information about the server:
   - **Version** This field displays the version of Exchange installed on the server.
   - **Edition** This field displays the Exchange Server edition. The edition is either Standard Edition or Enterprise Edition.
   - **Role(s)** This field displays the Exchange server roles installed on the server.

- **Product ID** This field displays the product ID for the Exchange server. If you haven't yet entered the product key for the server, the product ID displayed is **Unlicensed**. To license an unlicensed version of Exchange, see Enter Product Key.
- **Modified** This field displays the last date and time that a configuration change was made on this server.

4. On the **System Settings** tab, view the domain controller servers and global catalog servers. You can also enable an error reporting feature:
   - **Domain controller servers being used by Exchange** This read-only box displays a list of domain controller servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.
   - **Global catalog servers being used by Exchange** This read-only box displays a list of global catalog servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.
   - **Automatically send fatal service error report to Microsoft** Select this check box if you want to enable the error reporting feature and automatically send an error report to Microsoft in the event of a fatal error.
     If you enable the error reporting feature, information about fatal service errors is sent to Microsoft over encrypted channels. The information is used to improve Microsoft products. When this feature is enabled and the issue reported has a known solution, the server receives feedback from Microsoft. This feedback contains a link to information that may help resolve the problem.

5. On the **Customer Feedback Options** tab, you can enroll the selected server into the Customer Experience Improvement Program. For more information, see Opt-in or Opt-out of the Customer Experience Improvement Program.

6. Use the **External DNS Lookups** tab to specify whether to use the DNS servers that are configured on a network adapter installed on this server or to use specific DNS servers when resolving the addresses of mail servers for external mail delivery. External DNS servers are used by Send connectors that are configured to use the external DNS lookup configuration on the transport server. When messages are routed to these Send connectors, the external DNS lookup settings that are configured for the source servers are used to resolve IP addresses for the delivery destination.
   You can choose one of the following options:
   - **Use network card DNS settings** To select an installed network adapter from the list, select **Use network card DNS settings**, and then select a network adapter from the drop-down list. The server then uses the DNS servers configured on that network adapter. The default setting is **All Available IPv4**. If you select this setting, the server uses the DNS servers configured on all the adapters on that server.
   - **Use these DNS servers** To have the server select from a list of manually entered DNS servers to query when resolving a remote server, select **Use these DNS servers**. To add a server to the list, type the IP address of the external DNS server, and then click **Add**. To change the IP address of a previously added DNS server, select that server, and then click **Edit**. To remove a previously added DNS server, select that server, and then click  .

7. Use the **Internal DNS Lookups** tab to specify whether to use the DNS servers that are configured on a network adapter installed on this server or to use specific DNS servers when resolving the addresses of mail servers for

internal mail delivery. Internal DNS servers are used to resolve IP addresses for servers inside your organization.
You can choose one of the following options:

- **Use network card DNS settings** To select an installed network adapter from the list, select **Use network card DNS settings**, and then select a network adapter from the drop-down list. The server then uses the DNS servers configured on that network adapter. The default setting is **All Available IPv4**. If you select this setting, the server uses the DNS servers configured on all the adapters on that server.
- **Use these DNS servers** To have the server select from a list of manually entered DNS servers to query when it's resolving an internal server, select **Use these DNS servers**. To add a server to the list, type the IP address of the internal DNS server, and then click **Add**. To change the IP address of a previously added DNS server, select that server, and then click **Edit**. To remove a previously added DNS server, select that server, and then click  .

8. Use the **Limits** tab to specify the number of times that the server retries message delivery, to set notification for undelivered messages, and to specify connection restrictions.
   - **Outbound connection failure retry interval (minutes)** Select this option to specify the retry interval for subsequent connection attempts to a remote server where earlier connection attempts as specified by the transient failure retry attempts and the transient failure retry interval have failed. The valid input range is 1 minute to 28800 minutes (20 days). We recommend that you don't modify the default value unless Microsoft Customer Service and Support has advised you to do this. The default value is 10 minutes.
   - **Transient failure retry interval (seconds)** Select this option to specify the interval between each connection attempt specified by the **Transient failure retry attempts** option. The valid input range is 1 second to 43200 seconds (12 hours). The default value is 300 seconds (5 minutes).
   - **Transient failure retry attempts** Select this option to specify the maximum number of times that a server immediately retries when it encounters a connection failure with a remote server. The default value is 6. The valid input range is 0 to 15. When this parameter is set to 0, the server doesn't immediately try to reconnect.
   - **Maximum time since submission (days)** Select this option to specify the expiration time-out for a particular message. If a message remains in the queue for longer than this period of time, the message is returned to the sender as a hard failure. The default value is 2 days. The valid input range is 1 day to 90 days.
   - **Notify sender when message is delayed more than (hours)** Select this option to specify how long the server waits before it generates a delivery status notification (DSN) that notifies the sender of a delivery delay. The default value is 4 hours. The valid input range is 1 hour to 720 hours (30 days).
   - **Maximum concurrent outbound connections** Select this option to specify the maximum number of outgoing connections that can be open at a time. If the connection limit is reached, the server doesn't initiate new connections until the number of current connections decreases. The default value is 1000. The valid input range is 1 to 2147483647. To disable this restriction, clear the check box next to **Maximum concurrent outbound connections**.
   - **Maximum concurrent outbound connections per domain** Select this option to specify the maximum number of concurrent connections to any single domain. The default value is 20. The valid input range is 1 to 2147483647. To disable this restriction, clear the check box next to **Maximum concurrent outbound connections per domain**.

9. Use the **Log Settings** tab to enable or disable message tracking, enable or disable connectivity logging, and to view or change the path for the message tracking logs, connectivity logs, Send connector protocol logs, and Receive connector protocol logs. On the **Log Settings** tab, you can view or set the following options:
   - **Enable message tracking log** By default, message tracking is enabled on Hub Transport and Edge Transport servers. To disable message tracking, clear the check box next to **Enable message tracking log**. To enable message tracking, select the check box next to **Enable message tracking log**.
   - **Message tracking log path** This field displays the current location of the message tracking logs. By default, the message tracking logs are stored at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking. To change the location of the message tracking logs, type the path to the new log location. Before you can change the path, message tracking must be enabled.
   - **Enable connectivity log** By default, connectivity logging is disabled on Hub Transport and Edge Transport servers. To enable connectivity logging, select the check box next to **Enable connectivity log**. To disable connectivity logging, clear the check box next to **Enable connectivity log**.
   - **Connectivity log path** This field displays the current location of the connectivity logs. By default, the connectivity logs are stored at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Connectivity. To change the location of the connectivity logs, type the path to the new log location. Before you can change the path, connectivity logging must be enabled.
   - **Send protocol log path** This field displays the current location of the Send connector protocol logs. By default, the Send connector protocol logs are stored at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\ProtocolLog\SmtpSend. All the Send connectors that are configured on the Edge Transport server share the same protocol logs. By default, protocol logging is disabled on all Send connectors.

     To change the location of the Send connector protocol logs, type the path to the new log location.
   - **Receive protocol log path** This field displays the current location of the Receive connector protocol logs. By default, the Receive connector protocol logs are stored at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\ProtocolLog\SmtpReceive. All the Receive connectors that are configured on the Edge Transport server share the same protocol logs. By default, protocol logging is disabled on all Receive connectors.

     To change the location of the Receive connector protocol logs, type the path to the new log location.

Use the Shell to configure the properties of a Hub Transport server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

You use the **Set-TransportServer** cmdlet to configure the properties of a Hub Transport server. Although the EMC allows you to configure the most commonly used properties of a Hub Transport server, the **Set-TransportServer** cmdlet allows you to configure all the properties of a Hub Transport server. The following examples demonstrate how you can use the Shell to configure the most common properties of a Hub Transport server. For more information about the possible configuration options, see Managing Transport Servers.

This example configures a Hub Transport server to use a specific list of DNS servers for

external DNS lookups instead of the DNS servers configured on the adapters installed on that server.

```
Set-TransportServer Hub01 -ExternalDNSAdapterEnabled $false -ExternalDNSServers {
```

This example enables connectivity logging on the Hub Transport server and configures it to store the connectivity log files in the C:\SMTP Logs folder.

```
Set-TransportServer Hub01 -ConnectivityLogEnabled $true -ConnectivityLogPath "C:\
```

For detailed syntax and parameter information, see Set-TransportServer.

1.7.2.5 Configure Transport Settings Properties

Configure Transport Settings Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-12*

Transport settings define how all Hub Transport servers running Microsoft Exchange Server 2010 function in your organization. The options configured are used by all Hub Transport servers.

Looking for other management tasks related to transport servers? Check out Managing Transport Servers.

What Do You Want to Do?

- Use the EMC to configure global transport settings
- Use the Shell to configure global transport settings

Use the EMC to configure global transport settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport configuration" entry in the Transport Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, select the **Global Settings** tab, and then double-click **Transport Settings**.
3. Use the **General** tab to configure the transport limits and transport dumpster settings for all Hub Transport servers in your Exchange organization:
   - **Maximum receive size (KB)** This field specifies the maximum message size that can be received by recipients in the organization. The default value is 10240 KB. The valid input range is from 0 through 2097151 KB. If you clear the check box next to **Maximum receive size (KB)**, no limit is imposed on the message size that can be received by recipients in the organization.
   - **Maximum send size (KB)** This field specifies the maximum message size that can be sent by senders in the organization. The default value is 10240 KB. The valid input range is from 0 through 2097151 KB. If you clear the

check box next to **Maximum send size (KB)**, no limit is imposed on the message size that can be sent by senders in the organization.

- **Maximum number of recipients** This field specifies the maximum number of recipients in a message. The default is 5000. The valid input range is from 0 through 2147483647. If you clear the check box next to **Maximum number of recipients**, no limit is imposed on the number of recipients in a message. Exchange 2010 treats an unexpanded distribution group as one recipient.
- **Maximum size per mailbox database (MB)** This field specifies the maximum size of the transport dumpster for each mailbox database. The default value is 18 MB. The valid input range for this parameter is from 0 through 2097151 MB.

  To enable the transport dumpster, the value of **Maximum size per mailbox database (MB)** must be greater than 0, and the value of **Maximum retention time (days)** must be greater than 0.
- **Maximum retention time (days)** This field specifies how long an e-mail message should remain in the transport dumpster. The default value is 7 days. The valid input range is from 0 through 24855 days.

  To enable the transport dumpster, the value of **Maximum size per mailbox database (MB)** must be greater than 0, and the value of **Maximum retention time (days)** must be greater than 0.
- **Specify the external postmaster address** This field specifies the e-mail address used as the sender for system generated messages and notifications sent to senders external to your organization.

4. Use the **Message Delivery** tab to configure the IP addresses of internal SMTP servers installed in your perimeter network that are exempt from Sender ID and connection filtering. You can also configure the delivery status notification (DSN) codes that are monitored for internal senders. The non-delivery reports (NDRs) that correspond to these DSNs are copied to the postmaster mailbox.

   Note:
   NDRs are copied to the postmaster mailbox only when a mailbox is assigned to the Microsoft Exchange recipient. By default, no mailbox is assigned to the Microsoft Exchange recipient.

   On the **Message Delivery** tab, configure the following:
   Enter the IP addresses for servers deployed in the perimeter and the range of IP addresses for your organization. These IP addresses will be ignored by Sender ID and connection filtering Use this list to specify the IP addresses of the SMTP servers deployed in the perimeter of your organization:
   - **Add - IP Address** To enter an IP address without a subnet mask, or to specify the subnet mask by using Classless Interdomain Routing (CIDR) notation, click **Add** or the drop-down arrow located next to **Add** and select **IP Address**. In the **Add Internal SMTP Server IP Address** dialog box, enter the IP address directly or specify a subnet using the CIDR notation. For example, if you enter 192.168.1.1, only that host is added to the list of perimeter servers, but if you specify 192.168.1.0/24, the entire class C subnet of 192.168.1.0 is designated as your perimeter network, and messages from any server on that network aren't subject to Sender ID or connection filtering.

     Add - IP and Mask To enter an IP address or subnet together with a subnet mask in dotted decimal notation, click the drop-down arrow located next to **Add** and select **IP and Mask**. In the **Add Internal SMTP Server - IP and Mask** dialog box, specify the IP address and the subnet mask.
     Add - IP Range To specify an IP address range by using the first IP address and the last IP address in the range, click the

drop-down arrow located next to **Add** and select **IP Range**. In the **Add Internal SMTP Server IP Address - IP Range** dialog box, specify the start and end addresses of the IP address range.

- **Edit** To modify a previously added IP address, select the IP address and click **Edit**.
- **Remove** To remove an existing entry from the IP Block list, select the entry, and then click  .

Enter the delivery status notification (DSN) codes that are monitored for internal senders. NDRs with these DSN codes will be forwarded to the postmaster e-mail account Specify the DSN codes monitored for internal senders. Any NDRs with these DSN codes are copied to the mailbox of the Microsoft Exchange recipient. You can do the following:

- **Add** To add a DSN code, enter the 3-digit DSN code as **x.y.z**, and then click **Add**.
- **Edit** To edit an existing DSN code, select the DSN code, and then click **Edit**.

Remove To remove an existing DSN code, select the DSN code, and then click  .

Use the Shell to configure global transport settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport configuration" entry in the Transport Permissions topic.

You use the **Set-TransportConfig** cmdlet to configure the global transport settings in your organization. Unlike the EMC, which allows you to configure only the most commonly used properties of global settings, the **Set-TransportConfig** cmdlet allows you to configure all the global settings that define how your transport servers function.

The following are a few examples of how you can use this cmdlet.

You can use the **Set-TransportConfig** cmdlet to change the *MaxDumpsterSizePerDatabase* parameter settings for the transport dumpster. We recommend that you configure the maximum size per database (the MaxDumpsterSizePerdatabase parameter) to be 1.5 times the size of the largest message that can be sent. For example, if the maximum messages size is 10 megabytes (MB), you should set the value for the MaxDumpsterSizePerDatabase parameter to 15 MB. For organizations that don't have maximum message sizes, we recommend that you set the value for the maximum size per database to 1.5 times the size of the average-sized message that's sent in the organization.

This example configures postmaster@contoso.com to be the e-mail address that is used as the sender for NDRs and other system generated messages to senders outside your organization.

```
Set-TransportConfig -ExternalPostmasterAddress postmaster@contoso.com
```

This example enables shadow redundancy for your organization.

```
Set-TransportConfig -ShadowRedundancyEnabled $true
```

For detailed syntax and parameter information, see Set-TransportConfig.

1.7.2.6 Configure a Moderated Recipient

Configure a Moderated Recipient

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

When you configure a recipient for moderation, all messages sent to that recipient are subject to approval by the designated moderators. For more information about how Exchange 2010 handles recipient moderation, see Understanding Moderated Transport.

Caution:

If you want to moderate a distribution group or a dynamic distribution group and your organization contains older versions of Exchange, you must specify an Exchange 2010 Hub Transport server as the expansion server. This specification is required because previous versions of Exchange don't support moderated recipients. If a message that is sent to a moderated distribution group or dynamic distribution group is expanded on a Hub Transport server running Exchange Server 2007, it will be delivered to all members of that distribution group, bypassing the moderation process. By specifying an Exchange 2010 Hub Transport server as the expansion server, you will ensure that all messages are moderated.

What Do You Want to Do?

- Use the EMC to configure a recipient for moderation
- Use the Shell to configure a recipient for moderation

Use the EMC to configure a recipient for moderation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Moderated Transport" entry in the Transport Permissions topic.

Assume you want to accomplish the following scenario:

- Enable moderation for the All Employees distribution group.
- Designate Rich Haddock and Kim Ralls as the moderators.
- Allow the members of the distribution group HR to bypass moderation.
- Notify internal senders if their message to the distribution group is rejected, but do not send any notifications to senders external to your organization.

To accomplish the tasks in this example scenario, perform the following procedure:

1. In the EMC console tree, click **Recipient Configuration**.
2. In the result pane, click the **All Employees** distribution group and click **Properties**.
3. Select the **Mail Flow Settings** tab.
4. Select **Message Moderation** and then click **Properties**.
5. On the **Message Moderation** dialog, complete the following:
   - 5.a. Select the **Messages sent to this group have to be approved by a moderator** check box.
   - 5.b. For the **Specify group moderators** list, click **Add**.
   - 5.c. In the **Select Recipient** dialog, select Rich Haddock and Kim Ralls from the list and click **OK**.
   - 5.d. For the **Specify senders who don't require message approval** list, click **Add**.

5.e.In the **Select Recipient** dialog, select HR from the list and click **OK**.
5.f.Click the **Notify senders in your organization only when their message is not approved** option.
6. Click **OK**.
7. Click **OK**.

This example shows how to configure a distribution group for moderation, but the same steps can be followed to configure any recipient for moderation.

Use the Shell to configure a recipient for moderation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Moderated Transport" entry in the Transport Permissions topic.

Assume you want to accomplish the following:

- Enable moderation for the All Employees distribution group.
- Designate Rich Haddock and Kim Ralls as the moderators.
- Allow the members of the distribution group HR to bypass moderation.
- Notify internal senders if their message to the distribution group is rejected, but do not send any notifications to senders external to your organization.

To accomplish the tasks in this example scenario, run the following command:

```
Set-DistributionGroup "All Employees" -ModerationEnabled $true -ModeratedBy "rhad
```

For more information about syntax and parameters, see Set-DistributionGroup.

This example shows how to configure a distribution group for moderation, but the same steps can be followed to configure any recipient for moderation. Simply use the corresponding cmdlet.

1.7.2.7 Configure Shadow Redundancy

Configure Shadow Redundancy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-13*

Shadow redundancy in Microsoft Exchange Server 2010 provides a high availability mechanism for messages for the entire time that the messages are in transit. To learn more about shadow redundancy, see Understanding Shadow Redundancy. You can use the Exchange Management Shell to configure shadow redundancy in your organization.

Looking for other management tasks related to transport servers? Check out Managing Transport Servers.

What Do You Want to Do?

- Use the Shell to enable or disable shadow redundancy
- Use the Shell to configure the shadow redundancy heartbeat
- Use the Shell to configure the maximum age for shadow messages

- Use the Shell to configure the maximum acknowledgement delay on a Receive connector
- Enable Shadow Redundancy Promotion

Use the Shell to enable or disable shadow redundancy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Shadow redundancy" entry in the Transport Permissions topic.

Note:
You can't use the Exchange Management Console to enable or disable shadow redundancy.

Use the *ShadowRedundancyEnabled* parameter of the **Set-TransportConfig** cmdlet to enable or disable shadow redundancy in your organization. By default, shadow redundancy is enabled.

This example enables shadow redundancy for your organization.

```
Set-TransportConfig -ShadowRedundancyEnabled $true
```

For detailed syntax and parameter information, see Set-TransportConfig.

Use the Shell to configure the shadow redundancy heartbeat

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Shadow redundancy" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure the shadow redundancy heartbeat.

Use the *ShadowHearbeatTimeoutInterval* and *ShadowHearbeatRetryCount* parameters of the **Set-TransportConfig** cmdlet to configure the shadow redundancy heartbeat in your organization. The default value for the shadow redundancy time-out interval is 5 minutes in the release to manufacturing (RTM) version of Exchange 2010, and 15 minutes in Exchange 2010 Service Pack 1 (SP1) or later. The default value for the shadow redundancy heartbeat retry count is 3 in Exchange 2010 RTM, and 12 in Exchange 2010 SP1 or later. On each transport server running Exchange 2010, the shadow redundancy heartbeat is used to determine the availability of the other Exchange 2010 transport servers. For more information, see "Heartbeat" in Understanding Shadow Redundancy.

Assume that, because there are unreliable network connections between your Active Directory sites, you want to increase the total time transport servers wait before you determine that a remote server is unavailable. To do this, you want to have the Hub Transport servers wait 30 minutes between connection attempts before determining that a server is unavailable. As a result, you increase the maximum time for detecting a failure from the default value of 3 hours (15-minute time-out interval × 12 retries) to 6 hours (30-minute time-out interval × 12 retries). In the following example, the shadow redundancy heartbeat configuration is revised to increase the heartbeat time-out interval to 30 minutes.

```
Set-TransportConfig -ShadowHeartbeatTimeoutInterval 00:30:00
```

For detailed syntax and parameter information, see Set-TransportConfig.

Use the Shell to configure the maximum age for shadow messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Shadow redundancy" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure the maximum age for shadow messages.

Use the *ShadowMessageAutoDiscardInterval* parameter of the **Set-TransportConfig** cmdlet to configure the maximum age for shadow messages in your organization. By default, shadow messages are discarded automatically after two days.

Assume that due to the hardware constraints on your servers, you don't want to retain shadow copies for messages that are delayed. This example reduces the retention period of shadow messages to four hours for your organization.

```
Set-TransportConfig -ShadowMessageAutoDiscardInterval 04:00:00
```

Note:
When a message expires, the primary server queues a discard event for that message, and the shadow server discards the shadow message when it receives the discard notification. The value you configure for the *ShadowMessageAutoDiscardInterval* parameter should be equal to or lower than the message expiration time-out interval configured on your transport servers.

For detailed syntax and parameter information, see Set-TransportConfig.

Use the Shell to configure the maximum acknowledgement delay on a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure the maximum acknowledgement delay on a Receive connector.

Use the *MaxAcknowledgementDelay* parameter of the **Set-ReceiveConnector** cmdlet to configure how long the Receive connector delays SMTP acknowledgement when receiving messages from systems that don't support shadow redundancy. By default, Receive connectors delay acknowledgement up to 30 seconds. For more information, see "Delayed Acknowledgement" in Understanding Shadow Redundancy.

Example 1

Assume that you have a proprietary application that sends SMTP messages by using your Exchange infrastructure. If the rate of message delivery for messages that are generated by this application is more important than the reliability of message delivery, you may want to disable delayed acknowledgement on the Receive connector that receives

messages from this application. This example sets the maximum acknowledgement delay to zero (0) on the Receive connector Custom App Receive Connector.

```
Set-ReceiveConnector "Custom App Receive Connector" -MaxAcknowledgementDelay 0
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

Example 2

Assume that all messages are typically delivered within 20 seconds in your environment. However, because of performance requirements, you don't want to delay acknowledgement more than 15 seconds for messages received from the Internet. After you analyze the message flow, you conclude that 95 percent of messages are delivered within the 15-second interval. This example configures the Receive connector from the Internet to delay acknowledgement for only 15 seconds. In this scenario, your environment provides shadow redundancy for 95 percent of messages received from the Internet.

```
Set-ReceiveConnector "From the Internet" -MaxAcknowledgementDelay 00:00:15.
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

Enable Shadow Redundancy Promotion

To complete this procedure, you must have local administrator permissions on the Hub Transport server.

1. Edit the Edgetransport.exe.config file. By default, this file is located in the C:\Program Files\Microsoft\Exchange Server\V14\Bin directory.
2. In the Edgetransport.exe.config file, change the **shadowredundancypromotionenabled** key to **true**, and then save the changes.
3. Restart the Microsoft Exchange Transport service (MSExchangeTransport.exe).

For more information, see the "Delayed Acknowledgement" section in Understanding Shadow Redundancy.

1.7.2.8 Configure the External Postmaster Address

Configure the External Postmaster Address

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can configure and manage the external postmaster address. The external postmaster address is used as the sender for system-generated messages and notifications sent to message senders that exist outside the Microsoft Exchange Server 2010 organization. An external sender is any sender that has an e-mail address that contains a domain not defined in the list of accepted domains for the Exchange 2010 organization.

In Exchange 2010, configuration of the external postmaster address is controlled by the *ExternalPostmasterAddress* parameter in the **Set-TransportConfig** cmdlet. In Exchange Server 2007, you configure this parameter using the **Set-TransportServer** cmdlet on every computer running Exchange 2007 that has the Hub Transport server role or Edge Transport server role installed.

Important:
Because management of the external postmaster address changed in Exchange 2010, you must configure the external postmaster address in two places if you have both Exchange 2010 and Exchange 2007 servers in your organization. You need to configure the external postmaster address once for the Exchange 2010 environment and once per server for the Exchange 2007 environment.

By default, the value of the *ExternalPostmasterAddress* parameter on every Hub Transport server and Edge Transport server is set to the value `$null`. The value `$null` causes the following behavior on Hub Transport servers and Edge Transport servers in the Exchange organization:

- For all Hub Transport servers in the Exchange organization or an Edge Transport server that has been subscribed to the Exchange organization, the external postmaster address is postmaster@<*Default accepted domain*>.
- For any Edge Transport server that hasn't been subscribed to the Exchange organization, the external postmaster address is postmaster@<*Edge Transport server FQDN*>.
  After the Edge Transport server is subscribed to the Exchange organization, the external postmaster address becomes postmaster@<*Default accepted domain*>.

Note:
If you specify a custom value for the external postmaster address, that value isn't replicated to any Edge Transport servers subscribed to the Exchange organization. If you specify a custom value for the external postmaster address, you must manually configure the external postmaster address on any Edge Transport servers.

Looking for other management tasks related to transport servers? Check out Managing Transport Servers.

Use the EMC to modify the external postmaster address for your organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport configuration" entry in the Transport Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, select the **Global Settings** tab.
3. Right-click **Transport Settings**, and then select **Properties**.
4. On the **General** tab, type the e-mail address you want to use as the external postmaster address in the **Specify the external postmaster address** field.
5. Click **OK**.

Use the Shell to modify the external postmaster address for your organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport configuration" entry in the Transport Permissions topic.

This example designates postmaster@contoso.com as the external postmaster address.

```
Set-TransportConfig -ExternalPostmasterAddress postmaster@contoso.com
```

For detailed syntax and parameter information, see Set-TransportConfig.

Other Tasks

After you configure the external postmaster address, you may also want to:

- Create a Mailbox
- Add an E-Mail Address for a User Mailbox

1.7.2.9 Managing Accepted and Remote Domains

Managing Accepted and Remote Domains

Exchange Server 2010 > Transport > Managing Transport Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-01*

Create an Accepted Domain

Configure Accepted Domain Properties

Remove an Accepted Domain

Configure Exchange 2010 to Accept E-Mail for More Than One Authoritative Domain

Create a Remote Domain

Configure Remote Domain Properties

Remove a Remote Domain

Supported Character Sets for Remote Domain Configuration

1.7.2.9.1 Create an Accepted Domain

Create an Accepted Domain

Transport > Managing Transport Servers > Managing Accepted and Remote Domains >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

An accepted domain is any SMTP domain for which Microsoft Exchange accepts incoming messages. Accepted domains can be authoritative or relay domains. Accepted domains are configured as global settings for the Exchange organization and on computers that have the Edge Transport server role installed.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to transport servers? Check out Managing Transport Servers.

Prerequisites

- You can't create an accepted domain that has the same name as an already configured remote domain. For example, if you have fabrikam.com configured as a remote domain, you can't create an accepted domain for fabrikam.com.
- Before you configure an accepted domain, you must verify that a public Domain Name System (DNS) MX resource record for that SMTP namespace exists and that the MX resource record references a server name and an IP address associated with your Exchange organization.

What Do You Want to Do?

- Use the EMC to create an accepted domain
- Use the Shell to create an accepted domain

Use the EMC to create an accepted domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Accepted domains" entry in the Transport Permissions topic.

1. Open the Exchange Management Console. Perform one of the following steps:
   - To create an accepted domain on a computer that has the Edge Transport server role installed, on that computer, in the console tree, select **Edge Transport**, and then in the work pane, click the **Accepted Domains** tab.
   - To create an accepted domain on a computer that has the Hub Transport server role installed, on that computer, in the console tree, expand **Organization Configuration**, select **Hub Transport**, and then in the work pane, click the **Accepted Domains** tab.
2. In the action pane, click **New Accepted Domain**. The New Accepted Domain wizard appears.
3. On the **New Accepted Domain** page, complete the following fields:
   - **Name** To identify the accepted domain, type a unique name in the **Name** field. We recommend that you select a meaningful name to help you easily identify the purpose of this accepted domain. For example, you may want to use a name that easily identifies this as a subsidiary domain or as a hosted domain. You must use a unique name for each accepted domain.
   - **Accepted Domain** Use this field to identify the SMTP namespace for which the Exchange organization accepts e-mail messages. You can use a wildcard character to accept messages for a domain and all its subdomains. For example, you can type ***.contoso.com** to set Contoso.com and all its subdomains as accepted domains.
4. After you complete these fields on the **New Accepted Domain** page, select one of the following options to set the accepted domain type:
   - **Authoritative Domain** To specify that e-mail messages are delivered to a recipient that has a domain account in your Exchange organization, select this option.
   - **Internal Relay Domain** To specify that e-mail messages are either delivered to recipients in your organization or relayed to a server outside your Exchange organization but still under the authority of your company or IT department, select this option.
   - **External Relay Domain** To relay e-mail messages to an e-mail server outside the Exchange organization, select this option.
5. Click **New** to create the new accepted domain.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create an accepted domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Accepted domains" entry in the Transport Permissions topic.

You use the **New-AcceptedDomain** cmdlet to create new accepted domains in your organization. The following examples show how this cmdlet can be used.

The following example creates an authoritative domain.

```
New-AcceptedDomain -Name "Contoso" -DomainName contoso.com -DomainType Authoritat
```

The following example creates an internal relay domain.

```
New-AcceptedDomain -Name "Fourth Coffee" -DomainName fourthcoffee.com -DomainType
```

The following example creates an external relay domain.

```
New-AcceptedDomain -Name "Woodgrove Bank" -DomainName woodgrovebank.com -DomainTy
```

For detailed syntax and parameter information, see New-AcceptedDomain.

1.7.2.9.2 Configure Accepted Domain Properties

Configure Accepted Domain Properties

Transport > Managing Transport Servers > Managing Accepted and Remote Domains >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

An accepted domain is any SMTP domain for which Microsoft Exchange accepts incoming messages. Accepted domains can be authoritative or relay domains. Accepted domains are configured as global settings for the Exchange organization and on computers that have the Edge Transport server role installed.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to transport servers? Check out Managing Transport Servers.

What Do You Want to Do?

- Use the EMC to configure the properties of an accepted domain
- Use the Shell to configure the properties of an accepted domain

Use the EMC to configure the properties of an accepted domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Accepted domains" entry in the Transport Permissions topic.

1. If you're configuring an accepted domain on a Hub Transport server, in the console tree, navigate to **Organization Configuration** > **Hub Transport**. On an Edge Transport server, select **Edge Transport** in the console tree.
2. In the work pane, select the **Accepted Domains** tab on the right, and then double-click the accepted domain you want to configure.
3. Use the **General** tab to specify how Exchange handles the e-mail messages that it accepts for this domain:
   - **Name** The name of the accepted domain is displayed in the first field on the **General** tab. This is a display name for the accepted domain and doesn't have to match the actual SMTP domain.
   - **Authoritative Domain** Select this option if this domain is used for e-mail addresses of the recipients in your organization.
   - **Internal Relay Domain** To specify that e-mail messages are either delivered to recipients in your organization or relayed to a server outside your Exchange organization but still under the authority of your company or IT department, select this option.
   - **External Relay Domain** To specify that e-mail messages sent to recipients in this domain are relayed to an e-mail server outside your organization, select this option.

Use the Shell to configure the properties of an accepted domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Accepted domains" entry in the Transport Permissions topic.

You use the **Set-AcceptedDomain** cmdlet to configure the properties of an accepted domain. This example configures the accepted domain for Woodgrove Bank as an authoritative domain.

```
Set-AcceptedDomain "Woodgrove Bank" -DomainType Authoritative
```

For detailed syntax and parameter information, see Set-AcceptedDomain.

1.7.2.9.3 Remove an Accepted Domain

Remove an Accepted Domain

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Accepted domains are any Simple Mail Transfer Protocol (SMTP) namespace for which a Microsoft Exchange organization receives e-mail. This topic explains how to use the EMC

or the Shell to remove an accepted domain.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to accepted domains? Check out Managing Accepted and Remote Domains.

Prerequisites

- Before you remove an accepted domain, verify that the domain name isn't referenced in any e-mail address policy.
- After you remove an accepted domain, the Exchange organization no longer accepts e-mail messages that are addressed to recipients in that domain. Make sure the change doesn't adversely affect the mail flow in your organization.
- You can't delete an accepted domain that is set as the default accepted domain. To delete the default accepted domain, you must first create a new accepted domain, and then set the new accepted domain as the default accepted domain.

What Do You Want to Do?

Use the EMC to remove an Accepted domain

Use the Shell to remove an Accepted domain

Use the EMC to remove an Accepted domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Accepted domains" entry in the Transport Permissions topic.

1. Open the Exchange Management Console. Perform one of the following steps:
   1.a. To remove an accepted domain on a computer that has the Edge Transport server role installed, on that computer, in the console tree, select **Edge Transport**, and then in the work pane, click the **Accepted Domains** tab.
   1.b. To remove an accepted domain on a computer that has the Hub Transport server role installed, on that computer, in the console tree, expand **Organization Configuration**, select **Hub Transport**, and then in the work pane, click the **Accepted Domains** tab.
2. In the result pane, select the accepted domain that you want to remove, and then in the action pane, click **Remove**.
3. A dialog box appears with the text, "**Are you sure you want to remove '***Accepted Domain***'?**", where *Accepted Domain* is the name of the accepted domain that you want to remove. Click **Yes.**

Use the Shell to remove an Accepted

domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Accepted domains" entry in the Transport Permissions topic.

Use the **Remove-AcceptedDomain** cmdlet to remove an existing accepted domain from your organization. The following example removes the accepted domain named "Woodgrove Bank":

```
Remove-AcceptedDomain -Identity "Woodgrove Bank"
```

For detailed syntax and parameter information, see Remove-AcceptedDomain.

1.7.2.9.4 Configure Exchange 2010 to Accept E-Mail for More Than One Authoritative Domain

Configure Exchange 2010 to Accept E-Mail for More Than One Authoritative Domain

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure Microsoft Exchange Server 2010 to accept e-mail for more than one authoritative SMTP domain.

The following examples are scenarios in which your Exchange organization may have to receive and process e-mail for more than one authoritative SMTP domain:

- You are changing your SMTP domain name, but have to continue to accept e-mail for the old domain name for a time, in case customers send e-mail messages to the previous e-mail addresses. You can set the new e-mail address as the primary (reply to) address. This means that the new address will be the default e-mail address displayed on all e-mail messages sent by the recipient. You can set the old e-mail address as a secondary address. This will enable the recipient to continue to receive e-mail sent to the old e-mail address.
- You want to provision different e-mail addresses for business units within your organization. For example, if the Contoso.com forest contains subdomains for the subsidiaries Tailspin Toys and Fourth Coffee, you may want to assign the SMTP domain names Contoso.com, TailspinToys.com, and FourthCoffee.com to the recipients in those respective business units.
- You provide e-mail hosting services and have to accept e-mail for more than one SMTP domain name.

Looking for other management tasks related to accepted and remote domains? Check out Managing Accepted and Remote Domains.

Note:

If you have deployed an Edge Transport server in your organization and have created an Edge Subscription for that server, you perform these procedures only on the Hub Transport server. If the Edge Transport server isn't subscribed, you must create accepted domains on both the Edge Transport server and the Hub Transport server.

Caution:

When you create an accepted domain, you can use a wildcard character (*) in the address space to indicate that all subdomains of the SMTP address space are also accepted by the Exchange organization. For example, to configure Contoso.com and all its subdomains as accepted domains, enter ***.Contoso.com** as the SMTP address space. However, if the subdomain names will be used in an e-mail address policy, each subdomain must have an explicit accepted domain entry.

Prerequisites

- A public Domain Name System (DNS) MX resource record is required for each SMTP domain for which you accept e-mail from the Internet. Each MX record should resolve to the Internet-facing server that receives e-mail for your organization.
- You must configure Send connectors and Receive connectors so that the Exchange organization can send e-mail to and receive e-mail from the Internet. The configuration of the Internet Send connectors and Receive connectors is determined by your Exchange topology. For more information about configuring Internet mail flow, see Managing Message Routing.

Use the EMC to configure Exchange 2010 to accept e-mail for more than one domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Accepted domains" entry in the Transport Permissions topic and the "E-mail address policies" entry in the Mailbox Permissions topic.

1. Configure the accepted domain entry by following these steps:
   1.a. Expand the **Organization Configuration** node, and then click **Hub Transport**. In the results pane, click the **Accepted Domains** tab.
   1.b. In the action pane, click **New Accepted Domain**. The **New Accepted Domain** wizard appears.
   1.c. On the **New Accepted Domain** page, type a name to identify the accepted domain entry. In the **Accepted Domain** field, type the SMTP domain name. Select **Authoritative Domain. E-mail is delivered to a recipient in this Exchange organization**.
   1.d. Click **New**.
   1.e. On the **Completion** page, click **Finish**.
2. Configure an e-mail address policy for the authoritative domain by performing the steps in this section that meet the objectives of your scenario.
   To change the primary (reply to) e-mail address assigned to recipients and keep the existing e-mail address as a secondary e-mail address, follow these steps:
   2.a. Expand the **Organization Configuration** node, and then click **Hub Transport**. In the results pane, click the **E-mail Address Policies** tab. Select the e-mail address policy that you want to modify, and then in the action pane, click **Edit**.
   2.b. On the **Introduction** page, click **Next**.
   2.c. On the **Conditions** page, click **Next**.
   2.d. On the **E-mail Addresses** page, click **Add**. In the **SMTP E-mail Address** dialog box, select the option under **E-mail address local part** that determines how the recipient's e-mail address alias will be generated.
   2.e. Click the **Select the accepted domain for the e-mail address** option, and then click **Browse**. In the **Select Accepted Domain** dialog box, select an accepted domain, and then click **OK**. Click **OK** again to close the **SMTP E-mail Address** dialog box.
   2.f. On the **E-mail Addresses** page, select the new address entry, and then click **Set as Reply**. The e-mail address entry is displayed in bold type to

indicate that it's now the primary, or reply to, address for the recipients to which this e-mail address policy applies. Click **Next**.

2.g.On the **Schedule** page, select an option to specify when the e-mail address policy will be applied and the maximum length of time that the task is permitted to run. Click **Next**.

2.h.On the **Edit E-mail Address Policy** page, click **Edit** to save the changes to the policy and apply it to affected recipients.

2.i.On the **Completion** page, click **Finish**.

3. To create additional e-mail addresses that will be used as the primary e-mail address for a filtered set of recipients, follow these steps:

3.a.In the action pane, click **New E-mail Address Policy**. The **New E-mail Address Policy** wizard appears.

3.b.On the **Introduction** page, type a name for the e-mail address policy. If the users that will be assigned this new e-mail address policy are all in a specific organizational unit (OU), click **Browse** to restrict this e-mail address policy to that specific OU. Select an option under **Include these recipient types** to determine to which recipient types this e-mail address policy will be applied. Click **Next**.

3.c.On the **Conditions** page, in the **Step 1** box, select the condition that will be used to filter the recipients to which the policy is applied. For example, you can select **Recipient is in a Company** to apply the policy to only recipients whose properties identify a specific company affiliation. In the **Step 2** box, click the underlined value to specify the value that the filter must match. For example, if you selected **Recipient is in a Company**, click the word **specified**. The **Specify Company** dialog box opens. Type a company name, and then click **Add** to add the company name to the list of names that the recipient's Company attribute must match to have this policy applied to them. If you add multiple entries, the recipient attribute must match only one entry to meet the filter conditions. Click **OK** to close the dialog box, and then click **Next**.

3.d.On the **E-mail Addresses** page, click **Add**. In the **SMTP E-mail Address** dialog box, select the option under **E-mail address local part** that determines how the recipient's e-mail address alias will be generated.

3.e.Click the **Select the accepted domain for the e-mail address** option, and then click **Browse**. In the **Select Accepted Domain** dialog box, select an accepted domain, and then click **OK**. Click **OK** again to close the **SMTP E-mail Address** dialog box. The e-mail address entry is displayed in bold type to indicate that it's now the primary, or reply to, address for the recipients to which this e-mail address policy applies.

3.f.Click **Next**.

3.g.On the **Schedule** page, select an option to specify when the e-mail address policy will be applied and the maximum length of time that the task is permitted to run.

3.h.Click **Next**.

3.i.On the **New E-mail Address Policy** page, click **New** to save the policy and apply it to affected recipients.

3.j.On the **Completion** page, click **Finish**.

Note:

If a recipient meets the filter conditions of more than one e-mail address policy, the e-mail address policy that has the lowest number is set as the primary address. The e-mail address policy that has the lowest number is highest in the priority list. Any other e-mail address policies that also apply are set as secondary addresses.

Use the Shell to configure Exchange 2010 to accept e-mail for more than one

domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Accepted domains" entry in the Transport Permissions topic and the "E-mail address policies" entry in the Mailbox Permissions topic.

1. To create an authoritative accepted domain entry for each SMTP domain for which your Exchange organization will host recipient mailboxes, use the **New-AcceptedDomain** cmdlet. This example creates the authoritative domain FourthCoffee.com.

```
New-AcceptedDomain -Name "Fourth Coffee subsidiary" -DomainName Fourth
```

2. To change the primary e-mail address assigned to recipients and keep the existing e-mail address as a secondary address, use the **Set-EmailAddressPolicy** cmdlet to modify an existing e-mail address policy. If your default e-mail address policy sets recipient e-mail addresses to useralias@contoso.com, this example changes the primary (reply to) address to useralias@fourthcoffee.com and continues to use useralias@contoso.com as a secondary address.

```
Set-EmailAddressPolicy -Identity "Default Policy" -EnabledEmailAddress
```

Note:

If you type `SMTP` in all uppercase letters, this indicates the primary (reply to) address. If you type `smtp` in lowercase letters, this indicates the secondary address.

3. To apply the new e-mail address policy to recipients, use the **Update-EmailAddressPolicy** cmdlet. This example applies the new e-mail address policy to recipients.

```
Update-EmailAddressPolicy -Identity "Default Policy"
```

4. To create additional e-mail addresses that will be used as the primary e-mail address for a filtered set of recipients, use the **New-EmailAddressPolicy** cmdlet to create an e-mail address policy for each accepted domain that will be used as part of a recipient's e-mail address. This example creates an e-mail address policy for FourthCoffee.com, assigns that policy to the recipients in the Fourth Coffee department, and sets the highest priority for that e-mail address policy.

```
New-EmailAddressPolicy -Name "Fourth Coffee Recipients" -IncludedRecip
```

5. To apply the new e-mail address policy to recipients, use the **Update-EmailAddressPolicy** cmdlet. This example applies the new e-mail address policy to the Fourth Coffee recipients.

```
Update-EmailAddressPolicy -Identity "Fourth Coffee Recipients"
```

For detailed syntax and parameter information, see the following topics:

- New-AcceptedDomain
- Set-EmailAddressPolicy
- New-EmailAddressPolicy
- Update-EmailAddressPolicy

1.7.2.9.5 Create a Remote Domain

Create a Remote Domain

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Remote domains are SMTP domains that are external to your Microsoft Exchange organization. You can create remote domain entries to define the settings for message transfer between your Exchange organization and domains outside your Active Directory forest. The settings for remote domains are global configuration settings for the Exchange organization.

Looking for other management tasks related to transport servers? Check out Managing Transport Servers.

Prerequisites

You can't create a remote domain that has the same name as an already configured accepted domain. For example, if your organization accepts mail for fabrikam.com, you can't create a remote domain for fabrikam.com.

What Do You Want to Do?

- Use the EMC to create a remote domain
- Use the Shell to create a remote domain

Use the EMC to create a remote domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote domains" entry in the Transport Permissions topic.

1. In the console tree, navigate to **Organization Configuration**> **Hub Transport**.
2. In the result pane, click the **Remote Domains** tab.
3. In the action pane, click **New Remote Domain**. The New Remote Domain wizard appears.
4. On the **New Remote Domain** page, complete the following fields:
   - **Name** Use this field to identify the remote domain in the user interface. You can type any name that you want. We recommend that you select a meaningful name that helps you easily identify the purpose of this remote domain. You must use a unique name for each remote domain. The name can't exceed 64 characters. This field is required.
   - **Domain Name** Use this field to identify the SMTP namespace of the remote domain. For example, type **contoso.com**. The remote domain name can't exceed 256 characters. This field is required.
   - **Include all subdomains** To apply the remote domain configuration to all subdomains of the remote domain, such as mail.contoso.com, select this check box.
   - **Use this domain for my Office 365 tenant** If the new remote domain you're creating represents the part of your organization that is hosted on Microsoft Office 365, select this check box.
5. To create the remote domain entry with these settings, click **New**.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a remote domain entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote domains" entry in the Transport Permissions topic.

You use the **New-RemoteDomain** cmdlet to create new remote domains in your organization. This example shows how this cmdlet can be used to create a new remote domain for contoso.com.

```
New-RemoteDomain -Name Contoso -DomainName Contoso.com
```

For detailed syntax and parameter information, see New-RemoteDomain.

1.7.2.9.6 Configure Remote Domain Properties

Configure Remote Domain Properties

Transport > Managing Transport Servers > Managing Accepted and Remote Domains >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Remote domains are SMTP domains that are external to your Microsoft Exchange organization. You can create remote domain entries to define the settings for message transfer between your Exchange organization and domains outside your Active Directory forest. The settings for remote domains are global configuration settings for the Exchange organization.

Looking for other management tasks related to transport servers? Check out Managing Transport Servers.

What Do You Want to Do?

- Use the EMC to configure the properties of a remote domain
- Use the Shell to configure the properties of a remote domain

Use the EMC to configure the properties of a remote domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote domains" entry in the Transport Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.

2. In the work pane, select the **Remote Domains** tab on the right, and then double-click the remote domain you want to configure.

3. Use the **General** tab to configure the settings that determine the types of out-of-office messages sent to recipients in the remote domain. The type of out-of-office messages available in your organization depends on both the Exchange client version and the Exchange server version. The out-of-office message is set on the client and is sent by the server. Exchange Server 2010 and Exchange Server 2007 can send different out-of-office messages to internal and external users. Users that use Microsoft Office Outlook 2007 can set different internal and external out-of-office replies. Earlier versions of Outlook or Exchange only support a single type of out-of-office message used for both internal and external recipients.
   The **General** tab shows the following:
   - **Domain name** Shows the display name for the domain.
   - **Modified** Shows the date and time when the remote domain properties were last modified.
   - **Allow none** If you select this option, no out-of-office messages are delivered to the remote domain.
   - **Allow external out-of-office messages only** If you select this option, only out-of-office messages configured as external by an Outlook 2007 client, or by using Microsoft Office Outlook Web App for a mailbox located on an Exchange 2010 or Exchange 2007 Mailbox server are delivered to the remote domain.
   - **Allow external out-of-office messages and legacy out-of-office messages (configured by using Outlook 2003 or earlier clients, or configured on Exchange 2003 mailboxes)** If you select this option, out-of-office messages configured as external by an Outlook 2007 client or by using Outlook Web App for a mailbox located on an Exchange 2010 Mailbox server are delivered to the remote domain. Out-of-office messages set by Outlook 2003 or earlier clients, regardless of the server version of their mailbox store, are delivered to the remote domain. Out-of-office messages sent by Exchange 2003 or earlier servers, regardless of the client version used to set the out-of-office message, are delivered to the remote domain.
   - **Allow internal out-of-office messages and legacy out-of-office messages (configured by using Outlook 2003 or earlier clients, or configured on Exchange Server 2003 mailboxes)** If you select this option, out-of-office messages configured as internal by an Outlook 2007 client or by using Outlook Web App for a mailbox located on an Exchange 2010 Mailbox server are delivered to the remote domain. Out-of-office messages set by Outlook 2003 or earlier clients, regardless of the server version of their mailbox store, are delivered to the remote domain. Out-of-office messages sent by Exchange 2003 or earlier servers, regardless of the client version used to set the out-of-office message, are delivered to the remote domain.

4. Use the **Message Format** tab to specify message policy, format, and character sets for the messages sent to this remote domain.
   Use the **Message Format Options** section to specify message delivery and formatting:
   - **Allow automatic replies** To allow messages that are automatic replies from client e-mail programs in your organization, select this option.
   - **Allow automatic forward** To allow messages that are auto-forwarded by client e-mail programs in your organization, select this option.
   - **Allow delivery reports** To allow read receipts from client software in your organization to the remote domain, select this option.
   - **Allow non-delivery reports** To allow non-delivery reports (NDRs) from your organization, select this option.
   - **Display sender's name on messages** To have the sender's display name appear on messages, select this option. We recommend that you leave this

option selected.

- **Use message text line wrap at column** To allow line wrap in message text for outgoing messages, select this option, and then in the text box, type the line-wrap size, from 0 through 132. To set the value to unlimited, leave the field blank. The default value is unlimited (blank).
- **Always use** To always send messages that use Exchange rich-text format, select this text box.
- **Never use** To never send messages that use Exchange rich-text format, select this check box.
- **Determined by individual user settings** To send e-mail messages that use the Exchange rich-text settings specified by the Outlook user, select this check box.

Use the following character set options to specify acceptable character sets:

- **MIME character set** To identify a MIME character set, type the character encoding set in the text box.
- **Non-MIME character set** To identify a non-MIME character set, type the character encoding set in the text box.

5. Use the **Office 365 Tenant Domain** tab to specify whether this remote domain is used for your cloud-based organization.
   - **Use this domain for my Office 365 tenant** If the new remote domain you're creating represents the part of your organization that is hosted on Microsoft Office 365, select this check box.

Use the Shell to configure the properties of a remote domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote domains" entry in the Transport Permissions topic.

You use the **Set-RemoteDomain** cmdlet to configure the properties of a remote domain. This section provides examples on how to configure various properties of a remote domain.

This example makes sure that no out-of-office messages are sent to the domain.

```
Set-RemoteDomain "RemoteDomain" -AllowedOOFType None
```

This example allows only external out-of-office messages.

```
Set-RemoteDomain "RemoteDomain" -AllowedOOFType External
```

This example allows external out-of-office messages and out-of-office messages set by Outlook 2003 or earlier clients or sent by Exchange 2003 or earlier servers.

```
Set-RemoteDomain "RemoteDomain" -AllowedOOFType ExternalLegacy
```

This example allows internal out-of-office messages and out-of-office messages set by Outlook 2003 or earlier clients or sent by Exchange 2003 or earlier servers.

```
Set-RemoteDomain "RemoteDomain" -AllowedOOFType InternalLegacy
```

This example allows automatic replies to the remote domain. By default, this setting is disabled.

```
Set-RemoteDomain -Identity Contoso -AutoReplyEnabled $true
```

This example allows automatic forwards to the remote domain. By default, this setting is disabled.

```
Set-RemoteDomain -Identity Contoso -AutoForwardEnabled $true
```

This example disables delivery reports to the remote domain. By default, this setting is enabled.

```
Set-RemoteDomain -Identity Contoso -DeliveryReportEnabled $false
```

This example disables non-delivery reports to the remote domain. By default, this setting is enabled.

```
Set-RemoteDomain -Identity Contoso -NDREnabled $false
```

This example disables the display of the sender's name on messages. By default, this setting is enabled. We recommend that you leave this option enabled.

```
Set-RemoteDomain -Identity Contoso -DisplaySenderName $false
```

This example enables the line wrapping of message text and sets the column width to 76 characters.

```
Set-RemoteDomain -Identity Contoso -LineWrapSize 76
```

This example allows notification to be sent to a remote domain when a meeting request from a sender in the remote domain is forwarded to another recipient. By default, this setting is disabled.

```
Set-RemoteDomain -Identity Contoso -MeetingForwardNotificationEnabled $true
```

This example configures both the MIME and non-MIME characters sets to the Western European character set (ISO-8859-1).

```
Set-RemoteDomain -Identity Contoso -CharacterSet "ISO-8859-1" -NonMimeCharacterSe
```

This example specifies that Transport Neutral Encapsulation Format (TNEF) encoding is used for all messages sent to the remote domain. By default, the value for this setting is `$null`, and TNEF encoding is controlled by individual user settings. The TNEF settings are shown as the Exchange rich-text format options in the EMC.

```
Set-RemoteDomain -Identity Contoso -TNEFEnabled $true
```

For detailed syntax and parameter information, see Set-RemoteDomain.

1.7.2.9.7 Remove a Remote Domain

Remove a Remote Domain

Transport > Managing Transport Servers > Managing Accepted and Remote Domains >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Remote domains define override settings for the message transfer between the Microsoft Exchange Server 2010 organization and domains outside your Active Directory forest. When you create a remote domain entry, you control the types of messages sent to that domain. You can also apply message format policies and acceptable character sets for messages sent from mailbox users in your organization to the remote domain. The settings for remote domains are global configuration settings for the Exchange organization.

If you remove a remote domain entry, the settings for message transfer no longer apply to messages sent to the remote domain. Removing a remote domain entry doesn't disable mail flow to the remote domain. After a remote domain entry is removed, the configuration settings of the default remote domain apply to new messages sent to that domain. You can't remove the default remote domain.

Looking for other management tasks related to remote domains? Check out Managing Accepted and Remote Domains.

Use the EMC to remove a remote domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote domains" entry in the Transport Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **Remote Domains** tab.
3. In the result pane, select the remote domain entry that you want to remove.
4. In the action pane, click **Remove**.
5. A message appears asking "**Are you sure you want to remove '***Remote Domain***'?"** Click **Yes**.

Use the Shell to remove a remote domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote domains" entry in the Transport Permissions topic.

Use the **Remove-RemoteDomain** cmdlet to remove a remote domain. This example removes the remote domain Contoso.

```
Remove-RemoteDomain -Identity Contoso
```

For detailed syntax and parameter information, see Remove-RemoteDomain.

1.7.2.9.8 Supported Character Sets for Remote Domain Configuration

Supported Character Sets for Remote Domain Configuration

Transport > Managing Transport Servers > Managing Accepted and Remote Domains >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-06*

The following character sets are supported for the *CharacterSet* parameter and *NonMimeCharacterSet* parameter in the Set-RemoteDomain cmdlet. When you enter a value for the *CharacterSet* parameter and *NonMimeCharacterSet* parameter, use the value in the Name column in the following table.

Supported character sets for remote domain configuration

Name	Description
big5	Chinese Traditional (Big5)
DIN_66003	German (IA5)

euc-jp	Japanese (EUC)
euc-kr	Korean (EUC)
GB18030	Chinese Simplified (GB18030)
gb2312	Chinese Simplified (GB2312)
hz-gb-2312	Chinese Simplified (HZ)
iso-2022-jp	Japanese (JIS)
iso-2022-kr	Korean (ISO)
iso-8859-1	Western European (ISO)
iso-8859-2	Central European (ISO)
iso-8859-3	Latin 3 (ISO)
iso-8859-4	Baltic (ISO)
iso-8859-5	Cyrillic (ISO)
iso-8859-6	Arabic (ISO)
iso-8859-7	Greek (ISO)
iso-8859-8	Hebrew (ISO)
iso-8859-9	Turkish (ISO)
iso-8859-13	Estonian (ISO)
iso-8859-15	Latin 9 (ISO)
koi8-r	Cyrillic (KOI8-R)
koi8-u	Cyrillic (KOI8-U)
ks_c_5601-1987	Korean (Windows)
NS_4551-1	Norwegian (IA5)
SEN_850200_B	Swedish (IA5)
shift_jis	Japanese (Shift-JIS)
utf-8	Unicode (UTF-8)
windows-1250	Central European (Windows)
windows-1251	Cyrillic (Windows)
windows-1252	Western European (Windows)
windows-1253	Greek (Windows)
windows-1254	Turkish (Windows)
windows-1255	Hebrew (Windows)
windows-1256	Arabic (Windows)
windows-1257	Baltic (Windows)

windows-1258	Vietnamese (Windows)
windows-874	Thai (Windows)

1.7.2.10 Managing Anti-Spam and Antivirus Features

Managing Anti-Spam and Antivirus Features

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-06*

Anti-Spam Features

Connection Filtering

Enable or Disable Connection Filtering

Configure IP Allow List Properties

Configure IP Allow List Providers Properties

Configure IP Block List Properties

Configure IP Block List Providers Properties

Content Filtering

Enable or Disable Content Filtering

Configure Content Filtering Properties

Release Quarantined Messages from the Spam Quarantine Mailbox

Configure Outlook to Expose Original Sender Field in the Quarantine Mailbox

Specify a Spam Quarantine Mailbox

View Anti-Spam Stamps in Outlook 2010 and Outlook 2007

Enable Anti-Spam Functionality on a Hub Transport Server

Make the SCL Value Available to Edge Transport Rules

Recipient Filtering

Enable or Disable Recipient Filtering

Configure Recipient Filtering Properties

Sender Filtering

Enable or Disable Sender Filtering

Configure Sender Filtering Properties

Configure Safelist Aggregation

Sender ID

Enable or Disable Sender ID

Configure Sender ID Properties

Sender Reputation

Enable or Disable Sender Reputation

Configure Sender Reputation Properties

Configure Outbound Access for Detection of Open Proxy Servers for Sender Reputation

Other Anti-Spam Features

Manage Anti-Spam Agent Log Output

Configure Proxy Settings for WinHTTP

Antivirus Features

Using Edge Transport Rules to Manage Viruses

Configure Attachment Filtering

File-Level Antivirus Scanning on Exchange 2010

Other Antivirus and Anti-Spam Solutions from Microsoft

Microsoft Forefront Protection 2010 for Exchange Server

Microsoft Exchange Hosted Services

1.7.2.10.1 Configure Attachment Filtering

Configure Attachment Filtering

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Attachment filtering can block attachments from entering the Microsoft Exchange Server 2010 organization by attachment content type or by attachment file name. How the attachments are processed depends on how attachment filtering is configured.

Important:
Configuration changes that you make to attachment filtering by using the Shell are made only to the local computer that has the Edge Transport server role installed. If you have multiple instances of the Edge Transport server role running in your organization, you must apply attachment filter configuration changes to each computer.

You can configure an attachment filter entry to filter attachments by attachment content type or by attachment file name. Before you add an attachment filter entry, you must determine whether you want to filter by MIME content type or by file name. Your choice of

attachment filter type depends on your business needs and policies. For more information, see Understanding Attachment Filtering.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Use the Shell to enable the Attachment Filter agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport agents" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable the Attachment Filter agent.

By default, the Attachment Filter agent is enabled on the computer that has the Edge Transport server role installed.

This example enables the Attachment Filter agent if it isn't enabled.

```
Enable-TransportAgent -Identity "Attachment Filter agent"
```

For detailed syntax and parameter information, see Enable-TransportAgent.

Use the Shell to add an attachment filter entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

Note:
You can't use the EMC to add an attachment filter entry.

With Exchange 2010, you can configure multiple attachment filters on each Edge Transport server.

To add an attachment filter that filters e-mail attachments that have a specific MIME content type, use the following syntax.

```
Add-AttachmentFilterEntry -Name <MIMEContentType> -Type ContentType
```

This example filters all JPEG images by using an attachment filter. Note that you must run the following command on each Edge Transport server.

```
Add-AttachmentFilterEntry -Name image/jpeg -Type ContentType
```

To add an attachment filter that filters e-mail attachments based on a file name or file name extension, use the following syntax.

```
Add-AttachmentFilterEntry -Name <FileName> -Type FileName
```

This example filters all e-mail attachments that have the file name extension EXE.

```
Add-AttachmentFilterEntry -Name *.EXE -Type FileName
```

For detailed syntax and parameter information, see Add-AttachmentFilterEntry.

Use the Shell to configure attachment filtering behavior

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure attachment filtering behavior.

To configure attachment filtering on an Edge Transport server role, use the **Set-AttachmentFilterListConfig** cmdlet. This example makes the following configuration changes to the Attachment Filter agent.

- Sets the Attachment Filter agent to reject messages that have prohibited attachments.
- Configures a custom response for rejected messages.

```
Set-AttachmentFilterListConfig -Action -Reject -RejectResponse "The attachment yo
```

For detailed syntax and parameter information, see Set-AttachmentFilterListConfig.

1.7.2.10.2 Enable or Disable Content Filtering

Enable or Disable Content Filtering

Transport > Managing Transport Servers > Managing Anti-Spam and Antivirus Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

By default, in Microsoft Exchange Server 2010, content filtering is enabled on the Edge Transport server only for inbound, unauthenticated messages from the Internet. These messages are handled as external messages.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Prerequisites

- Review Understanding Anti-Spam and Antivirus Functionality to understand the general strategy for configuring all anti-spam agents so that they work together efficiently for your organization.
- Read Understanding Content Filtering.

Use the EMC to enable or disable content filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. Open the EMC on the Edge Transport server.
2. In the console tree, click **Edge Transport**.
3. In the work pane, click the **Anti-spam** tab, and then select **Content Filtering**.
4. In the action pane, click **Enable** or **Disable** as appropriate.

Use the Shell to enable or disable content filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

This example enables content filtering.

```
Set-ContentFilterConfig -Enabled $true
```

This example disables content filtering.

```
Set-ContentFilterConfig -Enabled $false
```

Use the Shell to enable or disable content filtering for internal and external messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable or disable content filtering for internal and external messages.

This example enables content filtering for external messages.

```
Set-ContentFilterConfig -ExternalMailEnabled $true
```

This example disables content filtering for external messages.

```
Set-ContentFilterConfig -ExternalMailEnabled $false
```

Note:
By default, content filtering functionality is enabled for external messages.

This example enables content filtering for internal messages.

```
Set-ContentFilterConfig -InternalMailEnabled $true
```

This example disables content filtering for internal messages.

```
Set-ContentFilterConfig -InternalMailEnabled $false
```

Note:
As a best practice, you should not filter messages from trusted partners or from inside your organization. When you run anti-spam filters, there's always a chance that the filters will detect false positives. To reduce the chance that filters will mishandle legitimate e-mail messages, you should enable anti-spam agents to run only on messages from potentially untrusted and unknown sources.

For detailed syntax and parameter information, see Set-ContentFilterConfig.

1.7.2.10.3 Configure Content Filtering Properties

Configure Content Filtering Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When the Content Filter agent is enabled on a computer, it filters all messages that come through all receive connectors on that computer. Only messages that come from non-authenticated sources are filtered.

This topic explains how to use the EMC or the Shell to configure content filtering on Exchange Edge Transport servers.

Note:

Content filtering is part of the suite of anti-spam features in Exchange. The anti-spam features are only available on Edge Transport servers by default. You can enable anti-spam features on a Hub Transport server even though it isn't recommended. To learn more about enabling anti-spam features on a Hub Transport server, see Enable Anti-Spam Functionality on a Hub Transport Server. The procedures listed in this topic are for configuring anti-spam functionality on an Edge Transport server, but the process is identical on Hub Transport servers.

What Do You Want to Do?

- Use the EMC to configure content filtering
- Use the Shell to configure content filtering
- Use the Shell to configure allowed and blocked phrases
- Use the Shell to configure recipient and sender exceptions
- Use the Shell to configure SCL thresholds
- Use the Shell to configure rejection response
- Use the Shell to configure Outlook e-mail postmark validation

Use the EMC to configure content filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the Edge Transport server you want to configure and then select the **Anti-spam** tab in the work pane.
3. Right-click **Content Filtering** and then select **Properties**.
4. The **General** tab displays the following information about the content filtering feature.
   - **Status** Shows whether content filtering is enabled or disabled.
   - **Modified** Shows the date and time when content filtering properties were last modified.
   - **Description** Provides a brief description of content filtering.
5. Use the **Custom Words** tab on to configure the Content Filter agent to

recognize and filter certain words or phrases. When the Content Filter agent encounters the specified words or phrases, it adjusts the Sender Confidence Level rating. The SCL rating is a number between 0 and 9. A higher SCL rating indicates that a message is more likely to be spam.

- **Allow messages containing these words or phrases** In this field, type a word or phrase that isn't likely to be contained in spam messages, and then click **Add** to add the word or phrase to the allowed phrases list.
  To remove a word or phrase from the allowed phrases list, select the word or phrase, and then click .
  When the Content Filter agent encounters an allowed word or phrase, the SCL rating on that message is set to 0.
- **Block messages containing these words or phrases (messages containing words or phrases listed above will not be blocked)** In this field, type a word or phrase that is likely to be contained in spam messages, and then click **Add** to add the word or phrase to the blocked phrases list. To remove a word or phrase from the list, select the word or phrase, and then click .
  When the Content Filter agent encounters a blocked phrase in a message, the SCL rating on that message is set to 9.

Note:
The allowed phrases list overrides the blocked phrases list. Therefore, if the message contains a phrase that is listed in the allowed phrases list, it is assigned an SCL rating of 0 even if it also contains blocked phrases.

6. Use the **Exceptions** tab to specify up to 100 recipients in your organization for whom messages should not be checked by the Content Filter agent. For example, if you have a customer support e-mail alias, you may want to accept all inbound e-mail messages for that address.
   - **Don't filter messages sent to the following recipients** In this field, type the full SMTP address of a recipient in your organization and then click **Add**.
     To change a recipient address that you have previously added, select the address and click **Edit**.
     To remove a recipient address that you have previously added, select the address and click .

7. Use the **Action** tab to define the action the Content Filter agent will take on messages according to their SCL rating. The Delete action takes precedence over the Reject action, and the Reject action takes precedence over the Quarantine action. Therefore, the SCL threshold for the Delete action must be greater than the SCL threshold for the Reject action, which in turn should be greater than the SCL threshold for the Quarantine action.
   - **Delete messages that have an SCL rating greater than or equal to** Select this option to configure an SCL threshold for the Delete action, and in the corresponding SCL rating box, type or select a number from 0 to 9.
   - **Reject messages that have an SCL rating greater than or equal to** Select this option to configure an SCL threshold for the Reject action, and in the corresponding SCL rating box, type or select a number from 0 to 9.
   - **Quarantine messages that have an SCL rating greater than or equal to** Select this option to configure an SCL threshold for the Quarantine action, and in the corresponding SCL rating box, type or select a number from 0 to 9.
     ? **Quarantine mailbox e-mail address** Use this field to type the SMTP address of the mailbox where you want to store any quarantined messages.

Use the Shell to configure content filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

You can use the **Set-ContentFilterConfig**, **Add-ContentFilterPhrase**, **Remove-ContentFilterPhrase** cmdlets to modify all available content filtering settings. The following examples show how you can use these cmdlets to accomplish various tasks.

Use the Shell to configure allowed and blocked phrases

You use the **Add-ContentFilterPhrase** cmdlet to add both allowed and blocked words and phrases. The value of the *Influence* parameter determines if the word or phrase is allowed or blocked. For example, if you want to allow all messages that contain the phrase "customer feedback", but block all messages that contain the phrase "stock tip", you need to run the following commands:

```
Add-ContentFilterPhrase -Phrase "customer feedback" -Influence GoodWord
Add-ContentFilterPhrase -Phrase "stock tip" -Influence BadWord
```

For detailed syntax and parameter information, see Add-ContentFilterPhrase.

Use the Shell to configure recipient and sender exceptions

You use the **Set-ContentFilterConfig** cmdlet to configure both recipient and send exceptions.

- The following example creates an exception for the recipient tiffany@contoso.com. Messages sent to this recipient aren't checked by the Content Filter agent:

  ```
  Set-ContentFilterConfig -BypassedRecipients tiffany@contoso.com
  ```

- The following example creates an exception for the sender joe@fabrikam.com. Messages received from this sender aren't checked by the Content Filter agent:

  ```
  Set-ContentFilterConfig -BypassedSenders joe@fabrikam.com
  ```

  To enter multiple SMTP addresses when specifying either recipient or sender exceptions, separate the addresses by using a comma. For example: joe@contoso.com, jeffrey@contoso.com. The maximum number of recipients you can specify is 100.

- You can also bypass content filtering for all messages received from specific domains. The following example creates an exception for the domain fabrikam.com. Messages received from this domain aren't checked by the Content Filter agent:

  ```
  Set-ContentFilterConfig -BypassedSenderDomains fabrikam.com
  ```

  To bypass content filtering of messages from specific domains and their subdomains, a wildcard character (*) can be used as shown in the following example:

  ```
  Set-ContentFilterConfig -BypassedSenderDomains *.fabrikam.com
  ```

  To enter multiple SMTP domains, separate the domains by using a comma. For example: fabrikam.com,*nwtraders.com. The maximum number of domains you can specify is 400.

For detailed syntax and parameter information, see Set-ContentFilterConfig.

Use the Shell to configure SCL thresholds

You use the **Set-ContentFilterConfig** cmdlet to configure SCL thresholds and actions. The

Delete action takes precedence over the Reject action, and the Reject action takes precedence over the Quarantine action. Therefore, the SCL threshold for the Delete action must be greater than the SCL threshold for the Reject action, which in turn should be greater than the SCL threshold for the Quarantine action.

- The following example enables the Delete action and sets the corresponding SCL threshold to 9:

```
Set-ContentFilterConfig -SCLDeleteEnabled $true -SCLDeleteThreshold 9
```

- The following example enables the Reject action and sets the corresponding SCL threshold to 8:

```
Set-ContentFilterConfig -SCLRejectEnabled $true -SCLRejectThreshold 8
```

- The following example enables the Quarantine action and sets the corresponding SCL threshold to 7:

```
Set-ContentFilterConfig -SCLQuarantineEnabled $true -SCLQuarantineThres
```

For detailed syntax and parameter information, see Set-ContentFilterConfig.

Use the Shell to configure the rejection response

If you enable the Reject action, you can also customize the response that is sent to the message originator when a message is rejected. The following example configures the Content Filter agent to send a customized rejection response.

```
Set-ContentFilterConfig -RejectionResponse "Your message was rejected because it
```

Note:

Don't write a rejection response that exceeds 240 characters.

For detailed syntax and parameter information, see Set-ContentFilterConfig.

Use the Shell to configure Outlook E-mail Postmarking

Outlook E-mail Postmarking validation is a computational proof that Microsoft Office Outlook applies to outgoing messages to help recipient messaging systems distinguish legitimate e-mail from junk e-mail. Postmarking first became available in Outlook 2007 or newer. Postmarking helps reduce false positives. To enable Outlook E-mail Postmarking, run the following command:

```
Set-ContentFilterConfig -OutlookEmailPostmarkValidationEnabled $true
```

To disable Outlook E-mail Postmarking, run the following command:

```
Set-ContentFilterConfig -OutlookEmailPostmarkValidationEnabled $false
```

For detailed syntax and parameter information, see Set-ContentFilterConfig.

1.7.2.10.4 Release Quarantined Messages from the Spam Quarantine Mailbox

Release Quarantined Messages from the Spam Quarantine Mailbox

Transport > Managing Transport Servers > Managing Anti-Spam and Antivirus Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use Microsoft Outlook to recover a quarantined message from the spam quarantine mailbox. This topic provides step-by-step instructions using Outlook 2007, but you can also use Outlook 2010.

Spam quarantine is a feature of the Content Filter agent that reduces the risk of losing legitimate messages. Spam quarantine provides a temporary storage location for messages that are identified as spam and that shouldn't be delivered to a user mailbox inside the organization. When a message meets the spam quarantine threshold, it's wrapped in a non-delivery report (NDR) and delivered to the spam quarantine mailbox. For more information about the spam quarantine feature, see Understanding Spam Quarantine.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Prerequisites

- A spam quarantine mailbox is configured. For more information, see Specify a Spam Quarantine Mailbox.
- You have been granted owner rights to the spam quarantine mailbox.

Use Outlook 2007 to release a message from the spam quarantine mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox access" entry in the Transport Permissions topic.

Any quarantined messages will be stored as NDRs in the Inbox folder of your quarantine mailbox. To access the quarantine mailbox, you need to configure an Outlook profile for that mailbox and then open the mailbox using Outlook. For more information about configuring and using multiple Outlook profiles, see Overview of Outlook e-mail profiles.

1. Log on to the quarantine mailbox using Outlook 2007 on a client computer.
2. In the **Mail Folders** list, select the **Inbox** folder.
3. Find the NDR of the message that you want to recover, and then double-click the NDR to open it.
4. On the **Report** tab, in the **Respond** group, click **Send Again**.
5. When the e-mail message opens, click **Send** to resend the e-mail message to the intended recipient.

Other Tasks

Because the quarantined messages are stored as NDRs in the quarantine mailbox, the postmaster address of your organization will be listed as the From: address for all messages. To make it easier to locate the message you want to recover, you can create a custom Outlook form and modify the default view to expose the original sender address in the list of messages. For detailed steps, see Configure Outlook to Expose Original Sender Field in the Quarantine Mailbox.

1.7.2.10.5 Configure Outlook to Expose Original Sender Field in the Quarantine Mailbox

Configure Outlook to Expose Original Sender Field in the Quarantine Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

Spam quarantine is a feature of the Content Filter agent that reduces the risk of losing legitimate messages. Spam quarantine provides a temporary storage location for messages that are identified as spam and that shouldn't be delivered to a user mailbox inside the organization.

When a message meets the spam quarantine threshold, it's wrapped in a non-delivery report (NDR) and delivered to the spam quarantine mailbox. Because the quarantined messages are stored as NDRs in the quarantine mailbox, the postmaster address of your organization will be listed as the From: address for all messages.

However, having the original sender address in the field list would make it easier to locate the message you want to recover. This topic explains how you can create a custom Outlook form and modify the default view to expose the original sender address in the list of messages.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Prerequisites

- A spam quarantine mailbox is configured. For more information, see Specify a Spam Quarantine Mailbox.
- You have been granted owner rights to the spam quarantine mailbox.
- You have an Outlook profile configured to access the spam quarantine mailbox on the management workstation you'll be using to perform this procedure.

Configure Outlook to expose original sender field in the quarantine mailbox

You need to be assigned owner permissions to the quarantine mailbox in Microsoft Office Outlook before you can perform this procedure.

The original sender field isn't a default field that you can choose. Therefore, before you can add the original sender field in the message view, you must first create an Outlook form that will add the original sender field as an option. After you create this custom form, you can then configure Microsoft Office Outlook 2007 to expose the original sender field in the message view.

1. Open an ASCII text editor, such as Notepad, and copy the following code into the document.

```
[Description]
MessageClass=IPM.Note
CLSID={00020D31-0000-0000-C000-000000000046}
DisplayName=Quarantine Extension Form
Category=Standard
Subcategory=Form
Comment=This forms allows the Original Sender Address to be viewed as
LargeIcon=IPML.ico
SmallIcon=IPMS.ico
Version=1.0
Locale=enu
Hidden=1
Owner=Microsoft Corporation
Contact=Your Name
[Platforms]
Platform1=Win16
```

```
Platform2=NTx86
Platform9=Win95
[Platform.Win16]
CPU=ix86
OSVersion=Win3.1
[Platform.NTx86]
CPU=ix86
OSVersion=WinNT3.5
[Platform.Win95]
CPU=ix86
OSVersion=Win95
[Properties]
Property01=OriginalSenderAddress
[Property.OriginalSenderAddress]
Type=30
NmidInteger=0x0067
DisplayName=Original Sender Address
[Verbs]
Verb1=1
[Verb.1]
DisplayName=&Open
Code=0
Flags=0
Attribs=2
[Extensions]
Extensions1=1
[Extension.1]
Type=30
NmidPropset={00020D0C-0000-0000-C000-000000000046}
NmidInteger=1
Value=1000000000000000
```

2. Save the file with a .cfg file name extension to a location on the local hard disk. For the rest of this procedure, we assume that the file is named QTNE.cfg.
3. If Outlook isn't open, start Outlook with the profile configured for the quarantine mailbox.
4. In Outlook 2007 on a client computer, click **Tools**, and then click **Options**.
5. In the **Options** dialog box, click the **Other** tab, and then under **General**, click **Advanced Options**.
6. In the **Advanced Options** dialog box, click **Custom Forms**, and then in the **Custom Forms** dialog box, click **Manage Forms**.
7. In the **Forms Manager** dialog box, click **Install**. Locate the directory where you saved QTNE.cfg in step 2. Select **QTNE.cfg**, and then click **Open** to install QTNE.cfg as the Quarantine Extension Form in your Personal Forms library.
8. Close the **Forms Manager** dialog box, and then click **OK** to close the remaining dialog boxes and return to the main Outlook interface. In the default message view of Outlook, in the Inbox, right-click the column heading row, and then select **Field Chooser**.

Note:

If you don't see Field Chooser as an option, you may need to expand the width of your message list.

9. In the **Field Chooser** drop-down menu, click **Forms**. You may have to scroll to find **Forms**.
10. In the **Select Enterprise forms for this Column** dialog box, from the drop-down menu, select **Personal Forms**, expand the **Standard** form, and then select **Quarantine Extension Form**. Click **Add**, and then click **Close**.

Note:

In some cases, you may have to remove the default **Message** form to add the **Quarantine Extension Form**.

11. In the **Field Chooser** dialog box, drag the **OriginalSenderAddress** property into the column heading row.

1.7.2.10.6 Specify a Spam Quarantine Mailbox

Specify a Spam Quarantine Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to specify a spam quarantine mailbox for content filtering. If the spam confidence level (SCL) quarantine threshold is enabled, all messages that are quarantined are wrapped as non-delivery reports (NDR) and are sent to the SMTP address that you specify as the spam quarantine mailbox. You can then review quarantined messages and, as appropriate, release them to their intended recipients by using the Send Again feature in Microsoft Office Outlook. For more information, see Release Quarantined Messages from the Spam Quarantine Mailbox.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Caution:

By the nature of the feature, the person responsible for the spam quarantine mailbox can view potentially private and sensitive messages, and then send mail on behalf of anybody in the Exchange organization.

Prerequisites

- Review Understanding Anti-Spam and Antivirus Functionality to understand the general strategy for configuring all anti-spam agents so that they work together efficiently for your organization.
- Read Understanding Content Filtering.
- Read Understanding Spam Quarantine.

Use the Shell to specify a spam quarantine mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

Note:

You can't use the EMC to specify a spam quarantine mailbox.

Specify a spam quarantine mailbox by using the following command syntax.

```
Set-ContentFilterConfig -QuarantineMailbox <SmtpAddress>
```

This example sends all messages that exceed the spam quarantine to spamQ@contoso.com.

```
Set-ContentFilterConfig -QuarantineMailbox spamQ@contoso.com
```

For detailed syntax and parameter information, see Set-ContentFilterConfig.

1.7.2.10.7 Enable or Disable Connection Filtering

Enable or Disable Connection Filtering

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Connection Filter agent is an anti-spam agent that's enabled on computers that have the Microsoft Exchange Server 2010 Edge Transport server role installed.

When the Connection Filter agent and the associated connection filtering features are enabled on a computer, the Connection Filter agent filters all messages that come through all Receive connectors on that computer. Only messages that come from external sources are filtered. *External sources* are defined as non-authenticated sources. These are considered anonymous Internet sources.

The Connection Filter agent is an underlying transport agent that enables the following features:

- IP Block list
- IP Allow list
- IP Block List providers
- IP Allow List providers

Each of these features can be enabled or disabled separately.

For more information about how to configure the connection filtering features, see the following topics:

- Configure IP Allow List Properties
- Configure IP Block List Properties
- Configure IP Allow List Providers Properties
- Configure IP Block List Providers Properties

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Note:

By default, the connection filtering features are enabled on the Edge Transport server for inbound messages that come from the Internet but aren't authenticated. The Connection Filtering agent must be enabled for the connection filtering features to operate. By default, the Connection Filter agent is enabled on Edge Transport servers. To enable the Connection Filter agent, use the Enable-TransportAgent cmdlet. To disable the Connection Filter agent, use the Disable-TransportAgent cmdlet.

Prerequisites

Review Understanding Anti-Spam and Antivirus Functionality to understand the general strategy for configuring all anti-spam agents so that they work together efficiently for your organization.

Use the EMC to enable or disable connection filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the work pane, click the **Anti-spam** tab, and then select one of the following:
   - **IP Allow List**
   - **IP Allow List Providers**
   - **IP Block List**
   - **IP Block List Providers**
3. In the action pane, click **Enable** or **Disable** as appropriate.
4. Repeat the steps for each connection filtering data store that you want to enable or disable.

Use the Shell to enable or disable connection filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

This example enables or disables the IP Allow list.

```
Set-IPAllowListConfig -Enabled <$true | $false>
```

This example enables or disables IP Allow List providers.

```
Set-IPAllowListProvider -Enabled <$true | $false>
```

This example enables or disables the IP Block list.

```
Set-IPBlockListConfig -Enabled <$true | $false>
```

This example enables or disables the IP Block List providers.

```
Set-IPBlockListProvider -Enabled <$true | $false>
```

For detailed syntax and parameter information, see the following topics:

- Set-IPAllowListConfig
- Set-IPAllowListProvider
- Set-IPBlockListConfig
- Set-IPBlockListProvider

1.7.2.10.8 Configure IP Allow List Properties

Configure IP Allow List Properties

Transport > Managing Transport Servers > Managing Anti-Spam and Antivirus Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When the IP Allow List feature is enabled on a computer, the Connection Filter agent analyzes all messages that come through all Receive connectors on that computer and it routes all messages from the addresses in the IP Allow list without additional processing by other anti-spam agents.

This topic explains how to use the EMC or the Shell to manage the IP Allow List.

Note:

Connection filtering is part of the suite of anti-spam features in Exchange. The anti-spam features are only available on Edge Transport servers by default. You can enable anti-spam features on a Hub Transport server even though it isn't recommended. To learn more about enabling anti-spam features on a Hub Transport server, see Enable Anti-Spam Functionality on a Hub Transport Server. The procedures listed in this topic are for configuring anti-spam functionality on an Edge Transport server, but the process is identical on Hub Transport servers.

What Do You Want to Do?

- Use the EMC to manage the IP Allow List
- Use the Shell to manage the IP Allow List

Use the EMC to manage the IP Allow list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the Edge server you want to configure and then select the **Anti-spam** tab in the work pane.
3. Right click **IP Allow** List and then select **Properties**.

4. The **General** tab displays the following information about the IP Allow List feature.
   - **Status** Shows whether the IP Allow List feature is enabled or disabled.
   - **Modified** Shows the date and time when IP Allow list properties were last modified.
   - **Description** Provides a brief description of the IP Allow List feature.

5. Use the **Allowed Addresses** tab to create and manage a list of IP addresses that are explicitly allowed. The Connection Filter agent will route all inbound messages from these IP addresses without additional processing by other anti-spam agents.
   - **Add - IP Address** To enter an IP address without a subnet mask, or to specify the subnet mask by using Classless Interdomain Routing (CIDR) notation, click **Add** or the drop-down arrow located next to **Add** and select **IP Address**. In the **Add Allowed IP Address - CIDR** dialog, enter the IP address directly or specify a subnet using the CIDR notation. For example, if you enter 192.168.1.1, only that host will be added to the IP Allow list, but if you specify 192.168.1.0/24, the entire class C subnet of 192.168.1.0 will be added to the IP Allow list.

     Add - IP and Mask To enter an IP address or subnet together with a subnet mask in dotted decimal notation, click the drop-down arrow located next to **Add** and select **IP and Mask**. In the **Add Allowed IP Address - IP and Mask** dialog, specify the IP address and the subnet mask.

     Add - IP Range To specify an IP address range by using the

first IP address and the last IP address in the range, click the drop-down arrow located next to **Add** and select **IP Range**. In the **Add Allowed IP Address - IP Range** dialog, specify the start and end addresses of the IP range.

- **Remove** To remove an existing entry from the IP Allow list, select the entry, and then click  .

Use the Shell to manage the IP Allow list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

You use the **Add-IPAllowListEntry** and **Remove-IPAllowListEntry** cmdlets to manage the addresses in the IP Allow list. You can specify individual IP addresses, IP subnets using the CIDR notation, or IP ranges.

The following example adds the IP address 192.168.0.100 to the IP Allow list.

```
Add-IPAllowListEntry -IPAddress 192.168.0.100
```

The following example adds the IP subnet 192.168.1.1/24 to the IP Allow list.

```
Add-IPAllowListEntry -IPRange 192.168.1.1/24
```

The following example adds the IP range 10.0.0.100-10.0.0.255 to the IP Allow list.

```
Add-IPAllowListEntry -IPRange 10.0.0.100-10.0.0.255
```

As you add entries to the IP Allow list, Exchange automatically assigns IDs to the entries. To remove an address from the IP Allow list using the Shell, you must specify this ID. However, an easier way to remove an address is to pipeline the output of the **Get-IPAllowListEntry** cmdlet to the **Remove-IPAllowListEntry** cmdlet. For example, if you want to remove the IP address 192.168.0.100 from your IP Allow list, run the following command:

```
Get-IPAllowListEntry -IPAddress 192.168.0.100 | Remove-IPAllowListEntry
```

If you want to remove a range, specify an IP address that is within that range for the *IPAddress* parameter of the **Get-IPAllowListEntry** cmdlet. The following example shows how you can remove the subnet 192.168.1.1/24:

```
Get-IPAllowListEntry -IPAddress 192.168.1.1 | Remove-IPAllowListEntry
```

When using the Shell to add an address to the IP Allow list, you can also specify an expiration date and time. After the specified date and time, messages received from the specified address receive no preferential treatment. The following example adds the IP address 10.0.10.25 to the IP Allow list and configures it to expire on January 1, 2010 at 10:00 AM.

```
Add-IPAllowListEntry -IPAddress 10.0.10.25 -ExpirationTime "1/1/2010 10:00"
```

For detailed syntax and configuration information, see the following topics:

- Add-IPAllowListEntry
- Get-IPAllowListEntry
- Remove-IPAllowListEntry

Configure IP Allow List Providers Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-24*

IP Allow List Providers is part of the connection filtering feature in Exchange. When the IP Allow List Providers feature is enabled on a computer, the Connection Filter agent queries the specified IP Allow List provider services to determine if the messaging server that has initiated the connection is a host that can be relied on to not send spam.

This topic explains how to use the EMC or the Shell to manage the IP Allow List Providers feature.

Note:

Connection filtering is part of the suite of anti-spam features in Exchange. The anti-spam features are only available on Edge Transport servers by default. You can enable anti-spam features on a Hub Transport server even though it isn't recommended. To learn more about enabling anti-spam features on a Hub Transport server, see Enable Anti-Spam Functionality on a Hub Transport Server. The procedures listed in this topic are for configuring anti-spam functionality on an Edge Transport server, but the process is identical on Hub Transport servers.

Note:

Make sure that the IP Allow list that you want to add does not contain more than 1,000 entries. The IP allow list cannot contain more than 1,000 entries because of a limitation in byte size that applies to this field. Instead, use IP address ranges if more than 1,000 entries are required.

What Do You Want to Do?

- Use the EMC to manage the IP Allow List Providers
- Use the Shell to manage the IP Allow List Providers

Use the EMC to manage IP Allow List provider services

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the Edge server you want to configure and then select the **Anti-spam** tab in the work pane.
3. Right-click **IP Allow List Providers** and then select **Properties**.
4. The **General** tab displays the following information about the IP Allow List Providers feature.
   - **Status** Shows whether the IP Allow List Providers feature is enabled or disabled.
   - **Modified** Shows the date and time when IP Allow List Providers properties were last modified.
   - **Description** Provides a brief description of the IP Allow List Providers feature.

5. Use the **Providers** tab to manage the IP Allow List provider services for the local computer. We recommend that you put the most reliable IP Allow List provider service first to optimize performance. If the Connection Filter agent receives an IP Allow list match from one of the providers, it stops querying other IP Allow List provider services.
   - **Add** Click **Add** to add a new IP Allow List provider service. In the dialog that appears, configure the following options:
     ? **Provider name** Type the name of the IP Allow List provider service. This name is for your own use to identify the provider.
     ? **Lookup domain** Type the domain name that the Connection Filter agent queries for updated IP Allow list information.
     ? **Return status codes** This field shows the IP address status code that is returned by the IP Allow List provider service. If the IP address of a remote server that is sending a message matches an IP address on an IP Allow List provider service's IP Allow list, the provider service may return different types of codes. Most IP Allow List provider services return either a bitmask or absolute value code type.
     Match any return code When you select this option, the Connection Filter agent treats any IP Address status code that is returned by the IP Allow List provider service as a match.
     Match specific mask and responses When you select this option, the Connection Filter agent acts only on messages that match the IP Address status code that is returned by the IP Allow List provider service.
     Providers that return bitmask status codes may return a status code of **127.0.0.***x*, where the integer *x* is any one of the following values:
     1: The IP address is on an IP Allow list.
     2: The Simple Mail Transfer Protocol (SMTP) server is configured to act as an open relay.
     4: The IP address supports a dial-up IP address.
     Providers that return absolute values and the explicit responses may return one of the following responses:
     127.0.0.2: The IP address is a direct spam source
     127.0.0.4: The IP address is a bulk mailer
     127.0.0.5: The remote server that is sending the message is known to support multistage open relays.
     Match to the following mask Type the bitmask status code you want to use.
     Match any of the following responses Type the responses you want to use and then click **Add**. To modify a previously added response, select the response and click **Edit**. To remove a previously added response, select the response and click  .
   - **Edit** To view or update settings for an IP Allow List provider, select a provider, and then click **Edit**.
   - **Remove** To delete an IP Allow List provider, select the provider, and then click  .
   - **Enable** To enable a disabled IP Allow List provider, select the provider, and then click **Enable**.
   - **Disable** To stop using the selected IP Allow List provider, but retain the provider information, click **Disable**.
   - **Up arrow** To move a provider higher in the **Provider name** list, select the provider, and then click  . The up arrow is enabled only when there is more than one provider in the **Provider name** list.
   - **Down arrow** To move a provider lower in the **Provider name** list, select the provider, and then click  . The down arrow is enabled only when there is more than one provider in the **Provider name** list.

Use the Shell to manage IP Allow List provider services

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

You use the **Add-IPAllowListProvider**, **Set-IPAllowListProvider,** and **Remove-IPAllowListProvider** cmdlets to manage the IP Allow List provider services you use in your organization.

The following example adds a new IP Allow List provider called "Contoso IP Allow List Provider", and configures it to match any return code:

```
Add-IPAllowListProvider -Name "Contoso IP Allow List Provider" -LookupDomain "con
```

The following example configures the same IP Allow List provider to be the top preferred provider:

```
Set-IPAllowListProvider "Contoso IP Allow List Provider" -Priority 1
```

For detailed syntax and parameter information, see the following topics:

- Add-IPAllowListProvider
- Set-IPAllowListProvider
- Remove-IPAllowListProvider

1.7.2.10.10 Configure IP Block List Properties

Configure IP Block List Properties

Transport > Managing Transport Servers > Managing Anti-Spam and Antivirus Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

IP Block List is part of the connection filtering feature in Exchange. When the IP Block List feature is enabled on a computer, the Connection Filter agent analyzes all messages that come through all Receive connectors on that computer and it block all incoming messages from addresses specified in the IP Block list.

This topic explains how to use the EMC or the Shell to manage the IP Block list.

Note:

Connection filtering is part of the suite of anti-spam features in Exchange. The anti-spam features are only available on Edge Transport servers by default. You can enable anti-spam features on a Hub Transport server even though it isn't recommended. To learn more about enabling anti-spam features on a Hub Transport server, see Enable Anti-Spam Functionality on a Hub Transport Server. The procedures listed in this topic are for configuring anti-spam functionality on an Edge Transport server, but the process is identical on Hub Transport servers.

What Do You Want to Do?

- Use the EMC to manage the IP Block List
- Use the Shell to manage the IP Block List

Use the EMC to manage the IP Block list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the Edge server you want to configure and then select the **Anti-spam** tab in the work pane.
3. Right-click **IP Block List** and then select **Properties**.
4. The **General** tab displays the following information about the IP Block List feature.
   - **Status** Shows whether the IP Block List feature is enabled or disabled.
   - **Modified** Shows the date and time when IP Block List properties were last modified.
   - **Description** Provides a brief description of the IP Block List feature.
5. Use the **Blocked Addresses** tab to manage a list of specific IP addresses for which e-mail messages are always blocked by the Connection Filter agent. If an originating IP address matches an IP address or IP address range on the IP Block list, the Connection Filter agent disconnects the SMTP session after all RCPT TO: headers in the message are processed.
   - **Add - IP Address** To enter an IP address without a subnet mask, or to specify the subnet mask by using Classless Interdomain Routing (CIDR) notation, click **Add** or the drop-down arrow located next to **Add** and select **IP Address**. In the **Add Blocked IP Address - CIDR** dialog, enter the IP address directly or specify a subnet using the CIDR notation. For example, if you enter 192.168.1.1, only that host will be added to the IP Block list, but if you specify 192.168.1.0/24, the entire class C subnet of 192.168.1.0 will be added to the IP Block list.

     Add - IP and Mask To enter an IP address or subnet together with a subnet mask in dotted decimal notation, click the drop-down arrow located next to **Add** and select **IP and Mask**. In the **Add Blocked IP Address - IP and Mask** dialog, specify the IP address and the subnet mask.

     Add - IP Range To specify an IP address range by using the first IP address and the last IP address in the range, click the drop-down arrow located next to **Add** and select **IP Range**. In the **Add Blocked IP Address - IP Range** dialog, specify the start and end addresses of the IP range.

     Regardless of the method you choose to add an IP address, the dialog also gives you the option to specify an expiration date. By default, the **Never let this address expire** option is selected and messages from this address are blocked permanently. However, if you want to specify an expiration date, select **Block until date and time** and specify a date. Messages from this IP address will no longer be blocked after the date you specified.
   - **Remove** To remove an existing entry from the IP Block list, select the entry, and then click  .

Use the Shell to manage the IP Block list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

You use the **Add-IPBlockListEntry** and **Remove-IPBlockListEntry** cmdlets to manage the addresses in the IP Block list. You can specify individual IP addresses, IP subnets using the CIDR notation, or IP ranges.

The following example adds the IP address 192.168.0.100 to the IP Block list.

```
Add-IPBlockListEntry -IPAddress 192.168.0.100
```

The following example adds the IP subnet 192.168.1.1/24 to the IP Block list.

```
Add-IPBlockListEntry -IPRange 192.168.1.1/24
```

The following example adds the IP range 10.0.0.100-10.0.0.255 to the IP Block list.

```
Add-IPBlockListEntry -IPRange 10.0.0.100-10.0.0.255
```

As you add entries to the IP Block list, Exchange automatically assigns IDs to the entries. To remove an address from the IP Block list using the Shell, you must specify this ID. However, an easier way to remove an address is to pipeline the output of the **Get-IPBlockListEntry** cmdlet to the **Remove-IPBlockListEntry** cmdlet. For example, if you want to remove the IP address 192.168.0.100 from your IP Block list, run the following command:

```
Get-IPBlockListEntry -IPAddress 192.168.0.100 | Remove-IPBlockListEntry
```

If you want to remove a range, specify an IP address that is within that range for the *IPAddress* parameter of the **Get-IPBlockListEntry** cmdlet. The following example shows how you can remove the subnet 192.168.1.1/24:

```
Get-IPBlockListEntry -IPAddress 192.168.1.1 | Remove-IPBlockListEntry
```

When using the Shell to add an address to the IP Block list, you can also specify an expiration date and time. After the specified date and time, messages received from the specified address will no longer be blocked. The following example adds the IP address 10.0.10.25 to the IP Block list and configures it to expire on January 1, 2010 at 10:00 AM.

```
Add-IPBlockListEntry -IPAddress 10.0.10.25 -ExpirationTime "1/1/2010 10:00"
```

For detailed syntax and configuration information, see the following topics:

- Add-IPBlockListEntry
- Get-IPBlockListEntry
- Remove-IPBlockListEntry

1.7.2.10.11 Configure IP Block List Providers Properties

Configure IP Block List Providers Properties

Transport > Managing Transport Servers > Managing Anti-Spam and Antivirus Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

IP Block List Providers are part of the connection filtering feature in Exchange. When the

IP Block List Providers feature is enabled on a computer, the Connection Filter agent queries the specified IP Block List provider services to determine if the messaging server that has initiated the connection is a host that is known to send spam.

This topic explains how to use the EMC or the Shell to manage the IP Block List Providers.

Note:

Connection filtering is part of the suite of anti-spam features in Exchange. The anti-spam features are only available on Edge Transport servers by default. You can enable anti-spam features on a Hub Transport server even though it isn't recommended. To learn more about enabling anti-spam features on a Hub Transport server, see Enable Anti-Spam Functionality on a Hub Transport Server. The procedures listed in this topic are for configuring anti-spam functionality on an Edge Transport server, but the process is identical on Hub Transport servers.

What Do You Want to Do?

- Use the EMC to manage the IP Block List Providers
- Use the Shell to manage the IP Block List Providers

Use the EMC to manage IP Block List provider services

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the Edge server you want to configure and then select the **Anti-spam** tab in the work pane.
3. Right-click **IP Block List Providers** and then select **Properties**.

4. The **General** tab displays the following information about the IP Block List Providers feature.
   - **Status** Shows whether the IP Block List Providers feature is enabled or disabled.
   - **Modified** Shows the date and time when IP Block List Providers properties were last modified.
   - **Description** Provides a brief description of the IP Block List Providers feature.

5. Use the **Providers** tab to manage the IP Block List provider services for the local computer. We recommend that you put the most reliable IP Block List provider service first to optimize performance. If the Connection Filter agent receives an IP Block List match from one of the providers, it stops querying other IP Block List provider services.
   - **Add** Click **Add** to add a new IP Block List provider service. In the dialog that appears, configure the following options:
     ? **Provider name** Type the name of the IP Block List provider service. This name is for your own use to identify the provider.
     ? **Lookup domain** Type the domain name that the Connection Filter agent queries for updated IP Block list information.
     ? **Return Status codes** This field shows the IP address status code that is returned by the IP Block List provider service. If the IP address of a remote server that is sending a message matches an IP address on an IP Block List provider service's IP Block list, the provider service may return different types of codes. Most IP Block List provider services return either a

bitmask or absolute value code type.
Match any return code When you select this option, the Connection Filter agent treats any IP Address status code that is returned by the IP Block List provider service as a match.
Match specific mask and responses When you select this option, the Connection Filter agent acts only on messages that match the IP Address status code that is returned by the IP Block List provider service.
Providers that return bitmask status codes may return a status code of **127.0.0.***x*, where the integer *x* is any one of the following values:
1: The IP address is on an IP Block list.
2: The Simple Mail Transfer Protocol (SMTP) server is configured to act as an open relay.
4: The IP address supports a dial-up IP address.
Providers that return absolute values and the explicit responses may return one of the following responses:
127.0.0.2: The IP address is a direct spam source
127.0.0.4: The IP address is a bulk mailer
127.0.0.5: The remote server that is sending the message is known to support multistage open relays.
Match to the following mask Type the bitmask status code you want to use.
Match any of the following responses Type the responses you want to use and then click **Add**. To modify a previously added response, select the response and click **Edit**. To remove a previously added response, select the response and click  .
Error Messages To configure the message text that will be delivered in the SMTP session to senders whose messages are blocked by the Connection Filter agent when an IP Block List provider service matches the sender's IP address, click **Error Messages** and configure the following:

Default error message	To send a standard SMTP 550 error message to blocked senders, select **Default error message**.
Custom error message	To compose and send a customized error message, select **Custom error message**, and then type the message text in the text box. We recommend that you specify the IP Block List provider service in the response so that legitimate senders can contact the IP Block List provider service, as in the following example: **Originating IP addresses matched contoso.com's IP Block List provider service**.

- **Edit** To view or update settings for an IP Block List provider service, select a provider, and then click **Edit**.
- **Remove** To delete an IP Block List provider service, select the provider, and then click  .
- **Enable** To enable a disabled provider service, select the provider, and then click **Enable**.
- **Disable** To stop using the selected provider service, but retain the

provider information, click **Disable**.

- **Up arrow** To move a provider higher in the **Provider name** list, select the provider, and then click  . The up arrow is enabled only when there is more than one provider in the **Provider name** list.
- **Down arrow** To move a provider lower in the **Provider name** list, select the provider, and then click  . The down arrow is enabled only when there is more than one provider in the **Provider name** list.

6. Use the **Exceptions** tab to specify recipients in your organization for which you don't want to use IP Block List provider services. For example, if you have a customer support e-mail alias, you may want to accept all inbound e-mail messages for that address.
   - **Do not block messages sent to the following e-mail addresses, regardless of provider feedback** In this field, type the SMTP address for an existing recipient for which you want to create an exception. For example, kim@contoso.com.
   - **Add** To add that recipient to the Exceptions list, after you type the recipient's SMTP address, click **Add**.
   - **Edit** To change a previously added SMTP address, select the recipient's SMTP address from the list, and then click **Edit.**
   - **Remove** To delete a recipient from the exceptions list, select the recipient's SMTP address, and then click  .

Use the Shell to manage IP Block List provider services

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

You use the **Add-IPBlockListProvider**, **Set-IPBlockListProvider,** and **Remove-IPBlockListProvider** cmdlets to manage the IP Block List Provider services you use in your organization.

The following example adds a new IP Block List provider service called "Contoso IP Block List Provider", and configures it to use bitmask matching for 127.0.0.1 (block messages from IP addresses that are on the block list):

```
Add-IPBlockListProvider -Name "Contoso IP Block List Provider" -LookupDomain "con
```

The following example configures the same IP Block List provider service to use a custom rejection response:

```
Set-IPBlockListProvider "Contoso IP Block List Provider" -RejectionMessage "Your
```

The following example adds another IP Block List provider service called "Fabrikam IP Block List Provider", and configures it to use explicit response matching for 127.0.0.2 and 127.0.0.5 (the host is a known spam source or is an open relay). The command also adds this new provider as the top preferred provider.

```
Add-IPBlockListProvider -Name "Fabrikam IP Block List Provider" -LookupDomain "fa
```

For detailed syntax and configuration information, see the following topics:

- Add-IPBlockListProvider
- Set-IPBlockListProvider
- Remove-IPBlockListProvider

1.7.2.10.12 Enable or Disable Recipient Filtering

Enable or Disable Recipient Filtering

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When recipient filtering functionality is enabled, it filters all messages that come through all Receive connectors on that computer. By default, recipient filtering is enabled on the computer that has the Edge Transport server role installed for inbound messages that come from the Internet but aren't authenticated. These messages are handled as external messages.

Note:

The Recipient Filter agent is the underlying agent for recipient filtering functionality. It's important to understand that when you perform the following procedures, recipient filtering functionality is enabled or disabled, but the underlying Recipient Filter agent is still enabled. To disable the underlying Recipient Filter agent, run the Disable-TransportAgent cmdlet.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Prerequisites

- Review Understanding Anti-Spam and Antivirus Functionality to understand the general strategy for configuring all anti-spam agents so that they work together efficiently for your organization.
- Read Understanding Recipient Filtering.
- Verify that the *AddressBookEnabled* parameter is set to `$true` on any Receive connectors that receive e-mail for the accepted domains in your organization. For more information, see Set-AcceptedDomain.

Use the EMC to enable or disable recipient filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. Open the EMC on the Edge Transport server.
2. In the console tree, click **Edge Transport**.
3. In the work pane, click the **Anti-spam** tab, and then select **Recipient Filtering**.
4. In the action pane, click **Enable** or **Disable** as appropriate.

Use the Shell to enable or disable recipient filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions

topic.

This example enables recipient filtering.

```
Set-RecipientFilterConfig -Enabled $true
```

This example disables recipient filtering.

```
Set-RecipientFilterConfig -Enabled $false
```

For detailed syntax and parameter information, see Set-RecipientFilterConfig.

1.7.2.10.13 Configure Recipient Filtering Properties

Configure Recipient Filtering Properties

Transport > Managing Transport Servers > Managing Anti-Spam and Antivirus Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Recipient Filter agent is an anti-spam agent that is enabled on Edge Transport servers. You can use the Recipient Filter to block incoming messages for specific recipients in your organization. You can also block incoming messages to recipients that do not exist in Active Directory.

This topic explains how to use the EMC or the Shell to add recipients to the list of blocked recipients.

Note:
Recipient filtering is part of the suite of anti-spam features in Exchange. The anti-spam features are only available on Edge Transport servers by default. You can enable anti-spam features on a Hub Transport server even though it isn't recommended. To learn more about enabling anti-spam features on a Hub Transport server, see Enable Anti-Spam Functionality on a Hub Transport Server. The procedures listed in this topic are for configuring anti-spam functionality on an Edge Transport server, but the process is identical on Hub Transport servers.

What Do You Want to Do?

- Use the EMC to configure recipient filtering
- Use the Shell to configure recipient filtering

Use the EMC to configure recipient filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the Edge server you want to configure and then select the **Anti-spam** tab in the work pane.
3. Right-click **Recipient Filtering** and then select **Properties**.
4. The **General** tab displays the following information about the recipient filtering feature.

- **Status** Shows whether recipient filtering is enabled or disabled.
- **Modified** Shows the date and time when recipient filtering properties were last modified.
- **Description** Provides a brief description of recipient filtering.

5. Use the **Blocked Recipients** tab to maintain the Recipient Block list, an administrator-defined list of up to 800 recipients for which incoming messages from the Internet should never be accepted.
   - **Block messages sent to recipients that do not exist in the directory** To prevent delivery to recipients that aren't in the organization's global address book, select this option. This feature is maintained through the EdgeSync process.
   - **Block messages sent to the following recipients** To create an administrator-maintained list of recipients that should be blocked from receiving messages from the Internet, this option, type the SMTP address for the recipient, and then click **Add**. You can enter up to 800 recipients.
     To change an existing recipient address, select the address and then click **Edit**.
     To remove an existing recipient address, select the address and click  .

Use the Shell to configure recipient filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

You use the **Set-RecipientFilterConfig** cmdlet to manage recipient filtering. The following example configures the Recipient Filter agent to block specific recipients:

```
Set-RecipientFilterConfig -BlockListEnabled $true
```

To add SMTP addresses to the Recipient Block list, you use the *BlockedRecipients* parameter of the **Set-RecipientFilterConfig** cmdlet. You can separate multiple SMTP addresses with commas. The following example adds the e-mail addresses mark@contoso.com and kim@contoso.com to the Recipient Block list:

```
Set-RecipientFilterConfig -BlockedRecipients mark@contoso.com,kim@contoso.com
```

The values that you specify by using the *BlockedRecipients* parameter replace the existing list of SMTP addresses. To preserve the existing list, you could specify the existing addresses along with new addresses you want to add. However, this can be a cumbersome task especially if you have many SMTP addresses for which you block incoming messages. Instead, you can use a temporary Shell variable to add an address to the Recipient Block list. The following example uses the temporary variable `$Configuration` to add the SMTP address john@contoso.com to the Recipient Block list:

```
$Configuration = Get-RecipientFilterConfig
$Configuration.BlockedRecipients += "john@contoso.com"
Set-RecipientFilterConfig -BlockedRecipients $Configuration.BlockedRecipients
```

To block messages to recipients that don't exist in your organization, run the following command:

```
Set-RecipientFilterConfig -RecipientValidationEnabled $true
```

For detailed syntax and parameter information, see Set-RecipientFilterConfig.

1.7.2.10.14 Enable or Disable Sender Filtering

Enable or Disable Sender Filtering

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Sender Filter agent is an anti-spam filter that is enabled on computers that have the Microsoft Exchange Server 2010 Edge Transport server role installed. The Sender Filter agent relies on the MAIL FROM: SMTP header to determine what action, if any, to take on an inbound e-mail message.

When sender filtering functionality is enabled on a computer, sender filtering functionality filters all messages that come through all Receive connectors on that computer.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Prerequisites

- Review Understanding Anti-Spam and Antivirus Functionality to understand the general strategy for configuring all anti-spam agents so that they work together efficiently for your organization.
- Read Understanding Sender Filtering.

Use the EMC to enable or disable sender filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. Open the EMC on the Edge Transport server.
2. In the console tree, click **Edge Transport**.
3. In the work pane, click the **Anti-Spam** tab, and then select **Sender Filtering**.
4. In the action pane, click **Enable** or **Disable** as appropriate.

Use the Shell to enable or disable sender filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

This example enables sender filtering.

```
Set-SenderFilterConfig -Enabled $true
```

This example disables sender filtering.

```
Set-SenderFilterConfig -Enabled $false
```

For detailed syntax and parameter information, see Set-SenderFilterConfig.

Configure Sender Filtering Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Sender Filter agent is an anti-spam agent that is enabled on Edge Transport servers. You can use the Sender Filter to block incoming messages from specific individual senders or domains.

This topic explains how to use the EMC or the Shell to configure sender filtering.

Note:

Sender filtering is part of the suite of anti-spam features in Exchange. The anti-spam features are only available on Edge Transport servers by default. You can enable anti-spam features on a Hub Transport server even though it isn't recommended. To learn more about enabling anti-spam features on a Hub Transport server, see Enable Anti-Spam Functionality on a Hub Transport Server. The procedures listed in this topic are for configuring anti-spam functionality on an Edge Transport server, but the process is identical on Hub Transport servers.

What Do You Want to Do?

- Use the EMC to configure sender filtering
- Use the Shell to configure sender filtering

Use the EMC to configure sender filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the Edge server you want to configure and then select the **Anti-spam** tab in the work pane.
3. Right-click **Sender Filtering** and then select **Properties**.
4. The **General** tab displays the following information about the sender filtering feature.
   - **Status** Shows whether sender filtering is enabled or disabled.
   - **Modified** Shows the date and time when sender filtering properties were last modified.
   - **Description** Provides a brief description of sender filtering.
5. Use the **Blocked Senders** tab to specify e-mail addresses or domains from which you want to block messages.
   - **Add** To add new addresses and domains to the blocked senders list, click **Add**. In the dialog that appears, use the following fields to specify a sender:
     ? **Individual e-mail address** To block an individual sender, select **Individual e-mail address** and then type the Simple Mail Transfer Protocol (SMTP) address of the sender that you want to block. For example, type **kim@contoso.com**.
     ? **Domain** To add all senders from a domain to the blocked senders list, select **Domain**, and then type the domain name in the domain field, such as **contoso.com**.

? **Include all subdomains** To include all subdomains to the blocked domain, select **Include all subdomains**. This check box is active only when you select **Domain**.

- **Edit** To change a blocked sender's address or domain, click the sender's address, and then click **Edit**.
- **Remove** To delete a blocked sender's address or domain, click the sender's address, and then click  .
- **Block messages that don't have sender information** To block messages that don't have sender information, select this check box.

6. Use the **Action** tab on the sender filtering properties to configure the Sender Filter agent to take one of the following actions when a blocked sender or domain is identified.
   - **Reject message** To reject the message and send a "554 5.1.0 Sender Denied" SMTP session error to the sending server, select **Reject message**. **Reject message** is the recommended setting.
   - **Stamp message with blocked sender and continue processing** To update the metadata of the message to indicate that this message was sent by a blocked sender, select this setting. This stamp is used by the Content Filter agent when it calculates the spam confidence level (SCL) for the message. Additionally, sender reputation uses the SCL for a particular message when it calculates a sender reputation level (SRL) for the sender of the message.

Use the Shell to configure sender filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

You use the **Set-SenderFilterConfig** cmdlet to manage sender filtering. The following example configures the Sender Filter agent to block messages from the specific e-mail addresses kim@contoso.com and john@contoso.com:

```
Set-SenderFilterConfig -BlockedSenders kim@contoso.com,john@contoso.com
```

The following example configures the Sender Filter agent to block messages from the specific domain fabrikam.com:

```
Set-SenderFilterConfig -BlockedDomains fabrikam.com
```

The following example configures the Sender Filter agent to block messages from the specific domain northwindtraders.com and all its subdomains:

```
Set-SenderFilterConfig -BlockedDomainsAndSubdomains northwindtraders.com
```

The values that you specify by using the parameters shown in the examples above replace the existing list of blocked senders. To preserve the existing list, you could specify the existing senders along with any new senders you want to add. However, this can be a cumbersome task especially if you have many SMTP addresses or domains from which you block incoming messages. Instead, you can use a temporary Shell variable to add an address or domain to the blocked senders list. The following example uses the temporary variable `$Configuration` to add the sender john@contoso.com and the domain tailspintoys.com to the blocked senders list:

```
$Configuration = Get-SenderFilterConfig
$Configuration.BlockedSenders += "john@contoso.com"
$Configuration.BlockedDomains += "tailspintoys.com"
Set-SenderFilterConfig -BlockedSenders $Configuration.BlockedSenders -BlockedDoma
```

The following example shows how to configure the Sender Filter agent to block messages

that don't specify a sender in the MAIL FROM: SMTP command:

```
Set-SenderFilterConfig -BlankSenderBlockingEnabled $true
```

For detailed syntax and parameter information, see Set-SenderFilterConfig.

1.7.2.10.16 Enable or Disable Sender ID

Enable or Disable Sender ID

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

By default, Sender ID is enabled on the Edge Transport server role for inbound messages that come from the Internet but aren't authenticated. These messages are handled as external messages.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Note:

The Sender ID agent is the underlying agent for Sender ID functionality. It's important to understand that when you perform the following procedures, the Sender ID functionality is enabled or disabled, but the underlying Sender ID agent is still enabled. To disable the underlying Sender ID agent, run the Disable-TransportAgent cmdlet.

Prerequisites

- Review Understanding Anti-Spam and Antivirus Functionality to understand the general strategy for configuring all anti-spam agents so that they work together efficiently for your organization.
- Read Understanding Sender ID.

Use the EMC to enable or disable Sender ID

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. Open the EMC on the Edge Transport server.
2. In the console, click **Edge Transport**.
3. In the work pane, click the **Anti-spam** tab, and then select **Sender ID**.
4. In the action pane, click **Enable** or **Disable** as appropriate.

Use the Shell to enable or disable Sender ID

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

This example enables Sender ID.

```
Set-SenderIDConfig -Enabled $true
```

This example disables Sender ID.

```
Set-SenderIDConfig -Enabled $false
```


1.7.2.10.17 Configure Sender ID Properties

Configure Sender ID Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Sender ID agent is an e-mail authentication technology protocol that helps address the problem of spoofing and phishing by verifying the domain name from which e-mail is sent. Sender ID validates the origin of e-mail by verifying the IP address of the sender against the purported owner of the sender domain.

This topic explains how to use the EMC or the Shell to configure Sender ID.

Note:

Sender ID is part of the suite of anti-spam features in Exchange. The anti-spam features are only available on Edge Transport servers by default. You can enable anti-spam features on a Hub Transport server even though it isn't recommended. To learn more about enabling anti-spam features on a Hub Transport server, see Enable Anti-Spam Functionality on a Hub Transport Server. The procedures listed in this topic are for configuring anti-spam functionality on an Edge Transport server, but the process is identical on Hub Transport servers.

What Do You Want to Do?

- Use the EMC to configure Sender ID action for spoofed messages
- Use the Shell to configure Sender ID
- Use the Shell to configure Sender ID action for spoofed messages
- Use the Shell to configure Sender ID action for transient errors
- Use the Shell to configure recipient and sender domain exceptions

Use the EMC to configure Sender ID action for spoofed messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the Edge server you want to configure and then select the **Anti-spam** tab in the work pane.
3. Right-click **Sender ID** and then select **Properties**.
4. The **General** tab displays the following information about the Sender ID feature.
   - **Status** Shows whether the Sender ID feature is enabled or disabled.

- **Modified** Shows the date and time when Sender ID properties were last modified.
- **Description** Provides a brief description of the Sender ID feature.

5. Use the **Action** tab on the Sender ID properties to configure Sender ID to take one of the following actions when Sender ID determines that a message is spoofed or when a transient error is returned.
   - **Reject message** To reject the message and send a SMTP error response to the sending server, select **Reject message**. The SMTP error response is a 5xx level protocol response with text that corresponds to the Sender ID status.
   - **Delete message** To delete the message without informing the sending server of the deletion, select **Delete message**. The Edge Transport server sends a fake "OK" SMTP command to the sending server and then deletes the message.
   - **Stamp message with Sender ID result and continue processing** To stamp the message with the Sender ID status, select this option. This metadata is evaluated by the Content Filter agent when a spam confidence level (SCL) is calculated. This setting is the default option for Sender ID properties.

Use the Shell to configure Sender ID

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

You use the **Set-SenderIDConfig** cmdlet to configure Sender ID options and actions. Although the EMC only allows you to configure actions for messages that are spoofed, you can also configure actions for transient failures using the Shell. For example, it's considered a transient error if a DNS server is unavailable when Exchange attempts to verify the Sender ID for a sending domain. Another thing you can only do in the Shell is to configure exceptions for specific sending domains or recipients. The following sections provide examples of how you can use the **Set-SenderIDConfig** cmdlet to accomplish these various tasks.

Use the Shell to configure Sender ID action for spoofed messages

The following example configures the Sender ID agent to reject any messages that were spoofed. These are messages where the IP address of the sending server isn't listed as an authoritative SMTP sending server in the DNS Sender Policy Framework record for the sending domain.

```
Set-SenderIDConfig -SpoofedDomainAction Reject
```

For detailed syntax and parameter information, see Set-SenderIdConfig.

Use the Shell to configure Sender ID action for transient errors

The following example configures the Sender ID agent to stamp the messages for which the Sender ID status can't be determined due to a temporary error. The message will be processed by other anti-spam agents and the Content Filter agent will use the mark when determining the SCL value for the message.

```
Set-SenderIDConfig -TempErrorAction StampStatus
```

For detailed syntax and parameter information, see Set-SenderIdConfig.

Use the Shell to configure recipient and sender domain exceptions

The following example configures the Sender ID agent to bypass the Sender ID check for the specific recipients kim@contoso.com and john@contoso.com:

```
Set-SenderIDConfig -BypassedRecipients kim@contoso.com,john@contoso.com
```

The following example configures the Sender ID agent to bypass the Sender ID check for messages that are received from the specific domain fabrikam.com.

```
Set-SenderIDConfig -BypassedSenderDomains fabrikam.com
```

The values that you specify by using the parameters shown in the examples in this section replace the existing list of exceptions. To preserve the existing list of recipients or sender domains, you could specify the existing values along with any new exceptions you want to add. However, this can be a cumbersome task especially if you have many recipients or domains for which you want to bypass Sender ID checking. Instead, you can use a temporary Shell variable to add a recipient or domain to the exceptions list. The following example uses the temporary variable `$Configuration` to add the domain tailspintoys.com to the list of domains for which you want to bypass Sender ID check:

```
$Configuration = Get-SenderIDConfig
$Configuration.BypassedSenderDomains += "tailspintoys.com"
Set-SenderIDConfig -BypassedSenderDomains $Configuration.BypassedSenderDomains
```

For detailed syntax and parameter information, see Set-SenderIdConfig.

1.7.2.10.18 Enable or Disable Sender Reputation

Enable or Disable Sender Reputation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Sender reputation is anti-spam functionality that's enabled on computers that have the Microsoft Exchange Server 2010 Edge Transport server role installed to block messages according to various characteristics of the sender. Sender reputation relies on persisted data about the sender to determine what action, if any, to take on an inbound message.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Note:

By default, sender reputation processing is enabled on the Edge Transport server for inbound messages that come from the Internet but aren't authenticated and are therefore handled as external messages.
The Protocol Analysis agent is the underlying agent for sender reputation functionality. It's important to understand that when you perform the following procedures, sender reputation functionality is enabled or disabled, but the underlying Protocol Analysis agent is still enabled. To disable the underlying Protocol Analysis agent, run the Disable-TransportAgent cmdlet.

Prerequisites

- Review Understanding Anti-Spam and Antivirus Functionality to understand the general strategy for configuring all anti-spam agents so that they work together efficiently for your organization.
- Read Understanding Sender Reputation.

Use the EMC to enable or disable sender reputation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. Open the EMC on the Edge Transport server.
2. In the console tree, click **Edge Transport**.
3. In the work pane, click the **Anti-spam** tab, and then select **Sender Reputation**.
4. In the action pane, click **Enable** or **Disable** as appropriate.

Use the Shell to enable or disable sender reputation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

This example enables sender reputation.

```
Set-SenderReputationConfig -Enabled $true
```

This example disables sender reputation.

```
Set-SenderReputationConfig -Enabled $false
```

For detailed syntax and parameter information, see Set-SenderReputationConfig.

Use the Shell to enable or disable sender reputation for internal and external messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable or disable sender reputation for internal and external messages.

This example enables sender reputation for external messages.

```
Set-SenderReputationConfig -ExternalMailEnabled $true
```

This example disables sender reputation for external messages.

```
Set-SenderReputationConfig -ExternalMailEnabled $false
```

Note:
By default, sender reputation is enabled for external messages.

This example enables sender reputation for internal messages.

```
Set-SenderReputationConfig -InternalMailEnabled $true
```

This example disables sender reputation for internal messages.

```
Set-SenderReputationConfig -InternalMailEnabled $false
```

For detailed syntax and parameter information, see Set-SenderReputationConfig.

1.7.2.10.19 Configure Sender Reputation Properties

Configure Sender Reputation Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Sender reputation is anti-spam functionality that can be used to block messages according to many characteristics of the sender. Sender reputation continuously monitors senders and their past SMTP interactions, such as the amount of spam and messages that aren't spam that a sender has sent. Sender reputation relies on such data about the sender to determine what action, if any, to take on an inbound message.

This topic explains how to use the EMC or the Shell to configure sender reputation.

Note:
Sender reputation is part of the suite of anti-spam features in Exchange. The anti-spam features are only available on Edge Transport servers by default. You can enable anti-spam features on a Hub Transport server even though it isn't recommended. To learn more about enabling anti-spam features on a Hub Transport server, see Enable Anti-Spam Functionality on a Hub Transport Server. The procedures listed in this topic are for configuring anti-spam functionality on an Edge Transport server, but the process is identical on Hub Transport servers.

What Do You Want to Do?

- Use the EMC to configure sender reputation
- Use the Shell to configure sender reputation

Use the EMC to configure sender reputation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the Edge server you want to configure and then select the **Anti-spam** tab in the work pane.
3. Right-click **Sender Reputation** and then select **Properties**.
4. The **General** tab displays the following information about the Sender Reputation feature.
   - **Status** Shows whether the Sender Reputation feature is enabled or disabled.
   - **Modified** Shows the date and time when sender reputation properties were last modified.
   - **Description** Provides a brief description of the Sender Reputation feature.
5. Use the **Sender Reputation** tab to enable or disable detection of open proxy servers. A test for open proxy servers is one of the characteristics that

sender reputation evaluates to calculate the sender reputation level (SRL). The SRL is a number between 0 and 9 that predicts the probability that a sender is a spammer or an otherwise malicious user. When it's enabled, sender reputation filters all external messages that come through all Receive connectors on that computer. If sender reputation verifies that the proxy server is an open proxy server, it adjusts the SRL rating appropriately. By default, detection of open proxy servers is enabled.

- **Perform an open proxy test when determining sender reputation level** To disable detection of open proxy servers, clear this check box. To enable the detection of open proxy servers, select the check box.

6. Use the **Action** tab to set the threshold for sender blocking based on SRL. The SRL block threshold defines the SRL value that must be exceeded for sender reputation to block a sender. By default, the SRL value is set at 7. Before you adjust the SRL value, you should monitor its effectiveness at the default level.
   - **Sender Reputation Level Block Threshold** Drag the slider to set the SRL block threshold.
   - **Threshold Action** Type or select the number of hours that the sender is put on the IP Block list if the SRL block threshold is exceeded. The value must be between 0 to 48 hours.

Use the Shell to configure sender reputation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

You use the **Set-SenderReputationConfig** cmdlet to configure sender reputation options for your organization.

The following example configures sender reputation to perform an open proxy test for determining sender confidence:

```
Set-SenderReputationConfig -OpenProxyDetectionEnabled $true
```

The following example configures sender reputation to add the IP addresses of hosts that fail the open proxy test to the IP Block List. When you use this parameter, you must also set the *OpenProxyDetectionEnabled* parameter to `$true`:

```
Set-SenderReputationConfig -SenderBlockingEnabled $true -OpenProxyDetectionEnable
```

The following example sets the SRL block threshold to 6 and configures sender reputation to add offending senders to the IP Block List for 36 hours:

```
Set-SenderReputationConfig -SrlBlockThreshold 6 -SenderBlockingPeriod 36
```

For detailed syntax and parameter information, see Set-SenderReputationConfig.

1.7.2.10.20 Configure Outbound Access for Detection of Open Proxy Servers for Sender Reputation

Configure Outbound Access for Detection of Open Proxy Servers for Sender Reputation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to configure outbound access for the detection of open proxy servers for sender reputation.

Looking for other management tasks related to managing anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Prerequisites

- **Configuring firewall ports** If you've enabled the detection of open proxy servers on sender reputation, you may have to perform additional configuration to enable sender reputation to traverse any firewalls that are between the Edge Transport server and the Internet. The open proxy detection test uses many protocols to test for open proxy servers. The following table lists the ports that must be opened outbound for sender reputation.

Protocols	Ports
SOCKS4, SOCKS5	1081, 1080
Wingate, Telnet, Cisco	23
HTTP CONNECT, HTTP POST	6588, 3128, 80

- **Configuring sender reputation to use a specific proxy server** If your organization uses a proxy server to manage outbound traffic through a firewall, you must configure sender reputation to use the proxy server. Sender reputation must have outbound connectivity to the Internet to detect open proxy servers. You must specify the proxy server name, type, and port number that sender reputation will use to access the Internet.
- **Review** Understanding Anti-Spam and Antivirus Functionality You need to understand the general strategy for configuring all anti-spam agents so that they work together efficiently for your organization.
- **Read** Configure Sender Reputation Properties You need to understand how to configure sender reputation properties.

Use the Shell to configure outbound access for detection of open proxy servers for sender reputation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure outbound access for detection of open proxy servers for sender reputation.

To successfully configure sender reputation to detect open proxy servers, you must provide the following information:

- The name of your organization's proxy server.
- The port number for your organization's proxy server.
- The type of proxy server that your organization runs.

To configure outbound access for the detection of open proxy servers, use the following

syntax.

```
Set-SenderReputationConfig -ProxyServerName <String> -ProxyServerPort <Int32> -Pr
```

This example configures sender reputation to use the open proxy server SERVER01 that uses an HTTP CONNECT protocol type with 80 as its server port.

```
Set-SenderReputationConfig - ProxyServerName SERVER01 -ProxyServerPort 80 -ProxyS
```

For detailed syntax and parameter information, see Set-SenderReputationConfig.

1.7.2.10.21 Configure Safelist Aggregation

Configure Safelist Aggregation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-28*

In Microsoft Exchange Server 2010, *safelist aggregation* refers to anti-spam functionality shared across Microsoft Outlook and Exchange. This functionality collects data from the anti-spam Safe Recipients Lists, Safe Senders Lists, Blocked Senders Lists, and contact data that Outlook users configure, and makes this data available to the anti-spam agents on the computer that has the Edge Transport server role installed. Safelist aggregation can help reduce the instances of false-positives in anti-spam filtering performed by the Edge Transport server.

This topic provides an overview about how to configure safelist aggregation. To learn more about safelist aggregation, see Understanding Safelist Aggregation.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Use the Shell to configure mailbox safelist collection limits

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

You can't use the EMC to configure mailbox safelist collection limits.

You can configure the maximum number of safe senders and blocked senders a user can configure for each user. You use the **Set-Mailbox** cmdlet to configure these limits. By default, users can configure up to 5,000 safe senders and 500 blocked senders. Typically, it isn't necessary to modify these limits.

This example configures the mailbox john@contoso.com to have a maximum of 2,000 safe senders and 200 blocked senders.

```
Set-Mailbox john@contoso.com -MaxSafeSenders 2000 -MaxBlockedSenders 200
```

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to run the Update-Safelist command

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam" entry in the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

You can't use the EMC to run the **Update-Safelist** command.

In Exchange 2010, safelist aggregation is done automatically; therefore, you no longer need to schedule or manually run the **Update-Safelist** cmdlet. However, you may still want to run this cmdlet when you're testing safelist aggregation.

The **Update-SafeList** cmdlet reads the safelist collection from the Microsoft Outlook user mailbox, hashes each entry, sorts the entries for easy search, and then converts the hash to a binary attribute. Finally, the command compares the binary attribute created to any value stored on the attribute. If the two values are identical, the command doesn't update the user attribute value with the safelist aggregation data.

Be mindful of the network and replication traffic that may be generated when you run this command. If you run the command on multiple mailboxes where safelists are heavily used, this may generate a significant amount of traffic. We recommend that if you run the command on multiple mailboxes, you should run the command during off-peak, non-business hours.

Important:

Safelist aggregation data contains both the user's Safe Senders List and the user's Safe Recipients List. When you use the **Update-Safelist** cmdlet, you can specify whether you update the Safe Senders List or the Safe Recipients List, or both. However, only Safe Senders List data is used by the safelist aggregation feature; the safelist aggregation feature doesn't act on Safe Recipients List data. Therefore, to reduce storage and replication in Active Directory, we don't recommend running the **Update-Safelist** cmdlet with the *Type* parameter set to the `SafeRecipients` or `Both` values. The default value for the *Type* parameter is `SafeSenders`. Safe sender data is used by the safelist aggregation feature.

Important:

Microsoft Exchange Server 2010 provides functionality that allows you to specify whether to include the safe domain data for the anti-spam agents on the Edge Transport server by using the **Update-Safelist** cmdlet. In most cases, we don't recommend that you include domains because users may include the domains of large Internet service providers (ISP), which could unintentionally provide addresses that may be used or spoofed by spammers.

This example writes the safe senders list for the mailbox john@contoso.com to Active Directory.

```
Update-Safelist -Identity john@contoso.com -Type SafeSenders
```

For detailed syntax and parameter information, see Update-SafeList.

Options available in the msexchangemailboxassistants.exe.config

file

To activate the options to include safe domains, or to change the maximum values for the default settings, you must change the msexchangemailboxassistants.exe.config file. Specifically, the following settings and values can be changed in the **appsettings** section of the msexchangemailboxassistants.exe.config file:

Setting	Value
IncludeSafeDomains	The value for this setting can be True or False.
UpdateInterval	By default, the value for this setting is 15 minutes. This setting can have a value from 15 minutes through 1 day.
TestUpdateInterval	TestUpdateInterval is used in test environments. This setting can have a value from 10 seconds through 1 hour.
MaxSafeSenders	3*1024
MaxSafeRecipients	2*1024
MaxBlockedSenders	By default, the value for this setting is 500. The maximum value is 1000.

For example, the settings in the **appsettings** section of the msexchangemailboxassistants.exe.config file may be as follows:

```
<configuration>
  <runtime>
    <gcConcurrent enabled="false" />
    <generatePublisherEvidence enabled="false" />
  </runtime>
  <appSettings>
        <add key="IncludeSafeDomains" value="true" />
</appSettings>
</configuration>
```

Verify safelist aggegation

You may need to verify that safelist aggregation when you first deploy your Edge Transport servers and configure EdgeSync replication, or when you're troubleshooting. Typically, you need to verify the following:

- Make sure that the safelist aggregation data is being replicated by the EdgeSync service.
- Make sure that content filtering is enabled.
- Verify the safelist aggregation functionality using a test message

The following sections provide step by step instructions for each scenario:

Use AD LDS to verify EdgeSync replication of safelist aggregation data

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

You can view the user objects in the Active Directory Lightweight Directory Services (AD LDS) instance on the Edge Transport server to verify that the safelist collection data is updated for the user objects and that the Microsoft Exchange EdgeSync service has

replicated the data to the AD LDS instance.

There are three safelist collection attributes for each user object:

- **msExchSafeRecipientsHash** This attribute stores the hash of the Safe Recipients List collection for the user.
- **msExchSafeSendersHash** This attribute stores the hash of the Safe Senders List collection for the user.
- **msExchBlockedSendersHash** This attribute stores the hash of the Blocked Senders List collection for the user.

If a hexadecimal string, such as `0xac 0xbd 0x03 0xca`, is present on the attribute, the user object was updated. If the attribute has a value of `<Not Set>`, the attribute wasn't updated.

You can search for and view the attributes by using the AD LDS Active Directory Service Interfaces (ADSI) Edit snap-in.

Verify that content filtering is enabled

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

The safelist aggregation feature relies on content filtering to recognize the senders on an Outlook user's Safe Senders List or Blocked Senders List. Verify that content filtering is enabled on each Edge Transport server on which the anti-spam and antivirus features are running. By default, content filtering is enabled.

Use the EMC to verify that content filtering is enabled

1. In the console tree, click **Edge Transport**.
2. In the result pane, click the **Anti-spam** tab, click **Content Filtering**, and then in the action pane, click **Enable**.

Use the Shell to verify that content filtering is enabled

This example verifies whether content filtering is enabled.

```
Get-ContentFilterConfig | Format-List Enabled
```

If the output shows the *Enabled* parameter to be `True`, content filtering is enabled. If it isn't, use the following command to enable content filtering.

```
Set-ContentFilterConfig -Enabled:$true
```

For detailed syntax and parameter information, see the Get-ContentFilterConfig or Set-ContentFilterConfig topics.

Use a message to verify that safelist aggregation is functioning

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" and "EdgeSync" entries in the Transport Permissions topic.

To test whether safelist aggregation is functioning, you need to send a message, which would be blocked by content filtering, from a sender marked as a safe sender. If safelist aggregation is functioning, the message should arrive in your Outlook Inbox.

1. Create an e-mail account by using a free Web-based e-mail provider like Hotmail.
2. Add that account to your Safe Senders List in Outlook.
3. Use the **Update-SafeList** cmdlet to have the safelist collection from that mailbox copied to Active Directory.
4. Run the **Start-EdgeSynchronization** cmdlet to force EdgeSync replication.

This will replicate the updated data to the Edge Transport servers. For detailed steps, see Force EdgeSync Synchronization.
5. Add a specific word as a blocked phrase to your content filtering configuration. For detailed steps, see Configure Content Filtering Properties.
6. From the Hotmail account you created in step 1, send a message to your Exchange mailbox that includes the blocked phrase you configured in step 5.

1.7.2.10.22 View Anti-Spam Stamps in Outlook 2010 and Outlook 2007

View Anti-Spam Stamps in Outlook 2010 and Outlook 2007

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Microsoft Outlook 2010 and Office Outlook 2007 to view the anti-spam stamps applied to an e-mail message. Anti-spam stamps are functionality in Microsoft Exchange Server 2010 that helps the messaging administrator diagnose spam-related problems by applying diagnostic metadata, or stamps, such as sender-specific information, puzzle validation results, and content filtering results, to messages as the messages pass through the anti-spam features that filter inbound messages from the Internet.

Looking for other management tasks related to managing anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

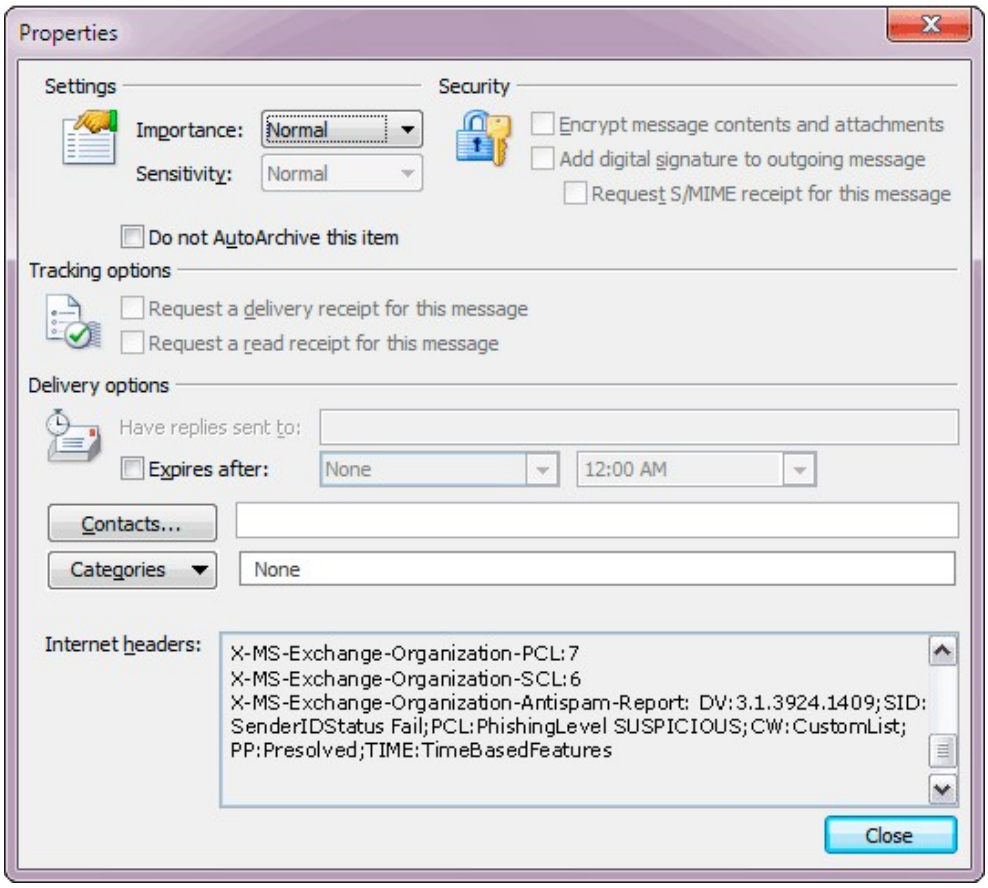
Prerequisites

- You have a mailbox to which you have owner rights.
- You have received messages to this mailbox from the Internet.
- You have reviewed Managing Anti-Spam and Antivirus Features.
- You have read Understanding Anti-Spam Stamps.

Use Outlook 2010 to view anti-spam stamps

The user account you use needs to be assigned Owner permissions on the mailbox before you can perform this procedure.

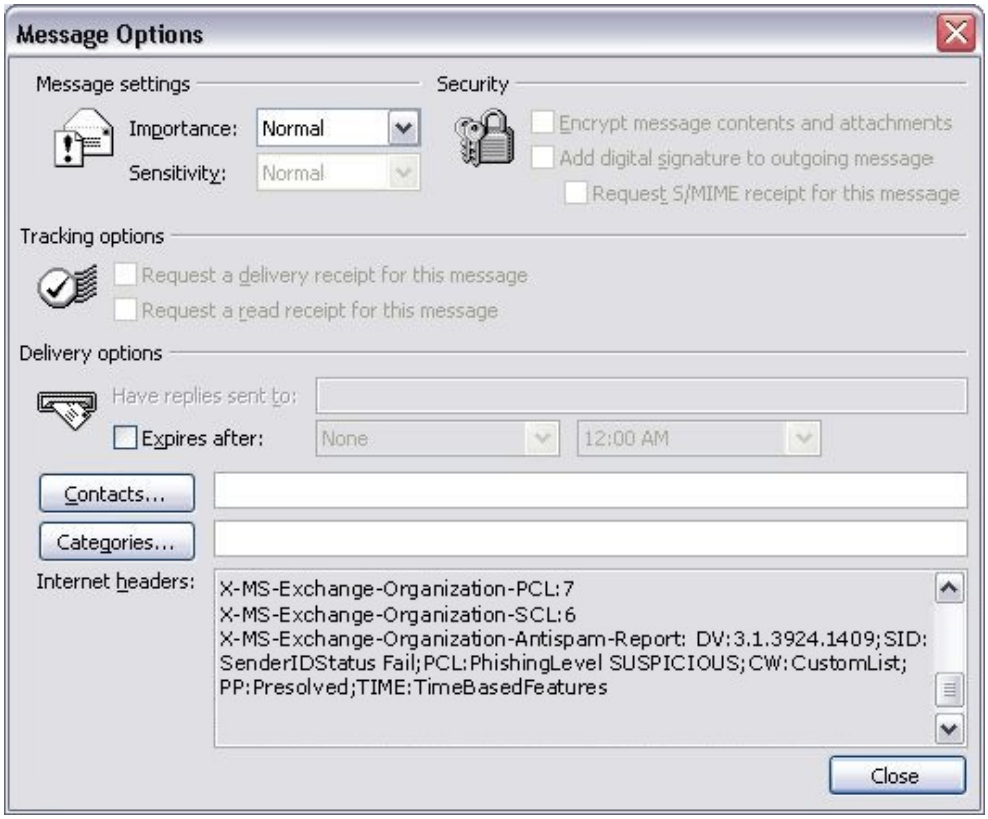
1. In Outlook 2010, on a client computer, in the **Mail** view, double-click a message to open it.
2. In the **Tags** section of the ribbon toolbar, click the **Options** icon to display the message **Properties** dialog box.
3. In the **Properties** dialog box, in the **Internet headers** section, use the scroll bar to view the anti-spam stamps as shown in the following figure.



Use Outlook 2007 to view anti-spam stamps

The user account you use needs to be assigned Owner permissions on the mailbox before you can perform this procedure.

1. In Outlook 2007, on a client computer, in the **Mail** view, double-click a message to open it.
2. On the **Message** tab, in the **Options** group, click **Message Options**.
3. In the **Message Options** dialog box, in the **Internet headers** section, use the scroll bar to view the anti-spam stamps as shown in the following figure.



1.7.2.10.23 Enable Anti-Spam Functionality on a Hub Transport Server

Enable Anti-Spam Functionality on a Hub Transport Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In some small organizations, it may make sense to run Microsoft Exchange Server 2010 anti-spam features on Hub Transport servers. For example, some organizations may not have enough e-mail volume to justify the cost of installing and maintaining a full perimeter network together with an Edge Transport server. You can enable Exchange anti-spam functionality on Hub Transport servers.

Important:

It isn't a best practice to run anti-spam functionality on the Hub Transport server. We recommend that you run anti-spam features on the Edge Transport server at the perimeter of your organization. Only run anti-spam features on the Hub Transport server if you haven't deployed an Edge Transport server.

To install and enable the anti-spam features on a Hub Transport server, you must run the Install-AntispamAgents.ps1 script. This script is installed when you run Exchange Setup. After you run the script, you must restart the Microsoft Exchange Transport service to finish the installation of the following anti-spam features:

- Connection filtering
- Content filtering
- Sender ID
- Sender filtering
- Recipient filtering
- Sender reputation

Notice that attachment filtering is an antivirus feature that isn't enabled or installed. Attachment filtering only runs on the Edge Transport server. However, the file filtering functionality that's provided by Microsoft Forefront Protection for Exchange Server includes advanced features that are unavailable in the default Attachment Filter agent that's included with Microsoft Exchange Server 2010 Standard Edition. Forefront Protection for Exchange Server is fully supported on the Hub Transport server role.

Important:

Most Exchange 2010 documentation doesn't refer to the anti-spam features in the context of the Hub Transport server. Therefore, as you read documentation about how to configure, manage, and maintain anti-spam features, remember that all functionality that's documented in the context of the Edge Transport server is also available on the Hub Transport server, unless specifically noted otherwise.

Looking for other management tasks related to managing anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Enable anti-spam functionality on a Hub Transport server

After you run the Install-AntispamAgents.ps1 script, restart the Microsoft Exchange Transport service, and set the *InternalSMTPServers* parameter.

Run the Install-AntispamAgents.ps1 script

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

1. Run the following command from the %system drive%/Program Files\Microsoft \Exchange Server\V14\Scripts folder.

```
.\install-AntispamAgents.ps1
```

2. After the script has run, restart the Microsoft Exchange Transport service by running the following command.

```
Restart-Service MSExchangeTransport
```

Use the Shell to set the InternalSMTPServers parameter

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport configuration" entry in the Transport Permissions topic.

You must specify all internal SMTP servers on the transport configuration object in Active Directory forest before you run connection filtering. Specify the internal SMTP servers by using the *InternalSMTPServers* parameter on the **Set-TransportConfig** cmdlet.

Important:

For all anti-spam features to work correctly, you must have at least one IP address of an internal SMTP server set on the *InternalSMTPServers* parameter on the **Set-TransportConfig** cmdlet. If the Hub Transport server on which you're running the anti-spam features is the only SMTP server in your organization, enter the IP address of that computer.

This example adds the internal SMTP server addresses 10.0.1.10 and 10.0.1.11 to the transport configuration of your organization.

```
Set-TransportConfig -InternalSMTPServers 10.0.1.10,10.0.1.11
```

For detailed syntax and parameter information, see Set-TransportConfig.

1.7.2.10.24 File-Level Antivirus Scanning on Exchange 2010

File-Level Antivirus Scanning on Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-03*

This topic describes the effects of file-level antivirus programs on computers that are running Microsoft Exchange Server 2010. If you implement the recommendations described in this topic, you can help enhance the security and health of your Exchange organization.

File-level scanners are frequently used. However, if they are configured incorrectly, they can cause problems in Exchange 2010. There are two types of file-level scanners:

- *Memory-resident file-level scanning* refers to a part of file-level antivirus software that is loaded in memory at all times. It checks all the files that are used on the hard disk and in computer memory.
- *On-demand file-level scanning* refers to a part of file-level antivirus software that you can configure to scan files on the hard disk manually or on a schedule. Some versions of antivirus software start the on-demand scan automatically after virus signatures are updated to make sure that all files are scanned with the latest signatures.

The following problems may occur when you use file-level scanners with Exchange 2010:

- File-level scanners may scan a file when the file is being used or at a scheduled interval. This can cause the scanners to lock or quarantine an Exchange log or a database file while Microsoft Exchange tries to use the file. This behavior may cause a severe failure in Microsoft Exchange and may also cause -1018 errors.
- File-level scanners don't provide protection against e-mail viruses, such as the Storm Worm. Storm Worm was a backdoor Trojan horse virus that propagated itself through e-mail messages. The worm joined the infected computer to a botnet, where the computer was used to send spam e-mail messages in periodic bursts. Such viruses can affect the performance of the computer and the network that it is attached to.

Recommendations for Using File-Level Scanning with Exchange 2010

If you're deploying file-level scanners on Exchange 2010 servers, make sure that the appropriate exclusions, such as directory exclusions, process exclusions, and file name extension exclusions, are in place for both memory-resident and file-level scanning. This section describes directory exclusions, process exclusions, and file name extension exclusions for each server or server role.

Directory Exclusions

You must exclude specific directories for each Exchange server or server role on which you run a file-level antivirus scanner. This section describes the directories that you should exclude from file-level scanning for each server or server role.

Mailbox server role

- Exchange databases, checkpoint files, and log files. By default, these are located in sub-folders under the %ExchangeInstallPath%\Mailbox folder. You can obtain the directory location by running the following commands in the Exchange Management Shell:
  - To determine the location of a mailbox database, transaction log, and checkpoint file, run the following command: `Get-MailboxDatabase -server <servername>| format-list *path*`
- Database content indexes. By default, these are located in the same folder as the database file.
- Group Metrics files. By default, these files are located in the %ExchangeInstallPath%\GroupMetrics folder.
- General log files, such as message tracking and calendar repair log files. By default, these files are located in subfolders under the %ExchangeInstallPath%\TransportRoles\Logs folder and %ExchangeInstallPath%\Logging folder. To determine the log paths being used, run the following command in the Exchange Management Shell: `Get-MailboxServer <servername> | format-list *path*`
- The Offline Address Book files. By default, these are located in subfolders under the %ExchangeInstallPath%\ExchangeOAB folder
- IIS system files in the %SystemRoot%\System32\Inetsrv folder
- The temporary folder that is used with offline maintenance utilities, such as Eseutil.exe. By default, this folder is the location where the .exe file is run from. However, you can configure where you perform the operation when you run the utility.
- The Mailbox database temporary folder: %ExchangeInstallPath%\Mailbox\MDBTEMP
- Any Exchange-aware antivirus program folders

Mailbox server that is a member of a Database Availability Group

All the items listed in the Mailbox server role list and in the %Winnt%\Cluster folder.

Witness server

- The witness directory files. These are located on another server in the environment, typically a Hub Transport server. By default, these files are located in \\%SystemDrive%:\DAGFileShareWitnesses\<DAGFQDN> and default share (<DAGFQDN>) on that server. For more information about a database availability group (DAG) and witness servers, see Managing Database Availability Groups.

Hub Transport server role

- General log files, for example, message tracking and connectivity logs. By default, these files are located in subfolders under the %ExchangeInstallPath%\TransportRoles\Logs folder. To determine the log paths being used, run the following command in the Exchange Management Shell: `Get-TransportServer <servername>| format-list *logpath*,*tracingpath*`
- Pickup and Replay message directory folders. By default, these folders are located under the %ExchangeInstallPath%\TransportRoles folder. To determine the paths being used, run the following command in the Exchange Management Shell: `Get-TransportServer <servername>| fl *dir*path*`
- The transport server role queue database, checkpoint, and log files. By default, these are located in the %ExchangeInstallPath%\TransportRoles\Data\Queue folder. For more information, see Managing Transport Queues.
- The transport server role Sender Reputation database, checkpoint, and log files. By default, these are located in the %ExchangeInstallPath%\TransportRoles\Data\SenderReputation folder.

- The transport server role IP filter database, checkpoint, and log files. By default, these are located in the %ExchangeInstallPath%\TransportRoles\Data\IpFilter folder.
- The temporary folders that are used to perform conversions:
  - By default, content conversions are performed in the Exchange server's TMP folder.
  - By default, OLE conversions are performed in %ExchangeInstallPath%\Working\OleConvertor folder.
- Any Exchange-aware antivirus program folders

Edge Transport server role

- The Active Directory Lightweight Directory Service database (AD LDS) and log files. By default, these are located in the %ExchangeInstallPath%\TransportRoles\Data\Adam folder. For more information about AD LDS database files, see Modify AD LDS Configuration.
- General log files, for example message tracking. By default, these files are located in subfolders under the %ExchangeInstallPath%\TransportRoles\Logs folder. To determine the log paths being used, run the following command in the Exchange Management Shell: `Get-TransportServer <servername> | format-list *logpath*,*tracingpath*`
- The Pickup and Replay message folders. By default, these are located under the %ExchangeInstallPath%\TransportRoles folder. To determine the log paths being used, run the following command in the Exchange Management Shell: `Get-TransportServer <servername>| format-list *dir*path*`
- The transport server role queue database, checkpoint, and log files. By default, these are located in the %ExchangeInstallPath%\TransportRoles\Data\Queue folder. For more information about transport server queues, see Managing Transport Queues.
- The transport server role Sender Reputation database, checkpoint, and log files. By default, these are located in the %ExchangeInstallPath%\TransportRoles\Data\SenderReputation folder
- The transport server role IP filter database, checkpoint, and log files. By default, these are located in the %ExchangeInstallPath%\TransportRoles\Data\IpFilter folder
- The temporary folders that are used to perform conversions:
  - By default, content conversions are performed in the server's TMP folder.
  - By default, OLE conversions are performed in %ExchangeInstallPath%\Working\OleConvertor folder.
- Any Exchange-aware antivirus program folders

Client Access server role

- For servers using Internet Information Services (IIS) 7.0, the compression folder that is used with Microsoft Outlook Web App. By default, the compression folder for IIS 7.0 is located at %SystemDrive%\inetpub\temp\IIS Temporary Compressed Files.
- For servers using IIS 6.0, the compression folder that is used with Microsoft Outlook Web App. By default, the compression folder for IIS 6.0 is located at %systemroot%\IIS Temporary Compressed Files. For more information about possible errors resulting from scanning the IIS compression folder, see Microsoft Knowledge Base article 817442, A 0-byte file may be returned when compression is enabled on a server that is running IIS.
- IIS system files in the %SystemRoot%\System32\Inetsrv folder
- Inetpub\logs\logfiles\w3svc
- The Internet-related files that are stored in the sub-folders of the %ExchangeInstallPath%\ClientAccess folder
- For servers that have protocol logging enabled for POP3 or IMAP4, the following folders:
  - POP3 folder: %ExchangeInstallPath%\Logging\POP3
  - IMAP4 folder: %ExchangeInstallPath%\Logging\IMAP4

- The temporary folders that are used to perform conversions:
  - By default, content conversions are performed in the server's TMP folder.
  - By default, OLE conversions are performed in %ExchangeInstallPath% \Working\OleConvertor folder.

Unified Messaging server role

- The grammar files for different locales, for example en-EN or es-ES. By default, these are stored in the subfolders in the %ExchangeInstallPath% \UnifiedMessaging\grammars folder.
- The voice prompts, greetings and informational message files. By default, these are stored in the subfolders in the %ExchangeInstallPath% \UnifiedMessaging\Prompts folder
- The voicemail files that are temporarily stored in the %ExchangeInstallPath %\UnifiedMessaging\voicemail folder.
- The temporary files generated by Unified Messaging. By default, these are stored in the %ExchangeInstallPath%\UnifiedMessaging\temp folder.

Microsoft Forefront Protection for Exchange

- The Forefront installation folder. By default, this is %Program Files (x86)% \Microsoft Forefront Protection for Exchange Server\.
- Any archived messages. By default, these are stored in the %Program Files (x86)%\Microsoft Forefront Protection for Exchange Server\Data\Archive folder.
- Any quarantined files. By default, these are stored in the %Program Files (x86)%\Microsoft Forefront Protection for Exchange Server\Data \Quarantine folder.
- The antivirus engine files. By default, these are stored in the subfolders of %Program Files (x86)%\Microsoft Forefront Protection for Exchange Server \Data\Engines\x86 folder or the %Program Files (x86)%\Microsoft Forefront Protection for Exchange Server\Data\Engines\amd64 folder.
- The configuration files. By default, these are stored in the %Program Files (x86)%\Microsoft Forefront Protection for Exchange Server\Data folder.

Process Exclusions

Many file-level scanners now support the scanning of processes, which can adversely affect Microsoft Exchange if the incorrect processes are scanned. Therefore, you should exclude the following processes from file-level scanners.

Cdb.exe	Microsoft.Exchange.Search.Exsearch.exe
Cidaemon.exe	Microsoft.Exchange.Servicehost.exe
Clussvc.exe	MSExchangeADTopologyService.exe
Dsamain.exe	MSExchangeFDS.exe
Microsoft.Exchange.EdgeCredentialSvc.exe	MSExchangeMailboxAssistants.exe
EdgeTransport.exe	MSExchangeMailboxReplication.exe
ExFBA.exe	MSExchangeMailSubmission.exe
GalGrammarGenerator.exe	MSExchangeRepl.exe
Inetinfo.exe	MSExchangeTransport.exe
Mad.exe	MSExchangeTransportLogSearch.exe
Microsoft.Exchange.AddressBook.Service.exe	MSExchangeThrottling.exe
Microsoft.Exchange.AntispamUpdateSvc.exe	Msftefd.exe

Microsoft.Exchange.ContentFilter.Wrapper.exe	Msftesql.exe
Microsoft.Exchange.EdgeSyncSvc.exe	OleConverter.exe
Microsoft.Exchange.Imap4.exe	Powershell.exe
Microsoft.Exchange.Imap4service.exe	SESWorker.exe
MSExchangeMailboxAssistants.exe	SpeechService.exe
Microsoft.Exchange.Monitoring.exe	Store.exe
Microsoft.Exchange.Pop3.exe	TranscodingService.exe
Microsoft.Exchange.Pop3service.exe	UmService.exe
Microsoft.Exchange.ProtectedServiceHost.exe	UmWorkerProcess.exe
Microsoft.Exchange.RPCClientAccess.Service.exe	W3wp.exe

If you're also deploying Forefront Protection for Exchange Server, exclude the following processes.

Adonavsvc.exe	FscStatsServ.exe
FscController.exe	FscTransportScanner.exe
FscDiag.exe	FscUtility.exe
FscExec.exe	FsEmailPickup.exe
FscImc.exe	FssaClient.exe
FscManualScanner.exe	GetEngineFiles.exe
FscMonitor.exe	PerfmonitorSetup.exe
FscRealtimeScanner.exe	ScanEngineTest.exe
FscStarter.exe	SemSetup.exe

File Name Extension Exclusions

In addition to excluding specific directories and processes, you should exclude the following Exchange-specific file name extensions in case directory exclusions fail or files are moved from their default locations.

Application-related extensions

- .config
- .dia
- .wsb

Database-related extensions

.chk	.jrs	.log
.edb	.jsl	.que

Offline address book-related extensions

- .lzx

Content Index-related extensions

.ci	.wid	.001

.dir	.000	.002

Unified Messaging-related extensions

- .cfg
- .grxml

GroupMetrics

- .dsc
- .bin
- .xml

Forefront Protection for Exchange Server–related extensions

.avc	.dt	.lst
.cab	.fdb	.mdb
.cfg	.fdm	.ppl
.config	.ide	.set
.da1	.key	.v3d
.dat	.klb	.vdb
.def	.kli	.vdm

The file name extensions listed for Forefront Protection for Exchange Server are the signature files from various antivirus directory engines. In most cases, these file name extensions don't change. However, file name extensions may be added in the future as third-party antivirus vendors update their antivirus signature files.

1.7.2.10.25 Configure Proxy Settings for WinHTTP

Configure Proxy Settings for WinHTTP

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Microsoft Exchange Server 2010, several server roles rely on the underlying Microsoft Windows HTTP Services (WinHTTP) to manage all HTTP and HTTPS traffic. Both Hub Transport servers and Edge Transport servers may use HTTP to access filter updates for the Microsoft Exchange Anti-spam Update service and the Microsoft Forefront Protection for Exchange Server anti-spam update service, and for certificate revocation list (CRL) validation. If your organization supports smart card authentication for clients to connect to Exchange, and the CRL for the presented client certificates is hosted outside your firewall, Client Access servers need to be configured for proxy servers to make outbound requests to perform CRL validation. Additionally, Exchange organizations that have their archives hosted by Windows Live require that their Client Access and Mailbox servers are able to make outbound HTTP requests to Microsoft datacenters.

In most organizations, a proxy server is used for HTTP and HTTPS communications with destinations on the Internet. If your organization uses a proxy server and your Exchange transport servers aren't configured to use the proxy server for HTTP and HTTPS, you must configure them so that HTTP-enabled CRL validation works.

The simplest way to configure WinHTTP is to use the Netsh.exe tool. Netsh.exe is a command-line tool included in the %System32% directory on all computers running Windows Server 2008. You can use Netsh.exe to set and view WinHTTP configurations. All the WinHTTP-related commands are included under the WinHTTP context within the Netsh.exe tool.

For more information about how to use the Netsh.exe tool, see How to Use the Netsh.exe Tool and Command-Line Switches.

Looking for other management tasks related to anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Use Netsh.exe to configure proxy settings for WinHTTP

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

To navigate to the WinHTTP context, open an administrator Command Prompt window, type **netsh**, and then type **winhttp**.

```
C:\Windows\system32>netsh
netsh>winhttp
netsh winhttp>
```

You use the **set proxy** command to configure the proxy settings. You can type the command followed by a question mark to see the syntax for this command.

```
netsh winhttp>set proxy /?
```

This example specifies that HTTP servers and HTTPS servers are accessed through the proxy server proxy_server, except for host names that don't contain a period specified by the "*<local>*" argument.

```
netsh winhttp>set proxy proxy_server "<local>"
```

This example imports proxy information used by Internet Explorer by using the **import proxy** command.

```
netsh winhttp>import proxy source=ie
```

This examples uses the **reset proxy** command to reset the WinHTTP proxy to DIRECT.

```
netsh winhttp>reset proxy
```

Even if you aren't running a proxy server, we recommend that you use Netsh.exe to check whether a previous proxy has been set. By running the tool without arguments, this example shows the current configuration.

```
netsh winhttp>show proxy
```

Important:

You must restart the Microsoft Exchange Transport service and the Microsoft Exchange Anti-spam Update service after you have made configuration changes to WinHTTP.

1.7.2.10.26 Make the SCL Value Available to Edge Transport Rules

Make the SCL Value Available to Edge Transport Rules

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to make the spam confidence level (SCL) value on messages available for processing in transport rules that run on computers that have the Edge Transport server role installed.

Looking for other management tasks related to managing anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Caution:
The following procedure stops and starts the Microsoft Exchange Transport service on the local Edge Transport server. Mail that flows through this Edge Transport server isn't delivered while the Microsoft Exchange Transport service is stopped.

Use the Shell to modify the priority of the Content Filter agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport agents" entry in the Transport Permissions topic.

Note:
You can't use the EMC to modify the priority of the Content Filter agent.

This example sets the priority value of the Content Filter agent to 3. Because the Edge Rule agent by default uses priority value 3, its priority value is increased to 4.

1. Use the Shell to set the priority value of the Content Filter agent to 3.

```
Set-TransportAgent "Content Filter Agent" -Priority 3
```

2. Stop the Microsoft Exchange Transport service.

```
Net Stop MSExchangeTransport
```

3. Start the Microsoft Exchange Transport service.

```
Net Start MSExchangeTransport
```

For detailed syntax and parameter information, see Set-TransportAgent.

Use the Shell to verify transport agent priority order

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport agents" entry in the Transport Permissions topic.

Note:
You can't use the EMC to verify transport agent priority order.

You can verify the transport agent priority order by sending a test message through the Edge Transport server that you just configured. Then you can use the **Get-TransportPipeline** cmdlet to view the transport agent priority order. You must send a message through the Edge Transport server because the **Get-TransportPipeline** cmdlet retrieves information about the transport pipeline that's built dynamically every time a message is sent.

This example verifies the transport agent priority order.

1. Send a message through the Edge Transport server that you just configured.
2. Run the following command.

```
Get-TransportPipeline
```

The output produced by this procedure will resemble the following example. In the following example, the Content Filter agent is listed before the Edge Rule agent on the OnEndOfData SMTP event. This indicates that the Content Filter agent is now being applied to messages before the Edge Rule agent on the OnEndOfData SMTP event.

```
Event           : OnConnectEvent
TransportAgents : {Connection Filtering Agent, Protocol Analysis Agent}
Event           : OnHeloCommand
TransportAgents : {}
Event           : OnEhloCommand
TransportAgents : {}
Event           : OnAuthCommand
TransportAgents : {}
Event           : OnEndOfAuthentication
TransportAgents : {}
Event           : OnMailCommand
TransportAgents : {Connection Filtering Agent, Sender Filter Agent}
Event           : OnRcptCommand
TransportAgents : {Connection Filtering Agent, Address Rewriting Inbound Agent,
                  Recipient Filter Agent}
Event           : OnDataCommand
TransportAgents : {}
Event           : OnEndOfHeaders
TransportAgents : {Connection Filtering Agent, Address Rewriting Inbound Agent,
                   Sender Id Agent, Sender Filter Agent, Protocol Analysis Agen
                  t}
Event           : OnEndOfData
TransportAgents : {Content Filter Agent, Edge Rule Agent, Protocol Analysis Age
                  nt, Attachment Filtering Agent}
Event           : OnHelpCommand
TransportAgents : {}
Event           : OnNoopCommand
TransportAgents : {}
Event           : OnReject
TransportAgents : {Protocol Analysis Agent}
Event           : OnRsetCommand
TransportAgents : {Protocol Analysis Agent}
Event           : OnDisconnectEvent
TransportAgents : {Protocol Analysis Agent}
Event           : OnSubmittedMessage
TransportAgents : {Address Rewriting Outbound Agent}
Event           : OnRoutedMessage
TransportAgents : {Address Rewriting Outbound Agent}
```

For detailed syntax and parameter information, see Get-TransportPipeline.

1.7.2.10.27 Manage Anti-Spam Agent Log Output

Manage Anti-Spam Agent Log Output

Transport > Managing Transport Servers > Managing Anti-Spam and Antivirus Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the EdgeTransport.exe.config file to manage the anti-spam agent log files. By default, Microsoft Exchange Server 2010 logs all anti-spam agent activity in the %programfiles%\Microsoft\Exchange Server\V14\TransportRoles\Logs\AgentLog directory. To filter the anti-spam agent logs, use the **Get-AgentLog** cmdlet. For more information, see Get-AgentLog.

The default configuration of the agent log files are as follows:

- Maximum size of the agent log directory: 250 megabytes (MB)
- Maximum size of a single agent log file: 10 MB
- Maximum age of log files: 30 days

Looking for other management tasks related to managing anti-spam and antivirus features? Check out Managing Anti-Spam and Antivirus Features.

Modifying the EdgeTransport.exe.config File

All modifications of configuration options for managing agent log output must be made in the EdgeTransport.exe.config file that's located in the %programfiles%\Microsoft \Exchange Server\V14\Bin directory. The EdgeTransport.exe.config file is an XML application configuration file that's associated with the Microsoft Exchange Transport service. Changes that are saved to the EdgeTransport.exe.config file are applied after the Microsoft Exchange Transport service is restarted.

You can add new configuration options or modify existing configuration options in the `<appSettings>` section.

Agent Log Output Keys

Agent log output is managed by various keys in the EdgeTransport.exe.config file. By default, only the `AgentLogEnabled` key is present in the EdgeTransport.exe.config file. You must add all other keys. The following table explains each key in more detail.

Key	Value type	Description
`AgentLogEnabled`	System.Boolean	Valid values for this key are `true` or `false`. The default value is `true`.
`AgentLogMaxDirectorySize`	System.Int32	The value of this key specifies the maximum size, in bytes, of the AgentLog directory. When this value is exceeded, the oldest log file in the directory is deleted and a new log file is created. If this key isn't specified, the default value is 250 MB, or 262144000 bytes, which is determined as follows: 250×1,024×1,024.
`AgentLogMaxFileSize`	System.Int32	The value of this key specifies the maximum size, in bytes, of each log file in the directory. When a log file reaches the size specified, a new log file is created. If this key isn't specified, the default is 10 MB, or 10485760 bytes, which is

		determined as follows: 10×1024×1024.
AgentLogMaxAge	System.TimeSpan	The value of this key specifies the maximum age limit of a specified log file. When a log file exceeds the age limit, it's deleted. This key is of system type TimeSpan. The value of this key can be represented as a string in the format *d.hh:mm:ss.ff* where *d* is days, *hh* is hours, *mm* is minutes, *ss* is seconds, and *ff* is fractions of a second. If this key isn't specified, the default value is 30 days, or 30.00:00:00.00.

Add and configure the agent log output keys in the EdgeTransport.exe.config file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

This example adds and configures agent log output keys for the AgentLogEnabled key in the EdgeTransport.exe.config file.

1. On the Hub Transport server or Edge Transport server on which you want to manage the agent log output, open the EdgeTransport.exe.config in an ASCII text editor such as Notepad. The EdgeTransport.exe.config file is located in the %programfiles%\Microsoft\Exchange Server\V14\Bin directory.
2. Locate the AgentLogEnabled key. By default, the keys are listed in alphabetical order under <appsettings>.
3. Paste the following keys under the AgentLogEnabled key.

```
<add key="AgentLogMaxDirectorySize" value="system.int32" />
<add key="AgentLogMaxFileSize" value="system.int32" />
<add key="AgentLogMaxAge" value="system.timespan" />
```

4. Verify that the AgentLogEnabled key is set to true, and add values for the other keys.
5. When you have finished updating the EdgeTransport.exe.config file, save the file and close it.
6. You must restart the Microsoft Exchange Transport service before the configuration changes will take effect.

1.7.2.11 Managing Connectors

Managing Connectors

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-19*

Send Connectors

Create an SMTP Send Connector

Create Linked Connectors

Configure a Dedicated Send Connector for a Specific Domain

Configure Send Connector Properties

Enable or Disable a Send Connector

Remove a Send Connector

Receive Connectors

Create an SMTP Receive Connector

Configure Receive Connector Properties

Modify the Default SMTP Banner

Allow Anonymous Relay on a Receive Connector

Enable or Disable a Receive Connector

Remove a Receive Connector

Foreign Connectors

Create a Foreign Connector

View the Configuration of a Foreign Connector

Modify the Configuration of a Foreign Connector

Configure the Drop Directory

Enable or Disable a Foreign Connector

Remove a Foreign Connector

Configure the Pickup Directory

Configure the Replay Directory

Create an SMTP Send Connector

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Send connectors create a logical connection to remote e-mail systems and are responsible for outbound transmission of e-mail messages. If you use the EdgeSync process, it will configure the Send connectors required for mail flow to the Internet and to the Edge Transport servers in your Microsoft Exchange Server 2010 organization. If your organization requires a Send connector with specific configuration options, or if you don't use the EdgeSync process, you must manually configure Send connectors.

You can use the EMC or the Shell to create a Send connector for Exchange 2010.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to connectors? Check out Managing Connectors.

Prerequisites

You should determine the specific usage for the Send connector before you create it so you can correctly configure its properties. To learn more about Send connectors, see Understanding Send Connectors.

What Do You Want to Do?

- Use the EMC to create a Send connector
- Use the Shell to create a Send connector

Use the EMC to create a Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

1. Open the Exchange Management Console. Perform one of the following:
   - On a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the work pane, click the **Send Connectors** tab.
   - To create a Send connector on a Hub Transport server role, in the console tree, expand **Organization Configuration**, select **Hub Transport**, and then in the work pane, click the **Send Connectors** tab.
2. In the action pane, click **New Send Connector**. The New SMTP Send Connector wizard starts.

3. On the **Introduction** page, follow these steps:
   - In the **Name** field, type a meaningful name for this connector. Specify a name for the Send connector that helps you distinguish this Send connector from other Send connectors in your configuration.
   - In the **Select the intended use for this connector** field, select the usage

type for the connector. The usage type determines the default permission sets assigned on the connector and grants those permissions to trusted security principals. The following usage types are available:

Custom Select this option to create a customized connector to connect with systems that aren't servers running Exchange 2010.

Internal Internal Send connectors send e-mail to servers in your Exchange organization. This connector is configured to route e-mail to your internal Exchange servers as smart hosts.

Internet Internet Send connectors send e-mail to the Internet. This connector is configured to use Domain Name System (DNS) MX records to route e-mail.

Partner Partner Send connectors send e-mail to partner domains. This connector is configured to only allow connections to servers that authenticate with Transport Layer Security (TLS) certificates for SMTP domains included in the list of domain-secured domains. You can add domains to this list by using the *TLSSendDomainSecureList* parameter in the **Set-TransportConfig** command.

For more information about Send connector usage types, see Understanding Send Connectors.

- Click **Next**.

4. On the **Address space** page, specify an address space to which the Send connector sends mail.
   You can configure either an SMTP address space or a custom address space. Custom address spaces may only be configured on Send connectors that exist on Hub Transport servers. If you use a custom address space type, you must use a smart host to route e-mail.

Note:

Although you can configure custom address spaces on a Send connector, the Hub Transport server still uses SMTP as the transport mechanism to send messages to other messaging servers using this Send connector. To send messages to messaging servers that don't use SMTP as their primary transport mechanism, such as a third-party fax gateway server, you must use a Foreign connector. For more information about Foreign connectors, see Understanding Foreign Connectors.

To configure an address space, do the following:

- **Add** To specify an address space for which this Send connector is responsible, click **Add** or the drop-down arrow located next to **Add**. If you click **Add**, the address space type is SMTP. If you click the drop-down arrow located next to **Add**, you can select **SMTP Address Space** or **Custom Address Space**. For each new address space, you need to configure the following:
  - **Type** This field describes the address space that you enter in the **Address** field. If you clicked **Add**, this field is set to SMTP and is unavailable.
  - **Address** Specify the address space for the Send connector. If you entered **SMTP** or **X400** in the **Type** field, Exchange verifies the syntax of the address space that you enter. Exchange can't verify any other types of addresses; therefore, you need to make sure that you specify any custom addresses using the correct syntax. If you're entering an SMTP address, you can include the wildcard character (*) in the address space as defined in RFC 1035. For example, `*`, `*.com`, and `*.contoso.com` are permitted, but `*contoso.com` isn't permitted.
  - **Include all subdomains** This option is only available when you're specifying an SMTP address space. Select this option if

you also want to use this connector to route mail to all subdomains of the specified address space. If you entered an address space that contains the wildcard character, this option is automatically selected.

• **Cost** Use the address space cost to set the selection priority when more than one Send connector is configured for the same address space. During routing resolution, when the connector selection is made, the least cost routing path to the destination address space is selected. The valid input range is from 1 through 100.

- **Edit** To modify an existing address space in the address space list, select the address space, and then click **Edit**. You can configure the same options described for the **Add** button previously, with the exception of **Type**. You can't change the type of an existing address space.
- **Remove** To delete the domain name from the list of domains, select a domain name, and then click  .
- **Scoped send connector** By default, all Send connectors that you create can be used by all the Hub Transport servers in your Exchange organization. However, you can limit the scope of any Send connector so that it can be used only by other Hub Transport servers that exist in the same Active Directory site. To limit the scope of this Send connector, select **Scoped send connector**.

After you finish, click **Next**.

5. On the **Network settings** page, select how to send e-mail with the Send connector. The following options are available:
   - **Use domain name system (DNS) "MX" records to route mail automatically** This option is available only if you selected a usage type of **Custom**, **Partner**, or **Internet** in step 3. When you select this option, the Send connector uses DNS to resolve the IP address of the remote SMTP servers and route mail.
   - **Route mail through the following smart hosts** This option is available only if you selected a usage type of **Custom**, **Internal**, or **Internet** in step 3. Select this option to route all outbound mail to specific smart hosts instead of using DNS to resolve the IP addresses of remote SMTP servers. After you select this option, you can select the following:

     Add To add a smart host, click **Add**. You can specify either of the following options in the window that appears:

     ? **IP Address** Select this option to identify the smart host by IP address (for example: 192.168.100.1).

     ? **Fully qualified domain name (FQDN)** Select this option to identify the smart host by FQDN (for example, smarthost.contoso.com).

     Edit To edit an existing smart host, select the smart host, and then click **Edit**.

     Remove To remove an existing smart host, select the smart host, and then click  .
   - **Use the External DNS Lookup settings on the transport server** Select this check box if you want to use a specific list of external DNS servers instead of the DNS servers configured on the network adapters of the source servers configured for this Send connector.

     Important:

     Verify that you have configured the external DNS servers list by using the **Set-TransportServer** cmdlet, or by using the **External DNS Lookups** tab in the properties of the Hub Transport server object or the Edge Transport server object.

   After you finish, click **Next**.

6. On the Configure **smart host authentication settings** page, select the method used to authenticate to the smart host.
   By default, no authentication is used. To configure the smart host authentication settings, click **Change**. You can specify one of the following options in the window that appears:
   • **None** Select this option if the smart host is configured to accept anonymous connections.
   • **Basic Authentication** Select this option if the smart host requires Basic authentication. Basic authentication requires that you provide a user name and password. We strongly recommend that you use an encrypted connection if you're using Basic authentication, because the user name and password are sent in clear text. Select the **Basic Authentication over TLS** check box to enable encryption on the connection. Also, if you specify more than one smart host for this Send connector, all of the specified smart hosts must accept the same user name and password.
   • **Exchange Server Authentication** Select this option to authenticate to a smart host by using an Exchange authentication mechanism, such as TLS direct trust or TLS\Kerberos.
   • **Externally Secured (for example, with IPsec)** Select this option if the connection to the smart host is secured by external means, such as being physically secured over a private network or secured using Internet Protocol security (IPsec). When you select this option, you make an assertion of external security that can't be programmatically verified by Exchange.
   Click **Next**.

7. The **Source Server** page only appears on Hub Transport servers. By default, the Hub Transport server that you are currently working on is listed as a source server. To add a source server, click **Add**. In the **Select Hub Transport or Subscribed Edge Transport Server** dialog box, select the Hub Transport servers or the subscribed Edge Transport servers that will be used as the source server for sending messages to the address space that you provided in step 4. The list of source servers can contain all Hub Transport servers or all subscribed Edge Transport servers, but not a combination of both. After you finish adding additional source servers, click **OK**.
   To add more source servers, click **Add** and repeat this step.
   To remove an existing source server, select the source server, and then click  .

   Note:
   Removing a subscribed Edge Transport server from the list doesn't remove the Send connector from the Edge Transport server. It just stops the Microsoft Exchange EdgeSync service from propagating this Send connector configuration to that Edge Transport server.

   After you finish, click **Next**.

8. On the **New Connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Send connector by using the settings in the configuration summary, click **New**.

9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a Send connector

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

This command creates a Send connector.

```
New-SendConnector -Name <Connector Name> -AddressSpaces <Address Space> <Optional
```

This example creates a Send connector called `Subsidiary Send Connector` that has the following settings:

- Connector usage type is **Custom**.
- Connector sends messages to the SMTP address space Contoso.com and all subdomains. The address space cost is 5.
- Connector sends messages to the SMTP address space named Fabrikam.com and all subdomains. The address space cost is 8.
- E-mail is routed through a smart host at IP address 192.168.1.20.
- Maximum message size of 20 MB is allowed on this connector.

```
New-SendConnector -Name "Subsidiary Send Connector" -Usage Custom -AddressSpace "
```

For detailed syntax and parameter information, see New-SendConnector.

1.7.2.11.2 Create Linked Connectors

Create Linked Connectors

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to create linked connectors on a computer running Microsoft Exchange Server 2010 that has the Hub Transport server role or Edge Transport server role installed. A *linked connector* is a Receive connector linked to a Send connector. For linked connectors, the regular routing logic based on the destination domain is overridden. All messages received by the Receive connector are forwarded to the Send connector to which the Receive connector is linked. This scenario is useful when you want to send messages to a third-party anti-spam and antivirus service for processing, and then return the messages to the Exchange 2010 organization for delivery.

Looking for other management tasks related to connectors? Check out Managing Connectors.

Prerequisites

- Only one Receive connector can be linked to one Send connector.
- The Receive connector must exist before it can be linked to a Send connector.
- A linked Send connector must route messages to a smart host. You can use an IP address or the fully qualified domain name (FQDN) of the smart host to specify the smart host identity.

Linked Connector Scenario

This section describes a typical linked connector scenario on an Edge Transport server. The following table describes the Send connectors and Receive connectors in that scenario.

Send connectors and Receive connectors in a typical linked connector scenario on an Edge Transport server

Connector name	Linked status	Connector description
ReceiveConnectorA	Linked to SendConnectorC	This connector receives all messages from the Internet.
ReceiveConnectorB	Not linked	This connector receives messages only from the third-party anti-spam and antivirus service.
SendConnectorC	Contains linked ReceiveConnectorA	This connector sends all messages to the third-party anti-spam and antivirus service smart host.
SendConnectorD	Not linked	This connector sends all messages into the Exchange organization.

In this scenario, all messages destined for the Exchange 2010 organization arrive at the Edge Transport server through ReceiveConnectorA. Because ReceiveConnectorA is linked to SendConnectorC, the messages are immediately redirected to the third-party anti-spam and antivirus service through SendConnectorC. After the third-party anti-spam and antivirus service has finished processing the messages, the messages are delivered back to the Edge Transport server through ReceiveConnectorB.

ReceiveConnectorB is an unlinked Receive connector, which is important in this scenario. Without ReceiveConnectorB, the messages would return to the Edge Transport server through ReceiveConnectorA, and would then be forwarded back to the third-party anti-spam and antivirus service. This process would continue indefinitely. However, because ReceiveConnectorB isn't linked to a Send connector, the Edge Transport server is free to select the route into the Exchange organization. This will occur through SendConnectorD. The messages are then delivered to the original recipients in the Exchange organization through SendConnectorD.

Use the Shell to link a Receive connector to a new Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

Note:

You can't use the EMC to link a Receive connector to a new Send connector.

Use the **New-SendConnector** cmdlet to create a Send connector that's linked to a specific Receive connector. This example links the Receive connector From Internet on server Edge01 to a new Send connector with the following configuration options:

- Send connector name: "To Hygiene Service"
- Linked Receive connector identity: "Edge01\From Internet"
- Smart host identity: hygiene.contoso.com
- Smart host authentication mechanism: `ExternalAuthoritative`
- No message size limits imposed on the Send connector

```
New-SendConnector -Name "To Hygiene Service" -LinkedReceiveConnector "Edge01\From
```

For detailed syntax and parameter information, see New-SendConnector.

Use the Shell to link a Receive connector to an existing Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

Note:
You can't use the EMC to link a Receive connector to an existing Send connector.

Use the **Set-SendConnector** cmdlet to link an existing Send connector to a specific Receive connector. This example links the Receive connector From Internet on server Edge01 to the Send connector To Hygiene Service with the following configuration options:

- Send connector identity: "To Hygiene Service"
- Linked Receive connector identity: "Edge01\From Internet"
- Smart host identity: hygiene.contoso.com
- Smart host authentication mechanism: `ExternalAuthoritative`
- No message size limits imposed on the Send connector

```
Set-SendConnector "To Hygiene Service" -LinkedReceiveConnector "Edge01\From Inter
```

For detailed syntax and parameter information, see Set-SendConnector.

Use the Shell or the EMC to remove a linked connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" and "Receive connectors" entries in the Transport Permissions topic.

After you link a Receive connector to a Send connector, you may want to break the link at some time. Here are options for breaking the link:

- **Remove the Send connector to which the Receive connector is linked** You can remove the Send connector by using the EMC or by using the **Remove-SendConnector** cmdlet in the Shell. After you remove the Send connector, you don't have to modify the configuration of the Receive connector.
- **Remove the Receive connector linked to the Send connector** You can remove the Receive connector by using the EMC or by using the **Remove-ReceiveConnector** cmdlet in the Shell. After you remove the Receive connector, you must modify the configuration of the Send connector. After the linked Receive connector is removed, the Send connector will have no address spaces configured. If you try to view or modify the Send connector, you receive an error message that states that the Send connector is corrupted. To configure an address space for the Send connector, you can use the EMC or the **Set-SendConnector** cmdlet in the Shell.

For step-by-step instructions for removing connectors, see the following topics:

- Remove a Send Connector
- Remove a Receive Connector

1.7.2.11.3 Configure a Dedicated Send Connector for a Specific Domain

Configure a Dedicated Send Connector for a Specific Domain

See Also

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-11-19*

In some Microsoft Exchange Server 2010 environments, you may want to configure conditional SMTP forwarding so that all messages that are sent to a specific domain are routed through a separate Send connector. To do this in Exchange 2010, create a dedicated Send connector, and specify a different recipient domain for each Send connector.

Use the Exchange Management Console to create a dedicated Send connector

1. Open the Exchange Management Console on a computer that has the Hub Transport server role.
2. In the console tree, expand **Organization Configuration**, select **Hub Transport**, and then click the **Send Connectors** tab in the work pane.
3. In the action pane, click **New Send Connector**.

   Note:
   The New SMTP Send Connector wizard starts.
4. On the **Introduction** page, type a name for the connector in the **Name** field.
5. In the **Select the intended use for this connector** field, click **Custom**.
6. On the **Address space** page, click **Add**.
7. In the **SMTP Address Space** dialog box, specify the address to which you want to route the mail. To do this, enter the recipient's domain name under **Address space**. to For example, enter **contoso.com**.

   Note:
   If it's applicable, click to select the **Include all subdomains** check box, click **OK**, and then click **Next**.
8. On the **Network Settings** page, select **Route mail through the following smart hosts**, and then click **Add**.
9. In the **Add smart host** dialog box, enter the FQDN of the smart host that you want to use to route mail to the recipient's domain. For example, to send connector to route mail to the contoso.com domain, use the smart host for contoso.com.
10. Click **OK**.
11. On the "Configure smart host authentication settings" page, select the method that's used to authenticate to the smart host. By default, no authentication is used. To configure the smart host authentication settings, click **Change**, and then specify one of the following options in the window

that opens:

- **None** Select this option if the smart host is configured to accept anonymous connections.
- **Basic Authentication** Select this option if the smart host requires Basic authentication. Basic authentication requires that you provide a user name and password. We strongly recommend that you use an encrypted connection if you're using Basic authentication. This is because the user name and password are sent in clear text. Select the **Basic Authentication over TLS** check box to enable encryption on the connection. Also, if you specify more than one smart host for this Send connector, all the specified smart hosts must accept the same user name and password.
- **Exchange Server Authentication** Select this option to authenticate to a smart host by using an Exchange authentication mechanism, such as TLS direct trust or TLS\Kerberos.
- **Externally Secured (for example, with IPsec)** Select this option if the connection to the smart host is secured by external means, such as being physically secured over a private network or secured by using Internet Protocol security (IPsec).

12. Click **Next**.
13. On the Source Server page, select the Hub transport server that you are working on. To use a different Hub Transport server, click **Add**, and then select the Hub Transport servers that you want in the **Select Hub Transport or Subscribed Edge Transport Server** dialog box.
14. To create the Send connector, click **New**.

Repeat these steps for each new Send connector. Make sure that you specify a different recipient domain name on the "Address space" page for each dedicated Send connector for which you want to configure conditional forwarding.

See Also

Concepts

Understanding Send Connectors

1.7.2.11.4 Configure Send Connector Properties

Configure Send Connector Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Send connectors create a logical connection to remote e-mail systems and are responsible for outbound transmission of e-mail messages. If you use the EdgeSync process, it configures the Send connectors required for mail flow to the Internet, and to the Edge Transport servers in your Microsoft Exchange organization. If your organization requires a Send connector with specific configuration options, or if you don't use the EdgeSync process, you must manually configure Send connectors.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to transport servers? Check out Managing Transport Servers.

Prerequisites

- Send connector. For detailed steps about creating a new Send connector, see Create an SMTP Send Connector.
- You should determine the specific usage for this Send connector so you can correctly configure its properties. To learn more about Send connectors, see Understanding Send Connectors.

What Do You Want to Do?

- Use the EMC to configure the properties of a Send connector
- Use the Shell to configure the properties of a Send connector

Use the EMC to configure the properties of a Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

1. If you're configuring a Send connector on a Hub Transport server, in the console tree, navigate to **Organization Configuration** > **Hub Transport**. On an Edge Transport server, select **Edge Transport** in the console tree.
2. In the work pane, select the **Send Connectors** tab on the right, and then double-click the Send connector you want to configure.
3. Use the **General** tab to modify the general properties of the Send connector:
   - **Connector name** To rename the connector, type a new name in the connector name field, and then click **Apply**.
   - **Connector status** This field shows whether the connector is enabled or disabled. You can't change a connector's status from the properties page. You need to use the **Enable** or **Disable** actions in the EMC or the corresponding Shell commands. For detailed steps about enabling or disabling Send connectors, see Enable or Disable a Send Connector.
   - **Modified** This field shows the last date that the connector settings were modified.
   - **Protocol logging level** Use this pull-down list to select the protocol logging level. Select **None** to turn off protocol logging. Select **Verbose** to turn on protocol logging.
   - **Specify the FQDN this connector will provide in response to HELO or EHLO** When a transport server uses this Send connector to transmit outbound messages, it needs to establish an SMTP connection to the destination messaging server. This field specifies the fully qualified domain name (FQDN) used in that SMTP connection to identify the source server. The value of this field is displayed to the destination messaging servers whenever a source server name is required. To learn more about how the value of this field is used, see Understanding Send Connectors.
   - **Maximum message size (KB)** To set a maximum message size for messages that can pass through this connector, select the check box, and then enter a value in KB in the adjacent field. The valid input range is from 0 through 2147483647 KB. To remove any restriction on the maximum message size, clear the check box next to **Maximum message size (KB)**.
4. Use the **Address Space** tab to maintain the list of address spaces for which

this Send connector is responsible.
You can configure either an SMTP address space or a custom address space. Custom address spaces may only be configured on Send connectors that exist on Hub Transport servers. If you use a custom address space type, you must use a smart host to route e-mail.

Note:
Although you can configure custom address spaces on a Send connector, the Hub Transport server still uses SMTP as the transport mechanism to send messages to other messaging servers using this Send connector. To send messages to messaging servers that don't use SMTP as their primary transport mechanism, such as a third-party fax gateway server, you must use a Foreign connector. For more information about Foreign connectors, see Understanding Foreign Connectors.

To configure an address space, do the following:

- **Add** To specify an address space for which this Send connector is responsible, click **Add** or the drop-down arrow located next to **Add**. If you click **Add**, the address space type is SMTP. If you click the drop-down arrow located next to **Add**, you can select **SMTP Address Space** or **Custom Address Space**. For each new address space, you need to configure the following:
  - **Type** This field describes the address space that you enter in the **Address** field. If you clicked **Add**, this field is set to SMTP and is unavailable.
  - **Address** Specify the address space for the Send connector. If you entered **SMTP** or **X400** in the **Type** field, Exchange verifies the syntax of the address space that you enter. Exchange can't verify any other types of addresses; therefore, you need to make sure that you specify any custom addresses using the correct syntax. If you're entering an SMTP address, you can include the wildcard character (*) in the address space as defined in RFC 1035. For example, `*`, `*.com`, and `*.contoso.com` are permitted, but `*contoso.com` isn't permitted.
  - **Include all subdomains** This option is only available when you're specifying an SMTP address space. Select this option if you also want to use this connector to route mail to all subdomains of the specified address space. If you entered an address space that contains the wildcard character, this option is automatically selected.
  - **Cost** Use the address space cost to set the selection priority when more than one Send connector is configured for the same address space. During routing resolution, when the connector selection is made, the least cost routing path to the destination address space is selected. The valid input range is from 1 through 100.
- **Edit** To modify an existing address space in the address space list, select the address space, and then click **Edit**. You can configure the same options described for the **Add** button previously, with the exception of **Type**. You can't change the type of an existing address space.
- **Remove** To delete the domain name from the list of domains, select a domain name, and then click  .
- **Scoped send connector** By default, all Send connectors that you create can be used by all the Hub Transport servers in your Exchange organization. However, you can limit the scope of any Send connector so that it can be used only by other Hub Transport servers that exist in the same Active Directory site. To limit the scope of this Send connector, select **Scoped send connector**.

5. Use the **Network** tab to configure how outbound mail is routed through the

Send connector:

- **Use domain name system (DNS) "MX" records to route mail automatically** Select this option to use DNS to route outbound mail. The connector uses DNS to resolve the IP address of the remote SMTP server.
- **Enable Domain Security (Mutual Auth TLS)** Select this check box to configure this Send connector to attempt to establish a mutual Transport Layer Security (TLS) connection with remote servers when sending mail. There are additional configuration steps required before you can start using TLS. For more information about how to configure mutual TLS, see Using Domain Security: Configuring Mutual TLS.
- **Route mail through the following smart hosts** Select this option to route all outbound mail to specific smart hosts instead of using DNS to resolve the IP addresses of remote SMTP servers.
- **Add** To add a new smart host, click **Add**. You can specify either of the following options in the window that appears:
  IP Address Select this option to identify the smart host by IP address (for example: 192.168.100.1).
  Fully qualified domain name (FQDN) Select this option to identify the smart host by FQDN (for example, smarthost.contoso.com).
- **Edit** To edit an existing smart host, select the smart host, and then click **Edit**.
- **Remove** To remove an existing smart host, select the smart host, and then click  .
- **Smart host authentication** This field shows the authentication type that the connector uses to authenticate with the smart hosts.
  By default, no authentication is used. To configure the smart host authentication settings, click **Change**. You can specify one of the following options in the window that appears:
  • **None** Select this option if the smart host is configured to accept anonymous connections.
  • **Basic Authentication** Select this option if the smart host requires Basic authentication. Basic authentication requires that you provide a user name and password. We strongly recommend that you use an encrypted connection if you're using Basic authentication, because the user name and password are sent in clear text. Select the **Basic Authentication over TLS** check box to enable encryption on the connection. Also, if you specify more than one smart host for this Send connector, all of the specified smart hosts must accept the same user name and password.
  • **Exchange Server Authentication** Select this option to authenticate to a smart host by using an Exchange authentication mechanism, such as TLS direct trust or TLS \Kerberos.
  • **Externally Secured (for example, with IPsec)** Select this option if the connection to the smart host is secured by external means, such as being physically secured over a private network or secured using Internet Protocol security (IPsec). When you select this option, you make an assertion of external security that can't be programmatically verified by Exchange.
- **Use the External DNS Lookup settings on the transport server** Select this option to use the external DNS servers list to resolve the names of the remote SMTP servers.

Important:
Verify that you have configured the external DNS servers list by using the **Set-TransportServer** cmdlet or by using the **External DNS Lookups** tab in the properties of the Hub Transport server object, or the Edge Transport server object.

6. Use the **Source Server** tab to specify the transport servers that can use this Send connector. The list of source servers can contain only Hub Transport servers or only subscribed Edge Transport servers, but not a mix of both. Only those Hub Transport servers in the list use this Send connector for outbound messages. In the case of subscribed Edge Transport servers, the EdgeSync service propagates this Send connector configuration to only the Edge Transport servers in the list.

   Note:
   The **Source Server** tab is only available on Hub Transport servers.

   Select one of the following:
   - **Add** Click to add a Hub Transport server or a subscribed Edge Transport server.
   - **Remove** To remove a server from the list, select the server, and then click  .

     Note:
     Removing a subscribed Edge Transport server from the list doesn't remove the Send connector from the Edge Transport server. It just stops the EdgeSync service from propagating this Send connector configuration to that Edge Transport server.

Use the Shell to configure the properties of a Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

You can use the **Set-SendConnector** cmdlet to modify all available settings for an existing Send connector. The following command is an example of how you can use this cmdlet to update the properties of a Send connector. In this example, the following changes are made to the configuration of a Send connector named "Connection to Contoso.com":

- Changes the maximum message size allowed on the connector to 50 MB.
- Enables protocol logging on the Send connector.

```
Set-SendConnector "Connection to Contoso.com" -MaxMessageSize 50MB -ProtocolLoggi
```

The values that you specify by using the **Set-SendConnector** cmdlet parameters replace the existing values configured on the Send connector. This isn't an issue for single value attributes such as maximum message size, but it can be a problem for multivalued attributes such as smart hosts or address spaces. To preserve any existing values in a multivalued attribute, you must specify the existing value and any new values that you want to add when you run the **Set-SendConnector** cmdlet.

For example, assume that you want to add an address space to the "Connection to Contoso.com" Send connector. Currently, this Send connector has a single address space defined, contoso.com, with a cost of 1. You want to add an address space for fabrikam.com with a cost of 10. The following command accomplishes this by specifying the existing value along with the new value being added.

```
Set-SendConnector "Connection to Contoso.com" -AddressSpaces "SMTP:contoso.com;1"
```

If you have numerous values for a multivalued property, you may not want to retype all of the values just to add another value. To avoid that, you can make use of temporary Shell variables. The following example also adds the fabrikam.com address space with a cost of 10 to the "Connection to Contoso.com" Send connector using a temporary variable called *$ConnectorConfiguration*.

```
$ConnectorConfiguration = Get-SendConnector "Connection to Contoso.com"
$ConnectorConfiguration.AddressSpaces += "SMTP:fabrikam.com;10"
Set-SendConnector "Connection to Contoso.com" -AddressSpaces $ConnectorConfigurat
```

For detailed syntax and configuration information, see Set-SendConnector.

1.7.2.11.5 Enable or Disable a Send Connector

Enable or Disable a Send Connector

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can use the EMC or the Shell to modify the status of an existing Send connector for a computer that has the Microsoft Exchange Server 2010 Edge Transport server role or the Hub Transport server role installed.

In Exchange 2010, Send connectors are responsible for outbound transmission of e-mail messages. A Send connector must be enabled for it to send messages. Disable a Send connector to stop sending messages by using the configuration represented by that connector. By default, when you create a Send connector, it's enabled.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to connectors? Check out Managing Connectors.

What Do You Want to Do?

- Use the EMC to modify the status of a Send connector
- Use the Shell to modify the status of a Send connector

Use the EMC to modify the status of a Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

1. Perform one of the following:
   - To modify the status of an existing Send connector on an Edge Transport server, in the console tree, select **Edge Transport**, and then click the **Send Connectors** tab.
   - To modify the status of an existing Send connector on a Hub Transport server, in the console tree, expand **Organization Configuration**, select **Hub Transport**, and then click the **Send Connectors** tab.
2. Select a Send connector. If the connector is enabled and you want to disable it, in the action pane, click **Disable**. If the connector is disabled and you want to enable it, in the action pane, click **Enable**.

Use the Shell to modify the status of a Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

Use the **Set-SendConnector** cmdlet to modify the status of a Send connector.

This example disables the Send connector Contoso.com Send Connector.

```
Set-SendConnector -Identity "Contoso.com Send Connector" -Enabled $false
```

This example enables the same Send connector.

```
Set-SendConnector -Identity "Contoso.com Send Connector" -Enabled $true
```

You may want to temporarily stop all Hub Transport servers from sending messages. To do this, you can disable all Send connectors in your organization. This example first gets a list of all Send connectors using the **Get-SendConnector** cmdlet, and then disables all Send connectors that are returned:

```
Get-SendConnector | Set-SendConnector -Enabled $false
```

For detailed syntax and parameter information, see Set-SendConnector.

1.7.2.11.6 Remove a Send Connector

Remove a Send Connector

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You use Send connectors to create a connection to the Internet and to remote e-mail systems that require a specific configuration. For example, some remote e-mail systems may use a smart host or may require that you send e-mail messages that are larger than your standard Exchange organization limit. This topic shows you how to remove an existing Send connector in Microsoft Exchange Server 2010.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to connectors? Check out Managing Connectors.

Prerequisites

Removing a Send connector may affect mail flow in your organization. Make sure you understand how the Send connector is being used prior to removing it.

What Do You Want to Do?

Use the EMC to remove a Send connector

Use the Shell to remove a Send connector

Use the EMC to remove a Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

1. Open the Exchange Management Console. Perform one of the following steps:
   - To remove an existing Send connector on an Edge Transport server, in the console tree, select **Edge Transport**.
   - To remove an existing Send connector on a Hub Transport server, expand **Organization Configuration** in the console tree, and select **Hub Transport**.
2. In the work pane, click the **Send Connectors** tab, and select the Send connector to remove.
3. Under the name of the Send connector in the action pane, click **Remove**.
4. A warning appears that asks you, "Are you sure you want to remove *<selected Send connector>*?" Click **Yes**.

Use the Shell to remove a Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

Use the **Remove-SendConnector** cmdlet to remove a Send connector. This example removes the existing Send connector connection to Contoso.com.

```
Remove-SendConnector "Connection to Contoso.com"
```

For detailed syntax and parameter information, see Remove-SendConnector.

1.7.2.11.7 Create an SMTP Receive Connector

Create an SMTP Receive Connector

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Receive connectors represent a logical gateway through which all inbound messages are received. Receive connectors are configured on a per-server basis, and they control how that server receives messages from the Internet, e-mail clients, and other messaging servers.

By default, the Receive connectors required for internal mail flow are automatically created when the Hub Transport server role is installed. Similarly, when you install the Edge Transport server role, the Receive connector capable of receiving mail from the Internet and from Hub Transport servers is automatically created. However, end-to-end mail flow is possible only after the Edge Transport server has been subscribed to the Active Directory

site by using the Edge Subscription process. Other scenarios, such as an Internet-facing Hub Transport server or an Edge Transport server that doesn't use EdgeSync, require manual connector configuration to establish end-to-end mail flow.

You can use the EMC or the Shell to create a new Receive connector for Microsoft Exchange Server 2010.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to connectors? Check out Managing Connectors.

Prerequisites

You should determine the specific usage for the Receive connector before you create it so you can correctly configure its properties. To learn more about Receive connectors, see Understanding Receive Connectors.

What Do You Want to Do?

- Use the EMC to create a Receive connector
- Use the Shell to create a Receive connector

Use the EMC to create a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

1. Open the Exchange Management Console. Perform one of the following:
   - On a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the work pane, click the **Receive Connectors** tab.
   - To create a Receive connector on a Hub Transport server role, in the console tree, expand **Server Configuration**, and select **Hub Transport**. In the result pane, select the server on which you want to create the connector, and then click the **Receive Connectors** tab.
2. In the action pane, click **New Receive Connector**. The New SMTP Receive Connector wizard starts.
3. On the **Introduction** page, follow these steps:
   - In the **Name** field, type a meaningful name for this connector. Specify a name for the Receive connector that helps you distinguish this Receive connector from other Receive connectors in your configuration.
   - In the **Select the intended use for this Receive connector** field, select the usage type for this connector. The usage type determines the permissions granted to sessions that connect to the Receive connector and the supported authentication mechanisms. The following usage types are available:

     Client Client Receive connectors receive e-mail from users of Microsoft Exchange. This connector is configured to only accept client submissions from authenticated Microsoft Exchange users.

The **Client** usage type is only available for Receive connectors configured on Hub Transport servers.
Custom Select this option to create a customized connector that connects with systems that don't include servers running Exchange.
Internet Internet Receive connectors receive e-mail from servers on the Internet. This connector is configured to accept connections from anonymous users.

Note:
We strongly recommend against configuring Receive connectors to accept anonymous connections from unknown IPv6 addresses. If you configure a Receive connector to accept anonymous connections from unknown IPv6 addresses, the amount of spam that enters your organization is likely to increase. Currently, there is no broadly accepted industry standard protocol for looking up IPv6 addresses. Most IP Block list providers don't support IPv6 addresses. Therefore, if you allow anonymous connections from unknown IPv6 addresses on a Receive connector, you increase the chance that spam messages bypass IP Block list providers and are successfully delivered into your organization.

Internal Internal Receive connectors are used to receive e-mail from servers within your Exchange organization. This connector is configured to only accept connections from Exchange servers.
Partner Partner Receive connectors are used to receive e-mail from partner domains. This connector is configured to receive mail from domains included in the list of secure receive domains. You can add domains to this list by using the *TLSReceiveDomainSecureList* parameter in the **Set-TransportConfig** command. Mutually authenticated TLS connections are required for domains that are on this list.

- Click **Next**.

4. On the **Local network settings** page, do the following:
   - Specify the IP addresses and port numbers on which this Receive connector listens for incoming mail. The **Local network settings** page appears only if you selected a usage type of **Custom**, **Partner**, or **Internet** in step 3. By default, all available local IP addresses are listed. The following options are available:

Add To add a new IP address or port number, click **Add** and specify the following:
• **Use all IP addresses available on this server** Select this option to use all IP addresses associated with this computer. This is the recommended option.
• **Specify an IP address** Select this option to use a specific IP address associated with this computer.

Important:
You must specify a local IP address that's valid for the Hub Transport server or Edge Transport server on which the Receive connector is located. If you specify an invalid local IP address, the Microsoft Exchange Transport service may fail to start when the service is restarted.

• **Port** This field identifies the TCP port number on which this Receive connector listens for incoming mail. TCP port 25 is the default port used for message transmission between SMTP servers.
Edit Click **Edit** to change an existing IP address or port.

Remove Click  to remove an existing IP address.

- In the **Specify the FQDN this connector will provide in response to HELO or EHLO** field, type the name advertised in response to the SMTP HELO or EHLO verb. If you leave this field blank, the fully qualified domain name (FQDN) of the Hub Transport server or Edge Transport server is automatically added when the connector is created.
- Click **Next**.

5. On the **Remote network settings** page, enter the IP address or IP address range of the remote servers from which the connector accepts incoming connections. The **Remote network settings** page appears only if you selected a usage type of **Custom**, **Partner**, **Internal**, or **Client** in step 3. To add the remote IP address or remote IP address range, use one of the following methods:
   Add - IP Address To enter an IP address without a subnet mask, or to specify the subnet mask by using Classless Interdomain Routing (CIDR) notation, click **Add** or the drop-down arrow next to **Add** and select **IP Address**. In the **Add IP address(es) of Remote Servers** dialog box, enter the IP address directly or specify a subnet using the CIDR notation. For example, if you enter 192.168.1.1, the Receive connector accepts messages from that host only, but if you specify 192.168.1.0/24, the Receive connector accepts messages from the entire class C subnet of 192.168.1.0.
   Add - IP and Mask To enter an IP address or subnet together with a subnet mask in dotted decimal notation, click the drop-down arrow next to **Add** and select **IP and Mask**. In the **Add Remote Servers - IP and Mask** dialog box, specify the IP address and the subnet mask.
   Add - IP Range To specify an IP address range by using the first IP address and the last IP address in the range, click the drop-down arrow next to **Add** and select **IP Range**. In the **Add Remote Servers - IP Range** dialog box, specify the start and end addresses of the IP range.
   Edit To edit an existing IP address range, select the IP address range, and then click **Edit**.
   Remove To remove an existing IP address range, select the IP address range, and then click  .
   After you finish, click **Next**.

6. On the **New Connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Receive connector by using the settings in the configuration summary, click **New**.

7. On the **Completion** page, click **Finish**.

Use the Shell to create a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

This example creates a Receive connector on the local server that has the default settings for the **Internal** usage type, and accepts connections from the specified remote IP address range.

```
New-ReceiveConnector -Name "Contoso.com Receive Connector" -Usage Internal -Remot
```

For detailed syntax and parameter information, see New-ReceiveConnector.

1.7.2.11.8 Configure Receive Connector Properties

Configure Receive Connector Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-26*

Receive connectors represent a logical gateway through which all inbound messages are received. Receive connectors are configured on a per-server basis, and they control how that server receives messages from the Internet, e-mail clients, and other messaging servers.

By default, the Receive connectors required for internal mail flow are automatically created when the Hub Transport server role is installed. Similarly, when you install the Edge Transport server role, the Receive connector capable of receiving mail from the Internet and from Hub Transport servers is automatically created. However, end-to-end mail flow is possible only after the Edge Transport server is subscribed to the Active Directory site by using the Edge Subscription process. Other scenarios, such as an Internet-facing Hub Transport server or an Edge Transport server that doesn't use EdgeSync, require manual connector configuration to establish end-to-end mail flow.

You can use the EMC or the Shell to configure the properties of a Receive connector.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to connectors? Check out Managing Connectors.

Prerequisites

- You must have an existing Receive connector. For detailed steps about creating a Receive connector, see Create an SMTP Receive Connector.
- You should determine the specific usage for this Receive connector so you can correctly configure its properties. To learn more about Receive connectors, see Understanding Receive Connectors.

What Do You Want to Do?

- Use the EMC to configure the properties of a Receive connector
- Use the Shell to configure the properties of a Receive connector

Use the EMC to configure the properties of a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

1. If you are configuring a Receive connector on a Hub Transport server, expand **Server Configuration** in the console tree, and select **Hub Transport**. On an Edge Transport server, select **Edge Transport** in the console tree.
2. In the work pane, select the **Receive Connectors** tab, and then double-click

the Receive connector you want to configure.

3. Use the **General** tab to modify the general properties of the Receive connector:
   - **Connector name** To rename the connector, type a new name in the **Connector name** field, and then click **Apply**.
   - **Connector status** This field shows whether the connector is enabled. You can't change a connector's status from the properties page. You need to use the **Enable** or **Disable** actions in the EMC or the corresponding Shell commands. For detailed steps about enabling or disabling Receive connectors, see Enable or Disable a Receive Connector.
   - **Modified** This field shows the last date that the connector settings were modified.
   - **Protocol logging level** Use this drop-down list to select the protocol logging level. Select **None** to turn off protocol logging. Select **Verbose** to turn on protocol logging.
   - **Specify the FQDN this connector will provide in response to HELO or EHLO** This field specifies the fully qualified domain name (FQDN) that the transport server uses to identify itself whenever a destination server name is required during an inbound SMTP connection. To learn more about how the value of this field is used, see Understanding Receive Connectors.
   - **Maximum message size (KB)** To set a maximum message size for messages that can pass through this connector, select the check box next to **Maximum message size (KB)** and enter a value in kilobytes (KB). The valid input range is from 64 through 2097151 KB. To remove any restriction on the maximum message size, clear the check box next to **Maximum message size (KB)**.

4. Use the **Network** tab to specify the IP addresses and TCP ports on which this Receive connector receives connections. You can also configure the IP address ranges from which this Receive connector accepts connections. The following options are available:
   - **Use these local IP Addresses to receive mail** Use this list to specify the IP addresses and port numbers on which this Receive connector listens for incoming mail. For each entry, you must specify a different set of IP addresses or specify all available IP addresses. The following options are available:

     Add To add a new IP address or port number, click **Add.** The following options are available in the window that appears:
     • **Use all IP addresses available on this server** Select this option to use all IP addresses associated with this computer. This is the recommended option.
     • **Specify an IP address** Select this option to use a specific IP address associated with this computer.

     Important:
     You must specify a local IP address that's valid for the Hub Transport server or Edge Transport server on which the Receive connector is located. If you specify an invalid local IP address, the Microsoft Exchange Transport service may fail to start when the service is restarted.

     • **Port** This field identifies the TCP port number on which this Receive connector listens for incoming mail. TCP port 25 is the default port used for message transmission between SMTP servers.
     Edit Click **Edit** to change an existing IP address or port.
     Remove Click  to remove an existing IP address.
   - **Receive mail from remote servers that have these IP addresses** Use this list to specify the IP address or IP address range from which this Receive connector accepts connections. To add the remote IP address or

remote IP address range, use one of the following methods:

Add - IP Address To enter an IP address without a subnet mask, or to specify the subnet mask by using Classless Interdomain Routing (CIDR) notation, click **Add** or the drop-down arrow next to **Add** and select **IP Address**. In the **Add IP address(es) of Remote Servers** dialog box, enter the IP address directly or specify a subnet using the CIDR notation. For example, if you enter 192.168.1.1, the Receive connector accepts messages from that host only, but if you specify 192.168.1.0/24, the Receive connector accepts messages from the entire class C subnet of 192.168.1.0.

Add - IP and Mask To enter an IP address or subnet together with a subnet mask in dotted decimal notation, click the drop-down arrow next to **Add** and select **IP and Mask**. In the **Add Remote Servers - IP and Mask** dialog box, specify the IP address and the subnet mask.

Add - IP Range To specify an IP address range by using the first IP address and the last IP address in the range, click the drop-down arrow next to **Add** and select **IP Range**. In the **Add Remote Servers - IP Range** dialog box, specify the start and end addresses of the IP range.

Edit To edit an existing IP address range, select the IP address range, and then click **Edit**.

Remove To remove an existing IP address range, select the IP address range, and then click  .

5. Use the **Authentication** tab to configure security options for incoming SMTP connections:
   - **Transport Layer Security (TLS)** Select this option to offer Transport Layer Security (TLS) transmission for all messages received by this connector. When you select this option, the **STARTTLS** keyword is advertised in the EHLO response to connecting SMTP servers, and TLS authentication is accepted.
     - **Enable Domain Security (Mutual Auth TLS)** To instruct this Receive connector to accept a mutual TLS connection from a remote server, select this check box. There are additional configuration steps required before you can enable mutual TLS. For more information about configuring mutual TLS, see Using Domain Security: Configuring Mutual TLS.
   - **Basic Authentication** Select this option to offer Basic authentication for all mail received by this connector. When you select **Basic Authentication**, the **AUTH** keyword is advertised in the EHLO response to connecting SMTP servers, and Basic authentication is accepted. Because the user name and password are sent in plaintext when Basic authentication is used, Basic authentication without encryption isn't recommended.
     - **Offer Basic Authentication only after starting TLS** When you select this option, the connector starts TLS first, and then after TLS encryption is complete, the connector offers Basic authentication.
   - **Exchange Server authentication** Select this option to authenticate by using an Exchange authentication mechanism, such as TLS direct trust or Kerberos through TLS.
   - **Integrated Windows authentication** Select this option to use Integrated Windows authentication, which represents NTLM, Kerberos, and Negotiate authentication mechanisms.
   - **Externally Secured (for example, with IPsec)** Use this option if the incoming connections to this Receive connector are secured by external means. For example, use this option if the connection is physically secured over a private network or by using Internet Protocol security (IPsec). When you select this option, you make an assertion of external security that can't

be programmatically verified by Exchange. Before you select this authentication method, you must first select the **Exchange servers** permissions group on the **Permission Groups** tab.

6. Use the **Permission Groups** tab to select the permission groups assigned to this Receive connector. A permission group is a predefined set of permissions granted to well-known groups of users, computers, or security groups. Members of the selected permission groups on this tab are allowed to submit messages to this Receive connector.

   Important:
   When selected on this tab, each permission group is granted a different set of permissions. For example, members of the Exchange users permission group are granted the ms-Exch-Bypass-Anti-Spam extended right whereas anonymous users aren't. To see a complete list of extended rights granted to each permission group, see "Permission Groups" in Understanding Receive Connectors.

   The following options are available:
   - **Anonymous users** Non-authenticated users
   - **Exchange users** Authenticated user accounts
   - **Exchange servers** Members of the Exchange Servers universal security group
   - **Legacy Exchange servers** Members of the ExchangeLegacyInterop universal security group
   - **Partners** Partner service accounts

Use the Shell to configure the properties of a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

You can use the **Set-ReceiveConnector** cmdlet to modify all available settings for an existing Receive connector. In this example, the following changes are made to the configuration of the Receive connector Connection from Contoso.com:

- Change the maximum message size allowed on the connector to 50 megabytes (MB).
- Enable protocol logging on the Receive connector.
- Set the tarpitting interval.

```
Set-ReceiveConnector "Connection from Contoso.com" -MaxMessageSize 50MB -Protocol
```

The values that you specify by using the **Set-ReceiveConnector** cmdlet parameters replace the existing values configured on the Receive connector. This isn't an issue for single value attributes such as maximum message size, but it can be a problem for multivalued attributes such as remote IP address ranges. To preserve any existing values in a multivalued attribute, you must specify the existing value and any new values that you want to add when you run the **Set-ReceiveConnector** cmdlet.

For example, assume that you want to add the subnet 10.0.10.0/24 to the IP addresses from which the Connection from Contoso.com Receive connector accepts messages. Currently, this Receive connector is configured to accept messages only from the IP range of 192.168.180.0 to 192.168.180.255. This example does this by specifying the existing value along with the new value being added.

```
Set-ReceiveConnector "Connection from Contoso.com" -RemoteIPRanges "10.0.10.0/24"
```

If you have numerous values for a multivalued property, you may not want to retype all of

the values just to add another value. Instead, you can use temporary Shell variables. This example also adds the 10.0.10.0/24 subnet to the remote IP ranges of the Connection from Contoso.com connector using the temporary variable *$ConnectorConfiguration*.

```
$ConnectorConfiguration = Get-ReceiveConnector "Connection from Contoso.com"
$ConnectorConfiguration.RemoteIPRanges += "10.0.10.0/24"
Set-ReceiveConnector "Connection from Contoso.com" -RemoteIPRanges $ConnectorConf
```

When you specify a tarpitting interval time on a Receive connector, tarpitting is enabled. The default value is 5 seconds, and we recommend that you start at this value. Use caution if you decide to change this value. An overly long interval could disrupt ordinary mail flow, whereas an overly brief interval may not be as effective in thwarting a directory harvest attack. If you change the tarpitting interval value, do it in small increments.

The following example changes the tarpitting interval of the "Connection from Contoso.com" connector by increasing it to 6 seconds.

```
Set-ReceiveConnector "Connection from Contoso.com" -TarpitInterval 00:00:06
```

For detailed syntax and configuration information, see Set-ReceiveConnector.

1.7.2.11.9 Modify the Default SMTP Banner

Modify the Default SMTP Banner

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The *SMTP banner* is the SMTP connection response that a remote SMTP messaging server receives after it connects to a Receive connector configured on a computer running Microsoft Exchange Server 2010 that has the Hub Transport server role or the Edge Transport server role installed. You may want to modify the default SMTP banner for Internet-facing SMTP Receive connectors on an Edge Transport server so that the server name and messaging server software aren't disclosed by the SMTP banner.

Looking for other management tasks related to connectors? Check out Managing Connectors.

Use the Shell to modify the default SMTP banner

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

Note:

You can't use the EMC to modify the default SMTP banner. Don't use the **Specify the FQDN this connector will provide in response to EHLO or HELO** field in the Receive connector properties page in the EMC.

You control the SMTP banner by using the *Banner* parameter in the **Set-ReceiveConnector** cmdlet or the **New-ReceiveConnector** cmdlet. The default value of the *Banner* parameter is `$null`. When the *Banner* parameter isn't specified on a Receive connector, or the *Banner* parameter is specified with the value of `$null`, a remote SMTP

messaging server that connects to that Receive connector receives the following response.

```
220 <Servername> Microsoft ESMTP MAIL service ready at <RegionalDay-Date-24HourTi
```

When you specify a value for the *Banner* parameter on a Receive connector, a remote SMTP messaging server that connects to that SMTP Receive connector receives the following response.

```
<220 BannerText>
```

Note:
The replacement SMTP banner text string must always start with 220. As defined in RFC 2821, the default service ready SMTP response code is 220.

This example modifies the SMTP banner on the existing Receive connector From the Internet so the SMTP banner displays 220 Contoso Corporation.

```
Set-ReceiveConnector "From the Internet" -Banner "220 Contoso Corporation"
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

1.7.2.11.10 Allow Anonymous Relay on a Receive Connector

Allow Anonymous Relay on a Receive Connector

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to create and configure a Receive connector that allows anonymous relay.

Looking for other management tasks related to managing connectors? Check out Managing Connectors.

Prerequisites

Allowing anonymous relay on a Receive connector is a security risk, especially on Internet-facing servers. Make sure you fully understand the implications by reading the "Using a Receive Connector for Anonymous Relay" section in Understanding Receive Connectors.

Grant the relay permission to anonymous connections

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

You can create the Receive connector using either EMC or the Shell; however, you must use the Shell to grant the relay permission to anonymous connections.

Use the EMC to create the Receive connector

1. Perform one of the following steps:

1.a.To create a Receive connector on a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the work pane, click the **Receive Connectors** tab.
1.b.To create a Receive connector on a Hub Transport server role, in the console tree, expand **Server Configuration** and select **Hub Transport**. In the result pane, select the server on which you want to create the connector, and then click the **Receive Connectors** tab.
2. In the action pane, click **New Receive Connector**. The New Receive Connector wizard starts.
3. On the **Introduction** page, follow these steps:
   3.a.In the **Name** field, type a meaningful name for this connector. This name is used to identify the connector.
   3.b.In the **Select the intended use for this Receive connector** field, select **Custom**.
   3.c.Click **Next**.
4. On the **Local Network settings** page, follow these steps:
   4.a.Select the existing **All Available IPv4** entry, and then click  .
   4.b.Click **Add**. In the **Add Receive Connector Binding** dialog box, select **Specify an IP address**. Type an IP address assigned to a network adapter on the local server that's best able to communicate with the remote messaging server. In the **Port** field, type **25**, and then click **OK**. Leave the **Specify the FQDN this connector will provide in response to HELO or EHLO** field blank.
   4.c.Click **Next**.
5. On the **Remote Network settings** page, follow these steps:
   5.a.Select the existing **0.0.0.0 - 255.255.255.255** entry, and then click  .
   5.b.Click **Add** or the drop-down arrow located next to **Add** and type the IP address or IP address range for the remote messaging server or servers that are allowed to relay mail on this server. When you're finished entering the IP addresses, click **OK**.
   5.c.Click **Next**.
6. On the **New Connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Receive connector by using the settings in the configuration summary, click **New**.
7. On the **Completion** page, click **Finish**.
8. In the work pane, select the Receive connector that you created.
9. Under the name of the Receive connector in the action pane, click **Properties** to open the **Properties** page.
10. Click the **Permission Groups** tab. Select **Anonymous users**.
11. Click **OK** to save your changes and exit the **Properties** page.

Use the Shell to create the Receive connector

This example uses the **New-ReceiveConnector** cmdlet to create the Receive connector Anonymous Relay that listens on local IP address 10.2.3.4 on port 25 from a source server at IP address 192.168.5.77.

```
New-ReceiveConnector -Name "Anonymous Relay" -Usage Custom -PermissionGroups Anon
```

For detailed syntax and configuration information, see New-ReceiveConnector.

Use the Shell to grant relay permission to anonymous connections on the new Receive connector

Note:
You can't use the EMC to perform this task.

This example retrieves the specified Receive connector information and pipes the result to the **Add-ADPermission** cmdlet to grant relay permission to anonymous connections on the new Receive connector.

```
Get-ReceiveConnector "Anonymous Relay" | Add-ADPermission -User "NT AUTHORITY\ANO
```

For detailed syntax and configuration information, see Get-ReceiveConnector or Add-ADPermission.

Configure the Receive connector as externally secured

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

Use the EMC to create the Receive connector as externally secured

1. Perform one of the following steps:
   1.a. To create a Receive connector on a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the work pane, click the **Receive Connectors** tab.
   1.b. To create a Receive connector on a Hub Transport server role, in the console tree, expand **Server Configuration** and select **Hub Transport**. In the result pane, select the server on which you want to create the connector, and then click the **Receive Connectors** tab.
2. In the action pane, click **New Receive Connector**. The New Receive Connector wizard starts.
3. On the **Introduction** page, follow these steps:
   3.a. In the **Name** field, type a meaningful name for this connector. This name is used to identify the connector.
   3.b. In the **Select the intended use for this Receive connector** field, select **Custom**.
   3.c. Click **Next**.
4. On the **Local Network settings** page, follow these steps:
   4.a. Select the existing **All Available** entry, and then click  .
   4.b. Click **Add**. In the **Add Receive Connector Binding** dialog box, select **Specify an IP address**. Type an IP address assigned to a network adapter on the local server that's best able to communicate with the remote messaging server. In the **Port** field, type **25**, and then click **OK**. Leave the **Specify the FQDN this connector will provide in response to HELO or EHLO** field blank.
   4.c. Click **Next**.
5. On the **Remote Network settings** page, follow these steps:
   5.a. Select the existing **0.0.0.0 - 255.255.255.255** entry, and then click  .
   5.b. Click **Add** or the drop-down arrow located next to **Add** and type the IP address or IP address range for the remote messaging server or servers that are allowed to relay mail on this server. When you're finished entering the IP addresses, click **OK**.
   5.c. Click **Next**.
6. On the **New Connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Receive connector by using the settings in the configuration summary, click **New**.
7. On the **Completion** page, click **Finish**.
8. In the work pane, select the Receive connector that you created.
9. Under the name of the Receive connector in the action pane, click **Properties** to open the **Properties** page.
10. Click the **Permission Groups** tab. Select **Exchange servers**.
11. Click the **Authentication** tab. Select **Externally Secured (for example, with IPsec)**.

12.Click **OK** to save your changes and exit the **Properties** page.

Use the Shell to create the Receive connector as externally secured

This example creates the Receive connector Anonymous Relay that listens on local IP address 10.2.3.4 on port 25 from a source server at IP address 192.168.5.77.

```
New-ReceiveConnector -Name "Anonymous Relay" -Usage Custom -AuthMechanism Externa
```

For detailed syntax and configuration information, see New-ReceiveConnector.

1.7.2.11.11 Enable or Disable a Receive Connector

Enable or Disable a Receive Connector

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can use the EMC or the Shell to modify the status of an existing Receive connector for a computer that has the Microsoft Exchange Server 2010 Edge Transport server role or the Hub Transport server role installed.

In Exchange 2010, you use Receive connectors to accept e-mail messages from remote e-mail systems. A Receive connector must be enabled for it to accept messages. Disable a Receive connector to stop accepting messages by using the configuration represented by that connector. By default, when you create a Receive connector, it's enabled.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Looking for other management tasks related to connectors? Check out Managing Connectors.

What Do You Want to Do?

- Use the EMC to modify the status of a Receive connector
- Use the Shell to modify the status of a Receive connector

Use the EMC to modify the status of a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

1. Perform one of the following:
   - To modify the status of an existing Receive connector on an Edge Transport server, in the console tree, select **Edge Transport**, and then click the **Receive Connectors** tab.
   - To modify the status of an existing Receive connector on a Hub Transport

server, in the console tree, expand **Organization Configuration**, select **Hub Transport**, and then click the **Receive Connectors** tab.

2. Select a Receive connector. If the connector is enabled and you want to disable it, in the action pane, click **Disable**. If the connector is disabled and you want to enable it, in the action pane, click **Enable**.

Use the Shell to modify the status of a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

Use the **Set-ReceiveConnector** cmdlet to modify the status of a Receive connector.

This example disables the Receive connector Contoso.com Receive Connector.

```
Set-ReceiveConnector -Identity "Contoso.com Receive Connector" -Enabled $false
```

This example enables the same Receive connector.

```
Set-ReceiveConnector -Identity "Contoso.com Receive Connector" -Enabled $true
```

You may want to temporarily stop all of your Hub Transport servers from accepting messages. To do this, you can disable all Receive connectors in your organization. This example first gets a list of all Receive connectors using the **Get-ReceiveConnector** cmdlet, and then disables all Receive connectors that are returned:

```
Get-ReceiveConnector | Set-ReceiveConnector -Enabled $false
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

1.7.2.11.12 Remove a Receive Connector

Remove a Receive Connector

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the EMC or the Shell to remove a Receive connector in Microsoft Exchange Server 2010. Receive connectors accept e-mail messages from the Internet and from remote e-mail systems that require specific configuration options.

Caution:

Deleting a Receive connector may affect mail flow throughout the organization. Make sure you understand how the Receive connector is being used before you remove it.

Looking for other management tasks related to connectors? Check out Managing Connectors.

What Do You Want to Do?

- Use the EMC to remove a Receive connector
- Use the Shell to remove a Receive connector

Use the EMC to remove a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

1. Perform one of the following:
   - To remove an existing Receive connector on an Edge Transport server, in the console tree, select **Edge Transport**, and then click the **Receive Connectors** tab.
   - To remove an existing Receive connector on a Hub Transport server, expand **Server Configuration** in the console tree, and select **Hub Transport**. In the result pane, select the server that has the Receive connector that you want to remove, and then click the **Receive Connectors** tab.
2. In the work pane, select the Receive connector to remove.
3. Under the name of the Receive connector in the action pane, click **Remove**.
4. A message appears asking "**Are you sure you want to remove** *selected Receive connector***?"** Click **Yes**.

Use the Shell to remove a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

Use the **Remove-ReceiveConnector** cmdlet to remove a Receive connector. This example removes the Receive connector `Connection from Contoso.com`.

```
Remove-ReceiveConnector "Connection from Contoso.com"
```

For detailed syntax and parameter information, see Remove-ReceiveConnector.

1.7.2.11.13 Create a Foreign Connector

Create a Foreign Connector

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can use the Shell to create a Foreign connector for Microsoft Exchange Server 2010. A Foreign connector can only be installed on a computer running Exchange 2010 that has the Hub Transport server role installed. A Foreign connector uses a Drop directory to send messages to a local messaging server that doesn't use SMTP as its primary transport mechanism. These messaging servers are known as foreign gateway servers. Examples of foreign gateway servers include Lotus Notes and third-party fax gateway servers. The address spaces assigned to a Foreign connector may be SMTP or non-SMTP.

Looking for other management tasks related to managing connectors? Check out Managing Connectors.

Prerequisites

- You should determine the specific usage for this Foreign connector so you can correctly configure its properties. To learn more about Foreign connectors, see Understanding Foreign Connectors.
- Exchange 2010 introduces a new feature called Delivery Agent connector, which is also used to route messages to foreign systems that don't use SMTP. Delivery Agent connectors provide better administrative control for messages addressed to foreign systems. Whenever possible, you should consider using Delivery Agent connectors instead of Foreign connectors. To learn more about Delivery Agent connectors, see Understanding Delivery Agents.

Use the Shell to create a Foreign connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Foreign connectors" entry in the Transport Permissions topic.

Use the **New-ForeignConnector** cmdlet to create a Foreign connector.

Note:

You can't create a Foreign connector by using the EMC. To create a Foreign connector, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example creates a Foreign connector that has the following settings:

- The connector sends messages to the X.400 address space o=MySite;p=MyOrg;a=contoso;c=us. The address space cost is 1.
- The connector is assigned to Hub Transport servers Hub01 and Hub02.

```
New-ForeignConnector -Name "Contoso.com Foreign Connector" -AddressSpaces "X400:o
```

For detailed syntax and parameter information, see New-ForeignConnector.

1.7.2.11.14 View the Configuration of a Foreign Connector

View the Configuration of a Foreign Connector

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can use the Exchange Management Shell to view the configuration of an existing Foreign connector for a computer that has the Microsoft Exchange Server 2010 Hub Transport server role installed.

A Foreign connector can only be installed on a computer running Exchange 2010 that has the Hub Transport server role installed. A Foreign connector uses a Drop directory to send messages to a local messaging server that doesn't use SMTP as its primary transport mechanism.

Looking for other management tasks related to connectors? Check out Managing

Connectors.

Use the Shell to view the configuration of a Foreign connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Foreign connectors" entry in the Transport Permissions topic.

Note:
You can't use the EMC to view the configuration of a Foreign connector.

You can use the **Get-ForeignConnector** cmdlet to view the configuration of a Foreign connector. The *Identity* parameter specifies the Foreign connector that you want to view. The *Identity* parameter can be the GUID or the name of the Foreign connector. If you don't specify an identity, the command returns the configuration information for all Foreign connectors.

This example returns a list of all Foreign connectors in your organization.

```
Get-ForeignConnector
```

This example displays the detailed configuration of the Foreign connector Contoso.com Foreign Connector.

```
Get-ForeignConnector "Contoso.com Foreign Connector" | Format-List
```

For detailed syntax and parameter information, see Get-ForeignConnector.

1.7.2.11.15 Modify the Configuration of a Foreign Connector

Modify the Configuration of a Foreign Connector

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to modify a Foreign connector for Microsoft Exchange Server 2010. A Foreign connector can only be installed on a computer running Exchange 2010 that has the Hub Transport server role installed. A Foreign connector uses a Drop directory to send messages to a local messaging server that doesn't use SMTP as its primary transport mechanism.

Looking for other management tasks related to managing connectors? Check out Managing Connectors.

Prerequisites

You must have an existing Foreign connector. For detailed steps about creating a Foreign connector, see Create a Foreign Connector.

Use the Shell to modify a Foreign

connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Foreign connectors" entry in the Transport Permissions topic.

You can use the **Set-ForeignConnector** cmdlet to modify all available settings for a Foreign connector.

Note:

You can't modify the configuration of a Foreign connector by using the Exchange Management Console. To modify the configuration of a Foreign connector, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example makes the following changes to the settings on the Foreign connector Contoso.com Foreign Connector:

- Change the maximum message size allowed on the connector to 50 MB.
- Add a new address space for the SMTP domain named Contoso.com that has an address space cost of 5. You want to preserve the existing X.400 address space **o=MySite;p=MyOrg;a=contoso;c=us** that has an address space cost of 1, which is already configured on the connector.

```
Set-ForeignConnector "Contoso.com Foreign Connector" -AddressSpaces "X400:o=MySit
```

For detailed syntax and configuration information, see Set-ForeignConnector.

1.7.2.11.16 Configure the Drop Directory

Configure the Drop Directory

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-21*

You can use the Shell to configure the Drop directory used by a Foreign connector in Microsoft Exchange Server 2010. Every Foreign connector installed on or assigned to a computer running Exchange 2010 that has the Hub Transport server role installed uses a different Drop directory. The Drop directory is used by the Foreign connector to send messages to the foreign gateway server that doesn't use SMTP to transmit messages. Messages sent to recipients that exist in the address space defined on the Foreign connector are copied into the Drop directory of the Foreign connector.

Looking for other management tasks related to managing connectors? Check out Managing Connectors.

Prerequisites

- You must have an existing Foreign connector. For detailed steps about creating a foreign connector, see Create a Foreign Connector.
- You must have created the Drop directory for your Foreign connector. By default, the Drop directory isn't created automatically when you create a Foreign connector. You must manually create each Drop directory folder in Windows Explorer.

What Do You Want to Do?

- Use the Shell to configure the Drop directory location
- Use the Shell to configure the maximum size of the Drop directory

Use the Shell to configure the Drop directory location

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub server" entry in the Transport Permissions topic.

Two items control the location of the Drop directory for each Foreign connector:

- The RootDropDirectoryPath parameter in the **Set-TransportServer** cmdlet
  This option is used for all Foreign connectors that exist on the Hub Transport server. The value of the *RootDropDirectoryPath* parameter may be a local path or a Universal Naming Convention (UNC) path to a remote server. By default, the value of this parameter is blank. This indicates the value of the *RootDropDirectoryPath* parameter is the Exchange 2010 installation folder. The default Exchange 2010 installation folder is C:\Program Files\Microsoft \Exchange Server\.
- The DropDirectory parameter in the **Set-ForeignConnector** cmdlet
  This value is set for each Foreign connector that exists on the Hub Transport server. The value of the *DropDirectory* parameter may be a simple directory name or an absolute file path. If the value of the *RootDropDirectoryPath* is specified, the value of the *DropDirectory* parameter must be a simple directory name. If the value of the *RootDropDirectoryPath* isn't specified, the *DropDirectory* parameter may contain absolute path information or may be a simple directory name. By default, the value of the *DropDirectory* parameter is the name of the Foreign connector.
  If the value of the *DropDirectory* parameter doesn't contain absolute path information, the location of the Drop directory is defined by the combination of the *DropDirectory* and the *RootDropDirectoryPath* parameters. If the value of the *DropDirectory* parameter contains absolute path information, the value of the *RootDropDirectoryPath* parameter must be unspecified.

Note:

You can't configure the Drop directory by using the EMC. To configure the Drop directory, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example sets the root Drop directory for all Foreign connectors on the Exchange 2010 computer Hub01 to C:\Drop Directory. Then it configures the Foreign connector Fax Connector to use the Drop directory Fax. As a result of running these two commands, the Fax Connector Foreign connector uses C:\Drop Directory\Fax folder as its Drop directory.

```
Set-TransportServer Hub01 -RootDropDirectoryPath "C:\Drop Directory"
Set-ForeignConnector "Fax Connector" -DropDirectory "Fax"
```

When you change the location of the Drop directory, you have to be aware of the following:

- Changing the location of the Drop directory doesn't copy any existing message files from the old Drop directory to the new Drop directory. The new Drop directory location is active almost immediately after the configuration change, but any existing message files are left in the old Drop directory.
- The Drop directory must have the following permissions assigned to it:
  - Network Service: Full Control
  - System: Full Control

- Administrators: Full Control

For detailed syntax and parameter information, see Set-TransportServer and Set-ForeignConnector.

Use the Shell to configure the maximum size of the Drop directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Foreign connectors" entry in the Transport Permissions topic.

The maximum size of the Drop directory used by a Foreign connector is controlled by the **Set-ForeignConnector** cmdlet. When the specified maximum value is reached, no new message files can be copied into the Drop directory until the existing messages are delivered and deleted. By default, the maximum size of the Drop directory is `unlimited`.

Note:
You can't configure the Drop directory by using the EMC. To configure the Drop directory, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example sets the maximum size of the Drop directory to 400 MB for the Foreign connector named "Fax Connector."

```
Set-ForeignConnector "Fax Connector" -DropDirectoryQuota 400MB
```

The valid input range for this parameter is from 1 byte through about 2GB (2147483647 bytes).

For detailed syntax and parameter information, see Set-ForeignConnector.

1.7.2.11.17 Enable or Disable a Foreign Connector

Enable or Disable a Foreign Connector

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can use the Shell to enable or disable an existing Foreign connector for Microsoft Exchange Server 2010. A Foreign connector can only be installed on a computer running Exchange 2010 that has the Hub Transport server role installed. A Foreign connector uses a Drop directory to send messages to a local messaging server that doesn't use SMTP as its primary transport mechanism.

Looking for other management tasks related to managing connectors? Check out Managing Connectors.

Prerequisites

You must have an existing Foreign connector. For detailed steps about creating a Foreign connector, see Create a Foreign Connector.

Use the Shell to enable or disable a Foreign connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Foreign connectors" entry in the Transport Permissions topic.

You can use the **Set-ForeignConnector** cmdlet to enable or disable a Foreign connector. The *Identity* parameter specifies the Foreign connector that you want to enable or disable. The *Identity* parameter can be the GUID or the name of the Foreign connector.

Note:

You can't enable or disable a Foreign connector by using the Exchange Management Console. To enable or disable a Foreign connector, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example disables the Foreign connector Contoso.com Foreign Connector.

```
Set-ForeignConnector "Contoso.com Foreign Connector" -Enabled $False
```

This example enables the same Foreign connector.

```
Set-ForeignConnector "Contoso.com Foreign Connector" -Enabled $True
```

This example disables all Foreign connectors in your organization.

```
Get-ForeignConnector | Set-ForeignConnector -Enabled $False
```

For detailed syntax and parameter information, see Set-ForeignConnector.

1.7.2.11.18 Remove a Foreign Connector

Remove a Foreign Connector

Transport > Managing Transport Servers > Managing Connectors >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to remove an existing Foreign connector in Microsoft Exchange Server 2010. A Foreign connector can only be installed on a computer running Exchange 2010 that has the Hub Transport server role installed. A Foreign connector uses a Drop directory to send messages to a local messaging server that doesn't use SMTP as its primary transport mechanism.

Looking for other management tasks related to managing connectors? Check out Managing Connectors.

Use the Shell to remove a Foreign connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Foreign connectors" entry in the Transport Permissions topic.

You can use the **Remove-ForeignConnector** cmdlet to remove a Foreign connector. The *Identity* parameter specifies the Foreign connector that you want to remove. The *Identity* parameter can be the GUID or the name of the Foreign connector.

Note:

You can't remove a Foreign connector by using the Exchange Management Console. To remove a Foreign connector, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example removes the Foreign connector Contoso.com Foreign Connector.

```
Remove-ForeignConnector "Contoso.com Foreign Connector"
```

For detailed syntax and parameter information, see Remove-ForeignConnector.

1.7.2.11.19 Configure the Pickup Directory

Configure the Pickup Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to configure the properties of the Pickup directory in Microsoft Exchange Server 2010. By default, the Pickup directory exists on every computer running Exchange 2010 that has the Hub Transport server role or the Edge Transport server role installed. Correctly formatted e-mail message files that you copy to the Pickup directory are submitted for delivery. The Pickup directory is used by administrators for mail flow testing, or by applications that must create and submit their own messages.

Looking for other management tasks related to managing connectors? Check out Managing Connectors.

What Do You Want to Do?

- Use the Shell to configure the Pickup directory location
- Use the Shell to configure the maximum size for message headers
- Use the Shell to configure the maximum number of recipients per message
- Use the Shell to configure the maximum rate of message processing for the Pickup directory

Use the Shell to configure the Pickup directory location

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub server" entry in the Transport Permissions topic.

Use the *PickupDirectoryPath* parameter of the **Set-TransportServer** cmdlet to configure the location of the Pickup directory. By default, the Pickup directory is located at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\PickUp. The directory must be local to the Exchange 2010 computer.

Note:

You can't configure the Pickup directory by using the Exchange Management Console (EMC). To configure the Pickup directory, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example changes the Pickup directory location to C:\Pickup Directory on server Exchange 01.

```
Set-TransportServer Exchange01 -PickupDirectoryPath "C:\Pickup Directory"
```

When changing the location of the Replay directory, you need to be aware of the following:

- Setting the value of the *PickupDirectoryPath* parameter to `$null` disables the Pickup directory.
- The directory specified by the *PickupDirectoryPath* parameter and the *ReplayDirectoryPath* parameter can't be the same.
- Changing the location of the Pickup directory doesn't copy any existing message files from the old Pickup directory to the new Pickup directory. The new Pickup directory location is active almost immediately after the configuration change, but any existing message files are left in the old Pickup directory.

You also need to make sure that the permissions are configured correctly on the new location of the Pickup directory. To learn more about the permission requirements, see "Permissions for the Pickup and Replay Directories" in Understanding the Pickup and Replay Directories.

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to configure the maximum size for message headers

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub server" entry in the Transport Permissions topic.

Use the *PickupDirectoryMaxHeaderSize* parameter of the **Set-TransportServer** cmdlet to set the maximum message header size for a Pickup directory. By default, the maximum size for the header part of a message that can be processed by the Pickup directory is 64 KB. Messages that contain headers larger than the specified maximum value are rejected by the Exchange 2010 server.

Note:

You can't configure the Pickup directory by using the EMC. To configure the Pickup directory, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example configures the maximum size for message headers accepted by the Pickup directory to 96 KB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -PickupDirectoryMaxHeaderSize 96KB
```

The valid input range for the *PickupDirectoryMaxHeaderSize* parameter is from 32 KB through about 2 GB (2147483647 bytes).

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to configure the maximum

number of recipients per message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub server" entry in the Transport Permissions topic.

Use the *PickupDirectoryMaxRecipientsPerMessage* parameter of the **Set-TransportServer** cmdlet to set the maximum number of recipients per message that the Pickup directory accepts. By default, the maximum number of recipients in a message that can be processed by the Pickup directory is 100. Messages that contain more recipients than the specified maximum value are rejected by the Exchange 2010 server.

Note:
You can't configure the Pickup directory by using the EMC. To configure the Pickup directory, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example sets the maximum number of recipients in a message accepted by the Pickup directory to 200 on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -PickupDirectoryMaxRecipientsPerMessage 200
```

The valid input range for the *PickupDirectoryMaxRecipientsPerMessage* parameter is from 1 through 10000.

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to configure the maximum rate of message processing for the Pickup directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub server" entry in the Transport Permissions topic.

The rate of message processing for both the Pickup directory and the Replay directory is specified by the *PickupDirectoryMaxMessagesPerMinute* parameter of the **Set-TransportServer** cmdlet. By default, the Pickup directory can process messages at a rate of 100 messages per minute. Limiting the rate of message processing helps prevent performance issues caused by processing numerous messages in the Pickup directory.

Note:
You can't configure the Pickup directory by using the EMC. To configure the Pickup directory, you must use the Shell. For more information about how to use the Shell, see Exchange Management Shell.

This example increases the maximum rate of message processing for the Pickup and Replay directories to 200 messages per minute on server Exchange01.

```
Set-TransportServer Exchange01 -PickupDirectoryMaxMessagesPerMinute 200
```

The valid input range for the *PickupDirectoryMaxMessagesPerMinute* parameter is from 1 through 20000.

For detailed syntax and parameter information, see Set-TransportServer.

1.7.2.11.20 Configure the Replay Directory

Configure the Replay Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to configure the properties of the Replay directory in Microsoft Exchange Server 2010. By default, the Replay directory exists on every computer running Exchange 2010 that has the Hub Transport server role or the Edge Transport server role installed. Correctly formatted e-mail message files that you copy to the Replay directory are submitted for delivery. The Replay directory receives messages from non-SMTP foreign gateway servers and resubmits messages that administrators export from the queues of Exchange 2010 servers.

Looking for other management tasks related to managing connectors? Check out Managing Connectors.

Use the Shell to configure the Replay directory location

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to configure the Replay directory.

Use the *ReplayDirectoryPath* parameter of the **Set-TransportServer** cmdlet to configure the location of the Replay directory. By default, the Replay directory is located at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Replay. The directory must be local to the computer running Exchange 2010.

This example changes the Replay directory location to C:\Replay Directory on server Exchange01.

```
Set-TransportServer Exchange01 -ReplayDirectoryPath "C:\Replay Directory"
```

When changing the location of the Replay directory, you need to be aware of the following:

- Setting the value of the *ReplayDirectoryPath* parameter to `$null` disables the Replay directory.
- The directory specified by the *ReplayDirectoryPath* parameter and the *PickupDirectoryPath* parameter can't be the same.
- Changing the location of the Replay directory doesn't copy any existing message files from the old Replay directory to the new Replay directory. The new Replay directory location is active almost immediately after the configuration change, but any existing message files are left in the old Replay directory.

You also need to make sure that the permissions are configured correctly on the new location of the Replay directory. To learn more about the permission requirements, see "Permissions for the Pickup and Replay Directories" in Understanding the Pickup and Replay Directories.

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to configure the maximum rate of message processing for the Replay directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to configure the Replay directory.

The rate of message processing for both the Pickup directory and the Replay directory is specified by the *PickupDirectoryMaxMessagesPerMinute* parameter of the **Set-TransportServer** cmdlet. By default, the Replay directory can process messages at a rate of 100 messages per minute. Limiting the rate of message processing helps prevent performance issues caused by processing numerous messages in the Replay directory.

This example increases the maximum rate of message processing for the Pickup and Replay directories to 200 messages per minute on server Exchange01.

```
Set-TransportServer Exchange01 -PickupDirectoryMaxMessagesPerMinute 200
```

The valid input range for the *PickupDirectoryMaxMessagesPerMinute* parameter is from 1 through 20000.

For detailed syntax and parameter information, see Set-TransportServer.

1.7.2.12 Managing Delivery Status Notifications

Managing Delivery Status Notifications

Exchange Server 2010 > Transport > Managing Transport Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-01*

Create a Custom DSN Message

View or Modify an Existing Custom DSN Message

Remove a Custom DSN Message

1.7.2.12.1 Create a Custom DSN Message

Create a Custom DSN Message

Transport > Managing Transport Servers > Managing Delivery Status Notifications >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to create a customized delivery status notification (DSN) message on a computer running Microsoft Exchange Server 2010 that has the Hub Transport server role or the Edge Transport server role installed.

Looking for other management tasks related to DSNs? Check out Managing Delivery Status Notifications.

Prerequisites

Before you perform these procedures, you must specify the identity of the message and prepare the text that you want to include in the message. For more information about how to specify the identity of a DSN message and how to work with the text of a customized DSN message, including how to format HTML DSN messages, see DSN Message Identity and DSN Message Text.

Use the Shell to create a customized DSN message targeted to internal senders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "DSNs" entry in the Transport Permissions topic.

Note:
You can't use the EMC to create a customized DSN message targeted to internal senders.

Use the **New-SystemMessage** cmdlet to create a customized DSN. This example creates a customized DSN with the following settings:

- Customized DSN is created for DSN code 5.1.2.
- DSN is sent to internal senders only.
- DSN is customized for the English language.

```
New-SystemMessage -DSNCode 5.1.2 -Text "The mailbox you tried to send an e-mail m
```

For detailed syntax and parameter information, see New-SystemMessage.

Use the Shell to create a customized DSN message targeted to external senders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "DSNs" entry in the Transport Permissions topic.

Note:
You can't use the EMC to create a customized DSN message targeted to external senders.

Use the **New-SystemMessage** cmdlet to create a customized DSN. This example creates a customized DSN with the following settings:

- Customized DSN is created for DSN code 5.1.2.
- DSN is sent to external senders only.
- DSN is customized for the English language.

```
New-SystemMessage -DSNCode 5.1.2 -Text "The mailbox you tried to send an e-mail m
```

For detailed syntax and parameter information, see New-SystemMessage.

Use the Shell to create a customized HTML DSN message targeted to internal senders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "DSNs" entry in the Transport Permissions topic.

Note:
You can't use the EMC to create a customized HTML DSN message targeted to internal senders.

Use the **New-SystemMessage** cmdlet to create an HTML formatted customized DSN. This example creates a customized DSN with the following settings:

- Customized DSN is created for code 5.1.2.
- DSN text is HTML formatted, including a hyperlink.
- DSN is sent to internal senders only.
- DSN is customized for the English language.

```
New-SystemMessage -DSNCode 5.1.2 -Text 'The mailbox you tried to send an e-mail m
```

For detailed syntax and parameter information, see New-SystemMessage.

1.7.2.12.2 View or Modify an Existing Custom DSN Message

View or Modify an Existing Custom DSN Message

Transport > Managing Transport Servers > Managing Delivery Status Notifications >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to view or modify a custom delivery status notification (DSN) message on a computer running Microsoft Exchange Server 2010 that has the Hub Transport server role or the Edge Transport server role installed.

You can only use the **Set-SystemMessage** cmdlet to modify DSN messages that have already been customized by using the **New-SystemMessage** cmdlet. If you want to customize the original text of a default DSN message provided by Exchange 2010, you must use the **New-SystemMessage** cmdlet to create a custom DSN. For more information about how to create a custom DSN message, see Create a Custom DSN Message.

Looking for other management tasks related to DSNs? Check out Managing Delivery Status Notifications.

Prerequisites

Before you perform these procedures, you must specify the identity of the message and prepare the text that you want to include in the message. For more information about how to specify the identity of a DSN message and how to work with the text of a customized DSN message, including how to format HTML DSN messages, see DSN Message Identity and DSN Message Text.

Use the Shell to change the text of a custom DSN message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "DSNs" entry in the Transport Permissions topic.

Note:
You can't use the EMC to change the text of a custom DSN message.

Use the **Set-SystemMessage** cmdlet to modify the settings of a custom DSN message. This example changes the text assigned to the DSN customized for DSN code 5.1.2 for the English language.

```
Set-SystemMessage En\Internal\5.1.2 -Text "The mailbox you tried to send an e-mai
```

For detailed syntax and parameter information, see Set-SystemMessage.

Use the Shell to view a list of custom DSN messages in your organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "DSNs" entry in the Transport Permissions topic.

Note:
You can't use the EMC to view a list of custom DSN messages in your organization.

By default, the **Get-SystemMessage** cmdlet, which you use to view the configuration of custom DSN messages, returns a summary list of all custom DSN messages in your organization. This example returns a tabular list of all custom DSNs in your organization.

```
Get-SystemMessage
```

For detailed syntax and parameter information, see Get-SystemMessage.

Use the Shell to view a list of built-in DSN messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "DSNs" entry in the Transport Permissions topic.

Note:
You can't use the EMC to view a list of built-in DSN messages.

This example, which requires the **Get-SystemMessage** command with the *Original* parameter, returns a list of the original DSN messages included with Exchange 2010.

```
Get-SystemMessage -Original
```

For detailed syntax and parameter information, see Get-SystemMessage.

Use the Shell to view detailed information

about a custom DSN message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "DSNs" entry in the Transport Permissions topic.

Note:
You can't use the EMC to view detailed information about a custom DSN message.

Use the **Get-SystemMessage** command to view detailed configuration about a custom DSN message. This example shows detailed configuration for the internal 5.1.2 DSN customized for English.

```
Get-SystemMessage En\Internal\5.1.2 | Format-List
```

For detailed syntax and parameter information, see Get-SystemMessage.

1.7.2.12.3 Remove a Custom DSN Message

Remove a Custom DSN Message

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to remove a custom delivery status notification (DSN) message on a computer running Microsoft Exchange Server 2010 that has the Hub Transport server role or the Edge Transport server role installed.

Looking for other management tasks related to DSNs? Check out Managing Delivery Status Notifications.

Prerequisites

Before you perform this procedure, you must specify the identity of the DSN message or messages that you want to view. For more information about how to specify the identity of a DSN message, see DSN Message Identity.

Use the Shell to remove an existing DSN message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "DSNs" entry in the Transport Permissions topic.

Note:
You can't use the EMC to remove an existing DSN message.

When you remove a customiz DSN message, the DSN code associated with that message reverts to the original DSN message included with Exchange 2010.

Note:
You can't remove an original DSN message included with Exchange 2010. To change an original DSN message, you must create a customiz DSN message for the DSN code that you want to customize.

This example removes the customiz 5.1.2 DSN for the English locale configured to be sent to Internal senders.

```
Remove-SystemMessage En\Internal\5.1.2
```

For detailed syntax and parameter information, see Remove-SystemMessage.

1.7.2.13 Managing Edge Subscriptions

Managing Edge Subscriptions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-01*

Import an Edge Subscription File to an Active Directory Site

Create an Edge Subscription File on an Edge Transport Server

Force EdgeSync Synchronization

Remove an Edge Subscription

Verify EdgeSync Results for a Recipient

Modify AD LDS Configuration

1.7.2.13.1 Import an Edge Subscription File to an Active Directory Site

Import an Edge Subscription File to an Active Directory Site

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After you create a new Edge Subscription, the Edge Transport server referenced in the Edge Subscription file is associated with the Hub Transport servers in an Active Directory site. For more information about Edge Subscriptions, see Understanding Edge Subscriptions.

Looking for other management tasks related to transport servers? Check out Managing Transport Servers.

Prerequisites

- The Active Directory site to which the Edge Transport server is subscribed must contain at least one Hub Transport server.
- Verify that you have configured the settings on the Hub Transport server that are replicated to the Edge Transport server. For more information, see Understanding Edge Subscriptions.
- Read the following topics:

- Create an Edge Subscription File on an Edge Transport Server
- Understanding Edge Subscriptions

- Create the Edge Subscription file by running the **New-EdgeSubscription** cmdlet on the Edge Transport server. By running the **New-EdgeSubscription** cmdlet, you create an Edge Subscription file that you must copy to your Hub Transport server's hard disk.
- Copy the Edge Subscription file from the Edge Transport server to the Hub Transport server where you will perform this procedure.

Note:
It's a best practice to delete the Edge Subscription file from the Edge Transport server after you copy the file to the Hub Transport server where you will import the Edge Subscription file, and from the Hub Transport server after the subscription is imported.

What Do You Want to Do?

- Use the EMC to import the Edge Subscription file
- Use the Shell to import the Edge Subscription file

Use the EMC to import the Edge Subscription file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "EdgeSync" entry in the Transport Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **Edge Subscriptions** tab.
3. In the action pane, click **New Edge Subscription**. On the **New Edge Subscription** page, complete the following fields:
   - **Active Directory site** Click **Browse**, and then select an Active Directory site in the drop-down list. This field identifies the Active Directory site where the Hub Transport server is connecting to the Edge Transport server for which the Edge Subscription exists.
   - **Subscription file** Click **Browse**, and then select an Edge Subscription file.
   - **Automatically create a Send connector for this Edge Subscription** Select this check box to automatically create a Send connector that routes messages from the Exchange organization to the Internet. The Edge Subscription is configured as the source server for the Send connector. The Send connector is configured to route messages to all domains by using Domain Name System (DNS) MX resource records.
4. Click **New** to create the new Edge Subscription.
5. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to import the Edge Subscription file

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "EdgeSync" entry in the Transport Permissions topic.

This example subscribes an Edge Transport server to the specified site and creates the Internet Send connector and the Send connector from the Edge Transport server to the Hub Transport servers automatically.

```
New-EdgeSubscription -FileData ([byte[]]$(Get-Content -Path "C:\EdgeSubscriptionI
```

Note:
The default value of the *CreateInternetSendConnector* parameter and the *CreateInboundSendConnector* parameter is `$true`. It's shown here for demonstration only.

For detailed syntax and parameter information, see New-EdgeSubscription.

1.7.2.13.2 Create an Edge Subscription File on an Edge Transport Server

Create an Edge Subscription File on an Edge Transport Server

Transport > Managing Transport Servers > Managing Edge Subscriptions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can export an Edge Subscription file from a computer that has the Edge Transport server role installed. The Edge Subscription file is used in the EdgeSync process, and it contains information about the credentials that are used during the LDAP communication process. These credentials are used to authenticate and authorize the connection between Active Directory Lightweight Directory Service (AD LDS) and Active Directory during replication. To learn more about Edge Subscriptions, see Understanding Edge Subscriptions.

After you perform this procedure on the Edge Transport server, you must copy the Edge Subscription file to a location in your internal network and then import the file to your Exchange organization to complete the subscription process.

Note:
After you complete the subscription, it's a best practice to delete the Edge Subscription file from all locations: the Edge Transport server and the internal network location to which you copied the file for importing to your Exchange organization.

Looking for other management tasks related to managing Edge Subscriptions? Check out Managing Edge Subscriptions.

Use the Shell to create an Edge Subscription file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "EdgeSync" entry in the Transport Permissions topic.

Note:
You can't use the EMC to export an Edge Subscription file.

This example exports an Edge Subscription file.

```
New-EdgeSubscription -FileName "C:\EdgeSubscriptionInfo.xml"
```

Note:
When the **New-EdgeSubscription** cmdlet is run on the Edge Transport server, you receive a prompt to acknowledge the commands that will be disabled and the configuration that will be overwritten on the Edge Transport server. To bypass this confirmation, you must use the *Force* parameter. This parameter is useful when you script the **New-EdgeSubscription** cmdlet. The *Force* parameter is also used to overwrite an existing file with the same name as the file that you're creating when you resubscribe an Edge Transport server.

For detailed syntax and parameter information, see New-EdgeSubscription.

1.7.2.13.3 Force EdgeSync Synchronization

Force EdgeSync Synchronization

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can manually start synchronization of data from Active Directory to the subscribed Edge Transport servers.

The configuration and recipient data is kept up to date by periodically synchronizing changes from Active Directory to Active Directory Lightweight Directory Services (AD LDS). By default, configuration data is synchronized to AD LDS once every hour, and recipient data is synchronized to AD LDS once every four hours. You can change these intervals using the **Set-EdgeSyncService** cmdlet.

You may want to force EdgeSync synchronization to start initial replication immediately after you create the Edge Subscription, or if you've made significant changes to the configuration or recipients in Active Directory. The **Start-EdgeSynchronization** cmdlet resets the EdgeSync synchronization schedule. The time of the subsequent synchronization intervals is based on the time that this command is initiated. You can force a full replication or only the changes since last replication.

Looking for other management tasks related to managing Edge Subscriptions? Check out Managing Edge Subscriptions.

Use the Shell to force EdgeSync synchronization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "EdgeSync" entry in the Transport Permissions topic.

Note:
You can't use the EMC to force EdgeSync synchronization.

This example starts EdgeSync synchronization with the following options:

- The synchronization is initiated from the Hub Transport server Hub01.
- All Edge Transport servers are synchronized.
- Only the changes since the last replication are synchronized.

```
Start-EdgeSynchronization -Server Hub01
```

This example starts EdgeSync synchronization with the following options:

- The synchronization is initiated from the Hub Transport server Hub01.
- Only the Edge Transport server Edge03 is synchronized.
- All recipient and configuration data are fully synchronized.

```
Start-EdgeSynchronization -Server Hub01 -TargetServer Edge03 -ForceFullSync
```

For detailed syntax and parameter information, see Start-EdgeSynchronization.

1.7.2.13.4 Remove an Edge Subscription

Remove an Edge Subscription

Transport > Managing Transport Servers > Managing Edge Subscriptions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove an Edge Subscription. After you remove the Edge Subscription, synchronization of information from Active Directory to Active Directory Lightweight Directory Services (AD LDS) stops. All the accounts that are stored in AD LDS are removed, and the computer that has the Edge Transport server role installed is removed from the source server list of any Send connector. You will no longer be able to use the Edge Transport server features that rely on Active Directory data.

Note:

To completely remove the Edge Subscription, you must run this procedure on the Edge Transport server and on the Hub Transport server. To run this procedure on the Edge Transport server, you can only use the Shell. To run this procedure on the Hub Transport server, you can use the EMC or the Shell.

Looking for other management tasks related to managing Edge Subscriptions? Check out Managing Edge Subscriptions.

Use the EMC to remove an Edge Subscription

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Sync" entry in the Transport Permissions topic.

1. Expand **Organization Configuration**, select **Hub Transport**, and then in the result pane, click the **Edge Subscriptions** tab.
2. Select the Edge Subscription that you want to remove. In the action pane, click **Remove**.

Use the Shell to remove an Edge Subscription

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "EdgeSync" entry in the Transport Permissions topic.

To remove an Edge Subscription, use the following syntax.

```
Remove-EdgeSubscription -Identity <EdgeorHubServerName> -DomainController <dc.dom
```

Note:
The *DomainController* parameter is optional. Use this parameter when you want to specify the domain controller that will write this change to Active Directory.

For detailed syntax and parameter information, see Remove-EdgeSubscription.

1.7.2.13.5 Verify EdgeSync Results for a Recipient

Verify EdgeSync Results for a Recipient

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Shell to verify the EdgeSync synchronization results for a specific recipient.

Looking for other management tasks related to Edge Subscriptions? Check out Managing Edge Subscriptions.

Prerequisites

You must have an Edge server subscribed to your Internet-facing Active Directory site.

Use the Shell to verify EdgeSync results for a single recipient

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "EdgeSync" entry in the Transport Permissions topic.

Note:
You can't use the EMC to verify EdgeSync results for a single recipient.

Use the **Test-EdgeSynchronization** cmdlet to verify EdgeSync results for a single recipient. This cmdlet is also used to verify configuration replication. To verify a single recipient, you need to use the *VerifyRecipient* parameter.

The following command verifies EdgeSync results for the user kate@contoso.com:

```
Test-EdgeSynchronization -VerifyRecipient kate@contoso.com
```


1.7.2.13.6 Modify AD LDS Configuration

Modify AD LDS Configuration

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the ConfigureAdam.ps1 script in the Shell to modify the default configuration

of the Active Directory Lightweight Directory Services (AD LDS) on the Edge Transport server.

Important:
Don't modify the AD LDS configuration of an Edge Transport server after the Edge Transport server is subscribed to the Microsoft Exchange Server 2010 organization. If you modify the AD LDS configuration of a subscribed Edge Transport server, you must resubscribe the Edge Transport server to the Exchange organization. For more information, see Import an Edge Subscription File to an Active Directory Site.

After you install the Edge Transport server role, you can use the ConfigureAdam.ps1 script provided with Exchange 2010 to modify the ports and directories that AD LDS uses.

The ConfigureAdam.ps1 script invokes the **dsdbutil** command to change the registry settings for AD LDS. The **dsdbutil** command is a management tool for AD LDS that's intended for use by experienced administrators only.

Caution:
Don't modify the registry settings without using the script. Manual registry changes to the AD LDS configuration make the AD LDS instance unavailable.

The following table lists the parameters that can be used by the ConfigureAdam.ps1 script and how each parameter is used. You can use one, all, or a combination of any of these parameters to modify AD LDS. You must run the script by using the Shell.

ConfigureAdam.ps1 parameters and their use

Parameter	Use
Ldapport	Use this parameter to modify the port used for LDAP communication. By default, the Edge Transport server uses the nonstandard port 50389.
Sslport	Use this parameter to modify the communication port used for secure LDAP communication. By default, the Edge Transport server uses the nonstandard port 50636.
LogPath	Use this parameter to modify the location of the log files. By default, the Edge Transport server creates log files in the path C:\Program Files\Microsoft\Exchange server\V14\Transport Roles\Data\adam.
DataPath	Use this parameter to modify the location of the directory database file. By default, the Edge Transport server stores the directory database in the path C:\Program Files\Microsoft\Exchange server\V14\Transport Roles\Data\adam.

Looking for other management tasks related to Edge Subscription? See Managing Edge Subscriptions.

Prerequisites

- Determine the settings that you will use with this command.

- If you modify the LDAP port or the SSL port used by AD LDS, first verify that the selected port isn't being used by another application. You can use the **netstat** command to view ports being used on the Edge Transport server.

Use the ConfigureAdam.ps1 script in the Shell to modify AD LDS configuration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Edge Transport server" entry in the Transport Permissions topic.

The ConfigureAdam.ps1 script is located by default in the C:\Program Files\Microsoft \Exchange Server\V14\Scripts folder.

This example uses the ConfigureAdam.ps1 script to change the LDAP port to 5000.

```
ConfigureAdam.ps1 -LdapPort:5000
```

This example uses the ConfigureAdam.ps1 script to make the following changes to the AD LDS configuration:

- Changes the LDAP port to 5000
- Changes the SSL port to 5001
- Changes the log path to D:\Exchange Server\Data\ADLDS
- Changes the data path to D:\Exchange Server\Data\ADLDS

```
ConfigureAdam.ps1 -LdapPort:5000 -SslPort:5001 -LogPath:"D:\Exchange Server\Data\
```


1.7.2.14 Managing MailTips

Managing MailTips

Exchange Server 2010 > Transport > Managing Transport Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-04-03*

Configure Organizational Settings for MailTips

Configure Group Metrics

Configure Custom MailTips for Recipients

1.7.2.14.1 Configure Organizational Settings for MailTips

Configure Organizational Settings for MailTips

Transport > Managing Transport Servers > Managing MailTips >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

MailTips are informative messages displayed to users while they compose a message. Microsoft Exchange Server 2010 analyzes the message, including the list of recipients to which it's addressed. If a potential problem is detected, MailTips notify users prior to

sending the message. With the help of the information provided by MailTips, senders can adjust the message they are composing to avoid undesirable situations or non-delivery reports (NDRs). To learn more about MailTips, see Understanding MailTips.

You can configure various settings that define how you use MailTips in your organization.

Looking for other management tasks related to MailTips? Check out Managing MailTips.

Use the Shell to enable or disable MailTips

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "MailTips" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable or disable MailTips.

You use the **Set-OrganizationConfig** cmdlet to enable or disable MailTips in your organization. MailTips are enabled by default, when you install a new Exchange 2010 organization. This example shows how to enable MailTips in your organization.

```
Set-OrganizationConfig -MailTipsAllTipsEnabled $true
```

For detailed syntax and parameter information, see Set-OrganizationConfig.

Use the Shell to configure the large audience size for your organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "MailTips" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure the large audience size for your organization.

You use the **Set-OrganizationConfig** cmdlet to configure the large audience size for your organization. When senders address messages to more recipients than the size you configure, they are shown the Large Audience MailTip. The large audience size is set to 25 by default. This example configures the large audience size to 50 in your organization.

```
Set-OrganizationConfig -MailTipsLargeAudienceThreshold 50
```

For detailed syntax and parameter information, see Set-OrganizationConfig.

Use the Shell to enable or disable the External Recipients MailTip

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "MailTips" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable or disable the External Recipients MailTip.

When enabled, senders are notified that the message will leave your organization if they add an external recipient or a distribution group that contains external recipients. By default, the External Recipients MailTip is disabled.

Note:
The External Recipients MailTip relies on group metrics data. Therefore, if you enable the External Recipients MailTip, make sure that the group metrics MailTip is also enabled.

Depending on the communications profile of your organization, you may want to enable or disable the External Recipients MailTip. For example, travel agencies may choose to disable the External Recipients MailTip because most of their communication is with people outside their organization. In contrast, law firms may want to enable this to ensure that the senders are aware when information is being shared outside the firm.

You use the **Set-OrganizationConfig** cmdlet to enable or disable the External Recipients MailTip in your organization. This example enables the External Recipients MailTip.

```
Set-OrganizationConfig -MailTipsExternalRecipientsTipsEnabled $true
```

For detailed syntax and parameter information, see Set-OrganizationConfig.

Use the Shell to enable or disable MailTips that rely on mailbox data

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "MailTips" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable or disable MailTips that rely on mailbox data.

You use the **Set-OrganizationConfig** cmdlet to enable or disable MailTips that rely on mailbox data. The Recipient Out of Office and Mailbox Full MailTips rely on the mailbox data. The Client Access server evaluates these MailTips by querying the Mailbox server using RPC. By default, these MailTips are enabled. This example enables MailTips that rely on mailbox data.

```
Set-OrganizationConfig -MailTipsMailboxSourcedTipsEnabled $true
```

For detailed syntax and parameter information, see Set-OrganizationConfig.

Use the Shell to enable or disable MailTips that rely on group metrics data

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "MailTips" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable or disable MailTips that rely on group metrics data.

You use the **Set-OrganizationConfig** cmdlet to enable or disable MailTips that rely on group metrics data. By default, these MailTips are enabled. group metrics data consists of the membership count and external members count for all distribution groups and dynamic distribution groups in your organization. MailTips like Large Audience and External Recipients rely on this data. This example enables MailTips that rely on group metrics data in your organization.

```
Set-OrganizationConfig -MailTipsGroupMetricsEnabled $true
```

For detailed syntax and parameter information, see Set-OrganizationConfig.

Use the Shell to configure MailTips for organizational relationships

In Microsoft Exchange Server 2010 Service Pack 1 (SP1), you can configure organizational relationships with Exchange Online or other organizations. By establishing an organizational relationship, you can enhance the user experience for both organizations by sharing free/busy data, configuring secure message flow, and enabling message tracking. For more information about organizational relationships, see Understanding Federation.

You can use various settings to control how MailTips are used between two organizations that have established an organizational relationship. The procedures in this section illustrate these various controls. In all examples, the on-premises organization is contoso.com, the remote organization is online.contoso.com, and the organizational relationship is named Contoso Online.

You use the **Set-OrganizationRelationship** cmdlet to configure these settings.

Use the Shell to enable or disable MailTips between two organizations

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "MailTips" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable or disable MailTips between two organizations.

This example configures the organizational relationship so that MailTips are returned to senders in the remote organization when composing messages to recipients in your organization.

```
Set-OrganizationRelationship -Identity "Contoso Online" -MailTipsAccessEnabled $t
```

This example configures the organizational relationship to prevent MailTips from being returned to senders in the remote organization when composing messages to recipients in your organization.

```
Set-OrganizationRelationship -Identity "Contoso Online" -MailTipsAccessEnabled $f
```

For detailed syntax and parameter information, see Set-OrganizationRelationship.

Use the Shell to configure which MailTips are returned to the remote organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "MailTips" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure which MailTips are returned to the remote organization.

For each organizational relationship, you can determine which set of MailTips are returned to senders in the other organization. This example configures the organizational relationship so that all MailTips are returned.

```
Set-OrganizationRelationship -Identity "Contoso Online" -MailTipsAccessLevel All
```

This example configures the organizational relationship so that only the Automatic Replies, Oversize Message, Restricted Recipient, and Mailbox Full MailTips are returned.

```
Set-OrganizationRelationship -Identity "Contoso Online" -MailTipsAccessLevel Limi
```

This example configures the organizational relationship so that no MailTips are returned.

Note:
Don't use this method to disable MailTips for this relationship. To disable MailTips, set the *MailTipsAccessEnabled* parameter to `$false`.

```
Set-OrganizationRelationship -Identity "Contoso Online" -MailTipsAccessLevel None
```

For detailed syntax and parameter information, see Set-OrganizationRelationship.

Use the Shell to configure a specific group of users for whom recipient-specific MailTips are returned

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "MailTips" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure a specific group of users for whom recipient-specific MailTips are returned.

You can restrict the return of recipient-specific MailTips to a specific group of users. By default, when you enable MailTips for an organizational relationship, the following recipient-specific MailTips are returned for all users:

- Automatic Replies
- Mailbox Full
- Custom MailTip

You can specify a MailTips access group on the organizational relationship. After you specify a group, the recipient-specific MailTips are returned only for mailboxes, mail contacts, and mail users that are members of that group. This example configures the organizational relationship to return recipient-specific MailTips only for members of the ShareMailTips@contoso.com group.

```
Set-OrganizationRelationship -Identity "Contoso Online" -MailTipsAccessScope Shar
```

For detailed syntax and parameter information, see Set-OrganizationRelationship.

1.7.2.14.2 Configure Group Metrics

Configure Group Metrics

Transport > Managing Transport Servers > Managing MailTips >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

MailTips that provide information about the size of distribution groups and dynamic distribution groups rely on group metrics data. Group metrics data is generated on designated Mailbox servers and is copied to Client Access servers using the Microsoft Exchange File Distribution Service. For more information about group metrics, see Understanding Group Metrics.

You can enable or disable group metrics generation on a Mailbox server and configure the time when group metrics data is generated.

Looking for other management tasks related to MailTips and group metrics? Check out

Managing MailTips.

Prerequisites

Group metrics data is only used for MailTips. Make sure that group metrics MailTips are enabled in your organization. For detailed steps, see Configure Organizational Settings for MailTips. To learn more about MailTips, see Understanding MailTips.

Use the Shell to enable or disable group metrics generation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Group metrics" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to enable or disable group metrics generation.

Note:
By default, group metrics data is generated on any server responsible for generating the offline address book (OAB). The configuration shown in this example is only necessary for organizations that don't use OABs. For more information, see Understanding Group Metrics.

You use the **Set-MailboxServer** cmdlet to enable or disable group metrics generation on a Mailbox server. This example forces group metrics generation on server MBX1.

```
Set-MailboxServer MBX1 -ForceGroupMetricsGeneration $true
```

This example disables group metrics generation on server MBX1.

Note:
If this server is generating OABs, it will continue to generate group metrics data. This example is only applicable for servers that don't generate OABs.

```
Set-MailboxServer MBX1 -ForceGroupMetricsGeneration $false
```

Note:
In the release to manufacturing (RTM) version of Microsoft Exchange Server 2010, this parameter was named *GroupMetricsGenerationEnabled*.

For detailed syntax and parameter information, see Set-MailboxServer.

Use the Shell to configure the group metrics generation time

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Group metrics" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure the group metrics generation time.

You use the **Set-MailboxServer** cmdlet to configure the time of day when group metrics data is generated on a Mailbox server. You must use the 24-hour clock notation (*HH:MM*) when specifying the generation time. These examples configure group metrics generation on servers MBX1 and MBX3 to occur at 11:30 P.M. and 3:00 A.M. respectively.

```
Set-MailboxServer MBX1 -GroupMetricsGenerationTime 23:30
Set-MailboxServer MBX3 -GroupMetricsGenerationTime 03:00
```

For detailed syntax and parameter information, see Set-MailboxServer.

1.7.2.14.3 Configure Custom MailTips for Recipients

Configure Custom MailTips for Recipients

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

MailTips are informative messages displayed to users while they are composing a message. In Microsoft Exchange Server 2010, you can assign custom MailTips to recipients. You must specify a default custom MailTip.

You can assign MailTips in multiple languages. When a sender addresses a message to a recipient that has a custom MailTip configured, the MailTip translation that matches the language of the client the sender is using is displayed. If there's no MailTip translation that matches the client language, the default MailTip is displayed.

If some of your user mailboxes are hosted on Exchange Online and there's coexistence with an Exchange Online scenario, consider the following:

- You must set the *MailTipsAccessLevel* parameter on the organization relationship to `All`. Otherwise, the custom MailTips aren't returned when the sender and the recipient are on either side of the organizational relationship.
- Each mailbox is represented as a mail user on the other side of the organization relationship. For example, a mailbox hosted on Exchange Online is represented as a mail user in your on-premises deployment. If both of these recipients are configured with a custom MailTip, the local one is returned. In this example, the on-premises users that compose messages to that recipient will see the custom MailTip configured on the mail user, whereas Exchange Online users will see the custom MailTip configured on the mailbox.

Looking for other management tasks related to MailTips? Check out Managing MailTips.

Prerequisites

Make sure that MailTips are enabled in your organization. For detailed steps, see Configure Organizational Settings for MailTips. To learn more about MailTips, see Understanding MailTips.

Use the Shell to configure custom MailTips

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient data properties" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to configure custom MailTips.

You use the following cmdlets to configure custom MailTips for recipients:

- **Set-Mailbox**

- **Set-MailContact**
- **Set-MailUser**
- **Set-DistributionGroup**
- **Set-DynamicDistributionGroup**
- **Set-MailPublicFolder**

Custom MailTips can include HTML links, but no scripts are allowed. The length of a custom MailTip can't exceed 250 characters.

For example, assume that the response time service level agreement (SLA) for your Help Desk is two hours, and you have a Help Desk mailbox to which your users can submit problems. This example configures a custom MailTip for that mailbox to inform senders that they will receive a response within two hours.

```
Set-Mailbox -Identity "Help Desk" -MailTip "A Help Desk representative will conta
```

Custom MailTips are also useful for recipients whose display name may be misunderstood. For example, assume that you have a distribution group called HR that's used for departmental communications. This example informs senders what the distribution group is used for and directs them to the correct address if they have a question or complaint to submit to Human Resources.

```
Set-DistributionGroup -Identity "HR" -MailTip "This distribution group is used fo
```

Custom MailTip translations are stored in the multivalued property **MailTipTranslations** on a recipient object. When you're adding a MailTip translation, be sure that you don't overwrite any existing MailTip translations. This example creates a custom MailTip for the mailbox Notifications@contoso.com informing the user that it isn't a monitored mailbox, and then adds the Spanish translation. This is done by using the temporary variable *$Temp*.

```
Set-Mailbox -Identity Notifications@contoso.com -MailTip "This mailbox is not mon
$Temp = Get-Mailbox Notifications@contoso.com
$Temp.MailTipTranslations += "ES:Esta caja no se supervisa."
Set-Mailbox -Identity Notifications@contoso.com -MailTipTranslations $Temp.MailTi
```

Important:

You must use the preceding method when adding MailTip translations even if you're adding a single language. This is because the custom MailTip configured using the *MailTip* parameter is also stored in the *MailTipTranslations* parameter as the default translation.

For detailed syntax and parameter information, see the following topics:

- Set-Mailbox
- Set-MailContact
- Set-MailUser
- Set-DistributionGroup
- Set-DynamicDistributionGroup
- Set-MailPublicFolder

1.7.2.15 Managing Message Routing

Managing Message Routing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-01*

Configure a Hub Site

Set an Exchange Cost on an Active Directory IP Site Link

Configure Exchange 2010 to Route Messages for a Shared Address Space

Suppress Anonymous TLS Connections

Configure Internet Mail Flow Through a Subscribed Edge Transport Server

Configure Mail Flow Between an Edge Transport Server and Hub Transport Servers Without Using EdgeSync

Configure Internet Mail Flow Through Exchange Hosted Services or an External SMTP Gateway

Configure Internet Mail Flow Directly Through a Hub Transport Server

1.7.2.15.1 Configure a Hub Site

Configure a Hub Site

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can configure an Active Directory site as a hub site for message routing in Microsoft Exchange Server 2010. For more information about hub sites, see Understanding Message Routing.

Looking for other management tasks related to managing message routing? Check out Managing Message Routing.

Prerequisites

Examine the contents of the routing table logs and view the data in the ADTopologyPath ID section to verify that the selected site exists along the least cost routing path between two Active Directory sites. If this isn't the case, you need to assign Exchange-specific costs to the IP site links to make the least cost routing path go through the selected sites. For detailed steps, see Set an Exchange Cost on an Active Directory IP Site Link.

Use the Shell to configure an Active Directory site as a hub site

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Active Directory site and site link management" entry in the Transport Permissions topic.

Note:

You can't use the EMC to configure an Active Directory site as a hub site.

This example configures the Active Directory site Site A as a hub site.

```
Set-AdSite "Site A" -HubSiteEnabled $true
```

For detailed syntax and parameter information, see Set-AdSite.

1.7.2.15.2 Set an Exchange Cost on an Active Directory IP Site Link

Set an Exchange Cost on an Active Directory IP Site Link

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can set an Exchange cost on an Active Directory IP site link in Microsoft Exchange Server 2010. By default, Exchange uses the cost assigned to an IP site link for Active Directory replication purposes to compute a routing topology.

Looking for other management tasks related to managing message routing? Check out Managing Message Routing.

Prerequisites

- Understand how Exchange uses Active Directory sites to route messages. For more information, see Understanding Message Routing.
- Determine the name of the Active Directory IP site link for which you want to set an Exchange cost. You can examine the contents of the routing table logs and view the data in the ADTopologyPath ID section to view details about the calculated least cost routing path between two Active Directory sites.

Use the Shell to set an Exchange cost on an Active Directory IP site link

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Active Directory site and site link management" entry in the Transport Permissions topic.

Note:

You can't use the EMC to export an Edge Subscription file.

This example sets an Exchange specific cost of 10 to the IP site link IPSiteLinkAB.

```
Set-AdSiteLink -Identity IPSiteLinkAB -ExchangeCost 10
```

This example clears the Exchange specific cost on the IP site link IPSiteLinkAB.

```
Set-AdSiteLink -Identity IPSiteLinkAB -ExchangeCost $null
```

For detailed syntax and parameter information, see Set-AdSiteLink.

Configure Exchange 2010 to Route Messages for a Shared Address Space

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

An organization may have to share the same SMTP address space between two or more different e-mail systems. For example, you may have to share the SMTP address space between Exchange and a third-party e-mail system, or between Exchange environments that are configured in different Active Directory forests. In these scenarios, users in each e-mail system have the same domain suffix as part of their e-mail addresses.

You can use the EMC or the Shell to configure a Microsoft Exchange Server 2010 Hub Transport server to route messages for a shared address space.

Looking for other management tasks related to managing message routing? Check out Managing Message Routing.

Step 1: Create an internal relay domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Accepted domains" entry in the Transport Permissions topic.

To support routing messages for a shared address space, you must create an accepted domain that's configured as an internal relay domain. When you configure an accepted domain as an internal relay domain, Exchange first tries to deliver to a recipient in the Exchange organization. If the recipient isn't found, the message is routed to the Send connector that has the closest address space match.

Use the EMC to create an internal relay domain

1. In the console tree, expand **Organization Configuration**, select **Hub Transport**, and then in the work pane, click the **Accepted Domains** tab.
2. In the action pane, click **New Accepted Domain**. The New Accepted Domain wizard appears.
3. On the **New Accepted Domain** page, complete the following fields:
   - **Name** Use this field to identify the accepted domain in the user interface. You can type any name that you want. We recommend that you select a meaningful name that helps you easily identify the purpose of this accepted domain. For example, you may want to use a name that identifies this as a subsidiary domain or as a hosted domain. You must use a unique name for each accepted domain.
   - **Accepted Domain** Use this field to identify the SMTP namespace for which the Exchange organization will accept e-mail messages. You can use a wildcard character to accept messages for a domain and all its subdomains. For example, you can type *.contoso.com to set Contoso.com and all its subdomains as accepted domains.
4. After you complete these fields on the **New Accepted Domain** page, select the following option: **Internal Relay Domain**.
5. Click **New**.
6. On the **Completion** page, click **Finish**.

Use the Shell to create an internal relay domain

This example creates the internal relay domain Contoso for the SMTP domain

contoso.com.

```
New-AcceptedDomain -Name "Contoso" -DomainName contoso.com -DomainType InternalRe
```

For detailed syntax and parameter information, see New-AcceptedDomain.

Step 2: Create a Send connector to route e-mail to the shared domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

You must also add a Send connector that's sourced on a Hub Transport server and configured to send e-mail to the shared address space.

Caution:

To achieve the correct routing behavior, you must specify a Hub Transport server as the source server for the Send connector. If the Edge Transport server is specified as the source server for the Send connector, a routing loop will occur.

Use the EMC to create a Send connector to route e-mail to the shared domain

1. In the console tree, expand **Organization Configuration**, select **Hub Transport**, and then in the work pane, click the **Send Connectors** tab.
2. In the action pane, click **New Send Connector**. The New Send Connector wizard starts.
3. On the **Introduction** page, follow these steps:
   - In the **Name** field, type a meaningful name for this connector. This name is used to identify the connector.
   - In the **Select the intended use for this connector** field, select one of the following usage types for the connector. The usage type determines the default permission sets that are assigned on the connector and grants those permissions to trusted security principals:
     - **Internal** Select this usage type if the e-mail system with which Exchange 2010 shares an address space is another Exchange 2010 organization.
     - **Internet** Select this usage type if the e-mail system with which Exchange 2010 shares an address space is a third-party e-mail system.
4. Click **Next**.
5. On the **Address space** page, click **Add**. In the **SMTP Address Space** dialog box, enter the domain name to which this connector will send mail, for example, contoso.com or *.contoso.com. You may select the **Include all subdomains** check box to use this connector to send e-mail to all subdomains of the address space. If necessary, you can also provide a specific cost for this connector. When you're finished, click **OK**. Leave the **Scoped send connector** check box cleared, and then click **Next**.
6. On the **Network settings** page, select **Route mail through the following smart hosts**. Click **Add**.
7. In the **Add Smart Host** dialog box, select **IP Address** or **Fully qualified domain name (FQDN)** to specify how to locate the smart host. If you select **IP Address**, enter the IP address of the smart host. If you select **Fully qualified domain name (FQDN)**, enter the FQDN of the smart host. The sending server must be able to resolve the FQDN. When you're finished, click **OK**. To add more smart hosts, click **Add**, and repeat this step. If you want to use a specific list of external DNS servers instead of the DNS servers specified in the adapter settings, select the **Use the External DNS Lookup settings on**

the transport server check box. When you're finished, click **Next**.

8. On the **Configure smart host authentication settings** page, select the method that's used to authenticate to the smart host. The following smart host authentication methods are available:
   - **None**
   - **Basic Authentication**
   - **Basic Authentication over TLS**
   - **Exchange Server Authentication**
   - **Externally Secured (for example, with IPsec)**
9. Click **Next**.
10. On the **Source Server** page, click **Add** to add a source server. By default, the Hub Transport server that you're currently working on is listed as a source server. In the **Select Hub Transport or Subscribed Edge Transport** dialog box, select the Hub Transport servers that will be used as the source server for sending messages to the shared address space. When you finish adding source servers, click **OK**. Click **Next**.
11. On the **New Connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Send connector by using the settings in the configuration summary, click **New**.
12. On the **Completion** page, click **Finish**.

Use the Shell to create a Send connector to route e-mail to the shared domain

This example creates a Send connector with the following settings:

- Configures the connector as an Internet usage type
- Assigns the address space contoso.com
- Routes messages to the smart host smarthost.contoso.com
- Uses the Externally Secured authentication mechanism
- Sets the maximum message size to 20 megabytes (MB)

```
New-SendConnector -Name "Contoso.com Send Connector" -Internet -AddressSpace cont
```

For detailed syntax and parameter information, see New-SendConnector.

1.7.2.15.4 Suppress Anonymous TLS Connections

Suppress Anonymous TLS Connections

Transport > Managing Transport Servers > Managing Message Routing >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2007, Transport Layer Security (TLS) encryption is mandatory for all SMTP communication between Hub Transport servers. This increases overall security of hub-to-hub communications. However, in certain topologies where WAN Optimization Controller (WOC) devices are used, the TLS encryption of SMTP traffic may be undesirable. Exchange Server 2010 supports disabling TLS for hub-to-hub communications for these specific scenarios.

This topic provides step-by-step instructions on how to configure your Hub Transport servers to disable TLS. To learn more about this feature, see Disabling TLS Between Active Directory Sites to Support WAN Optimization.

Looking for other tasks related to managing message routing? Check out Managing Message Routing.

Caution:
Make sure you disable TLS only on connections that pass through WOC devices.

Prerequisites

- Exchange is deployed in multiple Active Directory sites, with at least one site connected to the other sites over a WAN link.
- WOC devices are deployed to compress SMTP traffic over the WAN link.
- A logical message flow path exists for Exchange going over the WAN link that has the WOC devices deployed.

Step 1: Use the Shell to configure the Hub Transport server to use downgraded Exchange Server authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this procedure.

You use the **Set-TransportServer** cmdlet to configure a Hub Transport server to use downgraded Exchange Server authentication. This example makes this configuration change on the server Hub01.

```
Set-TransportServer Hub01 -UseDowngradedExchangeServerAuth $true
```

For detailed syntax and parameter information, see Set-TransportServer.

Step 2: Use the Shell to create a Receive connector on the Hub Transport server for the specific remote IP address range of the target Active Directory site

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

You use the **New-ReceiveConnector** cmdlet to create a Receive connector on your Hub Transport server to use for non-encrypted traffic. This example creates the Receive connector WAN on server Hub01 with the following configuration options:

- The *RemoteIPRanges* parameter is set to 10.0.2.0/24. This IP address range should correspond to the remote Active Directory site from where this Receive connector will receive unencrypted connections. If there's more than one IP subnet in the remote site, you can enter them all separated by commas.
- The usage type is set to Internal.

```
New-ReceiveConnector -Name WAN -Server Hub01 -RemoteIPRanges 10.0.2.0/24 -Interna
```

For detailed syntax and parameter information, see New-ReceiveConnector.

You can also create the Receive connector using the EMC. If you choose to use the EMC, make sure you create the connector with the following settings:

- Select **Internal** for the intended usage for the connector.
- Specify the remote IP address range (for example, in the preceding example, 10.0.2.0/24).

For more information, see Create an SMTP Receive Connector.

Step 3: Use the Shell to disable X-ANONYMOUSTLS on the new Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this procedure.

You use the **Set-ReceiveConnector** cmdlet to disable TLS on the newly created Receive connector. This example disables TLS on the Receive connector WAN on server Hub01.

```
Set-ReceiveConnector Hub01\WAN -SuppressXAnonymousTLS $true
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

Step 4: Use the Shell to designate the Active Directory sites on either side of the WAN connection as hub sites

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Active Directory site and site link management" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this procedure.

You use the **Set-AdSite** cmdlet to configure a specific Active Directory site as a hub site. You need to do this once in each site that has Hub Transport servers that participate in non-encrypted traffic.

This example configures the Active Directory site Central Office Site 1 as a hub site.

```
Set-AdSite "Central Office Site 1" -HubSiteEnabled $true
```

For detailed syntax and parameter information, see Set-AdSite.

Step 5: Use the Shell to verify the lowest-cost routing path goes through the WAN

connection

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Active Directory site and site link management" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this procedure.

Depending on how the IP site link costs are configured in Active Directory, this step may not be necessary. You need to make sure that the network link with the WOC devices deployed lies on the least-cost message path. If this isn't the case, you'll need to assign an Exchange-specific cost to the particular IP site link to ensure messages are routed correctly. To learn more about this particular issue, see "Configuring Site Link Costs" in Disabling TLS Between Active Directory Sites to Support WAN Optimization.

This example configures an Exchange-specific cost of 15 on the IP site link Branch Office 2-Branch Office 1.

```
Set-AdSiteLink "Branch Office 2-Branch Office 1" -ExchangeCost 15
```

For detailed syntax and parameter information, see Set-AdSiteLink.

1.7.2.15.5 Configure Internet Mail Flow Through a Subscribed Edge Transport Server

Configure Internet Mail Flow Through a Subscribed Edge Transport Server

Transport > Managing Transport Servers > Managing Message Routing >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to configure Internet mail flow when your organization sends and receives Internet e-mail by relaying through a subscribed Edge Transport server.

To establish Internet mail flow for this scenario, you subscribe the Edge Transport server to an Active Directory site. We recommend this method for establishing Internet mail flow for your Exchange 2010 organization. This process automatically creates the following Send connectors, which are required for Internet mail flow:

- A Send connector configured to send e-mail to all Internet domains.
- A Send connector configured to send e-mail from the Edge Transport server to the Hub Transport server.

If you don't want to subscribe the Edge Transport server to an Active Directory site, you can manually create the Send connectors that are required to establish mail flow between the Hub Transport server and the Edge Transport server. For more information, see Configure Mail Flow Between an Edge Transport Server and Hub Transport Servers Without Using EdgeSync. We recommend that you subscribe the Edge Transport server to the Active Directory site whenever possible.

Looking for other management tasks related to message routing? Check out Managing Message Routing.

Prerequisites

- Authoritative domains are configured on the Hub Transport server. For more information, see Transport Server Post-Deployment Tasks.
- E-mail address policies are configured on the Hub Transport server. For more information, see Managing E-Mail Address Policies.
- Network communications over the secure LDAP port 50636/TCP are enabled through the firewall that separates your perimeter network from the Exchange organization.

Use the Shell to subscribe an Edge Transport server to an Active Directory site

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "EdgeSync" entry in the Transport Permissions topic.

Note:
You can't use the EMC to subscribe an Edge Transport server to an Active Directory site.

1. On the Edge Transport server, run the following command.

```
New-EdgeSubscription -FileName "C:\EdgeSubscriptionInfo.xml"
```

2. Copy the resulting XML file to a Hub Transport server in the Active Directory site to which you want to subscribe the Edge Transport server. On the Hub Transport server, run the following command.

```
New-EdgeSubscription -FileData ([byte[]]$(Get-Content -Path "C:\EdgeSu
```

Note:
By default, the value of the *CreateInternetSendConnector* parameter and *CreateInboundSendConnector* parameter is `$true`. You don't have to provide these parameters if you want to use the default configuration. They are shown here for illustration only.

Note:
You can also use the New Edge Subscription wizard in the EMC to import the Edge Subscription file you created in Step 1. For more information, see Import an Edge Subscription File to an Active Directory Site.

3. On the Hub Transport server, run the following command.

```
Start-EdgeSynchronization
```

For detailed syntax and parameter information, see New-EdgeSubscription or Start-EdgeSynchronization.

1.7.2.15.6 Configure Mail Flow Between an Edge Transport Server and Hub Transport Servers Without Using EdgeSync

Configure Mail Flow Between an Edge Transport Server and Hub Transport Servers Without Using EdgeSync

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

We always recommend that you use the Edge Subscription process to establish mail flow between the Exchange organization and a computer that's running Microsoft Exchange Server 2010 that has the Edge Transport server role installed. However, we realize that there are situations where you can't subscribe the Edge Transport server to the Exchange organization by using the Edge Subscription process. To manually establish mail flow between the Exchange organization and an Edge Transport server, you must create and configure the Send connectors and Receive connectors on the Edge Transport server and on the Hub Transport servers in the Exchange organization.

Looking for other tasks related to managing message routing? Check out Managing Message Routing.

Prerequisites

- This procedure uses Basic authentication over Transport Layer Security (TLS) to provide encryption and authentication. When you use Basic authentication over TLS, the receiving server must have an X.509 Secure Sockets Layer (SSL) server certificate installed. The fully qualified domain name (FQDN) value configured on the Receive connector must match the FQDN in the SSL server certificate. By default, the value of the FQDN on the Receive connector is the FQDN of the server that contains the Receive connector.
- You can also use the Externally Secured authentication method. However, if you do so, the communication between the Edge Transport server and Hub Transport server isn't authenticated or encrypted by Exchange. We recommend that you use the Externally Secured authentication method only when an additional encryption method is used. The encryption method can be an Internet Protocol security (IPsec) association or a virtual private network (VPN).
- An Edge Transport server is typically *multihomed*. This means that the Edge Transport server has network adapters that are connected to multiple network segments. Each of these network adapters has a unique IP configuration. The network adapter that's connected to the external, or public, network segment should be configured to use a public Domain Name System (DNS) server for name resolution. This enables the server to resolve SMTP domain names to MX resource records and route mail to the Internet. The network adapter that's connected to the internal, or private, network segment should be configured to use a DNS server in the perimeter network or should have a Hosts file available.
  For more information, see "Configuring DNS settings for the Edge Transport server role" in Planning Roadmap for New Deployments.
- You must create a user account in Active Directory and add the account to the Exchange Servers universal security group. This account is used by the Send connector on the Edge Transport server to authenticate to the destination Hub Transport server in the Exchange organization.

Important:

This account is granted the permissions that are associated with Exchange servers. Make sure that you safeguard the account credentials to prevent misuse of the account. You can configure the account to allow logon to specific computers only.

Edge Transport Server Procedures

The following connectors are required on the Edge Transport server:

- A Send connector configured to send messages to the Internet
- A Send connector configured to send messages to the Hub Transport servers in the Exchange organization
- A Receive connector configured to receive messages only from Hub Transport

servers in the Exchange organization
- A Receive connector configured to accept messages only from the Internet

By default, a single Receive connector is created during the installation of the Edge Transport server role. This connector can be used for both incoming Internet messages and incoming messages from the Hub Transport servers. Typically, the Edge Subscription process automatically configures the correct permissions and authentication on the default Receive connector. When you don't use the Edge Subscription process, we recommend that you modify the default Receive connector on the Edge Transport server to only accept messages from the Internet. You should then create a Receive connector on the Edge Transport server that's configured to only accept messages from internal Hub Transport servers.

The following sections walk you through all the configuration steps required to prepare your Edge Transport server to communicate with your Exchange organization.

Step 1: Create a Send connector configured to send messages to the Internet

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors - Edge Transport" entry in the Transport Permissions topic.

This Send connector requires the following configuration:

- **Name** To Internet.
- **Usage type** Internet.
- **Address spaces** "*" (all domains).
- **Network settings** Use DNS MX records to route mail automatically. Depending on your network configuration, you can also route mail through a smart host. The smart host then routes mail to the Internet.

Use the EMC to create a Send connector configured to send messages to the Internet

1. Open the EMC. Select **Edge Transport**, and then in the work pane, click the **Send Connectors** tab.
2. In the action pane, click **New Send Connector**. The New Send Connector wizard starts.
3. On the **Introduction** page, follow these steps:
   3.a. In the **Name** field, type a meaningful name for this connector, such as To Internet.
   3.b. In the **Select the intended use for this connector** field, select **Internet**.
4. Click **Next**.
5. On the **Address space** page, click **Add**. In the **SMTP Address Space** dialog box, enter *, and then click **OK**.
6. Click **Next**.
7. On the **Network settings** page, select **Use domain name system (DNS) "MX" records to route mail automatically**, and then click **Next**.
8. On the **New connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Send connector by using the settings in the configuration summary, click **New**.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   9.a. A status of **Completed** indicates that the wizard completed the task successfully.
   9.b. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a Send connector configured to send messages to the Internet

You use the **New-SendConnector** cmdlet to create a Send connector.

```
New-SendConnector -Name "To Internet" -AddressSpaces * -Usage Internet -DNSRoutin
```

For detailed syntax and parameter information, see New-SendConnector.

Step 2: Create a Send connector configured to send messages to the Exchange organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors - Edge Transport" entry in the Transport Permissions topic.

This Send connector requires the following configuration:

- **Name** To Internal Org
- **Usage type** Internal
- DNS Routing disabled (smart host routing enabled)
- **Address spaces** All accepted domains for the Exchange organization
- **Network settings** Fully qualified domain name (FQDN) of one or more Hub Transport servers as smart hosts andsmart host authentication setting configured to Basic authentication over TLS
- **Smart host authentication mechanism** Basic authentication and Basic authentication requiring TLS

Use the EMC to create the Send connector configured to send messages to the Exchange organization

1. Open the EMC. Select **Edge Transport**, and then in the work pane, click the **Send Connectors** tab.
2. In the action pane, click **New Send Connector**. The New Send Connector wizard starts.
3. On the **Introduction** page, follow these steps:
   3.a. In the **Name** field, type a meaningful name for this connector, such as To Internal Org.
   3.b. In the **Select the intended use for this connector** field, select **Internal**.
4. On the **Address space** page, follow these steps:
   4.a. Click **Add**.
   4.b. In the **SMTP Address Space** dialog box, enter the accepted domains for the Exchange organization. You may select the **Include all subdomains** check box to use this connector to send e-mail to all subdomains of the address space. When you're finished, click **OK**.
   To add more address spaces to this connector, click **Add**, repeat this step, and then click **OK**.
   4.c. When you're finished, click **Next**.
5. On the **Network settings** page, following these steps:
   5.a. Select **Route mail through the following smart hosts**, and then click **Add**.
   5.b. In the **Add Smart Host** dialog box, select **Fully qualified domain name (FQDN)**, and enter the FQDN of the destination Hub Transport server. The Edge Transport server must be able to resolve the specified FQDN of the destination Hub Transport server. When you're finished, click **OK**.
   To add more Hub Transport servers as smart hosts, click **Add** and repeat this step.
   5.c. When you're finished, click **Next**.
6. On the **Configure smart host authentication settings** page, select **Basic Authentication and Basic Authentication over TLS**. In the **Username** and **Password** fields, enter the credentials for the user account in the internal domain. Use the *domain**user* format or user principal name (UPN) format to enter the user name and provide the user's password. Click **Next**.
7. On the **New connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Send connector by using the settings in the configuration summary, click **New**.
8. On the **Completion** page, review the following, and then click **Finish** to close

the wizard:

8.a.A status of **Completed** indicates that the wizard completed the task successfully.

8.b.A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create the Send connector configured to send messages to the Exchange organization

You use the **New-SendConnector** cmdlet to create a Send connector.

Note:

Before you create the Send connector, you first need to run the **Get-Credential** command to save the user name and password you will use in a temporary variable. You need to do this because the **New-SendConnector** cmdlet doesn't accept the user credentials in plain text.

```
$HubCredentials = Get-Credential
New-SendConnector -Name "To Internal Org" -Usage Internal -AddressSpaces *.contos
```

For detailed syntax and parameter information, see New-SendConnector.

Step 3: Modify the default Receive connector to only accept messages from the Internet

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors - Edge Transport" entry in the Transport Permissions topic.

You should make the following configuration changes to the default Receive connector:

- Modify the name to reflect that the connector will be used solely to receive e-mail from the Internet
- Change the network bindings to accept messages only from the network adapter that is accessible from the Internet

Use the EMC to modify the default Receive connector to only accept messages from the Internet

1. Open the EMC. Select **Edge Transport**, and then in the work pane, click the **Receive Connectors** tab.
2. In the work pane, select the Receive connector to modify. The default Receive connector is named Default internal Receive connector *Servername*.
3. Under the name of the Receive connector in the action pane, click **Properties** to open the **Properties** page.
4. Click the **General** tab to modify the name of the connector and give it a specific name to signify that it will be used only for receiving messages from the Internet.
5. Click the **Network** tab. Under **Use these local IP addresses to Receive mail**, click **Edit**. In the **Edit Receive Connector Binding** dialog box, select **Specify an IP address**, and then enter the IP address of the Internet-facing network adapter. Click **OK**.
6. Click **OK** to save your changes and exit the **Properties** page.

Use the Shell to modify the default Receive connector to only accept messages from the Internet

You use the **Set-ReceiveConnector** cmdlet to modify the properties of the default Receive connector.

```
Set-ReceiveConnector "Default internal Receive connector Edge01" -Name "From Inte
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

Step 4: Create a Receive connector configured to only accept messages from the Exchange organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors - Edge Transport" entry in the Transport Permissions topic.

This Receive connector requires the following configuration:

- **Name** From Internal Org
- **Usage type** Internal
- **Local network bindings** Internal network-facing network adapter
- **Remote network settings** IP address of one or more Hub Transport servers in the Exchange organization
- **Authentication method** Basic authentication over TLS

Use the EMC to create a Receive connector configured to only accept messages from the Exchange organization

1. Open the EMC. Select **Edge Transport**, and then in the work pane, click the **Receive Connectors** tab.
2. In the action pane, click **New Receive Connector**. The New Receive Connector wizard starts.
3. On the **Introduction** page, follow these steps:
   3.a. In the **Name** field, type a meaningful name for this connector, such as From Internal Org.
   3.b. In the **Select the intended use for this connector** field, select **Internal**.
4. On the **Remote network settings** page, follow these steps:
   4.a. Select the default IP address range entry 0.0.0.0 - 255.255.255.255, and then click  .
   4.b. Click **Add** or the drop-down arrow located next to **Add** and type the IP address or IP address range of the internal Hub Transport server or servers. When you're finished, click **OK**.

        To add multiple destination Hub Transport servers to this connector, click **Add** and repeat this step. Each Hub Transport server that you define in this step must also be listed as a source server in the corresponding Send connectors that are configured on the Hub Transport servers.
   4.c. When you're finished, click **Next**.
5. On the **New Connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Receive connector by using the settings in the configuration summary, click **New**.
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   6.a. A status of **Completed** indicates that the wizard completed the task successfully.
   6.b. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. In the work pane, select the Receive connector that you created.
8. Under the name of the Receive connector in the action pane, click **Properties** to open the **Properties** page.
9. Click the **Network** tab. Under **Use these local IP addresses to Receive mail**, click **Edit**. In the **Edit Receive Connector Binding** dialog box, select **Specify an IP address**, and then enter the IP address of the internal organization-facing network adapter. Click **OK**.
10. Click the **Authentication** tab. Select **Basic Authentication** and **Offer Basic authentication only after starting TLS**.
11. Click **OK** to save your changes and exit the **Properties** page.

Use the Shell to create a Receive connector configured to only accept

messages from the Exchange organization
You use the **New-ReceiveConnector** cmdlet to create a Receive connector.

This example creates a Receive connector configured to accept messages from the Exchange organization.

```
New-ReceiveConnector -Name "From Internal Org" -Usage Internal -AuthMechanism TLS
```

For detailed syntax and parameter information, see New-ReceiveConnector.

Hub Transport Server Procedures

The following connector is required for the Hub Transport servers in your organization:

- A Send connector that's configured to send messages to the Edge Transport server in the perimeter network for relay to the Internet

By default, two Receive connectors are created during the installation of the Hub Transport server role. The connector named Client *ServerName* is configured to accept messages from all POP3 and IMAP messaging clients. The connector named Default *ServerName* is configured to accept messages from an Edge Transport server. No modifications to these connectors are required.

Create a Send connector configured to send outgoing messages to the Edge Transport server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

This Send connector requires the following configuration:

- **Usage type** To Edge
- **Usage type** Internal
- **Address spaces** *
- **Network settings** IP address or FQDN of the Edge Transport server as a smart host and smart host authentication setting configured to Basic Authentication over TLS

Use the EMC to create a Send connector configured to send outgoing messages to the Edge Transport server

1. Open the EMC. In the console tree, expand **Organization Configuration**, select **Hub Transport**, and then in the work pane, click the **Send Connectors** tab.
2. In the action pane, click **New Send Connector**. The New Send Connector wizard starts.
3. On the **Introduction** page, follow these steps:
   3.a. In the **Name** field, type a meaningful name for this connector, such as To Edge.
   3.b. In the **Select the intended use for this connector** field, select **Internal**.
4. On the **Address space** page, click **Add**. In the **SMTP Address Space** dialog box, enter * in the **Address** field, and then click **OK**.
   When you're finished, click **Next**.
5. On the **Network settings** page, follow these steps:
   5.a. Select **Route mail through the following smart hosts**, and then click **Add**.
   5.b. In the **Add Smart Host** dialog box, select **Fully qualified domain name (FQDN)**, and enter the FQDN of the destination Edge Transport server. The Hub Transport server must be able to resolve the specified FQDN of the destination Edge Transport server. Click **OK**.
   5.c. When you're finished, click **Next**.
6. On the **Configure smart host authentication settings** page, select **Basic**

Authentication and Basic Authentication over TLS. In the **Username** and **Password** fields, enter the credentials for the user account on the destination Edge Transport server. Click **Next**.

7. By default, the **Source Server** page lists the Hub Transport server on which you're performing this procedure. If you want to add more Hub Transport servers for fault tolerance, those Hub Transport servers must be configured as sources on the corresponding Receive connector on the Edge Transport server. To add more source servers, click **Add**. In the **Select Hub Transport servers and Edge Subscriptions** dialog box, select the Hub Transport servers that will be used as the source servers for sending messages to the Edge Transport server that you provided in step 6. When you're finished adding additional source servers, click **OK**.
   To add more source servers, click **Add** and repeat this step.
   When you're finished, click **Next**.
8. On the **New connector** page, review the configuration summary for the connector. If you want to modify the settings, click **Back**. To create the Send connector by using the settings in the configuration summary, click **New**.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   9.a. A status of **Completed** indicates that the wizard completed the task successfully.
   9.b. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a Send connector configured to send outgoing messages to the Edge Transport server

You use the **New-SendConnector** cmdlet to create a Send connector.

The following example creates a new Send connector with the following settings:

- Usage type: Internal
- Address Space: *
- DNS Routing disabled (smart host routing enabled)
- Smart hosts: edge01.contoso.net
- Source Transport servers: hub01.contoso.com, hub 02.contoso.com
- Smart host authentication mechanism: Basic authentication, basic authentication requiring TLS

Note:

Before you create the Send connector, you first need to run the **Get-Credential** command to save the user name and password you will use in a temporary variable. You need to do this because the **New-SendConnector** cmdlet doesn't accept the user credentials in plain text.

```
$EdgeCredentials = Get-Credential
New-SendConnector -Name "To Edge" -Usage Internal -AddressSpaces * -DNSRoutingEna
```

For detailed syntax and parameter information, see New-SendConnector.

1.7.2.15.7 Configure Internet Mail Flow Through Exchange Hosted Services or an External SMTP Gateway

Configure Internet Mail Flow Through Exchange Hosted Services or an External SMTP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure Internet mail flow through Microsoft Exchange Hosted Services or an external SMTP gateway.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

In Exchange Server 2010, to establish Internet mail flow through Exchange Hosted Services or an external SMTP gateway, you create a Send connector and a Receive connector between the Hub Transport servers in the Exchange organization and the external SMTP servers that process and route Internet e-mail.

The following authentication methods can be used in this scenario:

- **Basic authentication** The servers running the Exchange 2010 Hub Transport server role and the external SMTP servers authenticate by using Basic authentication. A user name and password is required. This authentication method is unavailable for Exchange Hosted Services.
- **Externally Secured** The network connection between the Hub Transport servers and the external SMTP servers is secured by using a method that's external to Exchange 2010.

  Note:

  Configuring a Receive connector as externally secured without using an Externally Secured authentication method is functionally equivalent to configuring the Receive connector as an open relay for the external SMTP server. The messages that originate from the external SMTP server are treated as authenticated messages. The messages bypass anti-spam checks and message size limit checks. The external SMTP server is allowed to submit messages as if they originated from internal senders within your Exchange organization. For more information, see Allow Anonymous Relay on a Receive Connector.

- **Anonymous relay** This method should be considered the method of last resort. If you allow an external SMTP server to anonymously relay messages by using the designated Receive connector on the Hub Transport server, you must apply the following restrictions on the Receive connector:
  - **Local network settings** If your Hub Transport server has multiple network adapters, restrict the Receive connector to listen only on the appropriate network adapter.
  - **Remote network settings** Restrict the Receive connector to accept connections only from the specified server or servers. This restriction is necessary because the Receive connector is configured to accept relay from anonymous users. Restricting the source servers by IP address is the only measure of protection that's allowed on this Receive connector.

  For more information, see Allow Anonymous Relay on a Receive Connector.

Looking for other management tasks related to managing message routing? Check out Managing Message Routing.

Prerequisites

- If you're using Basic authentication, a domain account must exist in the Active Directory forest. For example, create a domain user account that has the user principal name (UPN) smtpgateway@fabrikam.com as the credentials that must be used for authentication by the SMTP gateway when delivering mail to the Exchange servers in the Fabrikam domain.
- If you're using Basic authentication over Transport Layer Security (TLS), the target server must be configured to use an X.509 certificate that contains a fully qualified domain name (FQDN) that's the same as the FQDN of the Receive connector.
- If you're using external authentication, a trusted network connection must exist between the Hub Transport server and the SMTP gateway server. This connection can be an IPsec association or virtual private network (VPN). Alternatively, the servers may reside in a trusted physically controlled network.

Establish Internet mail flow between a Hub Transport server and an external SMTP gateway by using Basic authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

Note:

Because the default Receive connector will accept e-mail submissions from the authenticated SMTP gateway, a new Receive connector isn't needed when using Basic Authentication.

Use the EMC to establish Internet mail flow between a Hub Transport server and an external SMTP gateway by using Basic authentication

1. On the Hub Transport server, open the EMC. Expand **Organization Configuration**, click **Hub Transport**, and then, in the action pane, click **New Send connector**.
2. On the New Send Connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector.
3. From the **Select the intended use for this Send connector** drop-down list, select **Custom**, and then click **Next**.
4. On the **Address space** page, click **Add**. In the **SMTP Address Space** dialog box, type **"*"** in the **Address** field, and then click **OK**. Click **Next**.
5. On the **Network settings** page, only the **Route mail through the following smart hosts** setting can be selected. Select this setting and click **Add**.
6. In the **Add smart host** dialog box, in the **IP address** or **Fully qualified domain name (FQDN)** field, type the IP address or FQDN of the external SMTP gateway server, and then click **OK**. To specify more than one SMTP gateway as a smart host, click **Add** and enter additional IP addresses or FQDNs, and then click **Next**.
7. On the **Configure smart host authentication settings** page, select **Basic Authentication**, click **Basic Authentication over TLS**, type the user name and password that will be used to authenticate the connection, and then click **Next**.
8. On the **Source Server** page, click **Add**. In the **Select Hub Transport and subscribed Edge Transport servers** dialog box, select one or more Hub

Transport servers in your organization, click **OK**, and then click **Next**.

9. On the **New Connector** page, click **New**, and then on the **Completion** page, click **Finish**.

Use the Shell to establish Internet mail flow between a Hub Transport server and an external SMTP gateway by using Basic authentication

1. Run the following command.

```
$mycred = Get-Credential
```

2. In the dialog box that appears, enter the credentials for the user account on the external SMTP gateway server. Enter the user name and provide the user's password. Click **OK**.
3. This example creates the Send connector ToInternetGateway that's used by the Hub Transport server HubA that connects to the external SMTP gateway smtpgateway1.contoso.com by using basic authentication.

```
New-SendConnector -Name "ToInternetGateway" -AddressSpaces "*" -SmartH
```

For detailed syntax and parameter information, see New-SendConnector.

Establish Internet mail flow between a Hub Transport server and Exchange Hosted Services or an external SMTP gateway by using Externally Secured authentication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" and "Receive connectors" entries in the Transport Permissions topic.

Use the EMC to establish Internet mail flow between a Hub Transport server and Exchange Hosted Services or an external SMTP gateway by using Externally Secured authentication

1. Create a Send connector on the Hub Transport server to the external SMTP gateway by following these steps:
   1.a. Expand **Organization Configuration**, click **Hub Transport**, and then in the action pane, click **New Send connector**.
   1.b. On the New Send Connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector. From the **Select the intended use for this connector** drop-down list, select **Internal**, and then click **Next**.
   1.c. On the **Address Space** page, click **Add**. In the **Add Address Space** dialog box, type **"*"** in the **Address** field, and then click **OK**. Click **Next**.
   1.d. On the **Network Settings** page, only the **Route mail through the following smart hosts** setting can be selected. Click **Add**.
   1.e. In the **Add smart host** dialog box, in the **IP address** or **Fully qualified domain name (FQDN)** field, type the IP address or FQDN of the SMTP gateway server, and then click **OK**. To specify more than SMTP gateway server as a smart host, click **Add** and enter additional IP addresses or FQDNs, and then click **Next**.
   1.f. On the **Configure smart host authentication settings** page, select **Externally Secured (for example with IPsec)**, and then click **Next**.
   1.g. On the **Source Server** page, click **Add**. In the **Select Hub Transport and subscribed Edge Transport servers** dialog box, select one or more Hub

Transport servers in your organization, click **OK**, and then click **Next**.

1.h.On the **New Connector** page, click **New**, and then on the **Completion** page, click **Finish**.

2. Create a Receive connector on the Hub Transport server to receive mail from the external SMTP gateway by following these steps:
   2.a.Expand **Server Configuration**, click **Hub Transport**, and then in the action pane, click **New Receive Connector**.
   2.b.On the New Receive Connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector.
   2.c.From the **Select the intended use for this connector** drop-down list, select **Internal**, and then click **Next**.
   2.d.On the **Remote Network settings** page, remove the all network ranges entry, and then click **Add**.
   2.e.In the **Add IP Address(es) of Remote Servers** dialog box, type the IP address of the external SMTP gateway server, click **OK**, and then click **Next**.
   2.f.On the **New Connector** page, click **New**, and then on the **Completion** page, click **Finish**.
3. For the Receive connector that you just created, set the authentication method to Externally Secured by following these steps:
   3.a.In the task pane, select the Receive connector that you created in step 2, and then in the action pane, click **Properties**.
   3.b.Click the **Authentication** tab. Clear the check boxes for **Basic Authentication** and **Exchange Server**, select **Externally Secured (for example with IPsec)**, and then click **OK**.

Use the Shell to establish Internet mail flow between a Hub Transport server and Exchange Hosted Services or an external SMTP gateway by using Externally Secured authentication

1. This example creates the Send connector ToInternetGateway used by the Hub Transport server HubA that's configured to send outgoing e-mail through the external SMTP gateway smtpgateway1.contoso.com by using Externally Secured authentication.

```
New-SendConnector -Name "ToInternetGateway" -Usage Internal -AddressSp
```

2. This example creates the Receive connector FromInternetGateway on the Hub Transport server HubA that uses Externally Secured authentication to receive mail from the external SMTP gateway that has the IP address 192.168.1.10.

```
New-ReceiveConnector -Name "FromInternetGateway" -Server HubA -Usage I
```

For detailed syntax and parameter information, see New-SendConnector and New-ReceiveConnector.

Establish Internet mail flow between a Hub Transport server and an external SMTP gateway by using anonymous relay

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" and "Receive connectors" entries in the Transport Permissions topic.

Use the EMC and Shell to establish Internet mail flow between a Hub Transport server and an external SMTP gateway by using anonymous relay

Note:
This procedure uses the EMC for steps 1 through 4. The last step of this procedure, granting relay permission to anonymous access on the Receive connector, can't be performed by using the EMC. You must use the Shell for that step.

1. Create a Send connector on the Hub Transport server to the external SMTP gateway by following these steps:
   1.a. Expand **Organization Configuration**, click **Hub Transport**, and then in the action pane, click **New Send connector**.
   1.b. On the New Send Connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector. From the **Select the intended use for this Send connector** drop-down list, select **Internet**, and then click **Next**.
   1.c. On the **Address space** page, click **Add**. In the **SMTP Address Space** dialog box, type **"*"** in the **Address** field, and then click **OK**. Click **Next**.
   1.d. On the **Network settings** page, only the **Route mail through the following smart hosts** setting can be selected. Click **Add**.
   1.e. In the **Add smart host** dialog box, in the **IP address** or **Fully qualified domain name (FQDN)** field, type the IP address or FQDN of the SMTP gateway server, and then click **OK**. To specify more than SMTP gateway server as a smart host, click **Add** and enter additional IP addresses or FQDNs, and then click **Next**.
   1.f. On the **Configure smart host authentication settings** page, select **None**, and then click **Next**.
   1.g. On the **Source Server** page, click **Add**. In the **Select Hub Transport and subscribed Edge Transport servers** dialog box, select one or more Hub Transport servers in your organization, click **OK**, and then click **Next**.
   1.h. On the **New Connector** page, click **New**, and then on the **Completion** page, click **Finish**.
2. Create a Receive connector on the Hub Transport server to receive mail from the external SMTP gateway by following these steps:
   2.a. Expand **Server Configuration**, click **Hub Transport**, and then in the action pane, click **New Receive Connector**.
   2.b. On the New Receive Connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector.
   2.c. From the **Select the intended use for this connector** drop-down list, select **Custom**, and then click **Next**.
   2.d. On the **Local Network settings** page, remove the existing **All Available IPv4** entry, and then click **Add**.
   2.e. In the **Add Receive Connector Binding** dialog box, select **Specify an IP address**. Type an IP address assigned to a network adapter on the local server that's best able to communicate with the external SMTP gateway. Make sure that the **Port** field has the value **25** and click **OK**. Leave the **Specify the FQDN this connector will provide in response to HELO or EHLO** field blank, and then click **Next**.
   2.f. On the **Remote Network settings** page, remove the all network ranges entry, and then click **Add**.
   2.g. In the **Add IP Addresses of Remote Servers** dialog box, type the IP address of the external SMTP gateway server, click **OK**, and then click **Next**.
   2.h. On the **New Connector** page, review the **Configuration Summary**. If you're satisfied, click **New**. If you'd like to make changes, click **Back**.
   2.i. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
      - A status of **Completed** indicates that the wizard completed the task successfully.
      - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
3. For the Receive connector that you just created, add the Anonymous permission group by following these steps:

3.a.In the task pane, select the Receive connector that you created in step 2, and then in the action pane, click **Properties**.
3.b.Click the **Permission Groups** tab. Select **Anonymous users**, and then click **OK**. Click **OK** to save your changes and exit the **Properties** page.
4. For the Receive connector that you just modified, grant the relay permission to the Anonymous logon security principal by following these steps:
4.a.Open the Shell.
4.b.Run the following command using the name of the Receive connector that you created in step 2 and modified in step 3.

```
Get-ReceiveConnector "Receive Connector Name" | Add-ADPermi
```

For detailed syntax and parameter information, see Get-ReceiveConnector and Add-ADPermission topics.

Use the Shell to establish Internet mail flow between a Hub Transport server and an external SMTP gateway by using anonymous relay

1. This example creates the Send connector ToInternetGateway used by the Hub Transport server HubA that's configured to send outgoing e-mail through the external SMTP gateway smtpgateway1.contoso.com by using anonymous relay.

```
New-SendConnector -Name "ToInternetGateway" -Usage Internet -AddressSp
```

2. This example creates the Receive connector FromInternetGateway on the Hub Transport server HubA that listens on local IP address 10.2.3.4 on port 25 for anonymous connections from an SMTP gateway server at the IP address 192.168.5.77.

```
New-ReceiveConnector -Name "FromInternetGateway" -Server HubA -Usage C
```

3. This example grants the relay permission to the Anonymous logon security principal on the Receive connector that you created in step 2.

```
Get-ReceiveConnector "FromInternetGateway" | Add-ADPermission -User "N
```

For detailed syntax and parameter information, see New-SendConnector, New-ReceiveConnector, Get-ReceiveConnector, and Add-ADPermission.

1.7.2.15.8 Configure Internet Mail Flow Directly Through a Hub Transport Server

Configure Internet Mail Flow Directly Through a Hub Transport Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure an Internet-facing Hub Transport server. To establish Internet mail flow directly through a Hub Transport server, you create a Send connector that routes e-mail to the Internet. Also, you modify the configuration of the default Receive connector to accept e-mail from the Internet. In this scenario, the Microsoft Exchange Server 2010 Hub Transport server can be reached directly through the Internet. We don't recommend this topology because it increases security risks by exposing to the Internet the Exchange 2010 server and all roles installed on that server. We recommend that you implement a perimeter network-based SMTP gateway, such as

the Edge Transport server, instead.

If you decide to configure Internet mail flow directly through your Hub Transport server, you may want to install the anti-spam agents on your Hub Transport servers. For more information, see Enable Anti-Spam Functionality on a Hub Transport Server.

Looking for other management tasks related to managing message routing? Check out Managing Message Routing.

Prerequisites

- Register MX resource records for all accepted domains in a public domain name system (DNS) server. Consult the documentation of your DNS provider for information about how to register MX records for your domain. Detailed procedures about how to complete this step are outside the scope of this topic.
- Configure network gateways to allow SMTP traffic to and from the Hub Transport server. Consult the documentation for your network routers and firewalls for information about how to route SMTP traffic to and from the Hub Transport server. Detailed procedures about how to complete this step are outside the scope of this topic.

Step 1: Create a Send connector on the Hub Transport server to send e-mail to the Internet

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send connectors" entry in the Transport Permissions topic.

Use the EMC to create the Send connector

1. Expand **Organization Configuration**, click **Hub Transport**, and then in the action pane, click **New Send connector**.
2. On the New Send Connector wizard **Introduction** page, in the **Name** field, type a unique name for the connector. From the **Select the intended use for this Send connector** drop-down list, select **Internet**, and then click **Next**.
3. On the **Address space** page, click **Add**. In the **SMTP Address Space** dialog box, type **"*"** in the **Address** field, and then click **OK**. Click **Next**.
4. On the **Network settings** page, select **Use Domain Name System (DNS) to route mail automatically.** Select the **Use External DNS Lookup settings** check box. Click **Next**.

   Note:

   For more information about how to configure external DNS lookup settings, see Configure Hub Transport Server Properties.

5. On the **Source Server** page, click **Add**. In the **Select Hub Transport and subscribed Edge Transport servers** dialog box, select one or more Hub Transport servers in your organization, click **OK**, and then click **Next**.
6. On the **New Connector** page, click **New**, and then on the **Completion** page, click **Finish**.

Use the Shell to create the Send connector

This example creates a Send connector that's used by the Hub Transport server HubA to send e-mail to the Internet.

```
New-SendConnector -Name "Internet" -Usage Internet -AddressSpaces "*" -SourceTran
```

For detailed syntax and parameter information, see New-SendConnector.

Step 2: Modify the default Receive connector to allow anonymous connections

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

Use the EMC to configure the Receive connector

1. Expand **Server Configuration**, click **Hub Transport**, and in the work pane under the **Receive Connectors** tab, select the **Default <Server Name>** connector. In the action pane, click **Properties**.
2. In **<Connector> Properties**, select the **Permissions** tab.
3. Select **Anonymous Users** to add anonymous permissions. Click **OK**.

Use the Shell to configure the Receive connector

This example modifies the default Receive connector on the Hub Transport server HubA to allow anonymous connections.

```
Set-ReceiveConnector "HubA\Default HubA" -PermissionGroups AnonymousUsers,Exchang
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

1.7.2.15.9 Configure Windows Network Load Balancing for Hub Transport Servers

Configure Windows Network Load Balancing for Hub Transport Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure Windows Network Load Balancing (NLB) to distribute non-Exchange messages among your Hub Transport or Edge Transport servers. To learn more about load balancing SMTP traffic, see Understanding SMTP Failover and Load Balancing in Transport.

Caution:

Using a load balancing solution to handle message traffic between the Exchange servers in your organization isn't supported. You must exclude message traffic between Exchange servers from any load balancing solution you deploy in your environment.

Looking for other management tasks related to handling SMTP traffic? Check out Managing Message Routing.

Prerequisites

- Microsoft Exchange Server 2010 is deployed and functional in your organization.

- You have reviewed Understanding SMTP Failover and Load Balancing in Transport.

Step 1: Use DNS Manager to create the SMTP namespace

You first need to create an SMTP namespace that will be used for Windows NLB. The following steps apply to the Active Directory-integrated Windows Domain Name System (DNS). If you use a third-party DNS server, refer to that documentation to create the necessary DNS records with the attributes shown in this procedure.

To perform this step, the account you use must be delegated membership in the DNS Admins group or the Domain Admins group.

1. Log on to a computer that has the DNS management console installed, click **Start**, point to **Administrative Tools**, and then click **DNS** to open DNS Manager.
2. If you aren't connected to the DNS server of your domain, use the following steps to connect to a DNS server. If you are connected to the correct server, go to step 3.
   2.a. On the **Action** menu, select **Connect to DNS Server**.
   2.b. Click **The following computer**, type the name of the DNS server to which you want to connect, and then click **OK**.
3. On the menu, click **View**, and then select **Advanced mode** unless it's already selected.
4. Expand the server name, and then expand the **Forward Lookup Zones** node.
5. Right-click the zone in which you want to create the SMTP namespace, and then select **New Host (A)**.
6. Specify the host name for the SMTP namespace and the associated IP address, and then set **Time to live (TTL)** to 5 minutes. For example:
   6.a. **Name** mail
   6.b. **IP Address** 10.0.0.10

   Note:
   You will notice that when you type the host name, the **FQDN** box is automatically updated. Make sure that the **FQDN** box shows the exact name you want to use for your SMTP namespace.
7. Click **Add Host**.
8. Click **OK** in the confirmation window, and then click **Done**.
9. Close DNS Manager.

Step 2: Use Windows to install and configure NLB

The Windows NLB cluster must be created and configured before you can create additional Receive connectors on your Hub Transport servers, and all Hub Transport servers must be added to the Windows NLB cluster.

Create your Windows NLB cluster by following the guidance in Implementing a New Network Load Balancing Cluster in the Windows Server 2008 documentation. Use the DNS record for the SMTP namespace you created in step 1 as the name and IP address of your Windows NLB cluster.

After the Windows NLB cluster has been created and configured, an extra IP address is added to each Hub Transport server. This IP address is known as the virtual IP address.

Step 3: Use the EMC to create a Receive connector

This step should be completed for each Hub Transport server participating in Windows NLB.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" or "Receive connectors - Edge Transport" entry in the Transport Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Hub Transport**.
2. In the result pane, select the server on which you want to create the connector, and then click the **Receive Connectors** tab.
3. In the action pane, click **New Receive Connector**. The New SMTP Receive Connector wizard opens.
4. On the **Introduction** page, enter a name for the connector, and then select **Custom** in the **Select the intended use for this Receive connector** box. Click **Next**.
5. On the **Local network settings** page, select **(All Available IPv4)**, and then click **Edit**.
6. In the **Edit Receive Connector Binding** window, select **Specify an IP address**, and then enter the virtual IP address of the Hub Transport server created when you configured Windows NLB. Click **OK**.
7. On the **Local network settings** page, enter the SMTP namespace you created in step 1 in the **Specify the FQDN this connector will provide in response to HELO or EHLO** box, and then click **Next**.
8. On the **Remote network settings** page, leave the default values, and then click **Next**.
9. On the **New connector** page, click **New**.
10. Click **Finish** to exit the wizard.

Other Tasks

After you configure Windows NLB for Hub Transport servers, you may also want to do the following:

- If the Hub Transport server needs to accept messages from non-authenticated sources, make sure **Anonymous users** is enabled on the new Receive connector. For more information, see step 6 in Configure Receive Connector Properties.
- If the Receive connector also needs to be used for relaying purposes, you need to perform additional configuration. For example, you may have line-of-business (LOB) applications that need to relay messages through the local Exchange organization for delivery to external recipients. For more information, see Allow Anonymous Relay on a Receive Connector. Also, review the Exchange Server Team Blog article Allowing application servers to relay off Exchange Server.

Note:

The content of each blog and its URL are subject to change without notice. The content within each blog is provided "AS IS" with no warranties, and confers no rights. Use of included script samples or code is subject to the terms specified in the Microsoft Terms of Use.

Configure Hardware Load Balancing for Hub Transport Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure a hardware load balancing solution to distribute non-Exchange messages among your Hub Transport or Edge Transport servers. To learn more about load balancing SMTP traffic, see Understanding SMTP Failover and Load Balancing in Transport.

Caution:

Using a load balancing solution to handle message traffic between the Exchange servers in your organization isn't supported. You must exclude message traffic between Exchange servers from any load balancing solution you deploy in your environment.

Looking for other management tasks related to handling SMTP traffic? Check out Managing Message Routing.

Prerequisites

- Microsoft Exchange Server 2010 is deployed and functional in your organization.
- You have deployed and verified a hardware load balancing device.
- You have reviewed Understanding SMTP Failover and Load Balancing in Transport.

Step 1: Use DNS to create the SMTP namespace

You first need to create an SMTP namespace that will be used for Windows Network Load Balancing (NLB). The following steps apply to the Active Directory-integrated Windows Domain Name System (DNS). If you use a third-party DNS server, refer to that documentation to create the necessary DNS records with the attributes shown in this procedure.

To perform this step, the account you use must be delegated membership in the DNS Admins group or the Domain Admins group.

1. Log on to a computer that has the DNS management console installed, click **Start**, point to **Administrative Tools**, and then click **DNS** to open DNS Manager.
2. If you aren't connected to the DNS server of your domain, use the following steps to connect to a DNS server. If you are connected to the correct server, go to step 3.
   2.a. On the **Action** menu, select **Connect to DNS Server**.
   2.b. Click **The following computer**, type the name of the DNS server to which you want to connect, and then click **OK**.
3. On the menu, click **View**, and then select **Advanced mode** unless it's already selected.
4. Expand the server name, and then expand the **Forward Lookup Zones** node.
5. Right-click the zone in which you want to create the SMTP namespace, and then select **New Host (A)**.
6. Specify the host name for the SMTP namespace and the associated IP address, and then set **Time to live (TTL)** to 5 minutes. For example:

6.a. **Name** mail
6.b. **IP Address** 10.0.0.10

> **Note:**
> You will notice that when you type the host name, the **FQDN** box is automatically updated. Make sure that the **FQDN** box shows the exact name you want to use for your SMTP namespace.

7. Click **Add Host**.
8. Click **OK** in the confirmation window, and then click **Done**.
9. Close DNS Manager.

Step 2: Use your vendor documentation to configure the virtual SMTP service on your hardware load balancing solution

For the steps required to create and configure the virtual SMTP service on the hardware load balancing solution used within your organization, see the hardware load balancing documentation provided by your vendor. Most hardware load balancing vendors have detailed documentation about how their product works with Exchange 2010 including steps about how to create a virtual SMTP service that can distribute incoming SMTP traffic among the Hub Transport servers in your organization.

For more information about Exchange 2010 server load balancing solutions, see Microsoft Unified Communications Hardware Load Balancer Deployment.

Step 3: Use Network and Sharing Center to add additional IP addresses to your Hub Transport servers

This step should be completed for each Hub Transport server participating in the hardware load balancing solution.

To perform this step, the account you use must be delegated membership in the Server Operators group or the local Administrators group.

1. Click **Start**, click **Control Panel**, and then double-click **Network and Sharing Center**.
2. Click **Manage network connections**.
3. Right-click the connection for the internal network, and then select **Properties**.
4. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
5. Click the **Advanced** button.
6. Under **IP addresses**, click **Add**.
7. Enter the IP address and subnet mask to which your hardware load balancer will direct SMTP traffic.
8. Click **Add**, and then click **OK** twice to close the property page for **Internet Protocol Version 4 (TCP/IPv4)**.
9. Click **Close** to exit the property page for the connection.

Step 4: Use the EMC to create a Receive connector

This step should be completed for each Hub Transport server participating in the hardware load balancing solution.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" or "Receive connectors - Edge Transport" entry in the Transport Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Hub Transport**.
2. In the result pane, select the server on which you want to create the connector, and then click the **Receive Connectors** tab.
3. In the action pane, click **New Receive Connector**. The New SMTP Receive Connector wizard opens.
4. On the **Introduction** page, enter a name for the connector, and then select **Custom** in the **Select the intended use for this Receive connector** box. Click **Next**.
5. On the **Local network settings** page, select **(All Available IPv4)**, and then click **Edit**.
6. In the **Edit Receive Connector Binding** window, select **Specify an IP address**, and then enter the virtual IP address of the Hub Transport server that you added to this Hub Transport server in step 3. Click **OK**.
7. On the **Local network settings** page, enter the SMTP namespace you created in step 1 in the **Specify the FQDN this connector will provide in response to HELO or EHLO** box, and then click **Next**.
8. On the **Remote network settings** page, leave the default values, and then click **Next**.
9. On the **New connector** page, click **New**.
10. Click **Finish** to exit the wizard.

Other Tasks

After you configure hardware load balancing for Hub Transport servers, you may also want to do the following:

- If the Hub Transport server needs to accept messages from non-authenticated sources, make sure **Anonymous users** is enabled on the new Receive connector. For more information, see step 6 in Configure Receive Connector Properties.
- If the Receive connector also needs to be used for relaying purposes, you need to perform additional configuration. For example, you may have line-of-business (LOB) applications that need to relay messages through the local Exchange organization for delivery to external recipients. For more information, see Allow Anonymous Relay on a Receive Connector. Also, review the Exchange Server Team Blog article Allowing application servers to relay off Exchange Server.

Note:

The content of each blog and its URL are subject to change without notice. The content within each blog is provided "AS IS" with no warranties, and confers no rights. Use of included script samples or code is subject to the terms specified in the Microsoft Terms of Use.

1.7.2.16 Managing Transport Agents

Managing Transport Agents

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-01*

1.7.2.16.1 Install a Transport Agent

Install a Transport Agent

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When you install a transport agent, Microsoft Exchange Server 2010 only registers the DLLs associated with the transport agent. You must make sure all files, registry keys, and other objects that the transport agent depends on are installed correctly and configured. After Exchange loads the DLLs, it continues to reference the DLLs after the command has completed.

Transport agents are installed in a disabled state to make sure mail flow isn't affected by transport agents that haven't been configured. Therefore, after a transport agent has been configured correctly, you must enable the transport agent.

You can use the Shell to install a transport agent on a computer that has the Hub Transport server role or Edge Transport server role installed. For more information about transport agents, see Understanding Transport Agents.

Looking for other management tasks related to transport agents? Check out Managing Transport Agents.

Caution:

Transport agents have full access to all e-mail messages that they encounter. Exchange puts no restrictions on a transport agent's behavior. Transport agents that are unstable or contain security flaws may affect the stability and security of Exchange. Therefore, you must only install transport agents that you fully trust and that have been fully tested in a test environment.

Use the Shell to install a transport agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport agents" entry in the Transport Permissions

topic.

Note:
You can't use the EMC to install a transport agent.

Use the following syntax to install a transport agent.

```
Install-TransportAgent -Name <"TransportAgentID"> -TransportAgentFactory <"Transp
```

This example installs a fictitious transport agent that scans messages for viruses.

```
Install-TransportAgent -Name "Antivirus for Exchange" -TransportAgentFactory "ven
```

This example enables the newly installed transport agent.

```
Enable-TransportAgent "Antivirus for Exchange"
```

For detailed syntax and parameter information, see Enable-TransportAgent.

1.7.2.16.2 View or Configure a Transport Agent

View or Configure a Transport Agent

Transport > Managing Transport Servers > Managing Transport Agents >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to view or modify an existing transport agent on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or Edge Transport server role installed. For more information about transport agents, see Understanding Transport Agents.

Looking for other management tasks related to transport agents? Check out Managing Transport Agents.

Use the Shell to view a summary list of transport agents

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport agents" entry in the Transport Permissions topic.

Note:
You can't use the EMC to view a summary list of transport agents.

This example provides a summary list of transport agents configured on a local computer.

```
Get-TransportAgent
```

For detailed syntax and parameter information, see Get-TransportAgent.

Use the Shell to view detailed configuration of a specific transport agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport agents" entry in the Transport Permissions topic.

Note:
You can't use the EMC to view detailed configuration of a specific transport agent.

This example provides detailed configuration of the Journaling agent configured on a Hub Transport server.

```
Get-TransportAgent "Journaling agent" | Format-List
```

For detailed syntax and parameter information, see Get-TransportAgent.

Use the Shell to configure a transport agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport agents" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure a transport agent.

To modify the priority of an existing transport agent, use the following syntax.

```
Set-TransportAgent <TransportAgentID> [-Priority <Priority>]
```

This example modifies the priority of the existing transport agent Antivirus for Exchange.

```
Set-TransportAgent "Antivirus for Exchange" -Priority 3
```

For detailed syntax and parameter information, see Set-TransportAgent.

1.7.2.16.3 Uninstall a Transport Agent

Uninstall a Transport Agent

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to uninstall an existing transport agent on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or Edge Transport server role installed. You can uninstall transport agents configured on the local computer. When the transport agent is uninstalled, Exchange unregisters the DLL files used with the agent. Exchange doesn't remove any files, registry keys, or other objects added by the installation of the transport agent. For more information about transport agents, see Understanding Transport Agents.

Looking for other management tasks related to transport agents? Check out Managing Transport Agents.

Use the Shell to uninstall a transport

agent

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport agents" entry in the Transport Permissions topic.

Note:
You can't use the EMC to uninstall a transport agent.

Use the following syntax to uninstall an existing transport agent.

```
Uninstall-TransportAgent <TransportAgentID>
```

This example uninstalls an existing transport agent.

```
Uninstall-TransportAgent "Antivirus for Exchange"
```

For detailed syntax and parameter information, see Uninstall-TransportAgent.

1.7.2.16.4 View Transport Agents in the Transport Pipeline

View Transport Agents in the Transport Pipeline

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to view a list of transport agents in the transport pipeline on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or Edge Transport server role installed. You can view a list of all the enabled transport agents that have encountered messages in the transport pipeline and the SMTP events they are registered on.

For more information about transport agents, see Understanding Transport Agents.

Looking for other management tasks related to transport agents? Check out Managing Transport Agents.

Use the Shell to view a list of transport agents in the transport pipeline

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport agents" entry in the Transport Permissions topic.

Note:
You can't use the EMC to view a list of transport agents in the transport pipeline.

This example lists transport agents in the transport pipeline.

```
Get-TransportPipeline
```

Important:
Only transport agents that have encountered messages in the transport pipeline

between the time when the Exchange Transport service was started and the time when the **Get-TransportPipeline** cmdlet was run are displayed by the cmdlet. A transport agent that hasn't encountered a message in the transport pipeline won't appear in the results displayed by the **Get-TransportPipeline** cmdlet, even if that transport agent is enabled.

The **Get-TransportPipeline** cmdlet lists each SMTP event in the order that the SMTP events encounter messages in the transport pipeline. Listed next to each SMTP event is each transport agent that's registered on the SMTP event and has encountered a message. This example shows output from the **Get-TransportPipeline** cmdlet run on an Edge Transport server.

```
Event                                 TransportAgents
-----                                 ---------------
OnConnectEvent                        {Connection Filtering Agent}
OnHeloCommand                         {}
OnEhloCommand                         {}
OnAuthCommand                         {}
OnEndOfAuthentication                 {}
OnMailCommand                         {Connection Filtering Agent, Sender Fil
                                      ter Agent}
OnRcptCommand                         {Connection Filtering Agent, Address Re
                                      writing Inbound Agent, Recipient Filter
                                       Agent}
OnDataCommand                         {}
OnEndOfHeaders                        {Connection Filtering Agent, Address Re
                                      writing Inbound Agent, Sender Id Agent,
                                       Sender Filter Agent, Protocol Analysis
                                       Agent}
OnEndOfData                           {Edge Rule Agent, Content Filter Agent,
                                       Protocol Analysis Agent, Attachment Fi
                                      ltering Agent}
OnHelpCommand                         {}
OnNoopCommand                         {}
OnReject                              {Protocol Analysis Agent}
OnRsetCommand                         {Protocol Analysis Agent}
OnDisconnectEvent                     {Protocol Analysis Agent}
```

For detailed syntax and parameter information, see Get-TransportPipeline.

1.7.2.16.5 Enable Pipeline Tracing

Enable Pipeline Tracing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to enable pipeline tracing of e-mail messages as they move through the transport pipeline on computers that have the Exchange Server 2010 Hub Transport server role or Edge Transport server role installed. Pipeline tracing generates log files only for e-mail messages sent from the SMTP e-mail address that you specify by using the *PipelineTracingSenderAddress* parameter on the **Set-TransportServer** cmdlet. Pipeline tracing doesn't generate log files for messages sent from any other e-mail address. The SMTP e-mail address that you specify can be internal or external to your Exchange organization.

If you want to generate log files for messages generated by e-mail servers, such as automatic replies, delivery status notification (DSN) messages, journal reports, and other

system-generated messages, you can specify the value "<>" with the *PipelineTracingSenderAddress* parameter.

Caution:

Setting the value for the *PipelineTracingSenderAddress* parameter to "<>" captures all e-mail server-generated messages received by the Hub Transport or Edge Transport server that you are configuring. Depending on the amount of e-mail server-generated messages that your organization receives, this may place a significant load on the server and may quickly consume available disk space. Always monitor available disk space when pipeline tracing is enabled.

After you specify the pipeline tracing sender address, you can enable pipeline tracing.

Caution:

Pipeline tracing copies the complete contents of e-mail messages sent from the e-mail account configured by using the *PipelineTracingSenderAddress* parameter on the **Set-TransportServer** cmdlet. To avoid unwanted exposure of confidential information, you must set appropriate security permissions on the location of the pipeline tracing log file specified by the *PipelineTracingPath* parameter on the **Set-TransportServer** cmdlet. Don't enable pipeline tracing for long periods of time. Pipeline tracing creates verbose log files that can accumulate quickly. Always monitor available disk space when pipeline tracing is enabled.

For more information about the transport pipeline and transport agents, see Understanding Transport Pipeline and Understanding Transport Agents. Looking for other management tasks related to transport agents? Check out Managing Transport Agents.

Step 1: Use the Shell to configure the pipeline tracing sender address

Use the Shell to configure the pipeline tracing sender address to capture messages from a specific SMTP address

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

Note:

You can't use the Exchange Management Console (EMC) to configure the pipeline tracing sender address.

Use the following syntax to configure the pipeline tracing sender address to capture messages from a specific SMTP address.

```
Set-TransportServer <Identity> -PipelineTracingSenderAddress <SMTPAddress>
```

This example configures the SMTP address, chris@contoso.com, as the pipeline tracing sender address on the Server1 computer.

```
Set-TransportServer Server1 -PipelineTracingSenderAddress chris@contoso.com
```

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to configure the pipeline tracing sender address to capture messages generated by e-mail servers

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure the pipeline tracing sender address.

Use the following syntax to configure the pipeline tracing sender address to capture messages generated by e-mail servers.

```
Set-TransportServer <Identity> -PipelineTracingSenderAddress "<>"
```

This example configures <> as the pipeline tracing sender address on the Server2 computer.

```
Set-TransportServer Server2 -PipelineTracingSenderAddress "<>"
```

For detailed syntax and parameter information, see Set-TransportServer.

Step 2: Use the Shell to configure the location of the pipeline tracing log directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

Note:
You can't use the EMC to configure the location of the pipeline tracing log directory.

By default, the pipeline tracing log directory is located at C:\Program Files\Microsoft \Exchange Server\TransportRoles\Logs\PipelineTracing. The directory must be located on the Exchange 2010 computer.

Use the following syntax to configure the pipeline tracing log location.

```
Set-TransportServer <Identity> -PipelineTracingPath <LocalFilePath>
```

This example sets the location of the pipeline tracing log directory to C:\Pipeline Tracing Logs.

```
Set-TransportServer Server1 -PipelineTracingPath "C:\Pipeline Tracing Logs"
```

For detailed syntax and parameter information, see Set-TransportServer.

Step 3: Use the Shell to enable pipeline tracing

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable pipeline tracing.

By default, pipeline tracing is disabled on computers that run Exchange 2010. You can enable or disable pipeline tracing on each Exchange server.

Configure the pipeline tracing sender address according to the previous procedures

earlier in this topic. You must configure the pipeline tracing sender address before you enable pipeline tracing.

Use the following syntax to enable pipeline tracing.

```
Set-TransportServer <Identity> -PipelineTracingEnabled <$True | $False>
```

This example enables pipeline tracing on the Server1 computer.

```
Set-TransportServer Server1 -PipelineTracingEnabled $True
```

For detailed syntax and parameter information, see Set-TransportServer.

1.7.2.16.6 Create an Address Rewrite Entry

Create an Address Rewrite Entry

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to create an address rewrite entry on a computer that has the Microsoft Exchange Server 2010 Edge Transport server role installed. For more information about address rewriting, see Understanding Address Rewriting.

Looking for other management tasks related to transport agents? Check out Managing Transport Agents.

Note:
The Address Rewriting Inbound agent and the Address Rewriting Outbound agent must be enabled so that address rewrite entries are applied to e-mail messages that enter and leave the Edge Transport server. If address rewrite entries have been created, but the Address Rewriting agents are disabled, Exchange 2010 won't apply the address rewrite entries.

Use the Shell to verify that Address Rewriting agents are enabled

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:
You can't use the EMC to verify that Address Rewriting agents are enabled.

This example verifies whether Address Rewriting agents are enabled on the Edge Transport server. Make sure that the Address Rewriting Inbound and Address Rewriting Outbound agents are enabled.

```
Get-TransportAgent
```

For detailed syntax and parameter information, see Get-TransportAgent.

Use the Shell to enable Address Rewriting agents

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:
You can't use the EMC to enable Address Rewriting agents.

This example enables the Address Rewriting agents if they aren't enabled.

```
Enable-TransportAgent -Identity "Address Rewriting Inbound agent"
Enable-TransportAgent -Identity "Address Rewriting Outbound agent"
```

For detailed syntax and parameter information, see Enable-TransportAgent.

Use the Shell to rewrite a single e-mail address

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:
You can't use the EMC to rewrite a single e-mail address.

You can rewrite the headers of e-mail messages sent to and from specific internal e-mail addresses when messages are sent to and from the Internet.

When you configure Exchange 2010 to rewrite a single e-mail address, the headers of e-mail messages sent to and from that e-mail address are rewritten. For example, the internal address joe@contoso.com can be rewritten so that it appears to be support@contoso.com when e-mail is sent from that account to the Internet. When replies to that e-mail address or new messages to that address arrive, Exchange 2010 rewrites the recipient address in the header of the inbound messages by using the internal address joe@contoso.com.

When you rewrite e-mail addresses, there is a one-to-one correlation between the internal e-mail address and the external e-mail address. This correlation enables Exchange 2010 to automatically rewrite e-mail messages to and from the Internet.

This example creates an address rewrite entry that rewrites a single e-mail address.

```
New-AddressRewriteEntry -name "joe@contoso.com to support@northwindtraders.com" -
```

For detailed syntax and parameter information, see New-AddressRewriteEntry.

Use the Shell to rewrite a single domain

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:

You can't use the EMC to rewrite a single domain.

You can rewrite the headers of e-mail messages sent to and from recipients that send messages from specific internal domain names when messages are sent to and from the Internet.

For example, in the following procedure, the headers of e-mail messages sent from mailboxes in the internal contoso.com domain are rewritten so that the messages appear to originate from the fabrikam.com domain when they are sent to the Internet. When new messages, or replies to messages that originated from the rewritten domain, arrive at the computer that has the Edge Transport server role installed, Exchange 2010 rewrites the recipient address in the header of the inbound messages that have the internal domain contoso.com and delivers the message to the recipient.

This example creates an address rewrite entry that rewrites a single domain.

```
New-AddressRewriteEntry -Name "Contoso to Fabrikam" -InternalAddress contoso.com
```

For detailed syntax and parameter information, see New-AddressRewriteEntry.

Use the Shell to rewrite multiple subdomains

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:

You can't use the EMC to rewrite a multiple subdomains.

You can rewrite the headers of e-mail messages sent from mailboxes located in one of multiple internal subdomains. When you rewrite multiple subdomains, you have the following options:

- **Rewrite e-mail messages from all subdomains** This option enables you to rewrite all subdomains to a single external domain without exception. All e-mail messages from all subdomains will be rewritten.
- **Rewrite e-mail messages from specific subdomains** You may have to rewrite e-mail messages from specific subdomains, but don't want to affect other subdomains. This option is especially convenient when you have many subdomains but only want to rewrite addresses for a few of them. In Exchange 2010, you can configure address rewriting for only those specific subdomains without creating many exceptions.
- **Rewrite e-mail messages from all subdomains with exceptions** You may have to configure address rewriting for many subdomains, but may also have to prevent some subdomains from being rewritten. Instead of creating individual address rewrite entries for each subdomain, you can create an address rewrite entry that encompasses all subdomains, and then specify exceptions for those subdomains that you don't want to rewrite.

Before you configure address rewriting for multiple internal subdomains, you must first prepare your subdomains.

The following examples show how you can use the **New-AddressRewriteEntry** cmdlet to configure address rewriting for multiple subdomains.

This example creates an address rewrite entry that rewrites all e-mail messages sent from multiple subdomains and the parent domain.

```
New-AddressRewriteEntry -Name "Rewrite all contoso.com subdomains" -InternalAddre
```

This example creates an address rewrite entry that rewrites all e-mail messages sent from specific subdomains.

```
New-AddressRewriteEntry -Name "Rewrite sales.contoso.com to contoso.com" -Interna
New-AddressRewriteEntry -Name "Rewrite marketing.contoso.com to contoso.com" -Int
New-AddressRewriteEntry -Name "Rewrite research.contoso.com to contoso.com" -Inte
```

This example creates an address rewrite entry that rewrites all e-mail messages sent from multiple subdomains and the parent domain, except subdomains that you specify.

```
New-AddressRewriteEntry -name "Rewrite all contoso.com subdomains except legal.co
```

For detailed syntax and parameter information, see New-AddressRewriteEntry.

1.7.2.16.7 View or Configure an Address Rewrite Entry

View or Configure an Address Rewrite Entry

Transport > Managing Transport Servers > Managing Transport Agents >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to view or modify an existing address rewrite entry on a computer that has the Microsoft Exchange Server 2010 Edge Transport server role installed.For more information about address rewriting, see Understanding Address Rewriting.

Looking for other management tasks related to transport agents? Check out Managing Transport Agents.

Caution:

Be careful when you modify an address rewrite entry. Any changes that you make are applied immediately when the command is run. We recommend that you first run the command with the *WhatIf* parameter.
For more information about the *WhatIf* parameter, see WhatIf, Confirm, and ValidateOnly Switches.

Prerequisites

Read Create an Address Rewrite Entry.

Use the Shell to view a summary list of all address rewrite entries

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:

You can't use the EMC to view a summary list of all address rewrite entries.

This example provides a summary list of all address rewrite entries.

```
Get-AddressRewriteEntry
```

For detailed syntax and parameter information, see Get-AddressRewriteEntry.

Use the Shell to view detailed configuration of a single address rewrite entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:
You can't use the EMC to view detailed configuration of a single address rewrite entry.

To view detailed configuration of an address rewrite entry, you must pipe the output of the **Get-AddressRewriteEntry** command to the **Format-List** command by using the following command syntax.

```
Get-AddressRewriteEntry <GUID or address rewrite entry name> | Format-List
```

For more information about pipelining, see Pipelining. For more information about how to work with the information returned by a command, see Working with Command Output.

This example provides detailed configuration of the Rewrite Contoso.com to Northwindtraders.com address rewrite entry.

```
Get-AddressRewriteEntry "Rewrite Contoso.com to Northwindtraders.com" | Format-Li
```

For detailed syntax and parameter information, see Get-AddressRewriteEntry.

Use the Shell to modify an address rewrite entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:
You can't use the EMC to modify an address rewrite entry.

To modify an address rewrite entry, you must provide the *Identity* parameter of the address rewrite entry that you want to modify. You typically use the name of the address rewrite entry as its identity, although you can use its GUID.

You can modify several parameters configured on an address rewrite entry. To modify an address rewrite entry, specify the identity of the entry in double quotation marks. You don't have to specify the *Identity* parameter label because it's implied. Also, you should include each parameter that you want to modify, together with its value.

To modify an address rewrite entry, use the following syntax.

```
Set-AddressRewriteEntry <Identity> -Parameter <value>
```

This example modifies the *ExternalAddress* parameter.

Important:
On a single address rewrite entry, the *ExternalAddress* parameter and the *InternalAddress* parameter both must either be an e-mail address or a domain. You can't mix the two types of values on a single address rewrite entry.

```
Set-AddressRewriteEntry "Contoso to Northwindtraders" -ExternalAddress northwindt
```

This example modifies the *InternalAddress* parameter.

```
Set-AddressRewriteEntry "Northwindtraders to Contoso" -InternalAddress northwindt
```

This example modifies the *OutboundOnly* parameter.

Important:
You must use the *OutboundOnly* parameter when you configure address rewrite entries to rewrite multiple internal subdomains to a single external domain. If the *OutboundOnly* parameter is enabled on an address rewrite entry, Exchange 2010 doesn't rewrite inbound e-mail messages sent to the rewritten external domain that you specified.

```
Set-AddressRewriteEntry "Contoso to Northwindtraders" -OutboundOnly:$true
```

This example modifies the *ExceptionList* parameter.

```
Set-AddressRewriteEntry "Contoso to Northwindtraders" -ExceptionList sales.northw
```

Note:
If the **ExceptionList** property that the *ExceptionList* parameter modifies contains multiple values, be sure that you don't overwrite existing values when you add subdomains. For more information about how to add values to, and remove values from, the **ExceptionList** property, see Modifying Multivalued Properties.

This example modifies the *Name* parameter.

```
Set-AddressRewriteEntry "Contoso to Northwindtraders" -Name "Contoso to Woodgrove
```

For detailed syntax and parameter information, see Set-AddressRewriteEntry.

1.7.2.16.8 Remove an Address Rewrite Entry

Remove an Address Rewrite Entry

Transport > Managing Transport Servers > Managing Transport Agents >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to remove a single address rewrite entry and multiple address rewrite entries on a computer that has the Edge Transport server role installed.

In Microsoft Exchange Server 2010, you can use the Address Rewriting agent to modify the addresses of senders and recipients on messages that enter and leave an Exchange 2010 organization.

For more information about address rewriting, see Understanding Address Rewriting.

Looking for other management tasks related to transport agents? Check out Managing Transport Agents.

Caution:
Be careful when you remove an address rewrite entry or multiple address rewrite entries. The changes that you make are applied immediately. Make sure that you are removing the correct address rewrite entries and make a note of the configuration of any entry before you delete it. After you decide which address rewrite entries to remove, we recommend that you first run the command with the *WhatIf* parameter. For more information about the *WhatIf* parameter, see WhatIf, Confirm, and ValidateOnly Switches.

Use the Shell to remove a single address rewriting entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:
You can't use the EMC to remove a single address rewriting entry.

Remove a single address rewrite entry by using the following command syntax.

```
Remove-AddressRewriteEntry <GUID or address rewrite entry name>
```

This example runs the **Remove-AddressRewriteEntry** cmdlet with the *WhatIf* switch. The *WhatIf* switch lets the command run as if it were going to perform the action you specified but doesn't commit any changes. Instead, it displays the results of what would have happened, so you can verify that the actions are correct.

```
Remove-AddressRewriteEntry "Contoso.com to Northwindtraders.com" -WhatIf
```

This example removes a single address rewriting entry.

```
Remove-AddressRewriteEntry "Contoso.com to Northwindtraders.com"
```

For detailed syntax and parameter information, see Remove-AddressRewriteEntry.

Use the Shell to remove multiple address rewriting entries

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Note:
You can't use the EMC to remove multiple address rewriting entries.

To remove multiple address rewrite entries, you must use pipelining to pipe the output of the **Get-AddressRewriteEntry** command to the **Remove-AddressRewriteEntry** command. The **Get-AddressRewriteEntry** command accepts wildcard characters that let you specify matches based on partial names that you supply. The **Remove-AddressRewriteEntry** command accepts the results from the **Get-AddressRewriteEntry** command and removes the address rewrite entries that are returned.

For example, assume that you have configured the following address rewrite entries:

- "Rewrite sales.northwindtraders.com to contoso.com"
- "Rewrite marketing.northwindtraders.com to contoso.com"
- "Rewrite research.northwindtraders.com to contoso.com"

- "Rewrite john@northwindtraders to support@contoso.com"
- "Rewrite joe@northwindtraders to support@contoso.com"

You can use a wildcard character to match a subset of these address rewrite entries. The following examples show how to use a wildcard character to match specific entries in this list:

- Match only the subdomain address rewrite entries.

```
Get-AddressRewriteEntry "*to contoso.com"
```

- Match only the e-mail address rewrite entries.

```
Get-AddressRewriteEntry "*support@contoso.com"
```

Caution:

If you don't specify match criteria when you pipe the results of **Get-AddressRewriteEntry** to **Remove-AddressRewriteEntry**, all address rewrite entries on the local server will be deleted. Therefore, we recommend that you always use the *WhatIf* parameter to make sure that the changes that you are making are correct.

For more information about pipelining, see Pipelining.

Remove multiple address rewrite entries by using the following command syntax.

```
Get-AddressRewriteEntry <match criteria> | Remove-AddressRewriteEntry
```

This example runs the **Get-AddressRewriteEntry** cmdlet with the *WhatIf* switch. The *WhatIf* switch lets the command run as if it were going to perform the action you specified but doesn't commit any changes. Instead, it displays the results of what would have happened, so you can verify that the actions are correct.

```
Get-AddressRewriteEntry "*to contoso.com" | Remove-AddressRewriteEntry -WhatIf
```

This example removes multiple address rewriting entries.

```
Get-AddressRewriteEntry "*to contoso.com" | Remove-AddressRewriteEntry
```

For detailed syntax and parameter information, see Get-AddressRewriteEntry.

1.7.2.16.9 Import Address Rewrite Entries

Import Address Rewrite Entries

Transport > Managing Transport Servers > Managing Transport Agents >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Shell to import address rewrite entries into a computer that has the Microsoft Exchange Server 2010 Edge Transport server role installed.

The following are some of the common scenarios in which you may want to perform a bulk import of address rewrite entries:

- **Migration** You may want to bulk import address rewrite entries from a

previous solution that is being replaced by an Edge Transport server solution.
- **Outsourcing** You may have to bulk import address rewrite entries when you enter into agreements with third-party solution providers where their e-mail addresses must be rewritten.
- **Acquisition** You may have to bulk import address rewrite entries when the acquisition of other organizations requires the interim rewriting of the e-mail addresses of the acquired organizations.

If you have more than one Edge Transport server, we recommend that you use the following procedures to import address rewrite entries into a single Edge Transport server, and then clone the configuration of that Edge Transport server to other Edge Transport servers in your organization. For more information about how to clone an Edge Transport server, see Understanding Edge Transport Server Cloned Configuration.

Looking for other management tasks related to address rewrite entries? Check out Managing Transport Agents.

Prerequisites

You must be familiar with how to create an address rewrite entry before you try to use comma-separated value (CSV) files to perform bulk imports of address rewrite entries. For information, see Create an Address Rewrite Entry.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Rewriting agent" entry in the Transport Permissions topic.

Step 1: Create a CSV file

First, you must create a CSV file that contains columns of values that correlate to the parameters that are required by the **New-AddressRewriteEntry** cmdlet. The following values are required by the **New-AddressRewriteEntry** cmdlet and therefore must have corresponding columns in the CSV file:

- *Name* This parameter must be a string that uniquely identifies the address rewrite entry.
- *InternalAddress* This parameter specifies the internal SMTP address to be rewritten.
- *ExternalAddress* This parameter specifies the external SMTP address to be rewritten.

The following parameters are optional. You can include columns for them in the CSV file if you need them:

- *ExceptionList* This parameter specifies the list of subdomains that should not be rewritten. No SMTP addresses contained within the specified subdomains are rewritten. You must enclose the values that are used with the *ExceptionList* parameter in double quotation marks ("). If you want to specify multiple domains that have the *ExceptionList* parameter, you must separate each value by using commas (,). For example, the string `"domain1.com,domain2.com, domain3.com"` contains three domains enclosed with double quotation marks and separated by commas.
- *OutboundOnly* This parameter specifies whether the address rewrite entry should rewrite SMTP addresses on messages that are inbound and outbound to the Exchange 2010 organization, or rewrite only those messages that are outbound from the Exchange 2010 organization. Unlike Boolean usage elsewhere in the Shell, when you specify a value for the *OutboundOnly* parameter in a CSV file, you must specify a value of `True` or `False`, not `$True` or `$False`. This is because the value in the CSV file is converted to a Boolean value when the CSV file is interpreted on the command line.

Important:
If you specify values for optional columns in the CSV file, every row must include a value in that column. This is because the cmdlet expects a value for each parameter specified in the CSV file. If you want to create multiple address rewrite entries where some entries have optional parameters and some entries do not, you must separate those address rewrite entries and create two separate CSV files, and then import each of those CSV files.

Important:
You can only specify exception lists for address rewrite entries that are outbound-only. If you use both the *ExceptionList* and *OutboundOnly* columns in your CSV file, you can only put outbound-only address rewrite entries in that CSV file.

The following example shows how a CSV file can be populated with the optional *ExceptionList* and *OutboundOnly* parameters included:

```
Name,InternalAddress,ExternalAddress,ExceptionList,OutboundOnly
"Wingtip UK", *.wingtiptoys.co.uk, tailspintoys.com,"legal.wingtiptoys.co.uk,fina
"Wingtip USA", *.wingtiptoys.com, tailspintoys.com,"legal.wingtiptoys.com,finance
"Wingtip Canada", *.wingtiptoys.ca, tailspintoys.com,"legal.wingtiptoys.ca,financ
```

Step 2: Import a CSV file to create multiple address rewrite entries

You use the **New-AddressRewriteEntry** cmdlet in conjunction with the **Import-CSV** cmdlet to bulk import multiple address rewrite entries.

The following example imports the address rewrite entries that are listed in a previously created CSV file named ImportAddressRewriteEntries.csv.

```
Import-Csv C:\ImportAddressRewriteEntries.csv | ForEach { New-AddressRewriteEntry
```

For detailed syntax and parameter information, see New-AddressRewriteEntry.

1.7.2.17 Managing Transport Logs

Managing Transport Logs

Exchange Server 2010 > Transport > Managing Transport Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-01*

Configure Connectivity Logging

Configure Message Tracking

Search Message Tracking Logs

Configure Protocol Logging

Configure Routing Table Logging

Configure Connectivity Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to configure connectivity logging in Microsoft Exchange Server 2010. You must use the Shell to configure size and age restrictions on the connectivity log files.

Connectivity logging records the connection activity of the outgoing message delivery queues that exist on computers running Exchange 2010 that have the Hub Transport server role or Edge Transport server role installed. The purpose of the connectivity log isn't to track the transmission of individual e-mail messages. Rather, the connectivity log tracks the connection activity from the sending queue to the destination Mailbox server, smart host, or domain.

Looking for other management tasks related to transport logs? Check out Managing Transport Logs.

Enable or disable connectivity logging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

By default, connectivity logging is disabled on all Exchange 2010 computers that have the Hub Transport server role or Edge Transport server role installed.

Use the EMC to enable or disable connectivity logging

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the action pane, click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and select **Hub Transport**. In the action pane, click the **Properties** link that's directly under the server name.
2. On the **Properties** page, click the **Log Settings** tab.
3. In the **Connectivity log** section, perform one of the following steps:
   - Select **Enable connectivity logging** to enable connectivity logging.
   - Clear **Enable connectivity logging** to disable connectivity logging.
4. Click **Apply** to save changes and remain on the **Properties** page, or click **OK** to save changes and exit the **Properties** page.

Use the Shell to enable or disable connectivity logging

To enable or disable connectivity logging, use the following syntax.

```
Set-TransportServer <Identity> -ConnectivityLogEnabled <$true | $false>
```

This example enables connectivity logging on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ConnectivityLogEnabled $true
```

For detailed syntax and parameter information, see Set-TransportServer.

Configure the location of the connectivity log files

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

By default, the connectivity log files are stored in the C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Connectivity directory. The directory must be local to the Exchange 2010 computer.

Use the EMC to change the location of the connectivity log files

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the action pane, click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and select **Hub Transport**. In the action pane, click the **Properties** link that's directly under the server name.
2. On the **Properties** page, click the **Log Settings** tab.
3. In the **Connectivity log** section, click **Browse** next to **Connectivity log path**.
4. In the **Browse for folder** window, browse to the new location where you want to store the connectivity log files. If you want to create a folder, select a parent folder, click **Make New Folder**, and then type the name of the new folder. After you make your folder selection, click **OK** to close the **Browse for folder** window.
5. Click **Apply** to save changes and remain on the **Properties** page, or click **OK** to save changes and exit the **Properties** page.

Use the Shell to change the location of the connectivity log files

To change the location of the connectivity log files, use the following syntax.

```
Set-TransportServer <Identity> -ConnectivityLogPath <LocalFilePath>
```

This example changes the location of the connectivity log file to C:\Connectivity on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ConnectivityLogPath "C:\Connectivity"
```

Note:

If you set the value of the *ConnectivityLogPath* parameter to `$null`, you effectively disable connectivity logging. However, if you set the value of the *ConnectivityLogPath* parameter to `$null` when the value of the **ConnectivityLogEnabled** attribute is `$true`, event log errors are generated. The preferred method to disable connectivity logging is to use the *ConnectivityLogEnabled* parameter with the **Set-TransportServer** cmdlet.

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to change the maximum size of individual connectivity log files

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to change the maximum size of individual connectivity log files.

By default, the maximum size for each connectivity log file is 10 megabytes (MB). When a connectivity log file reaches its maximum size, Exchange 2010 opens a new connectivity log file. This process continues until either the connectivity log directory reaches its specified maximum size or a connectivity log file reaches its specified maximum age. After the maximum size or age limit is reached, circular logging deletes the oldest connectivity log files.

To change the maximum size of individual connectivity log files, use the following syntax.

```
Set-TransportServer <Identity> -ConnectivityLogMaxFileSize <FileSize>
```

This example sets the maximum size of a connectivity log file to 20 MB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ConnectivityLogMaxFileSize 20MB
```

Note:
The value of the *ConnectivityLogMaxFileSize* parameter must be less than or equal to the value of the *ConnectivityLogMaxDirectorySize* parameter. The valid input range for either parameter is 1 through 9223372036854775807 bytes.

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to change the maximum size of the connectivity log directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to change the maximum size of the connectivity log directory.

By default, the maximum size for the whole connectivity log directory is 250 MB. Circular logging deletes the oldest connectivity log files when either the connectivity log directory reaches its specified maximum size or a connectivity log file reaches its specified maximum age.

To change the maximum size of the connectivity log directory, use the following syntax.

```
Set-TransportServer <Identity> -ConnectivityLogMaxDirectorySize <DirectorySize>
```

This example sets the maximum size of the connectivity log directory to 400 MB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ConnectivityLogMaxDirectorySize 400MB
```

Note:
The value of the *ConnectivityLogMaxDirectorySize* parameter must be greater than or equal to the value of the *ConnectivityLogMaxFileSize* parameter. The valid input range for either parameter is 1 through 9223372036854775807 bytes.

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to change the maximum age of the connectivity log files

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to change the maximum age of the connectivity log files.

By default, the maximum age for any connectivity log file is 30 days. Circular logging deletes the oldest connectivity log files when either the connectivity log directory reaches its specified maximum size or a connectivity log file reaches its specified maximum age.

To change the maximum age of the connectivity log files, use the following syntax.

```
Set-TransportServer <Identity> -ConnectivityLogMaxAge <Age>
```

This example changes the maximum age of a connectivity log file to 45 days on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ConnectivityLogMaxAge 45.00:00:00
```

To specify an age value, enter it as a time span, as follows: *dd.hh:mm:ss*, where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is 00:00:00 through 24855.03:14:07. Setting the value of the *ConnectivityLogMaxAge* parameter to 00:00:00 prevents the automatic removal of connectivity log files because of their age.

For detailed syntax and parameter information, see Set-TransportServer.

1.7.2.17.2 Configure Message Tracking

Configure Message Tracking

Transport > Managing Transport Servers > Managing Transport Logs >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Message tracking records the SMTP transport activity of all messages transferred to and from a computer running Exchange 2010 that has the Hub Transport, Edge Transport, or Mailbox server role installed. You can use message tracking logs for message forensics, mail flow analysis, reporting, and troubleshooting.

Looking for other management tasks related to transport logs? Check out Managing Transport Logs.

Enable or disable message tracking

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" or "Edge Transport server" entries in the Transport Permissions topic and the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to enable or disable message tracking on Mailbox servers.

You can enable or disable message tracking on Hub Transport, Edge Transport, and Mailbox servers. By default, message tracking is enabled on all Exchange 2010 computers that have the Hub Transport, Edge Transport, or Mailbox server roles installed.

Use the EMC to enable or disable message tracking on transport servers

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the action pane, click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and select **Hub Transport**. In the action pane, click the **Properties** link that's directly under the server name.
2. On the **Properties** page, click the **Log Settings** tab.
3. In the **Message tracking log** section, perform one of the following steps:
   - Select **Enable message tracking log** to enable message tracking.
   - Clear **Enable message tracking log** to disable message tracking.
4. Click **Apply** to save changes and remain on the **Properties** page, or click **OK** to save changes and exit the **Properties** page.

Use the Shell to enable or disable message tracking on transport servers

This example disables message tracking on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -MessageTrackingLogEnabled:$false
```

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to enable or disable message tracking on Mailbox servers

This example disables message tracking on the Exchange 2010 computer Mailbox01.

```
Set-MailboxServer Mailbox01 -MessageTrackingLogEnabled:$false
```

For detailed syntax and parameter information, see Set-MailboxServer.

Configure the location of message tracking logs

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" or "Edge Transport server" entries in the Transport Permissions topic and the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure the location of message tracking logs on Mailbox servers.

By default, the message tracking logs are stored in the C:\Program Files\Microsoft \Exchange Server\V14\TransportRoles\Logs\MessageTracking directory. The directory must be local to the Exchange 2010 computer.

If you set the value of the *MessageTrackingLogPath* parameter to `$null`, you effectively disable message tracking. However, if you set the value of the *MessageTrackingLogPath* parameter to `$null` when the value of the *MessageTrackingLogEnabled* attribute is `$true`, event log errors are generated. The preferred method to disable message tracking is to use the *MessageTrackingLogEnabled* parameter with the **Set-TransportServer** cmdlet or the **Set-MailboxServer** cmdlet.

Use the EMC to change the location of message tracking logs on transport servers

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the action pane, click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and select **Hub Transport**. In the action pane, click the **Properties** link that's directly under the server name.
2. On the **Properties** page, click the **Log Settings** tab.
3. In the **Message tracking log** section, click **Browse** next to **Message tracking log path**.
4. In the **Browse for folder** window, browse to the new location where you want to store the message tracking log files. If you want to create a folder, select a parent folder, click **Make New Folder**, and then type the name of the new folder. After you make your folder selection, click **OK** to close the **Browse for folder** window.
5. Click **Apply** to save changes and remain on the **Properties** page, or click **OK** to save changes and exit the **Properties** page.

Use the Shell to change the location of message tracking logs on transport servers

To change the location of the message tracking logs on transport servers, use the following syntax.

```
Set-TransportServer <Identity> -MessageTrackingLogPath <LocalFilePath>
```

This example changes the location of the message tracking log to C:\Message Tracking on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -MessageTrackingLogPath "C:\Message Tracking"
```

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to change the location of message tracking logs on Mailbox servers

To change the location of message tracking logs on Mailbox servers, use the following syntax.

```
Set-MailboxServer <Identity> -MessageTrackingLogPath <LocalFilePath>
```

This example changes the location of the message tracking log to C:\Message Tracking on the Exchange 2010 computer Mailbox01.

```
Set-MailboxServer Mailbox01 -MessageTrackingLogPath "C:\Message Tracking"
```

For detailed syntax and parameter information, see Set-MailboxServer.

Configure the size of each message

tracking log file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" or "Edge Transport server" entries in the Transport Permissions topic and the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure the size of each message tracking log file.

By default, the maximum size for each message tracking log file is 10 megabytes (MB). When a message tracking log file reaches its maximum size, Exchange 2010 opens a new message tracking log file. This process continues until either the message tracking log directory reaches its specified maximum size or a message tracking log file reaches its specified maximum age. After the maximum size or age limit is reached, circular logging deletes the oldest message tracking log files.

Use the Shell to change the maximum size of each message tracking log file on transport servers

To change the maximum size of each message tracking log file on transport servers, use the following syntax.

```
Set-TransportServer <Identity> -MessageTrackingLogMaxFileSize <FileSize>
```

This example sets the maximum size of a message tracking log file to 20 MB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -MessageTrackingLogMaxFileSize 20MB
```

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to change the maximum size of each message tracking log file on Mailbox servers

To change the maximum size of each message tracking log file on Mailbox servers, use the following syntax.

```
Set-MailboxServer <Identity> -MessageTrackingLogMaxFileSize <FileSize>
```

This example sets the maximum size of a message tracking log file to 20 MB on the Exchange 2010 computer Mailbox01.

```
Set-MailboxServer Mailbox01 -MessageTrackingLogMaxFileSize 20MB
```

For detailed syntax and parameter information, see Set-MailboxServer.

Configure the size of the message tracking log directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" or "Edge Transport server" entries in the Transport Permissions topic and the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure the size of the message tracking log directory.

By default, the maximum size for the whole message tracking log directory is 250 MB.

Circular logging deletes the oldest message tracking log files when either a message tracking log file reaches its specified maximum age, or the message tracking log directory reaches its specified maximum size.

Important:

The maximum size of the message tracking log directory is calculated as the total size of all log files that have the same name prefix. Other files that don't follow the name prefix convention aren't counted in the total directory size calculation. Renaming old log files or copying other files into the message tracking log directory could cause the directory to exceed its specified maximum size.
When the Hub Transport server role and the Mailbox server role are installed on the same server, the maximum size of the message tracking log directory isn't the specified maximum size because the message tracking log files generated by the different server roles have different name prefixes.
Message tracking log files for the Hub Transport server role or Edge Transport server role begin with the name prefix *MSGTRK*. Message tracking log files for the Mailbox server role begin with the name prefix *MSGTRKM*. When the Hub Transport server role and the Mailbox server role are installed on the same server, the maximum size of the message tracking log directory is two times the specified value.

Use the Shell to change the maximum size of the message tracking log directory on transport servers

To change the maximum size of the message tracking log directory on transport servers, use the following syntax.

```
Set-TransportServer <Identity> -MessageTrackingLogMaxDirectorySize <DirectorySize
```

This example sets the maximum size of the message tracking log directory to 400 MB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -MessageTrackingLogMaxDirectorySize 400MB
```

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to change the maximum size of the message tracking log directory on Mailbox servers

To change the maximum size of the message tracking log directory on Mailbox servers, use the following syntax.

```
Set-MailboxServer <Identity> -MessageTrackingLogMaxDirectorySize <DirectorySize>
```

This example sets the maximum size of the message tracking log directory to 400 MB on the Exchange 2010 computer Mailbox01.

```
Set-TransportServer Mailbox01 -MessageTrackingLogMaxDirectorySize 400MB
```

For detailed syntax and parameter information, see Set-MailboxServer.

Configure the age of message tracking logs

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" or "Edge Transport server" entries in the Transport Permissions topic and the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to configure the age of message tracking logs.

By default, the maximum age for any message tracking log file is 30 days. Circular logging deletes the oldest message tracking log files if the message tracking log directory reaches its specified maximum size or a message tracking log file reaches its specified maximum age.

Use the Shell to change the maximum age of message tracking logs on transport servers

To change the maximum age of message tracking logs on transport servers, use the following syntax.

```
Set-TransportServer <Identity> -MessageTrackingLogMaxAge <Age>
```

This example changes the maximum age of a message tracking log file to 45 days on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -MessageTrackingLogMaxAge 45.00:00:00
```

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to change the maximum age of message tracking logs on Mailbox servers

To change the maximum age of message tracking logs on Mailbox servers, use the following syntax.

```
Set-MailboxServer <Identity> -MessageTrackingLogMaxAge <Age>
```

This example changes the maximum age of a message tracking log file to 45 days on the Exchange 2010 computer Mailbox01.

```
Set-MailboxServer Mailbox01 -MessageTrackingLogMaxAge 45.00:00:00
```

To specify an age value, enter it as a time span, as follows: *dd.hh:mm:ss* where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is 00:00:00 through 24855.03:14:07. Setting the value of the *MessageTrackingLogMaxAge* parameter to 00:00:00 prevents the automatic removal of message tracking log files because of their age.

For detailed syntax and parameter information, see Set-MailboxServer.

Configure message subject logging in message tracking logs

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" or "Edge Transport server" entries in the Transport Permissions topic and the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure message subject logging in message tracking logs.

By default, the subject line of an SMTP e-mail message is stored in the message tracking log. However, you may want to disable message subject logging to comply with increased security or privacy requirements. Before you enable or disable message subject logging, verify your organization's policy about revealing subject line information.

Use the Shell to enable or disable message subject logging in message tracking logs on transport servers

To enable or disable message subject logging in message tracking logs on transport servers, use the following syntax.

```
Set-TransportServer <Identity> -MessageTrackingLogSubjectLoggingEnabled <$true|$f
```

This example disables message subject tracking on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -MessageTrackingLogSubjectLoggingEnabled $false
```

For detailed syntax and parameter information, see Set-TransportServer.

Use the Shell to enable or disable message subject logging in message tracking logs on Mailbox servers

To enable or disable message subject logging in message tracking logs on Mailbox servers, use the following syntax.

```
Set-MailboxServer <Identity> -MessageTrackingLogSubjectLoggingEnabled <$true|$fal
```

This example disables message subject tracking on the Exchange 2010 computer Mailbox01.

```
Set-MailboxServer Mailbox01 -MessageTrackingLogSubjectLoggingEnabled $false
```

For detailed syntax and parameter information, see Set-MailboxServer.

1.7.2.17.3 Search Message Tracking Logs

Search Message Tracking Logs

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-21*

This topic describes how to use the Exchange Management Console or the Exchange Management Shell to search the message tracking logs.

A message tracking log is a detailed log of all message activity as messages are transferred to and from a Microsoft Exchange Server 2010-based computer that has the Hub Transport server role, the Mailbox server role, or the Edge Transport server role installed. Exchange servers that have the Client Access server role or Unified Messaging server role don't have message tracking logs. You can use message tracking logs for message forensics, for mail flow analysis, for reporting, and for troubleshooting.

You can use the **Get-MessageTrackingLog** cmdlet in the Exchange Management Shell and the Message Tracking tool in the Toolbox in the Exchange Management Console to search for entries in the message tracking logs by using specific search criteria.

Before You Begin

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Message tracking" entry in the Transport Permissions topic.

For more information about permissions, about delegating roles, and about the rights that are required to administer Exchange 2010, see Understanding Permissions.

When you search the message tracking log on a Hub Transport server or a Mailbox server, you cannot access the message tracking logs on an Edge Transport server. If you want to search the message tracking logs on an Edge Transport server, you must run the **Get-MessageTrackingLog** cmdlet or the Message Tracking tool directly from the Edge Transport server.

A search of the message tracking logs depends on the Microsoft Exchange Transport Log Search service. If you disable or stop this service, you cannot search the message tracking log files. However, stopping this service does not affect other features in Exchange.

Important:

You cannot copy the message tracking log files from a server that is running Microsoft Exchange and then search them by using the **Get-MessageTrackingLog** cmdlet or the Message Tracking tool. Also, if you save an existing message tracking log, the change in the date and time stamp on the message tracking log file breaks the query logic that Exchange uses to search the message tracking logs.

Criteria for Message Tracking Log Searches

Although many data fields are available for every message tracking log entry, not every field can be used as a search filter. Additionally, the Exchange Management Shell provides more flexibility for searching because of the many search filters that are available for use with the **Get-MessageTrackingLog** cmdlet.

Common Search Filters Used with the Get-MessageTrackingLog Cmdlet

The search filters described in the following list are available for use with the **Get-MessageTrackingLog** cmdlet in the Exchange Management Shell:

Note:

Use of a search filter that contains a partial value or multiple values is not supported unless otherwise noted.

- **Recipients** This search filter uses the recipient-address field. You must enter the complete e-mail address of the recipient. Multiple recipient values can be specified by using commas as a delimiter. Multiple individual recipients that are included in a single message are logged by using a single message tracking log entry. Unexpanded distribution group recipients are logged by using the distribution group's SMTP e-mail address.
- **Sender** This search filter uses the sender field. You must enter the complete e-mail address of the sender. The sender field contains the sender's e-mail address as specified in the `Sender:` header field, or in the `From:` header field if `Sender:` is not present.
- **Server** This search filter specifies the Exchange server that contains the message tracking logs to be searched. You can describe the server by using any of the following values:
  - Name
  - Fully qualified domain name (FQDN)
  - Distinguished name (DN)
  - Legacy Exchange DN
  - GUID
- **EventID** This search filter uses the event-id field. In the Message Tracking tool, you select the value of EventID from a drop-down list. In the **Get-MessageTrackingLog** cmdlet, you enter the value of EventID as text. However, the value must exactly match one of the possible EventID values. EventID is the event classification that is assigned to each message tracking

log entry. The available values are as follows:

- BADMAIL
- DEFER
- DELIVER
- DSN
- EXPAND
- FAIL
- POISONMESSAGE
- RECEIVE
- REDIRECT
- RESOLVE
- SEND
- SUBMIT
- TRANSFER

- **MessageID** This search filter uses the message-id field. MessageID is the value of the `Message-ID:` header field. If the `Message-ID:` header field does not exist or is blank, an arbitrary value is assigned. This value is constant for the lifetime of the message.
- **InternalMessageID** This search filter uses the internal-message-id field. InternalMessageID is a message identifier integer that is assigned by the Exchange server that is currently processing the message.
- **Subject** The parameter in the **Get-MessageTrackingLog** cmdlet is named *MessageSubject*. This search filter uses the message-subject field. Partial values are supported. This is the message's subject as specified in the `Subject:` header field. The tracking of message subjects is controlled by the *MessageTrackingLogSubjectLoggingEnabled* parameter in the **Set-TransportServer** cmdlet on Hub Transport servers and Edge Transport servers, and by the **Set-MailboxServer** cmdlet on Mailbox servers. By default, message subject logging is enabled. You can disable message subject logging by setting the value of the *MessageTrackingLogSubjectLoggingEnabled* parameter to `$False`.
- **Reference** This search filter uses the reference field. This field contains additional information for specific event types. For a DSN event, the reference field contains the `MessageID:` of the message that caused the DSN. For a SEND event, the reference field contains the `MessageID:` of any DSN messages. For a TRANSFER event, the reference field contains the `MessageID:` of the message that is being forked.
- **Start** This search filter uses the date-time field to look for message tracking entries that begin with the specified End date and time. You can use this filter by itself to retrieve all message tracking log entries after the specified date-time or as a lower limit with the *End* parameter.
- **End** This search filter uses the date-time field to look for message tracking entries up to but not including the specified End date and time. You can use this filter by itself to retrieve all message tracking log entries before the specified date-time or as an upper limit with the *Start* parameter.

Note:

The date-time field in the message tracking log stores information in Coordinated Universal Time (UTC). However, you should enter your date-time search criteria in the regional date-time format of the computer that you are using to perform the search. The message tracking log search tools automatically convert your regional date-time query into UTC. The search results are automatically converted from UTC back into your regional data-time format for display. The date-time field records the date-time of a particular message tracking event. The message origination date-time is the date-time that the message first enters the Exchange organization. The message origination date-time is stored in the message-info field for all SEND and DELIVER events.

Search Filters that are Different in the Exchange Management Console and the Exchange Management Shell

In the Exchange Management Shell, the **Get-MessageTrackingLog** cmdlet offers more control over the number of search results to display by using the *ResultSize* parameter. By default, a search displays up to 1,000 results. However, you can change the maximum value to a specific number. Alternatively, you can display all results by using the value of `Unlimited`. The Message Tracking tool in the Exchange Management Console does not have a way to customize the maximum number of search results that are displayed.

Searching the Message Tracking Logs by Using the Exchange Management Shell

The following table lists the search filters that are available by using the **Get-MessageTrackingLog** cmdlet in the Exchange Management Shell.

Search filters that are available by using the Get-MessageTrackingLog cmdlet

Search filter	Corresponding field in the message tracking log
End	date-time
EventId	event-id
InternalMessageId	internal-message-id
MessageId	message-id
MessageSubject	message-subject
Recipients	recipient-address
Reference	reference
ResultSize	None. This parameter limits the number of results that are displayed by the search.
Sender	sender-address
Start	date-time

All the parameters that are available with the **Get-MessageTrackingLog** cmdlet are optional. If you enter the **Get-MessageTrackingLog** cmdlet without any parameters, you will see a display of the last 1,000 message tracking log entries.

To use the Exchange Management Shell to search the message tracking logs

- Run the following command:

```
Get-MessageTrackingLog <SearchFilters>
```

For example, to search the message tracking log for all entries from 3/28/2011 8:00 AM to 3/28/2011 5:00 PM for all FAIL events sent by pat@contoso.com, run the following command:

```
Get-MessageTrackingLog -ResultSize Unlimited -Start "3/28/2011 8:00AM"
```

Controlling the Output of a Message

Tracking Log Search Performed in the Exchange Management Shell

When you perform a message tracking log search by using the **Get-MessageTrackingLog** cmdlet, not all the fields are displayed for each message tracking event. The following table lists the fields that are displayed by default by the **Get-MessageTrackingLog** cmdlet.

Fields that are displayed by default by the Get-MessageTrackingLog cmdlet

Search field	Corresponding field in the message tracking log
EventId	event-id
Source	message-source
Sender	sender-address
Recipients	recipient-address
MessageSubject	message-subject

You can control the output of the **Get-MessageTrackingLog** cmdlet by using command output options in the Exchange Management Shell according to the following guidelines:

- You can control the output format of the message tracking log search. You can display the results in a list or in a table.

  Important:
  Although the table format seems like a good choice for an output format, it may not be the best choice. If the field displayed in the table has values that are long, the values are truncated to fit in the columns of the table. Truncation also occurs if you try to display too many fields at the same time. The complete field values are always present if you use the list format. To view more columns, you can also increase the width of the Exchange Management Shell window from the default value of 80 characters. You adjust the size of the Exchange Management Shell window in the properties of the Exchange Management Shell window.

- You can display or hide specific fields that are returned from a message tracking log search. Wildcard characters (*) are supported.
- You can send the results of the search to a file.

The field names displayed by the results from the **Get-MessageTrackingLog** cmdlet are the same field names that you can use to filter the search results. These field names differ slightly from the actual field names that are stored in the message tracking log. The following table juxtaposes the field names that are used in the message tracking log and the field names that are used by the **Get-MessageTrackingLog** cmdlet.

Comparing the field names that are used in the message tracking log and the field names that are used by the Get-MessageTrackingLog cmdlet

Field name that is used in the message tracking log	Field name that is used to filter the Get-MessageTrackingLog results
date-time	Timestamp

client-ip	ClientIp
client-hostname	ClientHostname
server-ip	ServerIp
server-hostname	ServerHostname
source-context	SourceContext
connector-id	ConnectorId
source	Source
event-id	EventId
internal-message-id	InternalMessageId
message-id	MessageId
recipient-address	Recipients
recipient-status	RecipientStatus
total-bytes	TotalBytes
recipient-count	RecipientCount
related-recipient-address	RelatedRecipientAddress
reference	Reference
message-subject	MessageSubject
sender-address	Sender
return-path	ReturnPath
message-info	MessageInfo

To use the Exchange Management Shell to Control the Output of a Search of the Message Tracking Logs

- Use the following command:

```
Get-MessageTrackingLog <SearchFilters> | <Format-Table | Format-List> <
```

For example, to search the message tracking logs for the first 1,000 Send events, display the results that are shown in list format, display the values of any field names that begin with "Send" or "Receive," and write the results to a new file that is named "C:\send search.txt", run the following command:

```
Get-MessageTrackingLog -EventId "Send" | Format-List Send*,Receive* > "
```

Searching the Message Tracking Logs for a Message on Multiple Servers by Using the Exchange Management Shell

A message property that remains constant as it travels throughout the Exchange organization is the value of the `MessageID:` header field. This value is named

InternetMessageId in queue viewing utilities, and MessageId in the message tracking log utilities. After you have determined the value of MessageID:, you can search for that message in the message tracking logs on every Hub Transport server or Mailbox server in the Exchange organization.

To use the Exchange Management Shell to Search Message Tracking Log Entries for a Specific Message Across all Hub Transport Servers and Mailbox Servers

- Use the following command:

```
Get-ExchangeServer | where {$_.isHubTransportServer -eq $true -or $_.is
```

For example, to search the message tracking logs on all Hub Transport servers and Mailbox servers for any entries related to a message that has a MessageID: of ba18339e-8151-4ff3-aeea-87ccf5fc9796@contoso.com, to display the fields date-time, server-hostname, client-hostname, source, event-id, and recipient-address for each entry, and to sort the results by the date-time field, run the following command:

```
Get-ExchangeServer | where {$_.isHubTransportServer -eq $true -or $_.is
```

For detailed syntax and parameter information, see Get-MessageTrackingLog.

For more information about command output options in the Exchange Management Shell, see Exchange Management Shell.

Searching the Message Tracking Logs by Using the Exchange Management Console

To use the Exchange Management Console to Search the Message Tracking Log

1. Start the Exchange Management Console.
2. In the console tree, click **Toolbox**. In the result pane, click **Message Tracking**. In the action pane, click **Open tool**.
3. Log on to Outlook Web App when you are prompted.
4. In the **Select what to manage** list, click **My Organization**, and then click **Reporting** in the navigation pane.
5. Set the search criteria for your message tracking log search by configuring the values for the following available options:
   - **Mailbox to search** Click **Browse**, and then select the appropriate mailbox.
   - **Search for messages sent to** Click this option if you want to search for sent messages, and then click **Select users** to select one or more users.
   - **Search for messages received from** Alternatively, click this option to search for received messages, and then click Select a user to select the particular recipient.
   - **Search for these words in the subject line** Enter the search criteria text if you want to search for messages that contain a particular subject.
6. Click **Search**, and then review the results in the **Search Results** pane.

For More Information

For more information, see the following topics:

Understanding Message Tracking

Configure Message Tracking

1.7.2.17.4 Configure Protocol Logging

Configure Protocol Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Protocol logging records the SMTP conversations that occur between e-mail servers as part of message delivery. These SMTP conversations occur on Send connectors and Receive connectors configured on servers running Microsoft Exchange Server 2010 that have the Hub Transport server role or the Edge Transport server role installed. You can use protocol logging to diagnose mail flow problems.

By default, protocol logging is disabled on all Send connectors and Receive connectors. Protocol logging is enabled or disabled on a per-connector basis. Other protocol logging options are set on a per-connector type basis for the whole server. All the Receive connectors on a Hub Transport server or an Edge Transport server share the same protocol log files and protocol log options. These protocol log files and protocol log options are separate from the Send connector protocol log files and protocol log options that are on the same server. By default, Exchange 2010 uses circular logging to limit the protocol logs based on file size and file age to help control the hard disk space used by the protocol log files.

Looking for other management tasks related to transport logs? Check out Managing Transport Logs.

Caution:

Don't perform this procedure on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Instead, make the changes on the Hub Transport server. The changes are then replicated to the Edge Transport server next time EdgeSync synchronization occurs.

Enable or disable protocol logging on connectors

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" and "Send connectors" entries in the Transport Permissions topic.

Use the EMC to enable or disable protocol logging on connectors

1. Perform one of the following steps:
   - To modify an existing Receive connector on an Edge Transport server, in the console tree, select **Edge Transport**, and then in the work pane, click the **Receive Connectors** tab.
   - To modify an existing Receive connector on a Hub Transport server, expand **Server Configuration** in the console tree, and select **Hub Transport**. In the result pane, select the server that has the Receive connector that you want to modify, and then click the **Receive Connectors** tab.
2. In the work pane, select the Receive connector to modify.
3. Under the name of the Receive connector in the action pane, click **Properties** to open the **Properties** page.
4. Click the **General** tab and use the drop-down box next to **Protocol logging**

level to enable or disable protocol logging. **None** disables protocol logging, and **Verbose** enables protocol logging.

5. After you make your protocol logging selection, click **Apply** to save changes and remain on the **Properties** page, or click **OK** to save changes and exit the **Properties** page.

The procedure is similar for Send connectors. To access Send connectors, you navigate to **Organization Configuration** > **Hub Transport**.

Use the Shell to enable or disable protocol logging on connectors

This example enables protocol logging for the Receive connector Connection from Contoso.com.

```
Set-ReceiveConnector "Connection from Contoso.com" -ProtocolLoggingLevel Verbose
```

The procedure is similar for Send connectors. For Send connectors, you use the **Set-SendConnector** cmdlet.

For detailed syntax and parameter information, see Set-ReceiveConnector or Set-SendConnector.

Enable or disable protocol logging for the intra-organization Send connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

Note:

You can't use the EMC to enable or disable protocol logging for the intra-organization Send connector.

A special Send connector named the intra-organization Send connector exists on every Hub Transport server. This connector is implicitly created, invisible, and requires no management. The intra-organization Send connector is used to relay messages to the following destinations:

- To other Hub Transport servers in the Exchange organization
- To Exchange Server 2003 servers in the Exchange organization
- To Edge Transport servers in the Exchange organization

By default, protocol logging for the intra-organization Send connector is disabled. You can enable or disable protocol logging for the intra-organization Send connector by using the **Set-TransportServer** cmdlet.

This example enables protocol logging on the intra-organization Send connector on a Hub Transport server.

```
Set-TransportServer "Exchange01" -IntraOrgConnectorProtocolLoggingLevel Verbose
```

For detailed syntax and parameter information, see Set-TransportServer.

Configure the location of the protocol log files

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server"

entries in the Transport Permissions topic.

By default, the Receive connector protocol log files are located at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\ProtocolLog\SmtpReceive, and the Send connector protocol log files are located at C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\ProtocolLog\SmtpSend. The directory must be local to the Exchange 2010 computer.

Use the EMC to change the location of the Receive connector protocol log files

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the action pane, click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and select **Hub Transport**. In the action pane, click the **Properties** link that's directly under the server name.
2. On the **Properties** page, click the **Log Settings** tab.
3. In the **Protocol log** section, click **Browse** next to **Receive connector protocol log file path**.
4. In the **Browse for folder** window, browse to the new location where you want to store the Receive connector protocol log files. If you want to create a folder, select a parent folder, click **Make New Folder**, and then type the name of the new folder. After you make your folder selection, click **OK** to close the **Browse for folder** window.
5. Click **Apply** to save changes and remain on the **Properties** page, or click **OK** to save changes and exit the **Properties** page.

Use the Shell to change the location of the Receive connector protocol log files

This example sets the Receive connector protocol log directory to C:\Receive SMTP Log on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ReceiveProtocolLogPath "C:\Receive SMTP Log"
```

For detailed syntax and parameter information, see Set-TransportServer.

Use the EMC to change the location of the Send connector protocol log files

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, select **Edge Transport**, and then in the action pane, click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and select **Hub Transport**. In the action pane, click the **Properties** link that's directly under the server name.
2. On the **Properties** page, click the **Log Settings** tab.
3. In the **Protocol log** section, click **Browse** next to **Send connector protocol log file path**.
4. In the **Browse for folder** window, browse to the new location where you want to store the Send connector protocol log files. If you want to create a folder, select a parent folder, click **Make New Folder**, and then type the name of the new folder. After you make your folder selection, click **OK** to close the **Browse for folder** window.
5. Click **Apply** to save changes and remain on the **Properties** page, or click **OK** to save changes and exit the **Properties** page.

Use the Shell to change the location of the Send connector protocol log files

This example sets the Send connector protocol log directory to C:\Send SMTP Log on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -SendProtocolLogPath "C:\Send SMTP Log"
```

Setting the value of the *SendProtocolLogPath* parameter or *ReceiveProtocolLogPath* parameter to `$null` disables protocol logging for all Send connectors or all Receive connectors on the server. However, setting either of these parameters to `$null` when protocol logging is enabled for any Send connector, including the intra-organization Send connector, or Receive connector on the server generates event log errors. The preferred method of disabling protocol logging is to use the **Set-SendConnector** or **Set-ReceiveConnector** cmdlets to set the *ProtocolLoggingLevel* parameter to `None`. Also, you can use the **Set-TransportServer** cmdlet to set the *IntraOrgProtocolLoggingLevel* parameter to `None`.

For detailed syntax and parameter information, see Set-TransportServer.

Configure the maximum size of each protocol log file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to configure the maximum size of each protocol log file.

By default, the maximum size for each protocol log file is 10 MB. All Receive connectors on the server share the same protocol log files, and all Send connectors on the server share the same protocol log files. When a protocol log file reaches its maximum size, Exchange 2010 opens a new protocol log file. This process continues until either of the following conditions is true:

- The protocol log directory reaches its specified maximum size. For more information about how to change the maximum size of the protocol log directory, see "Configure the maximum size of the protocol log directory" later in this topic.
- A protocol log file reaches its specified maximum age. For more information about how to change the maximum age of a protocol log file, see "Configure the maximum age of the protocol log files" later in this topic.

After the maximum size or age limit is reached, circular logging deletes the oldest protocol log files.

This example sets the maximum size of Receive connector protocol log files to 20 MB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ReceiveProtocolLogMaxFileSize 20MB
```

This example sets the maximum size of Send connector protocol log files to 20 MB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -SendProtocolLogMaxFileSize 20MB
```

For detailed syntax and parameter information, see Set-TransportServer.

Configure the maximum size of the protocol log directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to configure the maximum size of the protocol log directory.

By default, the maximum size for the protocol log directory is 250 MB. All Receive connectors on the server share the same protocol log directory, and all Send connectors on the server share the same protocol log directory. Circular logging deletes the oldest protocol log files when either of the following conditions is true:

- The protocol log directory reaches its specified maximum size.
- A protocol log file reaches its specified maximum age.

This example sets the maximum size of the Receive connector protocol log directory to 400 MB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ReceiveProtocolLogMaxDirectorySize 400MB
```

This example sets the maximum size of the Send connector protocol log directory to 400 MB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -SendProtocolLogMaxDirectorySize 400MB
```

For detailed syntax and parameter information, see Set-TransportServer.

Configure the maximum age of the protocol log files

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to configure the maximum age of the protocol log files.

By default, the maximum age for any protocol log file is 30 days. All Receive connectors on the server share the same protocol log files, and all Send connectors on the server share the same protocol log files. Circular logging deletes the oldest protocol log files if either of the following conditions is true:

- The protocol log directory reaches its specified maximum size.
- A protocol log file reaches its specified maximum age.

This example sets the age limit of the Receive connector protocol log files to 45 days on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ReceiveProtocolLogMaxAge 45.00:00:00
```

This example sets the age limit of the Send connector protocol log files to 45 days on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -SendProtocolLogMaxAge 45.00:00:00
```

To specify an age value, enter the value as a time span: *dd.hh:mm:ss*, where *d* = days, *h*

= hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is from 00:00:00 through 24855.03:14:07. Setting the value of the *ReceiveProtocolLogMaxAge* parameter or the *SendProtocolLogMaxAge* parameter to 00:00:00 prevents the automatic removal of protocol log files because of their age.

For detailed syntax and parameter information, see Set-TransportServer.

1.7.2.17.5 Configure Routing Table Logging

Configure Routing Table Logging

Transport > Managing Transport Servers > Managing Transport Logs >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Routing table logging periodically records a snapshot of the routing table used by the server running Exchange 2010 that has the Hub Transport server role or Edge Transport server role installed. The routing table is used to route messages to their destinations.

Looking for other management tasks related to transport logs? Check out Managing Transport Logs.

Configure the location of the routing table logs

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to configure the location of the routing table logs.

By default, the routing table logs are stored in the C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Routing directory. The directory must be local to the Exchange 2010 computer.

This example changes the location of the routing table log to C:\Routing Table on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -RoutingTableLogPath "C:\Routing Table"
```

For detailed syntax and parameter information, see Set-TransportServer.

Configure the interval for automatic recalculation of the routing table

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

The routing table is recalculated and logged after a routing configuration change, or after a specified time interval has passed if no changes are detected. By default, the routing

table is automatically recalculated every 12 hours.

The interval for automatic recalculation of the routing table is controlled by the *RoutingConfigReloadInterval* parameter in the EdgeTransport.exe.config file located in C:\Program Files\Microsoft\Exchange Server\V14\Bin. The EdgeTransport.exe.config file is an XML application configuration file associated with the EdgeTransport.exe file. EdgeTransport.exe and MSExchangeTransport.exe are the executable files used by the Microsoft Exchange Transport service. This service runs on every Hub Transport server or Edge Transport server. Changes made to the EdgeTransport.exe.config file are applied after the Microsoft Exchange Transport service is restarted.

The following example shows the typical structure of the EdgeTransport.exe.config file.

```
<configuration>

<runtime>

<gcServer enabled="true" />

</runtime>

<appSettings>

<add key=" Configuration Option " value=" Value " />

...

</appSettings>

</configuration>
```

You can add new configuration options or modify existing configuration options in the <appSettings> section. Many available configuration options are unrelated to the routing table. Any configuration options that don't involve the routing table are outside the scope of this topic.

Note:
The parameter names in the <add key=../> section are case sensitive.

1. Open the following file by using Notepad: C:\Program Files\Microsoft \Exchange Server\ V14\Bin\EdgeTransport.exe.config.
2. Modify the following line in the <appSettings> section.

   ```
   <add key="RoutingConfigReloadInterval" value="<interval>" />
   ```

   This example changes the interval for automatic recalculation of the routing table to 10 hours, by modifying the *RoutingConfigReloadInterval* parameter.

   ```
   <add key="RoutingConfigReloadInterval" value="10:00:00" />
   ```

3. Save and close the EdgeTransport.exe.config file.
4. Restart the Microsoft Exchange Transport service.

To specify an age value, enter it as a time span, as follows: *hh:mm:ss*, where *h* = hours, *m* = minutes, and *s* = seconds.

The routing table will be recalculated and logged earlier than the value specified by the *RoutingConfigReloadInterval* parameter if any of the following conditions occur:

- A routing configuration change is detected. For example, a Send connector or a Receive connector is added, removed, or modified, or the 6 hour Kerberos token renewal occurs.
- The Microsoft Exchange Transport service is started.

Configure the maximum size of the routing table log directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to configure the maximum size of the routing table log directory.

By default, the maximum size for the whole routing table log directory is 50 megabytes (MB). Circular logging deletes the oldest routing table log files if either of the following conditions is true:

- The routing table log directory reaches its specified maximum size.
- A routing table log file reaches its specified maximum age.

This example sets the maximum size of the routing table log directory to 70 MB on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -RoutingTableLogMaxDirectorySize 70MB
```

For detailed syntax and parameter information, see Set-TransportServer.

Configure the maximum age of the routing table logs

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to configure the maximum age of the routing table logs.

By default, the maximum age for any routing table log file is 7 days. Circular logging deletes the oldest routing table log files if either of the following conditions is true:

- The routing table log directory reaches its specified maximum size.
- A routing table log file reaches its specified maximum age.

To configure the maximum age of the routing table logs, use the following syntax.

```
Set-TransportServer <Identity> -RoutingTableLogMaxAge <Age>
```

This example changes the maximum age of a routing table log file to 45 days on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -RoutingTableLogMaxAge 45.00:00:00
```

To specify an age value, enter it as a time span, as follows: *dd.hh:mm:ss*, where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is 00:00:00 through 24855.03:14:07. Setting the value of the *RoutingTableLogMaxAge* parameter to 00:00:00 prevents the automatic removal of routing table log files because of their age.

For detailed syntax and parameter information, see Set-TransportServer.

1.7.2.18 Managing Transport Queues

Managing Transport Queues

Exchange Server 2010 > Transport > Managing Transport Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-01*

1.7.2.18.1 Change the Location of the Queue Database

Change the Location of the Queue Database

Transport > Managing Transport Servers > Managing Transport Queues >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A *queue* is a temporary holding location for messages that are waiting to enter the next stage of processing. Each queue represents a logical set of messages that a transport server processes in a specific order.

Microsoft Exchange Server 2010 uses an Extensible Storage Engine (ESE) database for queue message storage. Formerly known as JET, ESE is a method that defines a low-level API to the underlying database structures in Exchange. All the different queues are stored

in a single ESE database. Queues exist only on servers that have the Hub Transport server role or the Edge Transport server role installed.

The location of the queue database and queue database transaction logs are controlled by the *QueueDatabasePath* and *QueueDatabaseLoggingPath* parameters in the EdgeTransport.exe.config application configuration file that's located in the C:\Program Files\Microsoft\Exchange Server\V14\Bin directory. The following list describes some important items to consider when you change the location of the queue database:

- If the target directory doesn't exist, it will be created for you if the parent directory has the following permissions applied to it:
  - Network Service: Full Control
  - System: Full Control
  - Administrators: Full Control
- The existing queue database files Mail.que and Trn.chk aren't moved. New queue database files are created at the new location after you save the EdgeTransport.exe.config application configuration file and restart the Microsoft Exchange Transport service. The existing database files are left at the old location. However, they're no longer used.
- If you want to change the location of the queue database but reuse the existing queue database files, you must move or copy the database files when the Microsoft Exchange Transport service is stopped.
- The existing queue database transaction log files Trn.log, Trntmp.log, Trn*nnn*.log, Trnres00001.jrs, Trnres00002.jrs, and Temp.edb aren't moved. New queue database transaction logs are created at the new location after you save the EdgeTransport.exe.config application configuration file and restart the Microsoft Exchange Transport service. The existing transaction log files are left at the old location. However, they're no longer used.

Note:

Temp.edb is used to verify the queue database schema when the Microsoft Exchange Transport service starts. Although Temp.edb isn't a transaction log file, it's kept in the same location as the transaction log files.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Change the location of the queue database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Use Notepad to create a queue database at a new location

1. Open the following file by using Notepad: C:\Program Files\Microsoft \Exchange Server\V14\Bin\EdgeTransport.exe.config.
2. Modify the following line in the <appSettings> section.

```
<add key="QueueDatabasePath" value="<LocalPath>" />
```

This example creates a queue database at the location C:\Queue\QueueDB.

```
<add key="QueueDatabasePath" value="C:\Queue\QueueDB" />
```

3. Save and close the EdgeTransport.exe.config file.
4. Restart the Microsoft Exchange Transport service.
5. Verify that the new Mail.que and Trn.chk files are created at the new location.
6. Remove the unused Mail.que and Trn.chk files from the original location.

Use Notepad to reuse an existing queue database at a new

location

1. Create the directory where you want to keep the queue database. Make sure that the correct permissions are applied to the directory.
2. Open the following file by using Notepad: C:\Program Files\Microsoft \Exchange Server\V14\Bin\EdgeTransport.exe.config.
3. Modify the following line in the <appSettings> section.

   ```
   <add key="QueueDatabasePath" value="<LocalPath>" />
   ```

   This example changes the location to C:\Queue\QueueDB.

   ```
   <add key="QueueDatabasePath" value="C:\Queue\QueueDB" />
   ```

4. Save and close the EdgeTransport.exe.config file.
5. Stop the Microsoft Exchange Transport service.
6. Copy the files Mail.que and Trn.chk from the original location to the new location.
7. Start the Microsoft Exchange Transport service.
8. Remove the unused Mail.que and Trn.chk files from the original location.

Change the location of the queue database transaction logs

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Use Notepad to create queue database transaction logs at a new location

1. Open the following file by using Notepad: C:\Program Files\Microsoft \Exchange Server\V14\Bin\EdgeTransport.exe.config.
2. Modify the following line in the <appSettings> section.

   ```
   <add key="QueueDatabaseLoggingPath" value="<LocalPath>" />
   ```

   This example creates a queue database at the location C:\Queue \QueueLogs.

   ```
   <add key="QueueDatabaseLoggingPath" value="C:\Queue\QueueLogs" />
   ```

3. Save and close the EdgeTransport.exe.config file.
4. Restart the Microsoft Exchange Transport service.
5. Verify that the new Trn.log, Trntmp.log, Trnres00001.jrs, Trnres00002.jrs, and Temp.edb files are created at the new location.
6. Remove the unused Trn.log, Trntmp.log, Trn*nnnnn*.log, Trnres00001.jrs, Trnres00002.jrs, and Temp.edb files from the original location.

Use Notepad to reuse existing queue database transaction logs at a new location

Under ordinary circumstances, you shouldn't have to reuse existing transaction logs at a new location. An ordinary shutdown of the Microsoft Exchange Transport service commits all uncommitted transaction log entries to the queue database. Circular logging is used. Therefore transaction logs that contain previously committed database changes aren't preserved. Only disaster recovery scenarios where the Microsoft Exchange Transport service wasn't shut down correctly or a hard disk drive failure would require that you restore and relocate an existing queue database and its existing transaction logs.

1. Create the directory where you want to keep the queue database transaction logs. Make sure that the correct permissions are applied to the directory.
2. Open the following file by using Notepad: C:\Program Files\Microsoft \Exchange Server\V14\Bin\EdgeTransport.exe.config.
3. Modify the following line in the <appSettings> section:

```
<add key="QueueDatabaseLoggingPath" value="<LocalPath>" />
```

This example changes the location to C:\Queue\QueueLogs.

```
<add key="QueueDatabaseLoggingPath" value="C:\Queue\QueueLogs" />
```

4. Save and close the EdgeTransport.exe.config file.
5. Stop the Microsoft Exchange Transport service.
6. Copy the existing Trn.log, Trntmp.log, Trn*nnnnn*.log, Trnres00001.jrs, Trnres00002.jrs, and Temp.edb files to the new location.
7. Start the Microsoft Exchange Transport service.
8. Remove the unused Trn.log, Trntmp.log, Trn*nnnnn*.log, Trnres00001.jrs, Trnres00002.jrs, and Temp.edb files from the original location.

1.7.2.18.2 Using Queue Viewer

Using Queue Viewer

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-02*

Queue Viewer is an Exchange Management Console snap-in that's installed when you install the Microsoft Exchange Server 2010 Hub Transport server role or the Edge Transport server role. Queue Viewer is located in the Toolbox node of the Exchange Management Console. You can use this tool to view information about queues on a transport server and the messages that are present in those queues and to perform management actions on queues and mail items. Queue Viewer is useful for troubleshooting mail flow and identifying spam.

When you're using Queue Viewer to manage queues, consider the following:

- You must connect to a transport server. By default, Queue Viewer focuses on the queuing database located on the server to which Queue Viewer connects to run the tasks. However, you can connect to a different server than the one on which you're running the Queue Viewer tasks. For more information, see Connect to a Server by Using Queue Viewer.
- The list of queues and messages can be large, depending on current mail flow, and the list of queues and messages changes when messages enter and leave the server. You can configure the options for Queue Viewer to control the interval at which the list of queues and messages is refreshed and the number of items displayed on each page. For more information, see Set Queue Viewer Options.
- You can create a filter to display the specific set of queues or messages that you want to monitor. After you locate the queues and messages that you want to monitor, you can view the property information for these queues and messages. This information is helpful when you troubleshoot the cause of mail flow problems. For more information, see Filter Queues and Filter Messages in Queues.
- You can use the **Export List** link in the action pane to export the list of queues or a list of messages. For more information, see Export Lists from the Exchange Management Console.

1.7.2.18.2.1 Connect to a Server by Using Queue Viewer

Connect to a Server by Using Queue Viewer

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Queue Viewer to connect to a remote computer that has a Microsoft Exchange Server 2010 Hub Transport server installed. By default, Queue Viewer connects to the queuing database on the server on which Queue Viewer is being run. When you use Queue Viewer on an Edge Transport server, you can't change the focus of the tool.

When you use Queue Viewer on an Exchange 2010 server that's located inside the Exchange organization, you can use Queue Viewer to connect to any Hub Transport server in the organization. You can start more than one instance of Queue Viewer so that each instance focuses on a different server. You can tile Queue Viewer windows so that you can easily monitor more than one Hub Transport server at a time.

You can also specify which server to connect to for the remote Shell. This doesn't need to match the remote server whose queues you're managing using the tool.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the EMC to choose a server to connect to for the remote Shell session

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Note:
You can't use the Shell to perform this task.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Properties**.
4. In the **Queue Viewer Properties** dialog box, select one of the following options:
   - **Connect to the automatically selected server** Select this option to automatically connect to the server whose queues you're managing for running remote Shell.
   - **Specify a server to connect to** Select this option to specify a server to run remote Shell. If you select this option, click **Browse** to open the **Select Exchange Server** dialog box. Select the server to which you want to connect for running the remote Shell, and then click **OK**.

For more information about remote Shell, see Overview of Exchange Management Shell.

Use the EMC to choose a server to manage its queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Note:

You can't use the Shell to perform this task.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Connect to server**.
4. In the **Connect to Server** window, click **Browse** to view a list of the available Hub Transport servers.
5. In the **Select Exchange Server** window, select a Hub Transport server. To search for a Hub Transport server to connect to, use one of the following procedures:
   - Enter the exact server name or the first few letters of the server name in the **Search** field, and then click **Find Now**. Select a server from the result pane.
   - Select the **View** menu, and then click **Show Filter**. In the **Name** column or **Version** column, click the filter icon, and then select the filter operator. Type the filter criteria in the **Enter text here** field. Press ENTER. Select a server from the result pane.
6. Click **OK** to close the **Select Exchange Server** window.
7. After you select a server, in the **Connect to server** window, select the **Set as default server** check box if you want Queue Viewer to focus on this server first whenever Queue Viewer is opened.
8. In the **Connect to server** window, click **Connect**.

1.7.2.18.2.2 Set Queue Viewer Options

Set Queue Viewer Options

Managing Transport Servers > Managing Transport Queues > Using Queue Viewer >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can set options in Queue Viewer to adjust the number of items that are displayed on the page and adjust the auto-refresh interval. The auto-refresh interval determines how frequently the results in Queue Viewer are updated.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the EMC to set Queue Viewer options

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Note:

You can't use the Shell to perform this task.

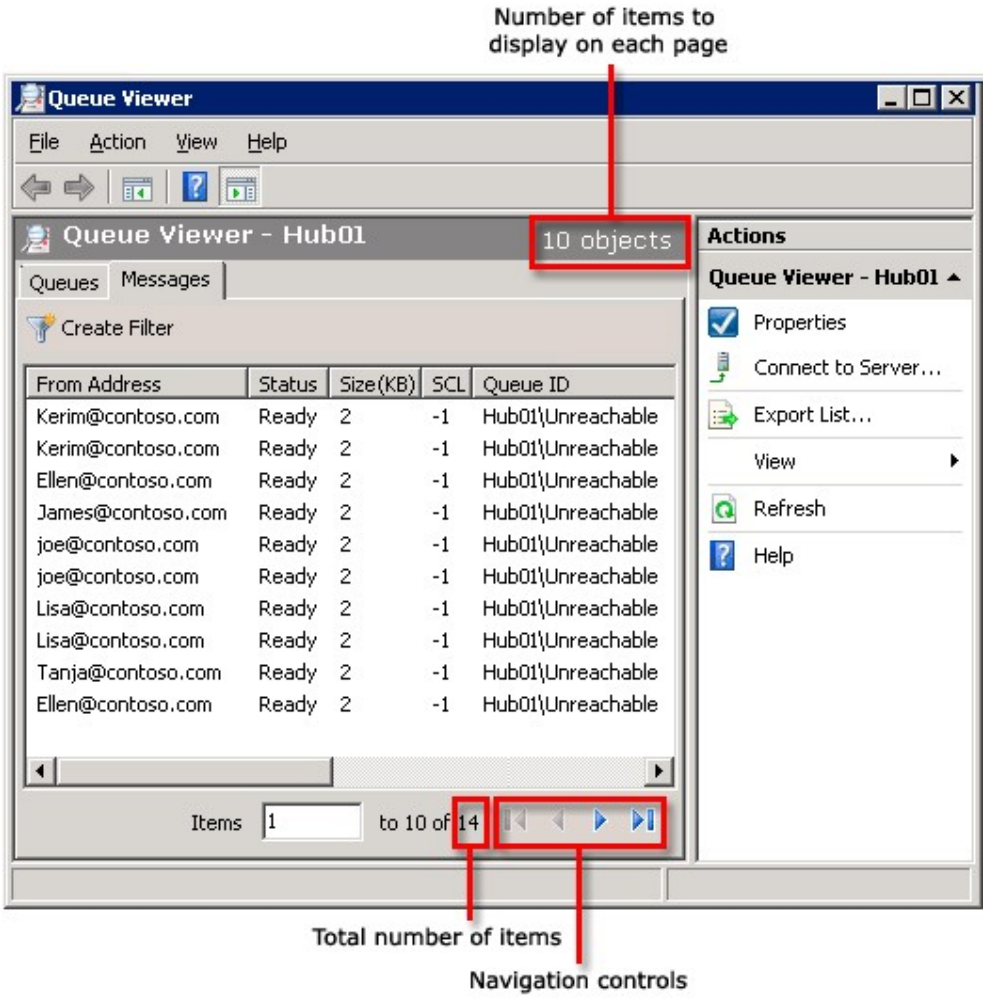
1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Open Tool**.
4. Navigate to **View** > **Options** to open the **Queue Viewer Options** dialog box. Configure the following settings:
   4.a. In the **Refresh interval (seconds)** field, enter the frequency at which Queue Viewer should update the display.

Note:

The default auto-refresh interval is 30 seconds and can't be set for a shorter time. If you disable auto-refresh functionality by clearing the **Auto-refresh screen** check box on the **Queue Viewer Options** page, you must manually update the results that are displayed in Queue Viewer by clicking **Refresh**.

4.b. In the **Number of items to display on each page** field, enter the maximum number of items to display in Queue Viewer. This number must be from 1 through 10,000. If you have more items than the limit, you will see the items in groups of the maximum number of items. For example, the following figure shows a queue with 14 messages with Queue Viewer configured to display 10 items on each page. The number of objects on the page is displayed on the upper right. At the bottom of the page, you can see the total number of items in the queue. You can use the navigation controls to see the additional items in the queue.

5. Click **OK**.



Using the Exchange Management Shell to Manage Queues

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

This topic explains how you can use the cmdlets and parameter sets in the Exchange Management Shell to create a query, retrieve the results, and perform modifying actions. For more information about the queue tasks and how they can be used for monitoring and troubleshooting, see Understanding Transport Queues.

In Microsoft Exchange Server 2010, you can use the Shell to perform management and configuration tasks and to create scripts to automate tasks. You can also use the Shell to view information about queues on a server and the messages in those queues, and to perform management actions on queues and mail items. These operations are useful for troubleshooting mail flow and identifying spam. For more information about how to use the Shell, see Exchange Management Shell.

Looking for management tasks related to queues? See Managing Transport Queues.

Contents

Managing Queues and Messages

Queue tasks are grouped into two categories:

- Viewing actions display queues and messages queued on the server and select how that data is grouped and sorted when it's displayed.
- Modifying actions change the status of queues and messages.

Both types of tasks access data by connecting to the transport worker process by using a remote procedure call (RPC).

By default, Queue Viewer focuses on the queuing database located on the server that Queue Viewer connects to, to run the tasks. However, you can connect to a different server than the one that you are running the Queue Viewer tasks on.

For more information about the Exchange 2010 transport process, see Understanding Transport Pipeline. For more information about how to use the Shell to view queues and messages, see View Queues and View Queued Message Properties.

Return to top

Queue Cmdlets

The following table lists the cmdlets available in the Shell for managing queues and the messages in the queues. For more information about how to use each cmdlet, see the Help topics listed in the **For more information** column.

Queue cmdlets

Cmdlet	Usage	For more information
Export-Message	This cmdlet saves a copy of a message in an administrator-specified file path.	Export-Message Export Messages from Queues
Get-Message	This cmdlet displays the details of the messages currently queued for delivery. You can use the **Get-Message** cmdlet to retrieve a set of messages and then pipe the results to one of the other message management cmdlets.	Get-Message View Queued Message Properties
Get-Queue	This cmdlet displays the configuration details of the queues on transport servers. You can use the **Get-Queue** cmdlet to retrieve a set of queues and then pipe the results to one of the other queue management cmdlets.	Get-Queue View Queues
Remove-Message	This cmdlet deletes a message from a queue. You can select whether a non-delivery report (NDR) is sent.	Remove-Message Remove Messages from Queues
Resume-Message	This cmdlet resumes delivery of a previously suspended message. You can also use the **Resume-Message** cmdlet to resubmit messages in the poison message queue to the Submission queue for the categorizer to reprocess.	Resume-Message Resume Messages Resubmit Messages in Queues
Resume-Queue	This cmdlet resumes deliveries of messages from a previously suspended queue.	Resume-Queue Resume Queues
Retry-Queue	This cmdlet forces a connection attempt for a queue that currently has a status of Retry. This connection attempt overrides the next scheduled retry. You can also use the **Retry-Queue** cmdlet together with the *Resubmit* parameter to send messages in delivery queues or in the Unreachable queue to the Submission queue for the categorizer to reprocess.	Retry-Queue Retry Queues Resubmit Messages in Queues

Suspend-Message	This cmdlet suspends delivery of a message located in a queue on an Exchange 2010 transport server.	Suspend-Message Suspend Messages
Suspend-Queue	This cmdlet suspends outgoing activities for a queue on an Exchange 2010 transport server.	Suspend-Queue Suspend Queues

Return to top

Queue Task Parameter Sets

Queue tasks support multiple parameter sets. These parameter sets are as follows: Identity, Filter, and Queue. The Identity, Filter, and Queue parameter sets can't be combined in a command. The Queue parameter set is available only with message commands.

You can also use the advanced paging parameters available in the Shell in combination with the Identity, Filter, and Queue parameter sets. The advanced paging parameters are used with the **Get-Message** and **Get-Queue** cmdlets to control how the result set is sorted and displayed. The advanced paging parameters are described in a table in "Advanced Paging Parameters" later in this topic.

You must use an Identity, Filter, or Queue parameter set when using a command that modifies messages or queues. If you don't provide any parameters, the **Get-Message** and **Get-Queue** cmdlets display every message or queue object that exists on the local server.

If the result set for a queue or message query contains more than 250,000 items, an error occurs, and you will be prompted to apply a filter to reduce the number of results.

Identity Parameter

Use the *Identity* parameter when the specific message or queue that you want to view or that you will take action against is known. The search by identity is faster than formulating the same query as a filter.

The server name can be expressed as a host name or as a fully qualified domain name (FQDN). You can enter the name of a remote server as part of the identity to initiate an RPC connection to that server so that you can query the queues on that server. If you don't use a server name, the local host is implied.

When an identity is provided to a modifying action, the object identified must be fully defined and unique. If the identity isn't explicit, the action won't be performed. If you omit the server part of the identity, the local computer will be assumed.

When you use the *Identity* parameter as part of a **Get-Queue** or **Get-Message** cmdlet, the *Identity* parameter supports the use of wildcard expressions.

Queue Identity

Persistent queues have unique names and can be specified by name. Delivery queues are assigned a unique database identity. You can use this database identity to specify a queue, or you can use the name of the delivery destination to specify a queue. To perform an operation on a queue by specifying its unique database identity, you must first run the **Get-Queue** cmdlet. The database identity will be returned in the results. The accepted identity formats for queues are shown in the following table.

Queue identity formats

Queue identity format	Usage
Server\QueueJetID (Int64)	The complete, unique identity for a delivery queue.
\QueueJetID	The identity of a queue on the local server. The server name is omitted. Therefore, the local server is implied.
Server*	Any queue on the specified server.
Server\NextHopDomain	A queue on the specified server holding messages for delivery to a specific remote domain.
\NextHopDomain	A queue holding messages destined for a specific domain and located on the local server.
Server\Poison	The poison message queue located on the specified server.
Server\Submission	The queue that contains items waiting to be processed by the categorizer.
Server\Unreachable	The queue that contains items that can't be routed and located on the specified server.

The following code is an example of how to use a queue identity with the **Get-Queue** cmdlet. This example returns a list of all queues holding messages for delivery to SMTP domain names that end in Contoso.com. This example also formats the result set as a detailed list.

```
Get-Queue -Identity Server\*Contoso.com | format-list
```

Message Identity

The identity of a message is an aggregation of the unique database mail item and the queue identity. An identity, in the form of an integer, is assigned to a message when the message enters the queuing Extensible Storage Engine (ESE) database (formerly known as Jet), and that integer is appended to the queue identity to create the message identity.

To perform an operation on a message by specifying its database identity, you must first run the **Get-Message** cmdlet. The identity is returned in the results. If you want to connect to a remote server, you can include the server name as part of the message identity. If the server name is omitted, the local server is assumed.

A message being sent to more than one recipient may be located in multiple queues. You can use a wildcard character to specify that you want to locate the message in every queue to which the message was routed. The following table provides examples of a valid message identity.

Message identity formats

Message identity format	Usage
Server\QueueJetId\MessageJetID	Full denomination of a message in a queue.
Server\Poison\MessageJetID	A message in the poison message queue.

MessageJetID	All messages that have this database identity and are routed to any queue on the local server (one message routed to multiple queues).
Server*\MessageJetID	All messages that have this database identity and are routed to any queue on the specified server.

The following code is an example of how to use a message identity with the **Get-Message** cmdlet. This example returns a list of all messages that have the specified identity and are located in any queue on the specified server. This example also formats the result set as a detailed list.

```
Get-message -Identity Server\*\1234 | Format-List
```

Filter Parameter

Queue tasks support the *Filter* parameter so you can specify criteria for which queues and messages should be retrieved. The queue and message properties are used as filter criteria. Create a filter to display a limited set of queues or messages. After you locate the queues and messages that you want to monitor, you can view property information for each object. This information is helpful when you troubleshoot mail flow problems.

Use the *Filter* parameter to supply an expression with logical and relational operators so that only the queue or message objects that meet the filter criteria are displayed. You can use the **-and** logical operator to specify multiple conditions that the results will match. If you use the **-and** operator, only objects that match all specified conditions of the expression are displayed. A subset of the properties of a message or a queue is used to specify the filter criteria. When you specify a property, it must be a valid property for the object for which you are querying, and the value to match must be expressed by using the correct syntax. When a property value is expressed as anything other than a single integer, make sure that you enclose the value in quotation marks.

The *Server* parameter can be included in a command together with the *Filter* parameter. Use the *Server* parameter to specify the host name or FQDN of the server that you want to connect to by using RPC to query the queues and messages on that server and retrieve a result set.

For more information about the properties that can be used for filtering, the correct syntax for these properties, and the supported operators, see the following topics:

- Filter Queues
- Filter Messages in Queues

Queue Parameter

The *Queue* parameter is used only with message commands. Use this parameter to specify the identity of the queue from which messages are retrieved. If a queue is specified, all messages in that queue are retrieved. You can retrieve all messages from a particular queue without having to use a filter expression. You can retrieve messages in multiple queues by using a wildcard character.

When you use the *Queue* parameter with a message command, use the queue identity format from the table in "Queue Identity" earlier in this topic. The following code example shows how to use the *Queue* parameter with a **Get-Message** cmdlet. This example produces a result set that contains only messages located on the specified server and queued for delivery to the SMTP domain Contoso.com.

```
Get-message -Queue Server\Contoso.com
```

Advanced Paging Parameters

Depending on current mail flow, queries against queues and messages can return a large set of objects. You can use the advanced paging parameters to control how query results are retrieved and displayed.

When you use the Shell to view queues and the messages in the queues, your query retrieves one page of information at a time. The advanced paging parameters control the size of the result set and can also be used to sort the results. All advanced paging parameters are optional and can be combined with any one of the parameter sets that can be used with the **Get-Queue** and **Get-Message** cmdlets. If you don't specify any advanced paging parameters, the query returns the results in ascending order of identity.

By default, when a sort order is specified, the message identity property is always included and is sorted in an ascending order. This is the default ordering relationship. The message identity property is included because the other properties that can be included in a sort order aren't unique. By explicitly including the message identity property in the sort order, you can specify that the results display the message identity sorted in descending order.

You can use the *BookmarkIndex* and *BookmarkObject* parameters to mark a position in the sorted result set. If the bookmark object no longer exists when the next page of results is retrieved, the default ordering relationship makes sure that the result set starts with the closest object to the bookmark. The closest object depends on the specified sort order.

The following table describes the advanced paging parameters.

Advanced paging parameters

Parameter	Description
BookmarkIndex	The *BookmarkIndex* parameter specifies the position in the result set where the displayed results start. The value of the *BookmarkIndex* parameter is a 1-based index in the total result set. If the value is less than or equal to zero, the first complete page of results is returned. If the value is set to Int.MaxValue, the last complete page of results is returned.
BookmarkObject	The *BookmarkObject* parameter specifies the object in the result set where the displayed results start. If you specify a bookmark object, that object is used as the point to start the search. The rows before or after that object, depending on the value of the *SearchForward* parameter, are retrieved. You can't combine the *BookmarkObject* parameter and the *BookmarkIndex* parameter in a single query.
IncludeBookmark	The *IncludeBookmark* parameter specifies whether to include the bookmark object in the result set. By default, this value is set to `$true` and the bookmark object is included. You may run a query for a limited result size, and then specify the last item in that result set as the bookmark for the next query. In this case, you may want to set *IncludeBookmark* to `$false` so that the object isn't included in both result sets.

ResultSize	The *ResultSize* parameter specifies the number of results to display per page. If you don't specify a value, the default result size of 1,000 objects is used. Exchange 2010 limits the result set to 250,000.
ReturnPageInfo	The *ReturnPageInfo* parameter is a hidden parameter. It returns information about the total number of results and the index of the first object of the current page. The default value is `$false`.
SearchForward	The *SearchForward* parameter specifies whether to search forward or backward in the result set. This parameter doesn't affect the order in which the result set is returned. It determines the direction of search relative to the bookmark index or object. If no bookmark index or object is specified, the *SearchForward* parameter determines whether the search starts from the first or last object in the result set. The default value for this parameter is `$true`. If the *SearchForward* parameter is set to `$true` and a bookmark is specified, the query searches forward from that bookmark. If you use this configuration and there are no results beyond the bookmark, the query returns the last full page of results. If the *SearchForward* parameter is set to `$false` and a bookmark is specified, the query searches backward from that bookmark. If you use this configuration and there is less than a full page of results beyond the bookmark, the query returns the first full page of results.
SortOrder	The *SortOrder* parameter specifies an array of message properties used to control the sort order of the result set. The sort order properties are specified in descending order of precedence. Each property is separated by a comma and appended with a plus sign (+) to sort in ascending order, or a minus sign (-) to sort in descending order. If an explicit sort order isn't specified by using this parameter, the records that match the query are displayed and sorted by the Identity field for the respective object type. The results are always sorted by identity in ascending order when a sort order isn't explicitly specified.

The following code example shows how to use the advanced paging parameters in a query. In this example, the command connects to the specified server and retrieves a result set that contains 500 objects. The results are displayed in a sorted order, first in

ascending order by sender address, and then in descending order of message size.

```
Get-message -Server Exchange.Contoso.com -ResultSize 500 -SortOrder
+FromAddress,-Size
```

If you want to view successive pages, you can set a bookmark for the last object retrieved in a result set and run an additional query. You must use the scripting capabilities of the Shell to perform this procedure.

The following example uses scripting to retrieve the first page of results, sets the bookmark object, excludes the bookmark object from the result set, and then retrieves the next 500 objects on the specified server.

1. Open the Shell and type the following command to retrieve the first page of results.

   ```
   $Results=Get-message -Server Exchange.Contoso.com -ResultSize 500 -Sor
   ```

2. To set the bookmark object, type the following command to save the last element of the first page to a variable.

   ```
   $temp=$results[$results.length-1]
   ```

3. To retrieve the next 500 objects on the specified server and to exclude the bookmark object, type the following command.

   ```
   Get-message -Server Exchange.Contoso.com -BookmarkObject:$temp -Includ
   ```

Return to top

1.7.2.18.4 Filter Queues

Filter Queues

Transport > Managing Transport Servers > Managing Transport Queues >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Queue Viewer or the Exchange Management Shell to filter queues on a computer that has the Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed. The list of queues can be lengthy, depending on current mail flow. The list of queues can also frequently change when messages enter and leave the server. By filtering queues, you can adjust your search to specific criteria and locate queues that are experiencing a mail flow problem. You can then perform operations that modify the status of those queues.

To learn more about filtering queues, see "Queue Filtering Scenarios" in Understanding Transport Queues.

Looking for other management tasks related to queues? Check out Managing Transport Queues.

Use Queue Viewer to filter queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. Open the EMC.
2. In the console tree, click **Toolbox**.
3. In the result pane, click **Exchange Queue Viewer**.

4. In the action pane, click **Open Tool**.
5. In Queue Viewer, click the **Queues** tab. A list of all queues on the server to which you are connected is displayed.
6. Click **Create Filter**, and enter your filter expression as follows:
   6.a. Select a queue property from the queue property drop-down list.
   6.b. Select a comparison operator from the comparison operator drop-down list.
   6.c. Enter a value from the value drop-down list. If the property has fixed values, select a value from the drop-down list. If the property requires a date/time expression, change the current date/time values or click the drop-down list to select a date from the calendar interface.
7. (Optional) Click **Add Expression** to specify additional filter criteria. Only queues that meet all filter criteria will be displayed.
8. Click **Apply Filter**. The results of queues that meet the filter criteria are displayed.

Use the Shell to filter queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

This example uses the **Get-Queue** cmdlet to view all queues that have a message count equal to or greater than 1,000 and that have a status of Retry.

```
Get-Queue -Filter {MessageCount -ge 1000 -and Status -eq "Retry"}
```

For detailed syntax and parameter information, see Get-Queue.

1.7.2.18.5 View Queues

View Queues

Transport > Managing Transport Servers > Managing Transport Queues >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can view queues that are present on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the EMC to view queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Open Tool**.
4. In Queue Viewer, click the **Queues** tab. A list of all queues on the server to which you're connected is displayed.
5. You can use the **Export List** link in the action pane to export the list of queues. For more information, see Export Lists from the Exchange Management Console.

Use the Shell to view queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

This example displays basic information about all queues on the Edge Transport server on which the command is run.

```
Get-Queue
```

This example displays detailed information for all queues on the Edge Transport server on which the command is run.

```
Get-Queue | Format-List
```

Note:
This command supports the use of paging parameters that let you control how results are displayed. For more information about how to use paging parameters, see Using the Exchange Management Shell to Manage Queues.

For detailed syntax and parameter information, see Get-Queue.

1.7.2.18.6 Resume Queues

Resume Queues

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can resume queues that are present on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed.

By resuming a queue, you restart outgoing activities on a queue that has a status of Suspended. The queue must have a status of Suspended for this action to have any effect. When you resume a queue, the status of messages in the queue doesn't change. Messages that have a status of Suspended remain suspended and don't leave the queue.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the EMC to resume queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Open Tool**.
4. In Queue Viewer, click the **Queues** tab. A list of all queues on the server to which you're connected is displayed.
5. Click **Create Filter**, and enter your filter expression as follows:
   5.a. Select **Status** from the queue property drop-down list.
   5.b. Select **Equals** from the comparison operator drop-down list.
   5.c. Select **Suspended** from the value drop-down list.

6. Click **Apply Filter**. All queues on the server that are currently suspended are displayed.
7. Select one or more queues from the list, right-click, and then select **Resume**.

Use the Shell to resume queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

To resume queues, use the following syntax.

```
Resume-Queue -Filter {property -operator "value"}
```

This example resumes all queues that have a status of Suspended.

```
Resume-Queue -Filter {status -eq "Suspended"}
```

For detailed syntax and parameter information, see Resume-Queue.

1.7.2.18.7 Retry Queues

Retry Queues

Transport > Managing Transport Servers > Managing Transport Queues >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can retry a mailbox delivery queue or a remote delivery queue that's present on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed.

When a transport server can't connect to the next hop, the delivery queue is put in a status of Retry. When you retry a delivery queue by using Queue Viewer or the Shell, you force an immediate connection attempt and override the next scheduled retry time. If the connection isn't successful, the retry interval timer is reset. The delivery queue must be in a status of Retry for this action to have any effect.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the EMC to retry a queue

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Open Tool**.
4. In Queue Viewer, click the **Queues** tab. A list of all queues on the server to which you're connected is displayed.
5. Click **Create Filter**, and enter your filter expression as follows:
   5.a. Select **Status** from the queue property drop-down list.
   5.b. Select **Equals** from the comparison operator drop-down list.
   5.c. Select **Retry** from the value drop-down list.
6. Click **Apply Filter**. All queues that currently have a retry status are displayed.
7. Select one or more queues from the list. Right-click, and then select **Retry Queue**. If the connection attempt is successful, the queue status changes to

Active. If no connection can be made, the queue remains in a status of Retry and the next retry time is updated.

Use the Shell to retry a queue

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

This example retries all queues with the status of Retry.

```
Retry-Queue -Filter {status -eq "retry"}
```

This example retries the queue Server\Queue.

```
Retry-Queue -Identity Server\Queue
```

For detailed syntax and parameter information, see Retry-Queue.

1.7.2.18.8 Suspend Queues

Suspend Queues

Transport > Managing Transport Servers > Managing Transport Queues >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can suspend a queue that's present on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed. By suspending a queue, you prevent messages from leaving the queue, but you don't change the status of messages in the queue. Messages that are in delivery through SMTP-send will finish operations. You can suspend a queue to stop mail flow, and then suspend one or more messages in the queue. When you resume the queue, the messages that were suspended won't leave the queue.

You can suspend a queue that has a status of Active or Retry. You can also suspend the Unreachable queue and the Submission queue.

If you suspend the Unreachable queue, items won't be resubmitted to the categorizer when configuration updates are received by the transport server until the queue is resumed. If you suspend the Submission queue, messages won't be picked up by the categorizer until the queue is resumed.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the EMC to suspend a queue

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Open Tool**.
4. In Queue Viewer, click the **Queues** tab. A list of all queues on the server to which you're connected is displayed. You can create a filter to display only queues that meet specific criteria.
5. Select one or more queues, right-click, and then select **Suspend**.

Use the Shell to suspend a queue

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

To suspend a queue, use the following syntax.

```
Suspend-Queue -Filter {property -operator "value"}
```

This example suspends all queues that have a message count equal to or greater than 1,000 and that have a status of Retry.

```
Suspend-Queue -Filter {MessageCount -ge 1000 -and Status -eq "Retry"}
```

For detailed syntax and parameter information, see Suspend-Queue.

1.7.2.18.9 Configure Message Retry, Resubmit, and Expiration Intervals

Configure Message Retry, Resubmit, and Expiration Intervals

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure message retry, resubmit, and expiration intervals on a server running Microsoft Exchange Server 2010 that has the Hub Transport server role or the Edge Transport server role installed.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Configure the queue glitch retry count

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

The queue glitch retry count specifies the number of connection attempts that are immediately tried when a transport server has trouble connecting with the destination server. The default queue glitch retry count is 4. The valid input range for this parameter is from 0 through 15. Typically, you don't have to modify this parameter unless the network is unreliable and continues to experience many accidentally dropped connections. If you set the queue glitch retry count to 0, the server doesn't immediately attempt to retry an unsuccessful connection, and the next connection attempt is controlled by the *transient failure retry attempts*.

1. Open the following file by using Notepad: C:\Program Files\Microsoft \Exchange Server\V14\Bin\EdgeTransport.exe.config.
2. Modify the following line in the <appSettings> section.

   ```
   <add key="QueueGlitchRetryCount" value="<Integer>" />
   ```

   This example changes the queue glitch retry count to 6.

   ```
   <add key="QueueGlitchRetryCount" value="6" />
   ```

3. Save and close the EdgeTransport.exe.config file.
4. Restart the Microsoft Exchange Transport service.

Configure the queue glitch retry interval

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

The queue glitch retry interval specifies the interval between each connection attempt specified by the *QueueGlitchRetryCount* parameter. The default queue glitch retry interval is 1 minute. To specify an age value, enter the value as a time span, as follows: *hh:mm:ss*, where *h* = hours, *m* = minutes, and *s* = seconds. Typically, you don't have to modify this parameter unless the network is unreliable and continues to experience many accidentally dropped connections.

1. Open the following file by using Notepad: C:\Program Files\Microsoft \Exchange Server\V14\Bin\EdgeTransport.exe.config.
2. Modify the following line in the <appSettings> section.

```
<add key="QueueGlitchRetryInterval" value="<hh:mm:ss>" />
```

   This example changes the queue glitch retry interval to 30 seconds,

```
<add key="QueueGlitchRetryInterval" value="00:00:30" />
```

3. Save and close the EdgeTransport.exe.config file.
4. Restart the Microsoft Exchange Transport service.

Configure the number of transient failure retry attempts

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

The number of transient failure retry attempts specifies the number of connection attempts that are tried after the connection attempts controlled by the *QueueGlitchRetryCount* and *QueueGlitchRetryInterval* parameters have failed. The default number of transient failure retry attempts is 6. The valid input range for this parameter is from 0 through 15. If you set the number of transient failure retry attempts to 0, the next connection attempt is controlled by the outbound connection failure retry interval.

Use the EMC to configure the number of transient failure retry attempts

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, in the console tree, select **Edge Transport**, and then click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and then select **Hub Transport**. In the result pane, select a server. In the action pane, click the **Properties** link that's directly under the server name.
2. Click the **Limits** tab.
3. Enter an integer next to **Transient failure retry attempts**.
4. Click **Apply** to save your changes and remain in the **Properties** page, or click **OK** to save your changes and exit the **Properties** page.

Use the Shell to configure the number of transient failure retry attempts

This example changes the number of transient failure retry attempts to 8 on the Edge Transport server Exchange01.

```
Set-TransportServer Exchange01 - TransientFailureRetryCount 8
```

For detailed syntax and configuration information, see Set-TransportServer.

Configure the transient failure retry interval

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

The transient failure retry interval specifies the interval between each connection attempt that's specified by the number of transient failure retry attempts. On a Hub Transport server, the default transient failure retry interval is 5 minutes. On an Edge Transport server, the default transient failure retry interval is 10 minutes.

Use the EMC to configure the transient failure retry interval

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, in the console tree, select **Edge Transport**, and then click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and then select **Hub Transport**. In the result pane, select a server. In the action pane, click the **Properties** link that's directly under the server name.
2. Click the **Limits** tab.
3. Enter a value in seconds next to **Transient failure retry interval (seconds)**. In the EMC, the valid input range is from 1 second through 43200 seconds (12 hours).
4. Click **Apply** to save your changes and remain in the **Properties** page, or click **OK** to save your changes and exit the **Properties** page.

Use the Shell to configure the transient failure retry interval

To configure the transient failure retry interval, use the following syntax.

```
Set-TransportServer <Identity> -TransientFailureRetryInterval <Age>
```

This example changes the transient failure retry interval to 1 minute on the Exchange 2010 Hub Transport server Exchange01.

```
Set-TransportServer Exchange01 - TransientFailureRetryInterval 00:01:00
```

To specify an age value, enter the value as a time span, as follows: *hh:mm:ss*, where *h* = hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is from 00:00:01 through 12:00:00.

For detailed syntax and configuration information, see Set-TransportServer.

Configure the outbound connection failure retry interval

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

The outbound connection failure retry interval specifies the retry interval for outgoing

connection attempts that have previously failed. The previously failed connection attempts are controlled by the transient failure retry attempts and the transient failure retry interval. The default value for the outbound connection failure retry interval on a Hub Transport server is 10 minutes. The default value on an Edge Transport server is 30 minutes.

Use the EMC to configure the outbound connection failure retry interval

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, in the console tree, select **Edge Transport**, and then click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and then select **Hub Transport**. In the result pane, select a server. In the action pane, click the **Properties** link that's directly under the server name.
2. Click the **Limits** tab.
3. Enter a value in minutes next to **Outbound connection failure retry interval (minutes)**. In the EMC, the valid input range is from 1 minute through 28800 minutes (20 days).
4. Click **Apply** to save your changes and remain in the **Properties** page, or click **OK** to save your changes and exit the **Properties** page.

Use the Shell to configure the outbound connection failure retry interval

This example changes the outbound connection failure retry interval to 45 minutes on the Exchange 2010 Edge Transport server Exchange01.

```
Set-TransportServer Exchange01 - OutboundConnectionFailureRetryInterval 00:45:00
```

To specify an age value, enter the value as a time span, as follows: *dd.hh:mm:ss*, where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is from 00:00:01 through 20.00:00:00.

For detailed syntax and configuration information, see Set-TransportServer.

Configure the mailbox delivery queue retry interval

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

The mailbox delivery queue retry interval specifies how frequently the mailbox delivery queues on a Hub Transport server try to connect to a Mailbox server destination that can't be successfully reached. By default, the mailbox delivery queue retry interval is 5 minutes. The mailbox delivery queue retry interval is controlled by the *MailboxDeliveryQueueRetryInterval* parameter in the EdgeTransport.exe.config application configuration file located in the C:\Program Files\Microsoft\Exchange Server\V14\Bin directory. Changes that are saved to the EdgeTransport.exe.config file take effect after the Microsoft Exchange Transport service is restarted.

1. Open the following file by using Notepad: C:\Program Files\Microsoft\Exchange Server\V14\Bin\EdgeTransport.exe.config.
2. Modify the following line in the <appSettings> section:

   ```
   <add key="MailboxDeliveryQueueRetryInterval" value="<hh:mm:ss>" />
   ```

   This example sets the mailbox delivery queue retry interval to 3 minutes.

```
<add key="MailboxDeliveryQueueRetryInterval" value="00:03:00" />
```

3. Save and close the EdgeTransport.exe.config file.
4. Restart the Microsoft Exchange Transport service.

To specify an age value, enter the value as a time span: *dd.hh:mm:ss*, where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is from 00:00:01 through 1.00:00:00.

Configure the message retry interval

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

The message retry interval specifies how frequently a Hub Transport server or an Edge Transport server resends a message that has a status of Retry. By default, the message retry interval is 1 minute. We recommend that you don't modify the default value unless Microsoft Customer Service and Support advises you to do this.

This example changes the message retry interval to 2 minutes on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -MessageRetryInterval 00:02:00
```

To specify an age value, enter the value as a time span: *dd.hh:mm:ss*, where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is from 00:00:01 through 1.00:00:00.

For detailed syntax and configuration information, see Set-TransportServer.

Configure the delay DSN message notification time-out interval

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

By default, the delay DSN message notification time-out interval is 4 hours. If the message isn't successfully delivered before the notification time-out interval has passed, a delay DSN message is delivered to the sender.

The value of the *DelayNotificationTimeout* parameter should always be greater than the value of the *TransientFailureRetryCount* parameter multiplied by the value of the *TransientFailureRetryInterval* parameter.

Use the EMC to configure the delay DSN message notification time-out interval

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, in the console tree, select **Edge Transport**, and then click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and then select **Hub**

Transport. In the result pane, select a server. In the action pane, click the **Properties** link that's directly under the server name.
2. Click the **Limits** tab.
3. Enter a value in hours next to **Notify sender when message is delayed more than (hours)**. In the EMC, the valid input range is from 1 hour through 720 hours (30 days).
4. Click **Apply** to save your changes and remain in the **Properties** page, or click **OK** to save your changes and exit the **Properties** page.

Use the Shell to configure the delay DSN message notification time-out interval

This example changes the delay DSN message notification time-out interval to 6 hours on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -DelayNotificationTimeout 06:00:00
```

To specify an age value, enter the value as a time span, as follows: *dd.hh:mm:ss*, where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is from 00:00:01 through 30.00:00:00.

For detailed syntax and configuration information, see Set-TransportServer.

Enable or disable the sending of delay DSN notifications to external message senders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

By default, delay DSN notification messages can be sent to message senders who are outside the Exchange organization.

This example prevents the sending of delay DSN notification messages to external senders on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -ExternalDelayDSNEnabled $false
```

For detailed syntax and configuration information, see Set-TransportServer.

Enable or disable the sending of delay DSN notifications to internal message senders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

By default, delay DSN notification messages can be sent to message senders who are inside the Exchange organization.

This example prevents the sending of delay DSN notification messages to internal senders on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -InternalDelayDSNEnabled $false
```

For detailed syntax and configuration information, see Set-TransportServer.

Configure the message resubmit interval

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

Undelivered messages are automatically resubmitted if the mailbox delivery queue or remote delivery queue is in the status of Retry for a specified amount of time, and the messages aren't in the Suspended state. That amount of time is controlled by the *MaxIdleTimeBeforeResubmit* parameter in the EdgeTransport.exe.config application configuration file. By default, the value of the *MaxIdleTimeBeforeResubmit* parameter is 12 hours.

1. Open the following file by using Notepad: C:\Program Files\Microsoft \Exchange Server\V14\Bin\EdgeTransport.exe.config.
2. Modify the following line in the <appSettings> section:

   ```
   <add key="MaxIdleTimeBeforeResubmit" value="<hh:mm:ss>" />
   ```

   This example changes the message resubmit interval to 6 hours.

   ```
   <add key="MaxIdleTimeBeforeResubmit" value="6:00:00" />
   ```

3. Save and close the EdgeTransport.exe.config file.
4. Restart the Microsoft Exchange Transport service.

Configure the message expiration time-out interval

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" and "Edge Transport server" entries in the Transport Permissions topic.

The message expiration time-out interval specifies the maximum length of time that an Edge Transport server or a Hub Transport server tries to deliver a failed message. If the message can't be successfully delivered before the message expiration time-out interval has passed, a non-delivery report (NDR) that contains the original message or the message headers is delivered to the sender, and the original message is removed from the queue.

By default, the message expiration time-out interval is 2 days.

Use the EMC to configure the message expiration time-out interval

1. Perform one of the following steps:
   - On a computer that has the Edge Transport server role installed, in the console tree, select **Edge Transport**, and then click the **Properties** link that's directly under the server name.
   - On a computer that has the Hub Transport server role installed, in the console tree, expand **Server Configuration**, and then select **Hub**

Transport. In the result pane, select a server. In the action pane, click the **Properties** link that's directly under the server name.
2. Click the **Limits** tab.
3. Enter a value in days next to **Maximum time since submission (days)**. In the EMC, the valid input range is from 1 day through 90 days.
4. Click **Apply** to save your changes and remain in the **Properties** page, or click **OK** to save your changes and exit the **Properties** page.

Use the Shell to configure the message expiration time-out interval

To configure the message expiration time-out interval, use the following syntax.

```
Set-TransportServer <Identity> -MessageExpirationTimeout <Age>
```

This example changes the message expiration time-out interval to 4 days on the Exchange 2010 computer Exchange01.

```
Set-TransportServer Exchange01 -MessageExpirationTimeout 4.00:00:00
```

To specify an age value, enter the value as a time span: *dd.hh:mm:ss*, where *d* = days, *h* = hours, *m* = minutes, and *s* = seconds. The valid input range for this parameter is from 00:00:05 through 90.00:00:00.

For detailed syntax and configuration information, see Set-TransportServer.

1.7.2.18.10 Filter Messages in Queues

Filter Messages in Queues

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Queue Viewer or the Exchange Management Shell to filter messages in the queues on a computer that has the Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed. The list of messages can be lengthy, depending on current mail flow. The list of messages changes when messages enter and leave the server.

When you filter messages by message properties, you can adjust your search to specific criteria and locate messages that may be causing a mail flow problem or are suspected spam. You can then perform operations that modify the status of those messages.

To learn more about filtering messages, see "Message Filtering Scenarios" in Understanding Transport Queues.

Looking for other management tasks related to queues? Check out Managing Transport Queues.

Use Queue Viewer to filter messages in queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. Open the EMC.

2. In the console tree, click **Toolbox**.
3. In the result pane, click **Exchange Queue Viewer**.
4. In the action pane, click **Open Tool**.
5. In Queue Viewer, click the **Messages** tab. A list of all messages in all queues on the server to which you are connected is displayed. To limit the view to a single queue, click the **Queues** tab, double-click the queue name, and then click the *Server\Queue* tab that appears.
6. Click **Create Filter**, and enter your filter expression as follows:
   6.a. Select a message property from the message property drop-down list.
   6.b. Select a comparison operator from the comparison operator drop-down list.
   6.c. Enter the value from the value drop-down list. If the property has fixed values, select a value from the drop-down list. If the property requires a date/time expression, change the current date/time values or click the drop-down list to select a date from the calendar interface.
7. (Optional) Click **Add Expression** to specify additional filter criteria. Only messages that meet all filter criteria will be displayed.
8. Click **Apply Filter**. The results of messages that meet the filter criteria are displayed.

Use the Shell to filter messages in queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

To filter messages in queues, use the following syntax.

```
Get-Message -Filter {property -operator "value"}
```

This example uses the **Get-Message** cmdlet to view all messages that have a spam confidence level (SCL) value equal to or greater than 6 and that were sent from any sender in the Contoso.com domain.

```
Get-Message -Filter {SCL -ge 6 -and FromAddress -eq "*Contoso.com"}
```

For detailed syntax and parameter information, see Get-Message.

1.7.2.18.11 View Queued Message Properties

View Queued Message Properties

Transport > Managing Transport Servers > Managing Transport Queues >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-07-21*

This topic explains how to use either the Exchange Queue Viewer in the EMC or the Shell to view the properties of a message that is queued for delivery.

What Do You Want to Do?

- Use Queue Viewer in the EMC to view the properties of a message
- Use the Shell to view the properties of a message

Use Queue Viewer in the EMC to view the

properties of a message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. In the console tree, select **Toolbox** to display a list of available tools in Exchange Server 2010.
2. Under Performance **tools**, double-click **Queue Viewer** to open the tool in a new window.
3. Select the **Messages** tab to see the list of messages that are currently queued for delivery in your organization.
4. Right-click the message whose properties you want to view and then select **Properties**.

5. The **General** tab displays the following detailed information about the message:
   - **Identity** This field shows the integer that represents a particular message. The message identity is assigned by the queuing database when the message is received for processing. You can include an optional server and queue identity to identify a unique instance of the message.
   - **Subject** This field shows the subject of a message and is expressed as a text string. The value is taken from the `Subject:` header field.
   - **Internet Message ID** This field shows the value of the `MessageID:` header field. The value of this property is expressed as a GUID followed by the SMTP address of the sending server, as in this example: 67D754D6103DC4FB3BA6BC7205DACABA61231@exchange.contoso.com
   - **From Address** This field shows the SMTP address of the sender of the message. This value is taken from MAIL FROM: in the message envelope.
   - **Status** This field shows the current message status. A message can have one of the following status values:
     ? **Active** If the message is in a delivery queue, the message is being delivered to its destination. If the message is in the Submission queue, the message is being processed by the categorizer.
     ? **Pending Remove** The message was deleted by the administrator but was already in delivery. The message will be deleted if the delivery ends in an error that causes the message to re-enter the queue. Otherwise, delivery will continue.
     ? **Pending Suspend** The message was suspended by the administrator but was already in delivery. The message will be suspended if the delivery ends in an error that causes the message to re-enter the queue. Otherwise, delivery will continue.
     ? **Ready** The message is waiting in the queue and is ready to be processed.
     ? **Retry** The last connection attempt failed for the queue in which this message is located. The message is waiting for the next queue retry.
     ? **Suspended** The message was suspended by the administrator.
   - **Size (KB)** This field shows the size of the message rounded up to the nearest kilobyte (KB).
   - **Message Source Name** This field shows the name of the component that submitted this message to the queue.
   - **Source IP** This field shows the IP address of the external server that submitted the message to the Exchange organization.
   - **SCL** This field shows the spam confidence Level (SCL) rating of the message. Valid SCL entries are integers 0 through 9. An empty SCL entry indicates that the message hasn't been processed by the Content Filter

agent.

- **Date Received** This field shows the date-time when the message was received by the server that holds the queue in which the message is located.
- **Expiration Time** This field shows the date-time when the message will expire and will be deleted from the queue if the message can't be delivered.
- **Last Error** This field shows the last error that was recorded for a message.
- **Queue ID** This field shows the identity of the queue that holds the message. The queue identity is expressed in the form *Server\destination*, where destination is a remote domain, mailbox server, persistent queue name, or the queue database identifier. The queue database identifier is represented as an integer and can be determined by viewing the message properties.
- **Recipients** This field shows the list of recipients to which the message is addressed.
- **Retry Count** This field shows the number of times that delivery of a message to a destination was tried.

6. The **Recipient Information** tab displays the following information about the message recipients:
   - **Address** This field shows the SMTP address of the recipient of the message. This value is taken from RCPT TO: in the message envelope.
   - **Status** This field shows the current message status. A message can have one of the following status values:
     ? **Active** If the message is in a delivery queue, the message is being delivered to its destination. If the message is in the Submission queue, the message is being processed by the categorizer.
     ? **Pending Remove** The message has been deleted by the administrator but was already in delivery. The message will be deleted if the delivery ends in an error that causes the message to re-enter the queue. Otherwise, delivery will continue.
     ? **Pending Suspend** The message has been suspended by the administrator but was already in delivery. The message will be suspended if the delivery ends in an error that causes the message to re-enter the queue. Otherwise, delivery will continue.
     ? **Ready** The message is waiting in the queue and is ready to be processed.
     ? **Retry** The last connection attempt failed for the queue in which this message is located. The message is waiting for the next queue retry.
     ? **Suspended** The message has been suspended by the administrator.
   - **Last Error** This field shows the last error that was recorded for a message.

Use the Shell to view the properties of a message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

You can use the **Get-Message** cmdlet to view the properties of a message that is currently queued for delivery. The following example tabulates the sender address, recipients, subject, and received date information for all messages that are currently in

retry state:

```
Get-Message -IncludeRecipientInfo -Filter {Status -eq "Retry"} | FT FromAddress,R
```

For detailed syntax and parameter information, see Get-Message.

1.7.2.18.12 Resume Messages

Resume Messages

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can resume a message that's in a queue on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed.

You can resume a message that currently has a status of Suspended. By resuming a message, you enable delivery of the message. If you resume a message located in the poison message queue, the message will be sent to the categorizer for processing. A message being sent to multiple recipients might be located in multiple queues. To resume a message in more than one queue in a single operation, you must use a filter.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the EMC to resume a message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Open Tool**.
4. In Queue Viewer, click the **Messages** tab. A list of all messages on the server to which you're connected is displayed. To adjust the action to focus on a single queue, click the **Queues** tab, double-click the queue name, and then click the *Server\Queue* tab that appears.
5. Click **Create Filter**, and enter your filter expression as follows:
   5.a.Select **Status** from the message property drop-down list.
   5.b.Select **Equals** from the comparison operator drop-down list.
   5.c.Select **Suspended** from the value drop-down list.
6. Click **Apply Filter**. All messages that have a status of Suspended are displayed.
7. Select one or more messages from the list, right-click, and select **Resume**.

Use the Shell to resume a message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

This example resumes all messages being sent from any sender in the Contoso.com domain.

```
Resume-Message -Filter {FromAddress -eq "*contoso.com"}
```

This example resumes the message with the message ID 3 in the unreachable queue on server Hub01.

```
Resume-Message -Identity Hub01\Unreachable\3
```

For detailed syntax and parameter information, see Resume-Message.

1.7.2.18.13 Suspend Messages

Suspend Messages

Transport > Managing Transport Servers > Managing Transport Queues >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can suspend one or more messages in the queues on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed.

By suspending a message, you prevent delivery of the message. A message that appears in the queue but is already in delivery won't be suspended. Delivery will continue, and the message status will be PendingSuspend. If the delivery fails, the message will re-enter the queue, and the message will then be suspended. You can't suspend a message in the Submission queue or in the poison message queue.

A message being sent to multiple recipients might be located in multiple queues. To suspend a message in more than one queue in a single operation, you must use a filter.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the EMC to suspend messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Open Tool**.
4. In Queue Viewer, click the **Messages** tab. A list of all messages on the server to which you're connected is displayed. To limit the view to a single queue, click the **Queues** tab, double-click the queue name, and then click the *Server\Queue* tab that appears.
5. Select one or more messages, right-click, and then select **Suspend**.

Use the Shell to suspend messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

This example suspends all messages in the queues that are from any sender in the domain Contoso.com.

```
Suspend-Message -Filter {FromAddress -eq "*contoso.com"}
```

This example suspends the message with the message ID 3 in the unreachable queue on

server Hub01:

```
Suspend-Message -Identity Hub01\Unreachable\3
```

For detailed syntax and parameter information, see Suspend-Message.

1.7.2.18.14 Remove Messages from Queues

Remove Messages from Queues

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove one or more messages that are in a queue on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed. A message that's being sent to multiple recipients might be located in more than one queue. To remove a message from more than one queue in a single operation, you must use a filter.

You can select whether to send a non-delivery report (NDR) when you remove messages from a queue. You can't remove a message from the Submission queue.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the EMC to remove messages from queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Open Tool**.
4. In Queue Viewer, click the **Messages** tab. A list of all messages on the server to which you're connected is displayed. To adjust the action to a single queue, click the **Queues** tab, double-click the queue name, and then click the *Server\Queue* tab that appears.
5. Select one or more messages from the list, right-click, and then select **Remove Messages (with NDR)** or **Remove Messages (without NDR)**. A dialog box appears that confirms the selected action and displays, **Do you want to continue?** Click **Yes**.
6. To remove all messages from a particular queue, click the **Queues** tab. Select a queue, right-click, and then select **Remove Messages (with NDR)** or **Remove Messages (without NDR)**. A dialog box appears that confirms the selected action and displays, **Do you want to continue?** Click **Yes**.

Note:

If you're working with a filtered list, the displayed page may not include all items in the filter. In this case, a prompt appears that displays: **This action will affect all items on this page. To expand the scope of this action to include all items in this filter, check the following box before you click OK.**

Use the Shell to remove messages from queues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

To remove messages from queues, use the following syntax.

```
Remove-Message -Filter {property -operator "value"} -WithNDR <$true | $false>
```

This example removes messages in the queues that have a subject of "Win Big." This example doesn't send an NDR.

```
Remove-Message -Filter {Subject -eq "Win Big"} -WithNDR $false
```

For detailed syntax and parameter information, see Remove-Message.

1.7.2.18.15 Export Messages from Queues

Export Messages from Queues

Transport > Managing Transport Servers > Managing Transport Queues >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-30*

You can use the Shell to export messages from a queue on a computer that has the Microsoft Exchange Server 2010 Hub Transport server role or the Edge Transport server role installed to a specified file path. You can't use Queue Viewer to perform this task. However, you can use Queue Viewer to locate, identify, and suspend the messages before you perform this task.

When you export a message from a queue to a file, the message isn't removed from the queue. A copy of the message is made in the specified location as a plain text file. The resulting file can be viewed in an application, such as a text editor or an e-mail client application, or the message file can be resubmitted by using the Replay directory on any other Hub Transport server or Edge Transport server inside or outside the Exchange organization.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Prerequisites

Before you export a message from a queue, you must follow these steps:

1. Verify the following information about the target directory location:
   - The target directory must exist before you export any messages. The directory won't be created for you. If an absolute path isn't specified, the current Shell working directory is used.
   - The path may be local to the Exchange 2010 computer, or it may be a Universal Naming Convention (UNC) path to a share on a remote server.
   - Your account must have the Write permission to the target directory.
2. Locate and identify the messages to be exported. For information about how to view messages, see View Queued Message Properties.
3. Suspend the messages to be exported to prevent their delivery during the

export process. The messages must be in a suspended state for the export process to be successful. You can export messages from remote delivery queues, mailbox delivery queues, the Unreachable queue, or the poison message queue. Messages in the poison message queue are already in a suspended state. You can't suspend or export messages that are in the Submission queue. For information about how to suspend messages, see Suspend Messages.

4. When you specify a file name, make sure that you include the .eml file name extension so that the file can be opened easily by e-mail client applications or processed correctly by the Replay directory.

Use the Shell to export a specific message from a specific queue

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

This example exports a copy of a message that has an **InternalMessageID** of 1234 that's located in the remote delivery queue for the domain Contoso.com on the server Exchange01 to the path C:\Contoso Export\export.eml.

```
Export-Message -Identity ExchSrv1\contoso.com\1234 | AssembleMessage -Path "c:\ex
```

For detailed syntax and parameter information, see Export-Message.

Use the Shell to export all messages from a specific queue

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

This example exports a copy of all the messages from the Contoso.com remote delivery queue on the server Exchange01 to the directory C:\Contoso Export on the local computer using the Internet Message IDs of each message as the file name. To accomplish this, the command does the following:

- Retrieves all messages in a specific queue using the **Get-Message** cmdlet.
- Pipelines the result into the **ForEach-Object** cmdlet, which executes the following actions for each message:
  - Prepares a file name including full path using the temporary variable `$Temp` that consists of the Internet Message ID with .eml extension. The Internet Message ID field contains angled brackets (> and <), which need to be removed because they're invalid file names. This is done using the **Replace** method of the temporary variable.
  - Exports the message using the file name prepared.

```
Get-Message -Queue "Exchange01\Contoso.com" | ForEach-Object {$Temp="C:\Contoso E
```

For detailed syntax and parameter information, see the Get-Message and Export-Message topics.

Use the Shell to export specific messages from all the queues on a server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

This example exports a copy of all the messages from senders in the Contoso.com domain from all queues on the server Exchange01 to the directory C:\Contoso Export on the local computer using the Internet Message IDs of each message as the file name. To accomplish this, the command does the following:

- Retrieves all messages that match the criteria using the **Get-Message** cmdlet with a filter.
- Pipelines the result into the **ForEach-Object** cmdlet, which executes the following actions for each message:
  - Prepares a file name including full path using the temporary variable `$Temp` that consists of the Internet Message ID with .eml extension. The Internet Message ID field contains angled brackets (> and <), which need to be removed because they're invalid file names. This is done using the **Replace** method of the temporary variable.
  - Exports the message using the file name prepared.

```
Get-Message -Filter {FromAddress -like "@Contoso.com"} -Server "Exchange01" | For
```

For detailed syntax and parameter information, see the Get-Message and Export-Message topics.

1.7.2.18.16 Resubmit Messages in Queues

Resubmit Messages in Queues

Transport > Managing Transport Servers > Managing Transport Queues >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can manually resubmit messages to the Submission queue for the categorizer to reprocess. You can manually resubmit messages that have the following status on a computer running Microsoft Exchange Server 2010 and that has the Hub Transport server role or the Edge Transport server role installed:

- Mailbox delivery queues or remote delivery queues that have the status of Retry. The messages in the queues must not be in the Suspended state.
- Messages in the Unreachable queue that aren't in the Suspended state.
- Messages in the poison message queue.

You can use the following methods to manually resubmit messages:

- Use the **Retry-Queue** cmdlet with the *Resubmit* parameter.
- Export the messages to .eml message files and resubmit them by using the Replay directory. For more information about this resubmission method, see Export Messages from Queues.
- Use Queue Viewer or the **Resume-Message** cmdlet to resubmit the messages in the poison message queue. The poison message queue can't be

resubmitted by using the **Retry-Queue** cmdlet with the *Resubmit* parameter. For more information, see Resume Messages.

By using the **Retry-Queue** cmdlet with the *Resubmit* parameter, you can force messages to be resubmitted back through the categorization process for a new attempt at delivery.

Using the **Retry-Queue** cmdlet without the *Resubmit* parameter forces the delivery queue to try to connect to the next hop immediately. The messages aren't resubmitted back through the categorization process. For information about how to retry the connection of a delivery queue, see Retry Queues.

Looking for other management tasks related to managing transport queues? Check out Managing Transport Queues.

Use the Shell to resubmit all messages located in a specific mailbox delivery queue or remote delivery queue

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

To resubmit all messages located in a specific mailbox delivery queue or remote delivery queue, use the following syntax.

```
Retry-Queue -Identity "<ServerName>\<Destination>" -Resubmit $true
```

This example resubmits all messages located in the remote delivery queue Contoso.com on the server Exchange01.

```
Retry-Queue -Identity "Exchange01\Contoso.com" -Resubmit $true
```

For detailed syntax and parameter information, see Retry-Queue.

Use the Shell to resubmit all messages located in all mailbox delivery queues or remote delivery queues that have the status of Retry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

To resubmit all messages located in all mailbox delivery queues or remote delivery queues that have the status of Retry, use the following syntax.

```
Retry-Queue -Filter {Status -eq "Retry"} -Server "<ServerName>" -Resubmit $true
```

This example resubmits all messages located in any remote delivery queues with the status of Retry on the server Exchange01.

```
Retry-Queue -Filter {Status -eq "Retry"} -Server "Exchange01" -Resubmit $true
```

For detailed syntax and parameter information, see Retry-Queue.

Use the Shell to resubmit all messages located in the Unreachable queue

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Note:

You can't use the EMC to perform this task.

To resubmit all messages located in the Unreachable queue, use the following syntax.

```
Retry-Queue -Identity "<ServerName>\Unreachable" -Resubmit $true
```

This example resubmits all messages located in the Unreachable queue on the server Exchange01.

```
Retry-Queue -Identity "Exchange01\Unreachable" -Resubmit $true
```

For detailed syntax and parameter information, see Retry-Queue.

Resubmit messages located in the poison message queue

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Queues" entry in the Transport Permissions topic.

Messages that are located in the poison message queue must be resubmitted by resuming the message. The poison message queue can't be resubmitted by using the **Retry-Queue** cmdlet with the *Resubmit* parameter. To resume a message from the poison message queue, you can use Queue Viewer or the **Resume-Message** cmdlet.

Note:

The poison message queue contains messages that are determined to be harmful to the Exchange 2010 system after a server failure. The messages may be genuinely harmful in their content or format. Alternatively, they may be victims of a poorly written agent that crashed the Exchange server while it was processing the supposedly bad messages. If you're unsure of the safety of the messages in the poison message queue, you should export them to files so that you can examine them. The poison message queue is only visible in Queue Viewer when there are messages in the poison message queue.

Use the EMC to resume messages in the poison message queue

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Queue Viewer**.
3. In the action pane, click **Open Tool**.
4. In Queue Viewer, click the **Queues** tab. A list of all queues on the server to which you're connected is displayed.
5. Click the poison message queue. In the action pane, select **View Messages**.
6. Select one or more messages from the list, right-click, and select **Resume**.

Use the Shell to resume messages in the poison message queue

1. Before you can resume a message from the poison message queue, you must first determine the Identity of the message. This example determines

the Identity of all messages in the poison message queue.

```
Get-Message -Queue "Poison" | Format-Table Identity
```

2. To resume a message from the poison message queue, use the Identity of the message from the previous step and use the following syntax.

```
Resume-Message <IdentityofPoisonMessage>
```

This example resumes a message from the poison message queue that has the message Identity value of 222.

```
Resume-Message 222
```

For detailed syntax and parameter information, see Resume-Message or Get-Message.

1.7.3 Securing Transport Servers

Securing Transport Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-25*

The security of your Transport servers is crucial to maintaining a robust and secure Exchange environment. This topic provides links to security-related topics that can help you understand the security model for Edge and Hub Transport servers in Microsoft Exchange Server 2010.

TLS Protection

All SMTP communications between Transport servers are protected by Transport Layer Security (TLS) encryption. For more information about TLS encryption in Exchange 2010, see the following topics:

- Understanding TLS Certificates
- TLS Functionality and Related Terminology in Exchange 2010
- Certificates

Exchange 2010 allows you to disable TLS encryption in certain scenarios. For example, if you're using WAN Optimization Controller (WOC) devices, the TLS-encrypted traffic may prevent the compression of SMTP communications over your WAN link. In such scenarios, you can disable TLS encryption. However, we recommend that you only disable TLS encryption on specific links and allow all other communications to continue to be protected by TLS. To learn more, see Disabling TLS Between Active Directory Sites to Support WAN Optimization.

Domain Security

Exchange 2010 provides a feature set called Domain Security that provides administrators a way to manage secure message paths with business partners over the Internet. The following topics provide information about Domain Security:

- Understanding Domain Security
- Using PKI on the Edge Transport Server for Domain Security
- Using Domain Security: Configuring Mutual TLS
- Test PKI and Proxy Configuration

Transport Permissions

Exchange 2010 uses Role Based Access Control (RBAC) for assigning permissions to users. With RBAC, you can control what resources administrators can configure and what features users can access. To learn more about RBAC, see Understanding Permissions.

For specific information about permissions required for managing Transport servers, see Transport Permissions.

1.7.4 Troubleshooting Reference for Transport Servers

Troubleshooting Reference for Transport Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-02*

After the Transport server role is installed on a computer that is running Microsoft Exchange Server 2010, you may want to test the functionality of the server or solve problems related to message flow. The following topics can help you make sure that your Transport server is configured correctly.

Can't Remove an Arbitration Mailbox that Is Associated with an Existing Approval Workflow

Troubleshooting Certificate Validation Errors

Use Telnet to Test SMTP Communication

1.7.4.1 Can't Remove an Arbitration Mailbox that Is Associated with an Existing Approval Workflow

Can't Remove an Arbitration Mailbox that Is Associated with an Existing Approval Workflow

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2008-10-13*

You may receive the following error when you attempt to remove an arbitration mailbox:

> Can't remove the arbitration mailbox "{0}", because it is being used for the approval workflow for existing recipients that either membership restrictions or moderation enabled. Please either disable the approval features on those recipients or specify a different arbitration mailbox for those recipients before removing this arbitration mailbox.

An arbitration mailbox can be used to handle the approval workflow for moderated recipients and distribution group membership approvals. If you receive this error, you need to do the following:

1. Determine which recipients use this arbitration mailbox for handling approval workflow using the **Get-Recipient** cmdlet.

For example, if you want to find all recipients that use the arbitration mailbox AMBX1 for approval features, you can run the following command:

```
Get-Recipient -RecipientPreviewFilter {ArbitrationMailbox -eq "CN=AMBX
```

If you don't want to type in the entire distinguished name, you can use variables instead. The following three commands accomplish the same goal as the one above without having to type the distinguished name for the arbitration mailbox. The first command stores the arbitration mailbox in the variable *$ArbitrationMailbox*, and the second command stores the distinguished name in the *$ArbitrationMailboxDN* variable. Finally, the third command returns all recipients that use AMBX1 as the arbitration mailbox.

```
$ArbitrationMailbox = Get-Mailbox -Identity "AMBX1" -Arbitration
$ArbitrationMailboxDN = $ArbitrationMailbox.DistinguishedName
Get-Recipient -RecipientPreviewFilter {ArbitrationMailbox -eq $Arbitra
```

2. Either specify a different arbitration mailbox using the *ArbitrationMailbox* parameter or disable that feature.
   For example, assume that the distribution group All Employees uses the arbitration mailbox AMBX1 for moderation. You can run the following command to specify a different arbitration mailbox:

```
Set-DistributionGroup -Identity "All Employees" -ArbitrationMailbox "A
```

Alternatively, you can run the following command to disable moderation:

```
Set-DistributionGroup -Identity "All Employees" -ModerationEnabled $fa
```

After you reconfigure all recipients that use the arbitration mailbox for approval features, you will be able to delete the arbitration mailbox.

For More Information

Understanding Moderated Transport

Configure a Moderated Recipient

1.7.4.2 Troubleshooting Certificate Validation Errors

Troubleshooting Certificate Validation Errors

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to resolve certificate validation errors or refers to documentation that may help you resolve the errors.

For more information about how the Microsoft Exchange Transport service selects certificates for Transport Layer Security (TLS), see the following topics:

- Selection of Inbound Anonymous TLS Certificates
- Selection of Inbound STARTTLS Certificates
- Selection of Outbound Anonymous TLS Certificates

Certificate Validation Errors or Status Messages

The certificate is valid but it is selfsigned.

This error is an informational status message. By default, the certificate that installed with Exchange Server 2010 is self-signed. It's generally a best practice to use certificates from trusted third-party certification authorities (CA).

For more information, see Using PKI on the Edge Transport Server for Domain Security.

Certificate subject does not match the passed value.

This status message indicates that the domain name in either the subject name or subject alternative name fields of the certificate does not match the fully qualified domain name (FQDN) of the sender or receiver domain name. To correct this error, a new certificate that matches the FQDN of the Send connector or Receive connector that tried to validate this certificate must be created.

For more information, see Understanding TLS Certificates.

The signature of the certificate cannot be verified.

This status message indicates that the Microsoft Exchange Transport service was unable to validate the certificate chain, or that the public key that was used to validate the certificate signature is not the correct key.

A certificate chain processed, but ended in a root certificate which is not trusted by the trust provider.

This status message indicates that the certificate that was used for this operation is not trusted by the computer certificate store. To trust this certificate, the root certification authority for the given certificate must be present in the certificate store for this computer.

For more information about how to manually add certificates to the local certificate store, see the Help file for the Certificate Manager snap-in in the Microsoft Management Console (MMC).

The certificate is not valid for the requested usage.

This status message indicates that you must enable the certificate for use in the current application. For example, if you're trying to use this certificate for Domain Security, the certificate must be enabled for SMTP.

For more information about how to enable certificates, see Enable-ExchangeCertificate.

Alternatively, this status message may indicate that the certificate that you're using doesn't have the correct data in the Enhanced Key Usage field. All certificates that are used for TLS must contain a Server Authentication object identifier (also known as OID). If you're trying to use a certificate for TLS that doesn't contain a Server Authentication OID in the Enhanced Key Usage Field, you must create a new certificate.

For more information, see Understanding TLS Certificates.

A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file.

This status message indicates that the system time is incorrect, the certificate has expired, or the time of the system that signed the file is incorrect. Verify that the following conditions are true:

- The local computer clock is accurate.
- The certificate has not expired.
- The sending system clock is accurate.

If the certificate has expired, you must generate a new certificate.

For more information, see Understanding TLS Certificates.

The validity periods of the certification chain do not nest correctly.

This status message indicates that the certificate chain is corrupted or otherwise unreliable. Generate a new certificate by using New-ExchangeCertificate cmdlet, or contact your certification authority to validate the certificate chain that was used for this certificate.

A certificate that can only be used as an end entity is being used as a CA or visa versa.

This status message indicates that the certificate is invalid because it was issued by an end-entity certificate and not a certification authority. An end-entity certificate is a certificate that has been created for specific application cryptographic usage. Generate a new certificate by using the New-ExchangeCertificate cmdlet, or contact your certification authority to validate the certificate.

The certificate or signature has been revoked.

Contact your certification authority to resolve this issue.

A certificate was explicitly revoked by its issuer.

Contact your certification authority to resolve this issue.

The revocation function was unable to check revocation because the revocation server was offline.

This status message indicates that the revocation server for the certificate could not be reached. In some cases, this is a temporary error because the revocation server is malfunctioning. Otherwise, make sure that this computer can access the revocation server. If there is a firewall or proxy server in between this computer and the revocation server, make sure that your computer is configured to traverse the obstacle.

For more information, see Using PKI on the Edge Transport Server for Domain Security.

The revocation process could not continue. The certificates could not be checked.

This status message indicates that the revocation process was interrupted by a general network failure. If there is a firewall or proxy server in between this computer and the revocation server, make sure that your computer is configured to traverse the obstacle.

For more information, see Using PKI on the Edge Transport Server for Domain Security.

1.7.4.3 Use Telnet to Test SMTP Communication

Use Telnet to Test SMTP Communication

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use Telnet to test Simple Mail Transfer Protocol (SMTP) communication between messaging servers. By default, SMTP listens on port 25. If you use Telnet on port 25, you can enter the SMTP commands that are used to connect to an SMTP server and send a message exactly as if your Telnet session was an SMTP messaging server. You can see the success or failure of each step in the connection and

message submission process.

Here are the scenarios where you may want to use Telnet to test SMTP communication to or from the transport servers that exist in your Microsoft Exchange Server organization:

- Connect to your organization's Edge Transport server from a host that is located outside your perimeter network and send a test message.
- Connect to a remote messaging server from your organization's Edge Transport server and send a test message.

The procedure in this topic shows you how to use Telnet Client, which is a component that is included with Microsoft Windows. Third-party Telnet clients may require a syntax that is different from that of the Windows Telnet component.

Prerequisites

- **Configure a Receive connector to allow anonymous access or Basic authentication** Because the message transfers that normally occur between Hub Transport servers are encrypted and authenticated, the internal Hub Transport server should have a Receive connector that is configured to allow anonymous access or Basic authentication to receive messages when using Telnet on port 25 to test communication. Anonymous access is required for Internet-facing servers

  Note:
  When you send a message to a Receive connector that accepts Basic authentication, you must have a utility to convert the text strings that are used for the username and password into the Base64 format. Because the user name and password are easily discernable when Basic authentication is used, we don't recommend Basic authentication without encryption.

- **Connect to a remote messaging server** You may also want to connect to a remote messaging server from your organization's Edge Transport server. This will help to avoid rejection of the test message by Internet-facing SMTP servers that are configured to validate the source IP address, the corresponding domain name system (DNS) domain name, and the reverse lookup IP address of any Internet host that tries to send a message to the server.
- **Install and/or enable the Telnet Client** You may need to perform one or more of the following tasks before you use Telnet to test SMTP communication between messaging servers:
  - Install Telnet Client if you haven't already done so. See Install Telnet Client for details about how to install Telnet Client on Windows Vista or Windows Server 2008.
  - Enable Telnet Client on Windows Server 2008. See the procedure later in this topic.
- **Find the FQDN or IP address of an SMTP server**. If you don't know the FQDN or IP address, you can use Nslookup to find the FQDN or IP address of an SMTP server. See the procedure later in this topic.

Enable Telnet Client in Windows Server 2008

Membership in the Windows Server 2008 local Administrators group, or equivalent, is the minimum required to complete this procedure.

In Windows Server 2008, Telnet Client is disabled by default. To enable it, complete the following steps:

1. Open **Server Manager.**
2. Click **Action,** and then select **Add Features.**
3. Select **Telnet Client**, and then click **Next.**
4. Click **Install,** and then click **Close** to complete the installation of Telnet Client.

Use Nslookup to find the FQDN or IP address of an SMTP server

To connect to a destination SMTP server by using Telnet on port 25, you must use the fully qualified domain name (FQDN) or the IP address of the SMTP server. If the FQDN or IP address is unknown, the easiest way to find this information is to use the Nslookup command-line tool to find the MX record for the destination domain.

1. At a command prompt, type **nslookup**, and then press ENTER. This command opens the Nslookup session.
2. Type **set type=mx** and then press ENTER.
3. Type **set timeout=20** and then press ENTER. By default, Windows DNS servers have a 15-second recursive DNS query time-out limit.
4. Type the name of the domain for which you want to find the MX record. For example, to find the MX record for the fabrikam.com domain, type **fabrikam.com.**, and then press ENTER.

   Note:

   The trailing period (**.**) indicates a FQDN. The use of the trailing period prevents any default DNS suffixes that are configured for your network from being unintentionally added to the domain name.

   The output of the command will resemble the following:

   ```
   fabrikam.com mx preference=10, mail exchanger = mail1.fabrikam.com
   fabrikam.com mx preference=20, mail exchanger = mail2.fabrikam.com
   mail1.fabrikam.com internet address = 192.168.1.10
   mail2 fabrikam.com internet address = 192.168.1.20
   ```

   You can use any of the host names or IP addresses that are associated with the MX records as the destination SMTP server. A lower value of preference indicates a preferred SMTP server. You can use multiple MX records and different values of preference for load balancing and fault tolerance.
5. When you're ready to end the Nslookup session, type **exit**, and then press ENTER.

Note:

Firewall or Internet proxy restrictions that are imposed on your organization's internal network may prevent you from using the Nslookup tool to query public DNS servers on the Internet.
MX records are not strictly required for internal message flow inside an Exchange organization. If you have to find the FQDN of any Hub Transport server or subscribed Edge Transport server in your organization, you can use the following command in the Exchange Management Shell: `Get-ExchangeServer | where {$_.isHubTransportServer -eq $true -or $_.isEdgeServer -eq $true} | Format-List Fqdn,ServerRole`
For more information, see Get-ExchangeServer and Pipelining.

Use Telnet on Port 25 to test SMTP communication

For purposes of providing an example, the following procedure uses the values that are described in the following list:

- **Destination SMTP server** mail1.fabrikam.com
- **Source domain** contoso.com
- **Sender's e-mail address** chris@contoso.com
- **Recipient's e-mail address** kate@fabrikam.com
- **Message subject** Test from Contoso
- **Message body** This is a test message

Note:

You should always use a valid sender e-mail address so that any non-delivery report (NDR) messages that are generated by the destination SMTP server

are delivered to the sender of the message.

The commands in Telnet Client are not case-sensitive. The SMTP command verbs are capitalized for clarity.

1. At a command prompt, type **telnet**, and then press ENTER. This command opens the Telnet session.
2. Type **set localecho** and then press ENTER. This optional command lets you view the characters as you type them. This setting may be required for some SMTP servers.
3. Type **set logfile** *<filename>*. This optional command enables logging of the Telnet session to the specified log file. If you only specify a file name, the location of the log file is the current working directory. If you specify a path and a file name, the path must be local to the computer. Both the path and the file name that you specify must be entered in the Microsoft DOS 8.3 format. The path that you specify must already exist. If you specify a log file that doesn't exist, it will be created for you.
4. Type **open mail1.fabrikam.com 25** and then press ENTER.

   Note:
   You can't use the backspace key after you have connected to the destination SMTP server within the Telnet session. If you make a mistake as you type an SMTP command, you must press ENTER and then type the command again. Unrecognized SMTP commands or syntax errors result in an error message that resembles the following:

   ```
   500 5.3.3 Unrecognized command
   ```

5. Type **EHLO contoso.com** and then press ENTER.
6. Type **MAIL FROM:chris@contoso.com** and then press ENTER.
7. Type **RCPT TO:kate@fabrikam.com NOTIFY=success,failure** and then press ENTER. The optional NOTIFY command defines the particular delivery status notification (DSN) messages that the destination SMTP server must provide to the sender. DSN messages are defined in RFC 1891. In this case, you're requesting a DSN message for successful or failed message delivery.
8. Type **DATA** and then press ENTER. You will receive a response that resembles the following:

   ```
   354 Start mail input; end with <CLRF>.<CLRF>
   ```

9. Type **Subject: Test from Contoso** and then press ENTER.
10. Press ENTER. RFC 2822 requires a blank line between the `Subject:` header field and the message body.
11. Type **This is a test message** and then press ENTER.
12. Press ENTER, type a period (**.**) and then press ENTER. You will receive a response that resembles the following:

    ```
    250 2.6.0 <GUID> Queued mail for delivery
    ```

13. To disconnect from the destination SMTP server, type **QUIT** and then press ENTER. You will receive a response that resembles the following:

    ```
    221 2.0.0 Service closing transmission channel
    ```

14. To close the Telnet session, type **quit** and then press ENTER.

Evaluate the Results of a Telnet Session

This section provides information about responses that may be provided to the following commands, which were used in the previous example:

- Open mail1.fabrikam.com 25
- EHLO contoso.com
- MAIL FROM:chris@contoso.com
- RCPT TO:kate@fabrikam.com NOTIFY=success,failure

Note:
The 3-digit SMTP response codes that are defined in RFC 2821 are the same for all SMTP messaging servers. The text descriptions may differ slightly for some SMTP messaging servers. In the previous example, the destination computer is running Exchange Server 2010.

Open mail1.fabrikam.com 25

Successful Response `220 mail1.fabrikam.com Microsoft ESMTP MAIL Service ready at <day-date-time>`

Failure Response `Connecting to mail1.fabrikam.com...Could not open connection to the host, on port 25: Connect failed`

Possible Reasons for Failure

- The destination SMTP service is unavailable.
- There are restrictions on the destination firewall.
- There are restrictions on the source firewall.
- An incorrect FQDN or IP address for the destination SMTP server was specified.
- An incorrect port number was specified.

EHLO contoso.com

Successful Response `250 mail1.fabrikam.com Hello [<sourceIPaddress>]`

Failure Response `501 5.5.4 Invalid domain name`

Possible Reasons for Failure There are invalid characters in the domain name. Alternatively, there are connection restrictions on the destination SMTP server.

Note:
EHLO is the Extended Simple Message Transfer Protocol (ESMTP) verb that is defined in RFC 2821. ESMTP servers can advertise their capabilities during the initial connection. These capabilities include their maximum accepted message size and their supported authentication methods. HELO is the older SMTP verb that is defined in RFC 821. Most SMTP messaging servers support ESMTP and EHLO.

MAIL FROM:chris@contoso.com

Successful Response `250 2.1.0 Sender OK`

Failure Response `550 5.1.7 Invalid address`

Possible Reasons for Failure There is a syntax error in the sender's e-mail address.

Failure Response `530 5.7.1 Client was not authenticated`

Possible Reasons for Failure The destination server does not accept anonymous message submissions. You receive this error if you try to use Telnet to submit a message directly to a Hub Transport server.

RCPT TO:kate@fabrikam.com NOTIFY=success,failure

Successful Response `250 2.1.5 Recipient OK`

Failure Response `550 5.1.1 User unknown`

Possible Reasons for Failure The specified recipient does not exist in the organization.

1.7.5 Performance Counter Reference for Transport Servers

Performance Counter Reference for Transport Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Ensuring that servers running Microsoft Exchange Server 2010 are operating reliably is a key objective for messaging operations. An important part of Exchange 2010 operations is monitoring the Exchange components to understand the health state of servers and server roles. For more information about Transport performance counters, see the following topics:

- Transport Server Counters
- Performance and Scalability Counters and Thresholds

1.7.6 Error and Event Reference for Transport Servers

Error and Event Reference for Transport Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-01*

Microsoft Exchange Server 2010 Transport components, features, and services generate Error events to let you effectively troubleshoot and monitor Hub Transport and Edge Transport servers.

Event Viewer is a Microsoft Management Console (MMC) snap-in that enables you to browse and manage event logs. You can also gather information about hardware and software problems, and monitor Microsoft Windows security events. Although Event Viewer isn't a Microsoft Exchange component, Event Viewer is useful when you troubleshoot problems with Exchange 2010 server roles. For more information, see Event Viewer. For more information about Exchange 2010 event logs, look for "MSExchange" event logs in the Event Viewer on your Exchange 2010 server.

Transport Errors and Events

The following Transport errors and events are grouped according to the Transport feature areas.

- Antispam Errors and Events
- Antispam Update Errors and Events
- EdgeSync Errors and Events
- Extensibility Errors and Events
- Mail Submission Errors and Events
- Messaging Policies Errors and Events
- Message Security Errors and Events
- Store Driver Errors and Events
- Transport Errors and Events
- TransportLogSearch Errors and Events

1.7.6.1 Antispam Errors and Events

Antispam Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Antispam events in Event Viewer so that you can troubleshoot and verify the Antispam features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Antispam Errors and Events

The following table provides a list of the Antispam events.

Event ID	Category	Event type	Value or description
MSExchange Antispam 100	General	Warning	Protocol Analysis Background agent warning. The queue this agent uses is full. This does not affect SRL calculations. Open proxy, reverse DNS, and sender blocking are affected.
MSExchange Antispam 101	General	Error	Protocol Analysis: DNS is not configured. Most likely, no DNS servers found. Sender Reputation calculations are disabled.
MSExchange Antispam 200	General	Warning	Protocol Analysis warning. No DNS entries were found for this server's authoritative domains. Open proxy detection is not available.
MSExchange Antispam 301	General	Error	Unable to initialize the Content Filter agent: %1
MSExchange	General	Warning	Unable to quarantine

Antispam 302			message because the spam quarantine mailbox is invalid. Please configure the quarantine mailbox.
MSExchange Antispam 303	General	Error	Microsoft Exchange was unable to initialize the Content Filter agent. Check the access control lists (ACLs) on the files under '%1' and make sure the Microsoft Exchange Transport service can access them. Details: %2
MSExchange Antispam 304	General	Warning	Microsoft Exchange was unable to initialize the Content Filter agent. Files under %1 may be corrupted. Details: %2
MSExchange Antispam 305	General	Error	Microsoft Exchange was unable to initialize the Content Filter agent. Notification of the file system change could not be initialized. Try restarting the Microsoft Exchange Transport service. Details: %1
MSExchange Antispam 306	General	Error	Microsoft Exchange was unable to initialize the Content Filter agent. It could not allocate sufficient memory for an internal buffer. Increase the available memory and restart the Microsoft Exchange Transport service. Details: %1
MSExchange Antispam 307	General	Error	The Content Filter wrapper process is not responding. Unable to scan the message.
MSExchange Antispam 308	General	Error	Content Filter wrapper process is

			now being restarted.
MSExchange Antispam 310	General	Error	Content Filter wrapper process could not be restarted in a timely manner. Restarting Microsoft Exchange Transport Service may solve the problem.
MSExchange Antispam 311	General	Error	An error occurred while sending the shutdown message to the Content Filter wrapper process. Details: %1
MSExchange Antispam 312	General	Warning	Content Filter wrapper did not timely respond to the last %1 messages.
MSExchange Antispam 313	General	Warning	A message could not be sent to the Content Filter wrapper because of an error. The message is being rejected. Details: %1
MSExchange Antispam 314	General	Warning	Microsoft Exchange couldn't initialize the Content Filter agent because ExSMime.dll couldn't be initialized. Verify that ExSMime.dll is properly registered by using Regsrv32.exe. Details: %1
MSExchange Antispam 315	General	Error	An unexpected failure occurred while trying to scan the message with ID %1. This message has not been assigned a spam confidence level (SCL) value. Details: %2
MSExchange Antispam 316	General	Error	Failed to read the current Microsoft Anti-spam Update service mode. Therefore, any recent change in the mode may not have taken effect. To solve the problem, try

			restarting the Microsoft Exchange Transport service. Details: %1
MSExchange Antispam 318	General	Error	Microsoft Exchange couldn't initialize the Content Filter agent because a required file could not be found on your system. Please run the Reset-AntispamUpdates script from the Exchange Management Shell and restart Microsoft Exchange Transport service to solve the problem. Details: %1
MSExchange Antispam 400	General	Error	Update agent warning. Microsoft Exchange couldn't load the IP reputation data file.
MSExchange Antispam 500	General	Error	A notification of a configuration change has been received for %1 but the new configuration could not be read. Please check network connectivity between this server and the Active Directory directory service. The agent will continue to run with the old configuration.
MSExchange Antispam 600	General	Error	Connection Filter agent: DNS is not configured. IP Allow List and Block List providers will be skipped
MSExchange Antispam 700	General	Error	Sender ID agent: DNS is not configured. Messages will be handled as if DNS requests have failed temporarily.

1.7.6.2 Antispam Update Errors and Events

Antispam Update Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-08-10*

Microsoft Exchange Server 2010 generates Anti-spam Update events in Event Viewer so that you can troubleshoot and verify the Anti-spam Update features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Anti-spam Update Errors and Events

The following table provides a list of the Antispam Update errors and events.

Event ID	Category	Event type	Value or description
MSExchange Anti-spam Update 1009	Update Service	Error	The download of update %1 failed with error %2
MSExchange Anti-spam Update 1012	Update Service	Error	The installation of update %1 failed with error %2
MSExchange Anti-spam Update 1015	Update Service	Error	Microsoft Exchange couldn't determine the version of the Microsoft Update agent, or the Microsoft Update agent is not current. Please see Microsoft Update, and then update your client. Anti-spam updates will not be downloaded until this problem is fixed.
MSExchange Anti-spam Update 1016	Update Service	Error	Microsoft Exchange couldn't complete the opt-in process for Microsoft Update: %1. Please see Microsoft Update, and then update your client manually. Anti-spam updates will not be downloaded until this problem is fixed.
MSExchange Anti-spam Update 1017	Update Service	Error	Microsoft Exchange couldn't successfully use the Microsoft

			Update agent: %1. Please see Microsoft Update, and then update your client manually. Antispam updates will not be downloaded until this problem is fixed.
MSExchange Anti-spam Update 1002	Update Service	Error	Unable to start the Microsoft Exchange Anti-spam Update service: %1
MSExchange Anti-spam Update 1003	Update Service	Error	Unable to stop the Microsoft Exchange Anti-spam Update service: %1
MSExchange Anti-spam Update 1000	Update Service	Information	The Microsoft Exchange Anti-spam Update service has started successfully.

1.7.6.3 EdgeSync Errors and Events

EdgeSync Errors and Events

Exchange Server 2010 > Transport > Error and Event Reference for Transport Servers >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates EdgeSync events in Event Viewer so that you can troubleshoot and verify the EdgeSync features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

EdgeSync Errors and Events

The following table provides a list of the EdgeSync errors and events.

Event ID	Category	Event type	Value or description
MSExchange EdgeSync 1004	Synchronization	Error	EdgeSync failed to confirm the credentials for replication account %1 for subscription server %2. The start date is %3. The password hash is %4. Please make sure Microsoft Exchange Credential service

			(MSExchangeEdgeCredential) is running properly on the subscription server.
MSExchange EdgeSync 10104	Synchronization	Warning	Microsoft Exchange couldn't match certificate when contacting %1. The connection was stopped.
MSExchange EdgeSync 1013	Synchronization	Warning	Synchronization failed because it could not read replication data from the Active Directory server %1, port %2 with exception: %3. Check network connectivity, and test the health of the domain controller.
MSExchange EdgeSync 1024	Topology	Warning	Failed to connect to the Edge Transport server ADAM instance with exception %1. This could be caused by a failure to resolve the Edge Transport server name %2 in DNS, a failure trying to connect to port %3 on %2, network connectivity issues, an invalid certificate, or an expired subscription. Verify your network and server configuration.
MSExchange EdgeSync 1025	Topology	Warning	Topology load generated exception %1. EdgeSync must be able to acquire current Exchange topology data from the Active Directory directory service to properly operate. Check network connectivity and test the health of the domain controller.
MSExchange EdgeSync 1032	Topology	Warning	Microsoft Exchange EdgeSync can't find the replication credential on %1 to synchronize with

			Edge server %2. This may happen if %1 joined the current Active Directory site after subscription for %2 was established. To have this Hub Transport server participate in EdgeSync, re-subscribe %2 to the current Active Directory site.
MSExchange EdgeSync 1033	Topology	Error	EdgeSync failed to decrypt the credential for Edge Transport server %1 using the private key of the default Exchange certificate with exception %2. The certificate's thumbprint is %3 and its subject is %4. Use either Enable-ExchangeCertificate or New-ExchangeCertificate to set the proper Exchange default certificate and re-subscribe the Edge Transport server %1 again.
MSExchange EdgeSync 1034	Synchronization	Error	EdgeSync failed to synchronize the following address %1 to MSERV with permanent error %2. EdgeSync could not retry this item.
MSExchange EdgeSync 1104	Synchronization	Warning	Failed to sync entry "%1" to EHF. Failure details: %2
MSExchange EdgeSync 1045	Initialization	Error	Initialization failed with exception: %1. If this warning frequently occurs, contact Microsoft Product Support.
MSExchange EdgeSync 1059	Initialization	Information	EdgeSync is starting

1.7.6.4 Extensibility Errors and Events

Extensibility Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Extensibility events in Event Viewer so that you can troubleshoot and verify the Extensibility features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Extensibility Errors and Events

The following table provides a list of Extensibility errors and events.

Event ID	Category	Event type	Value or description
MSExchange Extensibility 1050	MExRuntime	Warning	The execution time of agent '%1' exceeded %2 milliseconds while handling event '%3' for message with InternetMessageId: '%4'. This is an unusual amount of time for an agent to process a single event. However, Transport will continue processing this message.
MSExchange Extensibility 1051	MExRuntime	Warning	Agent '%1' caused an unhandled exception '%2: %3' while handling event '%4'
MSExchange Extensibility 1053	MExRuntime	Error	Agent '%1' failed to create an agent instance with error '%2'.

1.7.6.5 Mail Submission Errors and Events

Mail Submission Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Mail Submission events in Event Viewer so

that you can troubleshoot and verify the MSExchangeMailSubmission features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

MSExchangeMailSubmission Errors and Events

The following table provides a list of the MSExchangeMailSubmission errors and events.

Event ID	Category	Event type	Value or description
MSExchangeMailSubmission 1002	MSExchangeMailSubmission	Error	Unable to start the Microsoft Exchange Mail Submission service: %1
MSExchangeMailSubmission 1010	MSExchangeMailSubmission	Error	The hub server %1 is currently processing %2 submissions, which is the maximum allowed.
MSExchangeMailSubmission 1004	MSExchangeMailSubmission	Error	Unable to load the Microsoft Exchange Mail Submission service performance counters: %1

1.7.6.6 Messaging Policies Errors and Events

Messaging Policies Errors and Events

Exchange Server 2010 > Transport > Error and Event Reference for Transport Servers >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Messaging Policies events in Event Viewer so that you can troubleshoot and verify the Messaging Policies features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Messaging Policies Errors and Events

The following table provides a list of the Messaging Policies errors and events.

Event ID	Category	Event type	Value or description
MSExchange Messaging Policies	AttachFilter	Warning	An error occurred while loading the

2001			configuration for the Attachment Filter agent, the configuration may be corrupt, or Active Directory Application Mode (ADAM) may be unreachable. The Attachment Filter agent will use the last known "good" configuration.
MSExchange Messaging Policies 3001	AddressRewrite	Error	An error occurred while loading the configuration for the Address Rewriting Inbound agent and Address Rewriting Outbound agent. The configuration may be corrupt, or Active Directory Application Mode (ADAM) may be unreachable. The Address Rewriting Inbound agent and Address Rewriting Outbound agent will use the last known "good" configuration.
MSExchange Messaging Policies 6007	PolicyApplication	Error	Encryption Agent failed to get a delegation token for %1 for the target %2. Error is %3.
MSExchange Messaging Policies 6008	PolicyApplication	Warning	Federation is not enabled, but the %1 agent encountered a message that needs to be %2 %3
MSExchange Messaging Policies 6009	PolicyApplication	Warning	Failed to find certificate to decrypt the token. Please make sure that the organization private certificate is installed on this server and enabled for SMTP. The OrgPrivCertificate thumbprint is available from the get-federationtrust task. Messages that need to be decrypted will be temporarily rejected.

MSExchange Messaging Policies 6017	PolicyApplication	Warning	Failed to load federated delivery configuration when encrypting message '%1'. MSExchange Encryption agent will send an NDR for this message. The error is: '%2'
MSExchange Messaging Policies 4002	Rules	Information	'%1' rule collection was loaded successfully.

1.7.6.7 Message Security Errors and Events

Message Security Errors and Events

Exchange Server 2010 > Transport > Error and Event Reference for Transport Servers >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-14*

Microsoft Exchange Server 2010 generates Message Security events in Event Viewer so that you can troubleshoot and verify the Message Security features and services. Event Viewer tracks the following kinds of events in the given order based on importance:

- Error events
- Warning events
- Informational events

Message Security Errors and Events

The following table provides a list of Message Security errors and events.

Event ID	Category	Event type	Value or description
MSExchange Message Security 1003	EdgeCredentialService	Error	No valid Transport Layer Security (TLS) certificate was found. Microsoft Exchange can't update the Active Directory Application Mode (ADAM) credentials.
MSExchange Message Security 1005	EdgeCredentialService	Error	Could not decrypt EdgeSync credential %1 using Edge default certificate with thumbprint %2, The exception is %3. Please unsubscribe and resubscribe your Edge Transort server.
MSExchange Message Security	EdgeCredentialService	Error	Microsoft Exchange couldn't read the

1001			server configuration. The service will be stopped.
MSExchange Message Security 1000	EdgeCredentialService	Error	Microsoft Exchange couldn't read the server configuration because the directory is unavailable. The service will be stopped.
MSExchange Message Security 1004	EdgeCredentialService	Error	The local server couldn't be found. Microsoft Exchange can't update the Active Directory Lightweight Directory Services (AD LDS) credentials. Exception is %1. Make sure that the service account used by the Microsoft Exchange Edge Credential service has permission to access the local Exchange server object in the Active Directory service. Also make sure that the FQDN of the computer matches the FQDN attribute of the server object in Active Directory.
MSExchange Message Security 1007	EdgeCredentialService	Error	Microsoft Exchange couldn't read the registry information about the Secure Sockets Layer (SSL) port that is used by Active Directory Application Mode (ADAM), exception % 1. Using the default value for the SSL port that is used by ADAM: 50636.
MSExchange Message Security 1006	EdgeCredentialService	Error	Failed to update EdgeSync credential %1 in ADAM. The exception is: %2. Please make sure ADAM service is running.

1.7.6.8 Store Driver Errors and Events

Store Driver Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates MSExchange Store Driver events in Event Viewer so that you can troubleshoot and verify the Store Driver features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Store Driver Errors and Events

The following table provides a list of Store Driver errors and events.

Event ID	Category	Event type	Value or description
MSExchange Store Driver 1012	MSExchangeStoreDriver	Error	The store driver failed to submit event %1 mailbox %2 MDB %3 and couldn't generate an NDR due to exception %4.
MSExchange Store Driver 1018	MeetingMessageProcessing	Warning	An error occurred processing the meeting message with subject %1 in mailbox %2. Error: %3.
MSExchange Store Driver 1016	MSExchangeStoreDriver	Warning	The sender for event %1 mailbox %2 MDB %3 is invalid. The event will be ignored.
MSExchange Store Driver 1004	MSExchangeStoreDriver	Error	Unable to load the store driver performance counters: %1.
MSExchange Store Driver 1009	MSExchangeStoreDriver	Warning	The store driver encountered a poison message during message submission. The submission will be stopped for event %1 on mailbox %2 MDB %3. Exception is: %4.
MSExchange Store Driver 1011	MSExchangeStoreDriver	Warning	The store driver encountered a poison message during

			message submission. The submission will be stopped for event %1 on mailbox %2 Mdb %3.
MSExchange Store Driver 1017	MSExchangeStoreDriver	Warning	There are too many mail submission threads. The number of submission threads is currently limited to %1.

1.7.6.9 Transport Errors and Events

Transport Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates MSExchangeTransport events in Event Viewer so that you can troubleshoot and verify the Exchange Transport features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

MSExchange Transport Errors and Events

The following table provides a list of Certificate Deployment errors and events.

Event ID	Category	Event type	Value or description
MSExchangeTransport 10001	PoisonMessage	Warning	%1 messages have reached or exceeded the configured poison threshold of %2. After the Microsoft Exchange Transport service restarted, these messages were moved to the poison message queue.
MSExchangeTransport 10003	PoisonMessage	Error	The transport process failed during message processing with the following call stack: %1.
MSExchangeTransport 10005	PoisonMessage	Error	The transport process couldn't load poison message information from the registry.

			Access to the registry failed with the following error: %1.
MSExchangeTransport 10004	PoisonMessage	Warning	The processing of Pickup file %1 caused the transport process to fail. Pickup file %1 will be renamed.
MSExchangeTransport 10006	PoisonMessage	Error	The transport process couldn't save poison message information to the registry. Access to the registry failed with the following error: %1.
MSExchangeTransport 10007	PoisonMessage	Error	The transport process couldn't remove poison message information from the registry. Access to the registry failed with the following error: %1.
MSExchangeTransport 1003	SmtpReceive	Error	The configuration of one of the SMTP Receive connectors is invalid. The configuration change will be ignored. The description of the configuration error is: %1.
MSExchangeTransport 1012	SmtpReceive	Warning	Receive connector %1: Authentication failures have exceeded the maximum of %2 for the connection from %3. Disconnecting.
MSExchangeTransport 1018	SmtpReceive	Warning	The account '%1' provided valid credentials, but it does not have submit permissions on SMTP Receive connector '%2'; failing authentication.
MSExchangeTransport 1020	SmtpReceive	Warning	The account '%1' provided valid credentials, but is not authorized to use the server; failing authentication.

MSExchangeTransport 1021	SmtpReceive	Warning	Receive connector %1 rejected an incoming connection from IP address %3. The maximum number of connections per source (%2) for this connector has been reached by this source IP address.
MSExchangeTransport 1022	SmtpReceive	Warning	Anti-spam agents are enabled, but the list of internal SMTP servers is empty. If there are any MTAs between this server and the Internet, populate this list by using the Set-TransportConfig cmdlet in the Exchange Management Shell.
MSExchangeTransport 1025	SmtpReceive	Error	SMTP rejected a (%4) mail from '%1' with '%2' connector and the user authenticated as '%3'. The Active Directory lookup for the sender address returned validation errors. %5
MSExchangeTransport 1028	SmtpReceive	Error	SMTP rejected a mail from '%1', sender '%4' on '%2' connector, and user authenticated as '%3'. The Active Directory directory service lookup for the FROM address returned the following error: %5
MSExchangeTransport 1034	SmtpReceive	Error	Initialization of inbound authentication failed with error %1 for Receive connector %2. The authentication mechanism is %3. The source IP address of the client who tried to authenticate to us is [%4].
MSExchangeTranspo	SmtpReceive	Error	Inbound direct trust

rt 1036			authentication failed for certificate %1. The source IP address of the server that tried to authenticate to Microsoft Exchange is [%2]. Make sure EdgeSync is running properly.
MSExchangeTransport 11005	MessageSecurity	Error	Unable to validate the TLS certificate of the smart host for the connector %1. The certificate validation error for the certificate is %2. If the problem persists, contact the administrator of the smart host to resolve the problem.
MSExchangeTransport 11011	MessageSecurity	Error	A secure connection from domain-secured domain '%1' on connector '%2' failed to authenticate because validation of the Transport Layer Security (TLS) certificate failed with status '%3'. Contact the administrator of %1 to resolve the problem, or remove the domain from the domain-secured list.
MSExchangeTransport 11012	MessageSecurity	Error	A message from domain-secured domain '%1' on connector '%2' could not be authenticated because the server did not use Transport Layer Security (TLS). Contact the administrator for %1 to resolve the problem, or remove the domain from the domain-secured list.
MSExchangeTransport 11013	MessageSecurity	Error	The connection to secure domain '%1' on connector '%2' failed because Transport Layer Security (TLS)

			negotiation was unsuccessful. Error: '%3'. Please contact the administrator of %1 to resolve the problem.
MSExchangeTransport 11014	MessageSecurity	Error	A secure connection to domain secure domain '%1' on connector '%2' could not be established because TLS was not offered. Contact the administrator for %1 to resolve the problem or remove the domain from the domain-secured list.
MSExchangeTransport 11015	MessageSecurity	Error	A secure connection to domain secure domain '%1' on connector '%2' could not be established because TLS was not offered. Contact the administrator for %1 to resolve the problem or remove the domain from the domain-secured list.
MSExchangeTransport 11016	MessageSecurity	Error	Authentication of the connection to secure domain %1 failed because the Transport Layer Security (TLS) server certificate didn't contain the name of that domain. Either contact the administrator for domain %1 to resolve the problem with their certificate or remove the domain from the domain-secured list.
MSExchangeTransport 11017	MessageSecurity	Error	A message from domain-secured domain '%1' on connector '%2' failed to authenticate because no Transport Layer Security (TLS) certificate was supplied. Contact the administrator for %1

			to resolve the problem, or remove the domain from the domain-secured list.
MSExchangeTransport 11018	MessageSecurity	Error	The message could not be received from domain-secured domain %1 because of a configuration error on Receive connector %2. You must set Transport Layer Security (TLS) as the authentication mechanism on the connector to receive messages from domain-secured domains.
MSExchangeTransport 11019	MessageSecurity	Error	The connection to secure domain '%1' on Send connector '%2' failed because Transport Layer Security (TLS) negotiation failed with response '%3'. Contact the administrator of secure domain '%1' to resolve the problem or remove the domain from the domain-secured list.
MSExchangeTransport 11020	MessageSecurity	Error	A secure connection to domain-secured domain '%1' on connector '%2' could not be established because the validation of the Transport Layer Security (TLS) certificate for %1 failed with status '%3. Contact the administrator of %1 to resolve the problem, or remove the domain from the domain-secured list.
MSExchangeTransport 12008	TransportService	Error	Microsoft Exchange couldn't read the Receive connector configuration. The service will be

			stopped.
MSExchangeTransport 12010	TransportService	Error	Microsoft Exchange couldn't load the Active Directory recipient cache performance counters %1.
MSExchangeTransport 12011	TransportService	Error	Microsoft Exchange couldn't register the service principal name %1: %2
MSExchangeTransport 12012	TransportService	Error	The internal transport certificate that is used for SMTP authentication by Microsoft Exchange could not be read from Active Directory. The certificate may be missing. If an existing certificate that matches the fully qualified domain name (FQDN) of the server is already installed, run the Enable-ExchangeCertificate cmdlet to publish this certificate to Active Directory. If a certificate for the FQDN of the server is not installed, create a certificate by running the New-ExchangeCertificate cmdlet for the FQDN of the server.
MSExchangeTransport 12013	TransportService	Error	Microsoft Exchange could not load the certificate with thumbprint of %1 from the personal store on the local computer. This certificate was configured for authentication with other Exchange servers. Mail flow to other Exchange servers could be affected by this error. If the certificate with this thumbprint still

			exists in the personal store, run Enable-ExchangeCertificate %1 -Services SMTP to resolve the issue. If the certificate does not exist in the personal store, restore it from backup by using the Import-ExchangeCertificate cmdlet, or create a new certificate for the FQDN or the server enabled for SMTP by running the following command: New-ExchangeCertificate -DomainName serverfqdn -Services SMTP.
MSExchangeTransport 12014	TransportService	Error	Microsoft Exchange could not find a certificate that contains the domain name %1 in the personal store on the local computer. Therefore, it is unable to support the STARTTLS SMTP verb for the connector %2 with a FQDN parameter of %1. If the connector's FQDN is not specified, the computer's FQDN is used. Verify the connector configuration and the installed certificates to make sure that there is a certificate with a domain name for that FQDN. If this certificate exists, run Enable-ExchangeCertificate -Services SMTP to make sure that the Microsoft Exchange Transport service has access to the certificate key.
MSExchangeTransport 12016	TransportService	Error	There is no valid SMTP Transport Layer Security (TLS)

			certificate for the FQDN of %1. The existing certificate for that FQDN has expired. The continued use of that FQDN will cause mail flow problems. A new certificate that contains the FQDN of %1 should be installed on this server as soon as possible. You can create a new certificate by using the New-ExchangeCertificate task.
MSExchangeTransport 12018	TransportService	Warning	The STARTTLS certificate will expire soon: subject: %1, thumbprint: %2, hours remaining: %3. Run the New-ExchangeCertificate cmdlet to create a new certificate.
MSExchangeTransport 12020	TransportService	Error	A secure connection to the domain %1 could not be established because the Transport Layer Security (TLS) certificate for the domain has expired. Contact the administrator for %1 to resolve the problem.
MSExchangeTransport 12021	TransportService	Warning	Microsoft Exchange detected a configuration change but couldn't read the updated Receive connector configuration. The configuration change will be ignored.
MSExchangeTransport 14001	Process	Error	The worker process with process ID %1 is not responding and will be forced to shut down.
MSExchangeTranspo	Process	Error	The worker process

rt 14004			has failed to load application configuration file: %1.
MSExchangeTransport 15006	ResourceManager	Warning	Microsoft Exchange Transport is rejecting message submissions because the available disk space has dropped below the configured threshold. %1
MSExchangeTransport 15007	ResourceManager	Warning	The Microsoft Exchange Transport service is rejecting message submissions because the service continues to consume more memory than the configured threshold.%1.
MSExchangeTransport 16011	Configuration	Warning	MessageTrackingLog is enabled, but MessageTrackingLogPath is null. MessageTrackingLog will be disabled.
MSExchangeTransport 16013	Configuration	Warning	The SendProtocolLogPath parameter is set to $null. Setting the value of this parameter to $null disables protocol logging for all Send connectors on the server. No send protocol log is written.
MSExchangeTransport 16014	Configuration	Warning	The path to the protocol logging location for Receive connectors has not been set. Use the existing path.
MSExchangeTransport 16015	Configuration	Warning	The SendProtocolLogPath parameter is set to $null. Microsoft Exchange will continue to use the old location for protocol log storage.
MSExchangeTranspo	Configuration	Error	There is no default

rt 16016			authoritative domain or the domain name is empty.
MSExchangeTranspo rt 16017	Configuration	Error	Microsoft Exchange couldn't activate transport components because of the unexpected exception: %1.
MSExchangeTranspo rt 16018	Configuration	Warning	A configuration update occurred but the internal %1 cache failed to load. Microsoft Exchange will retain the existing configuration. %2
MSExchangeTranspo rt 16021	Configuration	Error	An accepted domain entry was damaged in Active Directory. Exchange is rejecting the configuration.
MSExchangeTranspo rt 16023	Configuration	Error	Microsoft Exchange couldn't start transport agents. The Microsoft Exchange Transport service will be stopped. Exception details: %1 : %2.
MSExchangeTranspo rt 16024	Configuration	Error	The data for an accepted domain entry included invalid data. Skipping record for %1.
MSExchangeTranspo rt 16025	Configuration	Warning	No DNS servers could be retrieved from network adapter %1. Check if the computer is connected to a network and Get-NetworkConnectionIn fo returns any results.
MSExchangeTranspo rt 17001	Storage	Error	Column %3 in Extensible Storage Engine (ESE) table % 2 from database %1 should contain data type %4, but instead it contains data type %5. The module that contains the database schema may have been

			updated and could be trying to open an older database. The old database must be removed before starting the Microsoft Exchange Transport service.
MSExchangeTransport 17002	Storage	Error	The non-nullable column %3 on the Extensible Storage Engine (ESE) table %2 from database %1 is part of the database schema but cannot be found in the actual database table. The module containing the database schema may have been updated and could be attempting to open an older database. The old database must be removed before starting the Exchange Server Transport service in Microsoft Exchange Server 2010.
MSExchangeTransport 17003	Storage	Error	%1: An operation has encountered a fatal error. The database may be corrupted. The Microsoft Exchange Transport service is shutting down. Manual database recovery or repair may be required. Exception details: %2
MSExchangeTransport 17004	Storage	Error	%1: An operation has encountered a fatal error. There wasn't enough disk space to complete the operation. The Microsoft Exchange Transport service is shutting down. The exception is %2.
MSExchangeTransport 17005	Storage	Error	%1: The database could not be opened because a log file is

			missing or corrupted. The Microsoft Exchange Transport service is shutting down. Manual database recovery or repair may be required. The exception is %2.
MSExchangeTransport 17006	Storage	Error	%1: The database could not be opened because the log file path that was supplied is invalid. The Microsoft Exchange Transport service is shutting down. The exception is %2.
MSExchangeTransport 17007	Storage	Error	%1: The database could not be opened because the database file does not match the log files. The Microsoft Exchange Transport service is shutting down. The exception is %2.
MSExchangeTransport 17011	Storage	Error	%1: The database could not be opened because the checkpoint file (.chk) is missing or corrupted. The Microsoft Exchange Transport service is shutting down. Manual database recovery or repair may be required. The exception is %2.
MSExchangeTransport 17101	Storage	Error	%1: MSExchangeTransport has detected a critical storage error but will not take any recovery actions. Manual actions should be taken to resolve issues encountered with this database (%2) and associated transaction logs (%3).
MSExchangeTranspo	Storage	Error	%1:

rt 17102			MSExchangeTransport has detected a critical storage error and has taken an automated recovery action. This recovery action will not be repeated until the target folders are renamed or deleted. %2.
MSExchangeTransport 17104	Storage	Error	%1: MSExchangeTransport has detected a critical storage error but failed to complete the desired recovery action on %2 due to error %3.
MSExchangeTransport 17105	Storage	Warning	%1: MSExchangeTransport has detected a critical storage error and will now stop. The service attempted to update the registry key (%2) used to initiate automated recovery but failed with the following error: %3. Please make sure Network Service has Full Control to this registry key.
MSExchangeTransport 2000	SmtpSend	Warning	Send connector %1: A DNS failure occurred with the following diagnostic information %2.
MSExchangeTransport 2002	SmtpSend	Error	Send connector %1: an error occurred while connecting to %2.
MSExchangeTransport 2003	SmtpSend	Warning	Send connector %1 has failed to authenticate with %2. The response from the remote site is %3.
MSExchangeTransport 2006	SmtpSend	Warning	Send connector %1: the connection to %2 was disconnected by the remote server.
MSExchangeTransport 2011	SmtpSend	Error	A secure connection with Exchange server

			%1 could not be established because the protocol negotiation did not find a mutually supported hash algorithm. Modify the configuration of either %1 or this server so that one hash algorithm is supported by both servers.
MSExchangeTransport 2014	SmtpSend	Error	Failed to bind to SourceIPAddress '%1' configured on send connector '%2'.
MSExchangeTransport 2015	SmtpSend	Error	Send connector %1 couldn't connect to remote domain %2. The send connector requires Transport Layer Security (TLS) authentication, but is unable to establish TLS with the receiving server for the remote domain. Check this connector's authentication setting and the EHLO response from the remote server %3.
MSExchangeTransport 2016	SmtpSend	Error	An authentication credential initialization error %1 occurred with Send connector %2. The authentication mechanism used was %3. The name of the server that we were trying to authenticate to was %4. This server was using the name %5. Try reentering the credential. If the problem persists, contact Microsoft Support Services.
MSExchangeTransport 2017	SmtpSend	Error	Outbound authentication failed with error %1 for Send connector %2. The authentication

			mechanism is %3. The target is %4.
MSExchangeTransport 2018	SmtpSend	Error	Outbound direct trust authentication failed for certificate %1. The target IP address of the Exchange server that Microsoft Exchange tried to authenticate to is [%2]. Make sure EdgeSync is running properly.
MSExchangeTransport 2019	SmtpSend	Warning	Unable to transmit ORAR information to remote server '%1' over send connector '%2'. Message '%3' will not be delivered to recipient '%4'.
MSExchangeTransport 3004	Dsn	Error	The generation of the quarantine message may fail because of an error reading the spam quarantine mailbox configuration from the directory. The configuration data may be corrupt or the Active Directory directory service may be unreachable.
MSExchangeTransport 3005	Dsn	Error	An error caused by reading the SystemMessage configuration from the directory indicates that generation of delivery status notifications (DSNs) and storage quota is using out-of-date or incomplete message customizations. The configuration data may be corrupt, or the Active Directory directory service may be unreachable. The error was '%1'.
MSExchangeTransport 5001	Routing	Error	Microsoft Exchange couldn't load the routing performance counters: %1.

MSExchangeTransport 5002	Routing	Error	Microsoft Exchange couldn't load routing tables because the Active Directory directory service is unavailable. Microsoft Exchange will continue to use the existing routing table if one is available.
MSExchangeTransport 5003	Routing	Error	Microsoft Exchange couldn't load configuration information for routing. The process will block and retry the operation in %1 seconds.
MSExchangeTransport 5004	Routing	Error	Microsoft Exchange cannot obtain the fully qualified domain name (FQDN) of Exchange server %1 in routing tables with timestamp %2. Recipients will not be routed to this server.
MSExchangeTransport 5005	Routing	Error	The Active Directory site for Exchange server %1 was not determined in routing tables with timestamp %2. Recipients will not be routed to this server.
MSExchangeTransport 5006	Routing	Error	Cannot find route to Mailbox Server %1 for store %2 in routing tables with timestamp %3. Recipients will not be routed to this store.
MSExchangeTransport 5007	Routing	Error	The topology doesn't contain a route to Active Directory site %1 in routing tables with the timestamp %2. Recipients will not be routed to servers in this Active Directory site. Hub Transport server %3 is unreachable.
MSExchangeTranspo	Routing	Error	The topology does

rt 5008			not contain any route to server %1 in Active Directory site %2 in routing tables with timestamp %3. Recipients will not be routed to this server.
MSExchangeTranspo rt 5009	Routing	Warning	Microsoft Exchange cannot find the route to mailbox database %1 for public folder hierarchy %2 in routing tables with timestamp %3.
MSExchangeTranspo rt 5010	Routing	Warning	No route has been created for public folder hierarchy %1 in routing tables with timestamp %2. Recipients will not be routed to this public folder. Check the routing logs for further information.
MSExchangeTranspo rt 5011	Routing	Error	Source routing group %1 was not found for routing group connector %2 in routing tables with timestamp %3. Microsoft Exchange is skipping the connector.
MSExchangeTranspo rt 5012	Routing	Error	Target routing group %1 was not found for routing group connector %2 in routing tables with timestamp %3; skipping the connector.
MSExchangeTranspo rt 5013	Routing	Error	The routing group for Exchange server %1 was not determined in routing tables with timestamp %2. Recipients will not be routed to this server.
MSExchangeTranspo rt 5014	Routing	Error	No source transport servers or home MTA server have been set for connector %1 in routing tables with timestamp %2.

			Ignoring the connector.
MSExchangeTransport 5015	Routing	Error	Microsoft Exchange cannot find a route to the source transport server or home MTA server %1 for connector %2 in routing tables with timestamp %3. Microsoft Exchange is ignoring the source transport server.
MSExchangeTransport 5016	Routing	Error	The Active Directory topology service could not discover any route to connector %1 in the routing tables with the timestamp %2. This connector will not be used.
MSExchangeTransport 5017	Routing	Error	Microsoft Exchange cannot find target bridgehead server %1 for routing group connector %2 in routing tables with timestamp %3. Microsoft Exchange is ignoring the target bridgehead server.
MSExchangeTransport 5018	Routing	Error	No target bridgehead servers were found for routing group connector %1 in routing tables with timestamp %2. Ignoring the routing group connector.
MSExchangeTransport 5019	Routing	Error	MSExchangeTransport found invalid smart hosts string %1 on SMTP connector %2 in routing tables with timestamp %3. MSExchangeTransport is ignoring the SMTP connector.
MSExchangeTransport 5020	Routing	Warning	The topology doesn't contain a route to Exchange 2000 Server or Exchange Server 2003 %1 in Routing Group %2 in

			routing tables with the timestamp %3.
MSExchangeTransport 5021	Routing	Error	The Exchange 2000 or Exchange 2003 server %1 was found in Exchange 2007 routing group %2 in routing tables with timestamp %3.
MSExchangeTransport 5023	Routing	Error	A transient configuration error was detected while the routing configuration was loading. Exception details: %1 : %2.
MSExchangeTransport 5024	Routing	Error	The maximum number of retries to load routing configuration data has been reached. The service will be stopped.
MSExchangeTransport 5025	Routing	Error	Non-SMTP address space '%1' was detected on the DNS SMTP connector '%2' in routing tables with timestamp %3. The address space is ignored on the connector because a non-delivery report (NDR) will be sent for the message or because the message will go to another connector. Exchange Server 2007 or Exchange 2010 tasks block this configuration. However, the connector may have been set up by Exchange Server 2003.
MSExchangeTransport 5026	Routing	Warning	Source servers belonging to different Active Directory sites were detected for connector '%1' in routing tables with timestamp %2. Only the closest site will be used and load-

			balancing will be affected.
MSExchangeTransport 5027	Routing	Error	Source routing group %1 was not found for the connector with connected routing groups %2 in routing tables with timestamp %3. Microsoft Exchange Transport is skipping the connector.
MSExchangeTransport 5028	Routing	Error	Source routing group %1 is the local routing group for a connector with connected routing groups %2 in routing tables with timestamp %3. Connectors with connected routing groups are only supported in routing groups with Exchange 2000 or Exchange 2003 servers.
MSExchangeTransport 5029	Routing	Error	Connected routing group %1 was not found for connector %2 in routing tables with timestamp %3.
MSExchangeTransport 5030	Routing	Error	Microsoft Exchange couldn't create routing table log file or directory %1. Exception details: %2 : %3.
MSExchangeTransport 5031	Routing	Error	Microsoft Exchange couldn't delete routing table log file %1. Exception details: %2 : %3.
MSExchangeTransport 5500	Logging	Warning	Transport pipeline tracing is active. This may degrade system performance.
MSExchangeTransport 7002	Components	Error	Database %1 is already in use. The service will be stopped. Exception details: %2
MSExchangeTranspo	RemoteDelivery	Error	A non-SMTP gateway

rt 8004			connection failure occurred on connector %1. When writing to the drop directory %2, an I/O exception %3 occurred.
MSExchangeTransport 8005	RemoteDelivery	Error	A non-SMTP gateway connection failure occurred on connector %1. The drop directory quota limit of %2(MB) has been exceeded.
MSExchangeTransport 8007	RemoteDelivery	Error	Non-SMTP Gateway Connection Failure on Connector %1. The drop directory filename %2 exceeds the system-defined maximum length.
MSExchangeTransport 8008	RemoteDelivery	Error	A connection failure occurred on the foreign connector %1. The Drop directory %2 does not exist.
MSExchangeTransport 8009	RemoteDelivery	Error	Non-SMTP connector %1 failed because the Drop directory %2 does not have the correct access permissions. Change the access permissions for directory %2 or use another directory.
MSExchangeTransport 8010	RemoteDelivery	Error	A message with the Internal Message ID %1 was rejected by the remote server. This message will be deferred and retried because it was marked for retry if rejected. Other messages may also have encountered this error.
MSExchangeTransport 9002	Pickup	Error	The Pickup directory doesn't have the necessary Read permissions and Delete Subfolders and Files permissions for Pickup directory %1.

MSExchangeTransport 9003	Pickup	Warning	Read-only files have been found in the directory %1. Read-only files cannot be processed by the Pickup directory or the Replay directory. Please remove the read-only attributes or remove the read-only files.
MSExchangeTransport 9004	Pickup	Error	File(s) cannot be deleted from %1 by the Pickup directory. This may cause duplicate mail. Please verify that the Network Service account has "Delete Subfolders and Files" permission for this directory.
MSExchangeTransport 9005	Pickup	Error	The Pickup directory cannot submit the message because of database problems.
MSExchangeTransport 9006	Pickup	Error	The Microsoft Exchange Transport service failed to create the Pickup directory: %1. Pickup will not function until the directory is created. The detailed error is %2.
MSExchangeTransport 9007	Pickup	Error	File(s) cannot be opened or renamed in %1 by the Pickup directory. Some mail may not be processed by the Pickup directory. Please verify that the Network Service account has "Create Files" permission for this directory, and that files in the directory do not deny read access to the Network Service account.
MSExchangeTransport 9009	Pickup	Error	The Pickup directory doesn't have permissions to write

			the pickup location to registry (%1). Please make sure Network Service has Full Control to the registry location. The error was %2.
MSExchangeTransport 9010	Pickup	Error	At least one file in %1 can't be processed. These files have .bad extensions. Please look for .bad files, and make sure that their content is valid.
MSExchangeTransport 9201	Categorizer	Error	Transport agent (%1) running on the OnSubmittedMessage event did not handle a catchable exception: (%2).
MSExchangeTransport 9202	Categorizer	Error	Transport agent (%1) running on the OnRoutedMessage event did not handle a catchable exception: (%2).
MSExchangeTransport 9212	Categorizer	Error	Microsoft Exchange couldn't load the resolver performance counters: %1.
MSExchangeTransport 9213	Categorizer	Warning	A non-expirable message with the Internal Message ID %1 could not be categorized. This message may be a journal report or other system message. The message will remain in the queue until administrative action is taken to resolve the error. Other messages may also have encountered this error. To further diagnose the error, use the Queue Viewer or the Exchange Mail Flow Troubleshooter.
MSExchangeTransport 1009	SmtpReceive	Warning	Receive connector %1 rejected an incoming

			connection. The maximum number of connections (%2) for this connector has been reached.
MSExchangeTransport 18001	Agents	Error	Agent '%1' did not close the MIME stream after handling the %2 event for message with ID '%3'. The message has been rejected. Please report this problem to the agent vendor.
MSExchangeTransport 7007	Components	Information	Online defragmentation has completed for database %1. The database has %2 free bytes.
MSExchangeTransport 7006	Components	Information	Scheduled online defragmentation will start for database %1. The database has %2 free bytes.
MSExchangeTransport 7005	Components	Information	A new database file %1 has been created.
MSExchangeTransport 7004	Components	Information	The activation of all modules took longer than expected to complete. Total Load Time: %1 Total Start Time: %2 Load Time Breakdown: %3 Start Time Breakdown: %4.
MSExchangeTransport 2021	SmtpSend	Information	Unable to transmit RDST (Routing Destination) to remote server '%1' over send connector '%2'. Message '%3' will not be delivered to recipient '%4'.
MSExchangeTransport 2020	SmtpSend	Information	Unable to transmit long ORAR address '%1' to remote server '%2' over send connector '%3'. Message '%4' will not be delivered to recipient '%5'.
MSExchangeTranspo	SmtpSend	Information	Send connector %1

rt 2007			has initiated a new session to %2.
MSExchangeTransport 2005	SmtpSend	Information	Send connector %1: Errors occurred with the connection to %2. The connection was acknowledged with SMTP response %3.
MSExchangeTransport 2004	SmtpSend	Information	Send connector %1: Message delivery was not successful. The message with message ID %2 was acknowledged with SMTP response %3.
MSExchangeTransport 10002	PoisonMessage	Information	PoisonCount for the message with the record ID %1 has been incremented. The new value is %2.
MSExchangeTransport 1002	SmtpReceive	Information	The connectors have been configured.
MSExchangeTransport 1010	SmtpReceive	Error	Receive connector %1 rejected a message at SMTP end of data with %2.
MSExchangeTransport 1023	SmtpReceive	Error	SMTP rejected a message from '%1' with '%2' connector. The authenticated user '%3' doesn't have permission to submit e-mail messages to this server.
MSExchangeTransport 1024	SmtpReceive	Error	SMTP rejected a (%4) mail from '%1' with '%2' connector and user authenticated as '%3'. There was a transient Active Directory directory service exception thrown with the following information. %5.
MSExchangeTransport 1026	SmtpReceive	Error	SMTP rejected a (%4) mail from '%1' with '%2' connector. The user '%3' does not have permissions to send as this address.

MSExchangeTransport 1027	SmtpReceive	Error	SMTP rejected a mail from '%1', sender '%4' with '%2' connector and user authenticated as '%3'. The Active Directory lookup for the FROM address threw a transient Active Directory exception with the following information. %5
MSExchangeTransport 1029	SmtpReceive	Information	SMTP rejected a mail from '%1', sender '%4' with '%2' connector and user authenticated as '%3'. The sender does not have permissions to send on behalf of the FROM address.
MSExchangeTransport 1031	SmtpReceive	Error	The connection for user [%1] with IP address [%2] is being dropped. The rate of message submissions from this connection has exceeded the throttling policy of %3 per minute.
MSExchangeTransport 1033	SmtpReceive	Error	An exception was thrown while processing data from client IP address %1. The exception is %2.
MSExchangeTransport 1035	SmtpReceive	Error	Inbound authentication failed with error %1 for Receive connector %2. The authentication mechanism is %3. The source IP address of the client who tried to authenticate to Microsoft Exchange is [%4].
MSExchangeTransport 1037	SmtpReceive	Error	Failure occurred while trying to determine the Mailbox server for mailbox database [%1]. Message submission quota for user [%2] with IP address [%3] will not

			be enforced. Exception details: %4
MSExchangeTransport 1039	SmtpReceive	Error	SMTP rejected a message from '%1' on '%2' connector. The user was authenticated as '%3'. The Active Directory lookup returned the following error: %4.
MSExchangeTransport 11021	MessageSecurity	Warning	A secure connection to domain-secured domain '%1' on connector '%2' could not be established because the DomainSecureEnabled flag on the connector was not set. Set the DomainSecureEnabled flag or remove the domain '%1' from the domain-secured list.
MSExchangeTransport 11022	MessageSecurity	Error	Failed to confirm domain capabilities '%1' on connector '%2' because validation of the Transport Layer Security (TLS) certificate failed with status '%3'. Contact the administrator of '%4' to resolve the problem, or remove the domain from the TlsDomainCapabilities list of the Receive connector.
MSExchangeTransport 11023	MessageSecurity	Error	Connection to remote endpoint '%1 (%2)' for send connector '%3' is dropped because the server did not advertise the XOORG (Originator Organization) ESMTP protocol extension.
MSExchangeTransport 11024	MessageSecurity	Warning	Remote certificate with thumbprint '%1' contains '%2' subject alternative names and exceeds the limit of %3. Subject

			alternative names of this certificate will be ignored. The limit can be changed by adding/modifying the SubjectAlternativeNameLimit parameter in the EdgeTransport.exe.config file.
MSExchangeTransport 12002	TransportService	Information	A configuration update occurred.
MSExchangeTransport 12003	TransportService	Information	The configured server role is invalid for this process.
MSExchangeTransport 12009	TransportService	Error	Microsoft Exchange couldn't read the Receive connector configuration because the directory is unavailable. The service will be stopped.
MSExchangeTransport 12015	TransportService	Information	An internal transport certificate expired. Thumbprint:%1
MSExchangeTransport 12017	TransportService	Information	An internal transport certificate will expire soon. Thumbprint:%1, hours remaining: %2.
MSExchangeTransport 12019	TransportService	Information	The remote internal transport certificate expired. Certificate subject: %1.
MSExchangeTransport 12023	TransportService	Information	Microsoft Exchange could not load the certificate with thumbprint of %1 from the personal store on the local computer. This certificate was configured for authentication with other Exchange servers. Mail flow to other Exchange servers could be affected by this error. If the certificate with this thumbprint still exists in the personal store, run Enable-

			ExchangeCertificate %1 -Services SMTP to resolve the issue. If the certificate does not exist in the personal store, restore it from backup by using the Import-ExchangeCertificate cmdlet, or create a new certificate for the FQDN or the server enabled for SMTP by running the following command: New-ExchangeCertificate -DomainName serverfqdn -Services SMTP. Meanwhile, the certificate with thumbprint %2 is being used.
MSExchangeTransport 12024	TransportService	Information	Microsoft Exchange could not load the certificate with thumbprint of %1 from the personal store on the local computer. This certificate was configured for authentication with other Exchange servers. Mail flow to other Exchange servers could be affected by this error. If the certificate with this thumbprint still exists in the personal store, run Enable-ExchangeCertificate %1 -services SMTP to resolve the issue. If the certificate does not exist in the personal store, restore it from backup by using the Import-ExchangeCertificate cmdlet, or create a new certificate for the FQDN or the server enabled for SMTP by running the following command: New-ExchangeCertificate -DomainName

			serverfqdn -Services SMTP. Meanwhile, an ephemeral, self-signed certificate with thumbprint %2 is being used.
MSExchangeTransport 12025	TransportService	Warning	Transport service is disconnecting performance counters with process lifetime from their old process.
MSExchangeTransport 12026	TransportService	Error	Transport service failed to disconnect performance counters with process lifetime in category : %1 from their old process.
MSExchangeTransport 12028	TransportService	Warning	The process with processId %1 is holding the performance counter %2 from instance %3 and category %4 while running processes are: %5.
MSExchangeTransport 12029	TransportService	Information	The transport server is healthy for time: %1.
MSExchangeTransport 15004	ResourceManager	Warning	The resource pressure increased from %1 to %2.%3.
MSExchangeTransport 15005	ResourceManager	Information	The resource pressure decreased from %1 to %2.%3.
MSExchangeTransport 16012	Configuration	Warning	The path to the protocol logging location for Receive connectors has not been set. No protocol log for Receive connectors was written. The default location is C:\Program Files\Microsoft Exchange \TransportRoles\Logs \ProtocolLog \SmtpReceive.
MSExchangeTransport 16019	Configuration	Error	Active Directory directory service encountered an error

			for %1. Microsoft Exchange will retain the existing configuration, if available. Exception details: %2.
MSExchangeTransport 16022	Configuration	Information	A configuration update for %1 has successfully completed.
MSExchangeTransport 16026	Configuration	Information	Microsoft Exchange failed to query a network adapter to obtain the IP addresses assigned to it. Microsoft Exchange will continue to use previously loaded IP address information if available. The Microsoft Exchange Transport service will be stopped if this error occurred during service startup. Exception details: %1.
MSExchangeTransport 16027	Configuration	Information	The configuration for %1 has had to be forcibly loaded %2 time(s). There might be a problem with AD notifications.
MSExchangeTransport 16028	Configuration	Information	A forced configuration update for %1 has successfully completed. Object details from last notification based reload: %2. New details: %3.
MSExchangeTransport 17008	Storage	Information	The Microsoft Exchange Transport service has started the background scan of the queue database. All messages that have not yet been delivered will be loaded.
MSExchangeTransport 17009	Storage	Information	The background scan of the transport

			queue database has been stopped. %1 message(s) found so far. There may be other messages left in the database that have not yet been loaded.
MSExchangeTransport 17010	Storage	Information	The background scan of the transport queue database has completed. %1 message(s) were found.
MSExchangeTransport 17012	Storage	Error	%1: The database could not allocate memory. Please close some applications to make sure you have enough memory for Exchange Server. The exception is %2.
MSExchangeTransport 17013	Storage	Error	%1: The database could not be opened because there is another process using it. The Microsoft Exchange Transport service is shutting down. The exception is %2.
MSExchangeTransport 17014	Storage	Error	%1: The database could not be opened because there is no such database found. The Microsoft Exchange Transport service is shutting down. The exception is %2.
MSExchangeTransport 17015	Storage	Error	%1: The database could not be opened because it does not belong with the current set of log files. The Microsoft Exchange Transport service is shutting down. The exception is %2.
MSExchangeTransport 17016	Storage	Error	%1: An operation has encountered a fatal error. The database may be fragmented

			and manual offline defragmentation using ESEUTIL may be required. The Microsoft Exchange Transport service is shutting down. Exception details: %2
MSExchangeTransport 17017	Storage	Error	%1: Quota was exceeded while performing a database operation. The Microsoft Exchange Transport service is shutting down. Exception details: %2.
MSExchangeTransport 17018	Storage	Error	%1: There are insufficient resources to perform a database operation. The Microsoft Exchange Transport service is shutting down. Exception details: %2.
MSExchangeTransport 17019	Storage	Error	%1: A database operation has encountered an I/O error. The Microsoft Exchange Transport service is shutting down. Exception details: %2.
MSExchangeTransport 17020	Storage	Error	%1: A database operation has encountered a fatal error. The Microsoft Exchange Transport service is shutting down. Exception details: %2.
MSExchangeTransport 17021	Storage	Error	%1: Exchange couldn't open the database because it can't find a table. The Microsoft Exchange Transport service is shutting down. Exception details: %2.
MSExchangeTransport 17022	Storage	Error	%1: Exchange couldn't open the database because it

			can't find a file. The Microsoft Exchange Transport service is shutting down. Exception details: %2.
MSExchangeTransport 17023	Storage	Error	%1: The database could not be started because a critical database file has the read-only attribute set. The Microsoft Exchange Transport service is shutting down. Exception details: %2.
MSExchangeTransport 17103	Storage	Error	%1: MSExchangeTransport has detected a critical storage error and has taken an automated recovery action. %2.
MSExchangeTransport 17106	Storage	Information	%1: MSExchangeTransport has detected a critical storage error, updated the registry key (%2) and as a result, will attempt self-healing after process restart.
MSExchangeTransport 12022	TransportService	Information	The internal transport certificate that is used for SMTP authentication by Microsoft Exchange could not be read from Active Directory. The certificate may be corrupted. If an existing certificate that matches the fully qualified domain name (FQDN) of the server is already installed, run the Enable-ExchangeCertificate cmdlet to publish this certificate to Active Directory. If a certificate for the FQDN of the server is not installed, create an internal transport certificate by running

			the New-ExchangeCertificate cmdlet for the FQDN of the server.

1.7.6.10 TransportLogSearch Errors and Events

TransportLogSearch Errors and Events

Exchange Server 2010 > Transport > Error and Event Reference for Transport Servers >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates TransportLogSearch events in Event Viewer so that you can troubleshoot and verify the TransportLogSearch features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

TransportLogSearch Errors and Events

The following table provides a list of TransportLogSearch errors and events.

Event ID	Category	Event type	Value or description
MSExchangeTransportLogSearch 7004	General	Error	The Microsoft Exchange Transport Log Search service could not be stopped.
MSExchangeTransportLogSearch 7005	General	Error	Microsoft Exchange couldn't read the configuration from the Active Directory directory service because of error: %1.
MSExchangeTransportLogSearch 7009	General	Warning	The Microsoft Exchange Transport Log Search service failed to access %1 because of insufficient access permissions. The exception message is: %2.
MSExchangeTransportLogSearch 7010	General	Error	The Microsoft Exchange Transport Log Search Service

			failed to access %1 due to I/O error. The exception message is: %2.
MSExchangeTransportLogSearch 7012	General	Error	The following message tracking log file is corrupted: '%1'. The corrupted record won't be included in the search results.
MSExchangeTransportLogSearch 7011	General	Error	The Microsoft Exchange Transport Log Search service failed because the parameter that sets the location of the message tracking logs was set to an invalid value.
MSExchangeTransportLogSearch 7013	General	Error	The Microsoft Exchange Transport Log Search service failed to start because of an Log Session Manager startup error.
MSExchangeTransportLogSearch 7014	General	Error	The Microsoft Exchange Transport Log Search service failed to start because of a message tracking log error.
MSExchangeTransportLogSearch 7015	General	Error	The Microsoft Exchange Transport Log Search service started but it is not functional because of an RPC server startup error.
MSExchangeTransportLogSearch 7016	General	Error	The Microsoft Exchange Transport Log Search service failed to create message tracking log directory: %1 because of error: %2.
MSExchangeTransportLogSearch 7032	General	Error	The Microsoft Exchange Transport Log Search service was unable to access registry. The following error was

			encountered: %1.
MSExchangeTransportLogSearch 7003	General	Information	The Microsoft Exchange Transport Log Search service has finished indexing all log files. The time taken to complete the indexing was: %1 seconds.
MSExchangeTransportLogSearch 7001	General	Information	The Microsoft Exchange Transport Log Search service has started successfully.

1.8 Mailbox

Mailbox

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-25*

The Mailbox server role hosts mailbox and public folder databases. It also generates the offline address book (OAB). Mailbox servers provide services that calculate e-mail address policies and address lists for recipients and enforce managed folders.

The following topics are gateways to information about Mailbox servers in Exchange 2010.

Understanding Mailbox

View a list of links to topics that provide detailed information about the Mailbox features in Exchange 2010.

Permissions to Manage Mailbox Servers

Learn about the permissions required to manage the features available on your Mailbox servers.

Upgrade from Exchange 2003 Mailbox

Learn about the process for upgrading an existing Exchange 2003 Mailbox deployment to Exchange 2010.

Upgrade from Exchange 2007 Mailbox

Learn about the process for upgrading an existing Exchange 2007 Mailbox deployment to Exchange 2010.

Managing Mailbox Servers

View a list of links to topics that provide information about managing mailbox features in your organization.

Securing Mailbox Servers

Learn about the security-related options for the Mailbox servers in your organization.

1.8.1 Understanding Mailbox

Understanding Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-17*

Microsoft Exchange Server 2010 Mailbox servers host mailbox databases and provide e-mail storage and advanced scheduling services for Microsoft Outlook and Microsoft Office Outlook Web App users. In addition, Mailbox servers can also host a public folder database, which provides a foundation for workflow, document sharing, and other forms of collaboration.

The following topics provide detailed information about the Mailbox features in Exchange 2010:

Overview of the Mailbox Server Role

Understanding Address Lists

Understanding Calendar Repair

Understanding E-Mail Address Policies

Understanding the Exchange 2010 Store

Understanding Exchange Search

Understanding Hierarchical Address Books

Understanding Mailbox Import and Export Requests

Understanding Move Requests

Understanding Offline Address Books

Understanding Public Folders

Understanding Quota Messages

Understanding Recipients

Understanding Recoverable Items

1.8.1.1 Overview of the Mailbox Server Role

Overview of the Mailbox Server Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-09*

In Microsoft Exchange Server 2010, the Mailbox server role is one of several server roles

that you can install and configure on a server running Windows Server 2008. The Mailbox server role is the most common server role and is at the core of an Exchange organization. Servers on which the Mailbox server role is installed are called *Mailbox servers*.

Mailbox servers perform the following functions:

- Host mailbox databases
- Provide e-mail storage
- Host public folder databases
- Calculate e-mail address policies
- Generate address lists and offline address books (OABs)
- Conduct Multi-Mailbox Searches
- Provide high availability and site resiliency
- Provide content indexing
- Provide messaging records management (MRM) and retention policies

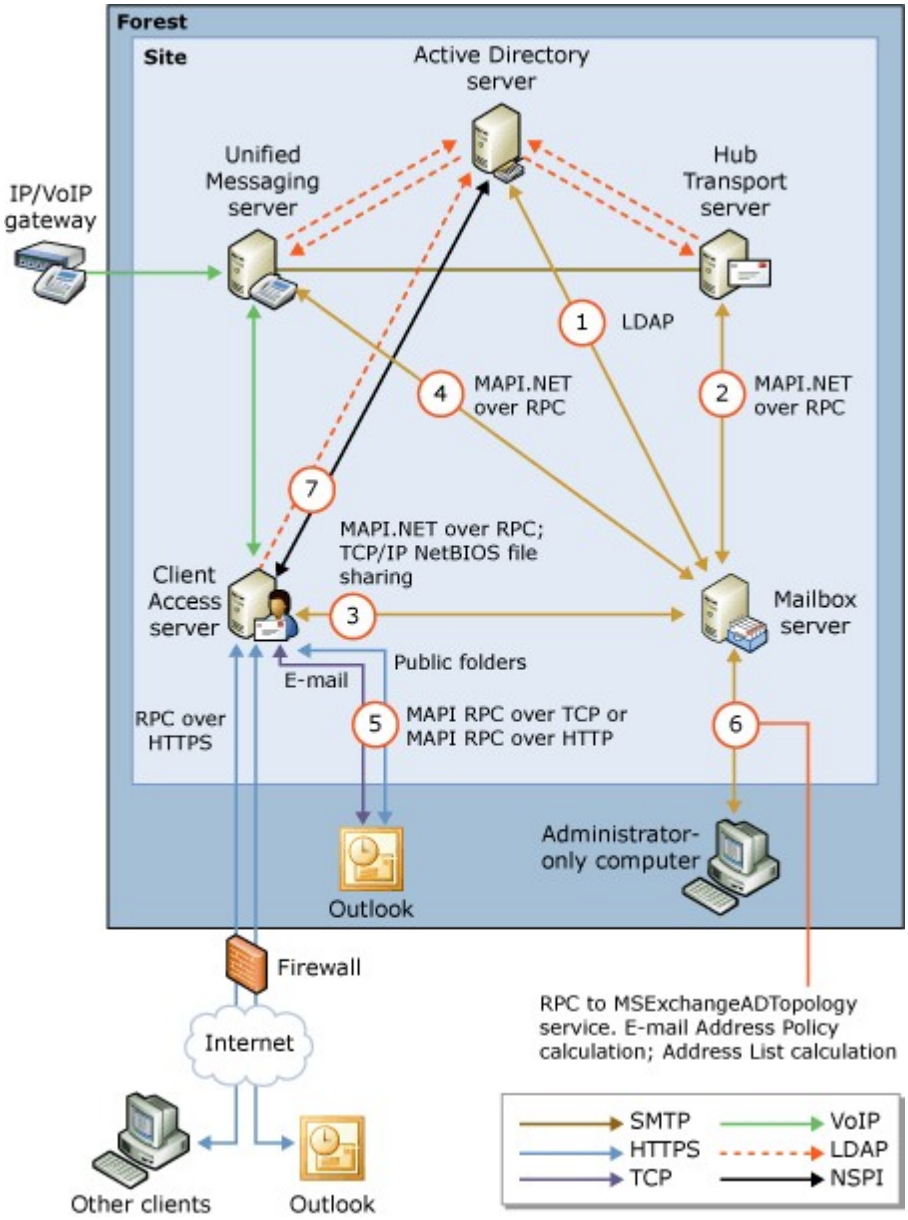
Looking for management tasks related to Mailbox servers? See Managing Mailbox Servers.

Contents

Mailbox Server Interactions

The Mailbox server must interact directly with the following:

- Active Directory
- Client Access server
- Hub Transport server
- Unified Messaging server
- Microsoft Outlook clients



The following process applies:

1. The Mailbox server uses LDAP to access recipient, server, and organization configuration information from Active Directory.
2. The store driver on the Hub Transport server places messages from the transport pipeline into the appropriate mailbox. The store driver on the Hub Transport server also adds messages from a sender's Outbox on the Mailbox server to the transport pipeline. To learn more about the store driver, see Understanding Moderated Transport.
3. The Client Access server sends requests from clients to the Mailbox server, and returns data from the Mailbox server to the clients. The Client Access server also accesses OAB files on the Mailbox server through NetBIOS file sharing. The types of data that the Client Access server sends between the client and the Mailbox server include messages, free/busy data, client profile settings, and OAB data.
4. The Unified Messaging server retrieves e-mail, voice mail messages, and calendar information from the Mailbox server for Outlook Voice Access. The

Unified Messaging server also retrieves storage quota information from the Mailbox server. To learn more about Outlook Voice Access, see Understanding Outlook Voice Access.

5. Outlook clients inside your firewall access the Client Access server to send and retrieve messages. Outlook clients outside the firewall can access the Client Access server by using Outlook Anywhere (which uses RPC over HTTP). However, Outlook clients that are viewing or modifying public folders access the Client Access server by using RPC over TCP. To learn more about Outlook Anywhere, see Understanding Outlook Anywhere.
6. The administrator-only computer retrieves Active Directory topology information from the Microsoft Exchange Active Directory Topology service. It also retrieves e-mail address policy information and address list information.
7. The Client Access server uses LDAP or Name Service Provider Interface (NSPI) to contact the Active Directory server and retrieve users' Active Directory information.

Return to top

Coexisting with Other Server Roles

The Client Access server role, Hub Transport server role, Mailbox server role, and Unified Messaging server role can coexist on the same computer in any combination. When considering what combination of server roles to deploy, you should base your decision on capacity and performance planning and on your security and availability requirements. For more information, see Mailbox Server Storage Design.

Return to top

Server Role Configuration

To configure the Mailbox server role, use the Set-MailboxServer cmdlet in the Exchange Management Shell. To retrieve Mailbox server role settings, use the Get-MailboxServer cmdlet. For more information, see Configure Mailbox Server Properties.

Return to top

Services and Port Executables

When you install the Exchange 2010 Mailbox server role on a computer running Windows Server 2008, the services and port executables shown in the following table are installed. The Microsoft Search (Exchange Server) and Microsoft Exchange Monitoring services are set to start manually. All other services are set to start automatically.

Services

Service short name	Service name	Associated executable	Port name
MSExchangeIS	Microsoft Exchange Information Store	Store.exe	MSExchangeISPorts
MSExchangeADTopology	Microsoft Exchange Active Directory Topology	MSExchangeADTopologyService.exe	MSExchangeADTopologyPorts
MSExchangeMailboxAssistants	Microsoft Exchange Mailbox Assistants	MSExchangeMailboxAssistants.exe	MSExchangeMailboxAssistantsPorts

MSExchangeSearch	Microsoft Exchange Search Indexer	Microsoft.Exchange.Search.ExSearch.exe	MSExchangeSearchPorts
MSExchangeServiceHost	Microsoft Exchange Service Host	Microsoft.Exchange.ServiceHost.exe	MSExchangeServiceHostPorts
MSExchangeMonitoring	Microsoft Exchange Monitoring	Microsoft.Exchange.Monitoring.exe	MSExchangeMonitoringPorts
MSExchangeSA	Microsoft Exchange System Attendant	Mad.exe	MSExchangeSAPorts
MSExchangeMailSubmission	Microsoft Exchange Mail Submission	MSExchangeMailSubmission.exe	MSExchangeMailSubmissionPorts
msftesql-Exchange	Microsoft Search (Exchange Server)	Msftesql.exe	msftesql-ExchangePorts
MSExchangeTranport LogSearch	Microsoft Exchange Transport Log Search	MSExchangeTransportLogSearch.exe	MSExchangeTransportLogSearchPorts

Return to top

Planning for Public Folders

Before you deploy public folders, it's important to familiarize yourself with the functionality that public folders provide to make sure that the public folders meet the needs of your organization.

Exchange public folders are intended to serve as a repository for information that's shared among many users. You should use public folders when your business requires data replication to multiple servers. Access to public folders is integrated with regular mailbox access through the MAPI protocol. For more information about public folders, see Understanding Public Folders and Managing Public Folders.

Return to top

1.8.1.2 Understanding Address Lists

Understanding Address Lists

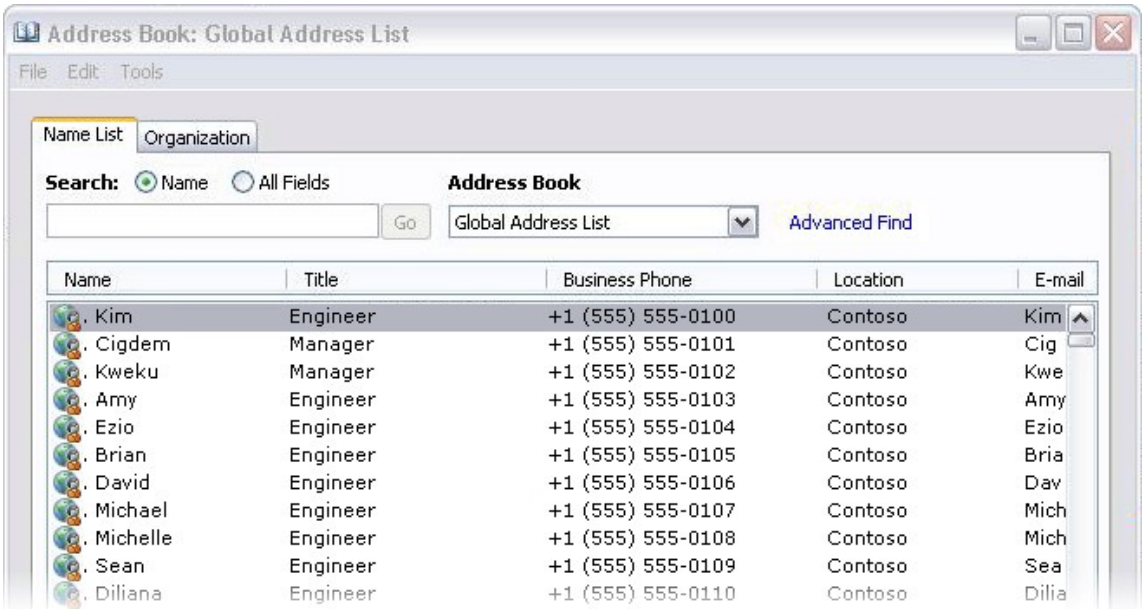
Exchange Server 2010 > Mailbox > Understanding Mailbox >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-01*

An *address list* is a collection of recipient and other Active Directory objects. Each address list can contain one or more types of objects (for example, users, contacts, groups, public folders, conferencing, and other resources). You can use address lists to organize recipients and resources, making it easier to find the recipients and resources you want. Address lists are updated dynamically. Therefore, when new recipients are added to your organization, they're automatically added to the appropriate address lists.

As shown in the following figure, client applications, such as Microsoft Outlook, display the available address lists that Exchange provides.



Address lists reside in Active Directory. Therefore, mobile users who are disconnected from the network are also disconnected from these server-side address lists. However, you can create offline address books (OABs) for users who are disconnected from the network. These OABs can be downloaded to a user's hard disk. Frequently, to conserve resources, OABs are subsets of the information in the actual address lists that reside on your servers. For more information, see Understanding Offline Address Books.

Looking for management tasks related to managing Mailbox servers? See Managing Mailbox Servers.

Contents

Changes to Address Lists in Exchange 2010 SP2

Global address list (GAL) segmentation (also known as GAL segregation) is the process whereby you segment users into specific groups to provide customized views of your organization's GAL. In Exchange Server 2007 and earlier, segmenting the GAL was complicated, requiring you to use either a Query Base DN (which acted as a root for directory searches) or access control lists (ACLs) to allow or deny access to each address list.

To simplify the process, Exchange 2010 Service Pack 2 (SP2) introduces address book policies (ABPs). When creating an ABP, you assign a GAL, an offline address book (OAB), a room list, and one or more address lists to the policy. You can then assign the ABP to mailbox users, providing them with access to a customized GAL in Outlook and Outlook Web App. The goal is to provide a simpler mechanism to accomplish GAL segmentation for on-premises organizations that require multiple GALs.

To learn more about ABPs, see Understanding Address Book Policies.

Default Address Lists

When users want to use their client application to find recipient information, they can select from available address lists. Several address lists, such as the global address list (GAL), are created by default. Exchange contains the following default address lists, which are then automatically populated with new users, contacts, groups, or rooms as they're added to your organization:

- **All Contacts** This address list contains all mail-enabled contacts in your organization. Mail-enabled contacts are those recipients who have an external e-mail address. If you want mail-enabled contact information to be available to all users in your organization, you must include the contact in the GAL. To learn more about mail contacts, see Understanding Recipients.
- **All Groups** This address list contains all mail-enabled groups in your organization. Mail-enabled groups are groups of recipients that are created to expedite the mass sending of e-mail messages and other information. When an e-mail message is sent to a mail-enabled group, all members of that list receive a copy of the message. To learn more about mail-enabled groups, see Understanding Recipients.
- **All Rooms** This address list contains all resources that have been designated as a room in your organization. Rooms are resources in your organization that can be scheduled by sending a meeting request from a client application. The user account that's associated with a room is disabled. For instructions about how to add resource mailboxes to an address list, see Add Resource Mailboxes to an Address List. To learn more about resource mailboxes, see Understanding Recipients.
- **All Users** This address list contains all mail-enabled users in your organization. A mail-enabled user represents a user outside your Exchange organization. Each mail-enabled user has an external e-mail address. All messages sent to mail-enabled users are routed to this external e-mail address. A mail-enabled user is similar to a mail contact, except that a mail-enabled user has Active Directory logon credentials and can access resources. To learn more about mail-enabled users, see Understanding Recipients.
- **Default Global Address List** This address list contains all mail-enabled users, contacts, groups, or rooms in the organization. During setup, Exchange creates various default address lists. The most familiar address list is the GAL. By default, the GAL contains all recipients in an Exchange organization. In other words, any mailbox-enabled or mail-enabled object in an Active Directory forest that has Exchange installed is listed in the GAL. For ease of use, the GAL is organized by name, not by e-mail address. For more information, see Managing Address Lists.
- **Public Folders** This address list contains all public folders in your organization. Access permissions determine who can view and use the folders. Public folders are stored on computers running Exchange. For more information about public folders, see Managing Public Folders.

Custom Address Lists

An Exchange organization can contain thousands of recipients. If you compile all your recipients in the default address lists, those lists could become quite large. To prevent this, you can create custom address lists to help users in your organization find what they are looking for more easily.

For example, consider a company that has two large divisions and one Exchange organization. One division, named Fourth Coffee, imports and sells coffee beans. The other division, Contoso, Ltd, underwrites insurance policies. For most day-to-day

activities, the employees at Fourth Coffee don't communicate with the employees at Contoso, Ltd. Therefore, to make it easier for employees to find recipients who exist only in their division, you can create two new custom address lists—one for Fourth Coffee and one for Contoso, Ltd. When searching for recipients in their division, these custom address lists allow employees to select only the address list that's specific to their division. However, if an employee is unsure about the division in which the recipient exists, the employee can search within the GAL, which contains all recipients in both divisions.

You can also create subcategories of address lists called hierarchical address lists. For example, you can create an address list that contains all recipients in Manchester and another that contains all recipients in Stuttgart.

Best Practices for Creating Address Lists

Although address lists are useful tools for users, poorly planned address lists can cause frustration. To make sure that your address lists are practical for users, consider the following best practices:

- Avoid creating so many address lists that users won't be sure which list to search for recipients.
- Name your address lists in such a way that, when users glance at them, they will know immediately which recipient types are contained in the list. If you have difficulty naming your address lists, create fewer lists and remind users that they can find anyone in your organization by using the GAL.

For detailed instructions about creating an address list, see Create an Address List.

1.8.1.3 Understanding Address Book Policies

Understanding Address Book Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-28*

Global address list (GAL) segmentation (also known as GAL segregation) is the process whereby administrators can segment users into specific groups to provide customized views of their organization's GAL. In Microsoft Exchange Server 2007 and earlier versions, segmenting the GAL was complicated and required that you use either a Query Base DN (which acted as a root for directory searches) or access control lists (ACLs) to allow or deny access to each address list. To learn more about how to configure GAL segmentation in Exchange 2007, see Configuring Virtual Organizations and Address List Segregation in Exchange 2007.

To simplify the process, Microsoft Exchange Server 2010 Service Pack 2 (SP2) introduces address book policies (ABPs). When creating an ABP, you assign a GAL, an offline address book (OAB), a room list, and one or more address lists to the policy. You can then assign the ABP to mailbox users, providing them with access to a customized GAL in Outlook and Outlook Web App. The goal is to provide a simpler mechanism to accomplish GAL segmentation for on-premises organizations that require multiple GALs.

Note:

ABPs are intended to optimize the GAL for each group of users, not make it impossible for them to see each other or to resolve other users in your organization. ABPs create only a

virtual separation of users, not a legal separation.

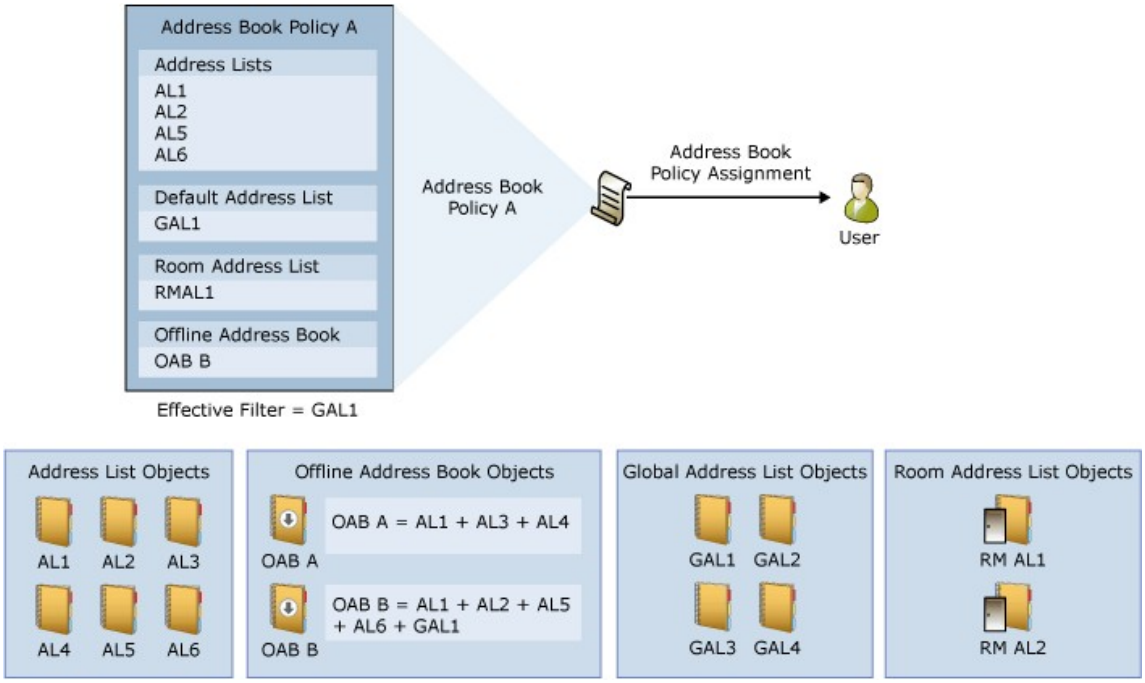
Important:
ABPs aren't available in Office 365. As a result, if you're in a hybrid deployment, the entire address book will be visible to your users with cloud-based mailboxes.

How ABPs Work

ABPs contain the following lists:

- One GAL
- One OAB
- One room list (for booking purposes)
- One or more address lists

In the following figure, Address Book Policy A consists of a subset of the various address objects that exist in the organization (shown in the bottom half of the figure). The resulting scope of an ABP is equal to that of the GAL contained in the policy, in this case GAL1. When the ABP is created and assigned to a user, the address objects in the ABP become the scope of the objects the user is able to view.



You can use the following methods to assign ABPs to individual mailbox users:

New or existing mailbox?	Shell	Exchange Management Console
New	**New-Mailbox** cmdlet with the *AddressBookPolicy* parameter	**Mailbox Settings** tab in the New Mailbox wizard
Existing	**Set-Mailbox** cmdlet with the *AddressBookPolicy* parameter	**Mailbox Settings** tab in the mailbox's property page

ABPs take effect when a user's client application connects to the Microsoft Exchange Address Book service on the Client Access server. If you change the ABP, the updated ABP doesn't take effect until the user restarts Outlook Outlook Web Access, or until you

restart the Microsoft Exchange Address Book service. To learn more, see Understanding the Address Book Service.

Entourage, Outlook for Mac, and ABPs

ABPs won't function for Entourage users or Outlook for Mac users who are connected to their corporate network. When inside the corporate network, Entourage and Outlook for Mac clients connect directly to the global catalog server and query Active Directory directly instead of using the Microsoft Exchange Address Book service. However, Outlook for Mac 2011 clients that connect from the Internet can use an OAB or Exchange Web Services (EWS). As a result, these clients can view the GAL based on the assigned ABP. To learn more about administering Outlook for Mac 2011, see Planning for Outlook for Mac 2011

Deploying ABPs

This section provides information about deploying ABPs in your organization, including best practices, scenarios, and general steps. To review all ABP management tasks, see Managing Address Book Policies.

Considerations and Best Practices

Consider the following when setting up ABPs in your organization:

- For ABPs to work correctly, the user mailbox to which you apply the ABP must be on a Microsoft Exchange Server 2010 SP2 server.
- Don't run the Client Access server role on the global catalog server. Doing so results in Active Directory being used for Name Service Provider Interface (NSPI) instead of the Microsoft Exchange Address Book service.
- You can't use hierarchical address books (HABs) and ABPs at the same time. To learn more about HABs, see Understanding Hierarchical Address Books.
- Any user assigned an ABP should exist in their own GAL.
- If you allow client applications to access Active Directory directly through LDAP, they will bypass the logic built into ABPs. Because Outlook 2011 and Entourage 2008 use direct LDAP queries to access, Active Directory those client applications won't function properly with ABPs if a domain controller or global catalog server is specified or provided to them by the Autodiscover service. Outlook 2011 can use EWS or a local OAB to access directory information. However, if Outlook 2011 can directly access an LDAP service, it will try to do so.
- The GAL used in an ABP must, at a minimum, contain all of the address lists, including the room address list, defined and specified in an ABP. Don't create a GAL that contains fewer objects than any of the address lists in the same ABP.
- We recommend creating distribution groups that don't cross virtual organization boundaries. Creating distribution groups that contain members of multiple virtual organizations results in the following issues:
  - If group members request delivery or read receipts when sending mail to the distribution group, they'll be able to see the e-mail addresses of the group members in other virtual organizations
  - If an encrypted message is sent to the distribution group and some group members don't have valid digital IDs, the sender will receive a warning message that includes the total number of members who don't have valid IDs and a list of their e-mail addresses. However, if some of those members without valid digital IDs are in a different organization than the sender, the warning message will include the correct count but won't include the e-mail addresses of the members in the other organization. As a result, the total count won't match the list of member addresses.

    For example, let's say a distribution group contains five members total from two organizations, Agency A and Agency B. Three group members are from Agency A, and one of those members

has as invalid digital ID. The other two members are from Agency B, and both of them have invalid digital IDs. If a member from Agency A sends an encrypted message to the distribution group, that member will receive a warning message stating that there are a total of three recipients without valid digital IDs. However, only the e-mail address for the recipient from Agency A will be listed in the warning message.

- ABP's don't apply to the Get-Group cmdlets. Therefore, any user or process that is able to run **Get-Group** will see all members of any group they have access to.

  We recommend that you modify the group management settings of the Exchange Control Panel (ECP) so users can't use ECP to manage groups. To prevent users from using ECP to manage groups, exclude the users from the MyDistributionGroupMembership RBAC role. For details see MyDistributionGroupMembership Role and Turn Off User's Ability to Create Distribution Groups.

- If you allow users to use Outlook or Outlook Web App to manage groups, the group owners must have full visibility to the group membership list.

- All ABPs must contain a room address list. However, if your organization doesn't use room address lists, you can create a default empty room address list.
- Deploying ABPs doesn't prevent users in one virtual organization from sending e-mail to users in another virtual organization. If you want to prevent users from sending e-mail across organizations, we recommend that you create a transport rule. For example, to create a transport rule that prevents Contoso users from receiving messages from Fabrikam users, but still allows Fabrikam's senior leadership team to send messages to Contoso users, run the following Shell command:

```
New-TransportRule -Name "StopFabrikamtoContosoMail" -FromMemberOf "AllF
```

  To learn more, see Create a Transport Rule.
- If you want to enforce the ABP in the Lync client, you can set the `msRTCSIP-GroupingID` attribute on specific user objects. For details, see PartitionByOU Replaced with msRTCSIP-GroupingID topic.

Deployment Scenarios

The following three scenarios describe possible deployment solutions for three different organization types. Although there are many more scenarios, the most common ones are covered here. The address lists and GALs in these scenarios were created based on filters, such as Custom Attributes, that grouped the objects logically.

Scenario 1: Two Separate Companies - One Exchange Organization

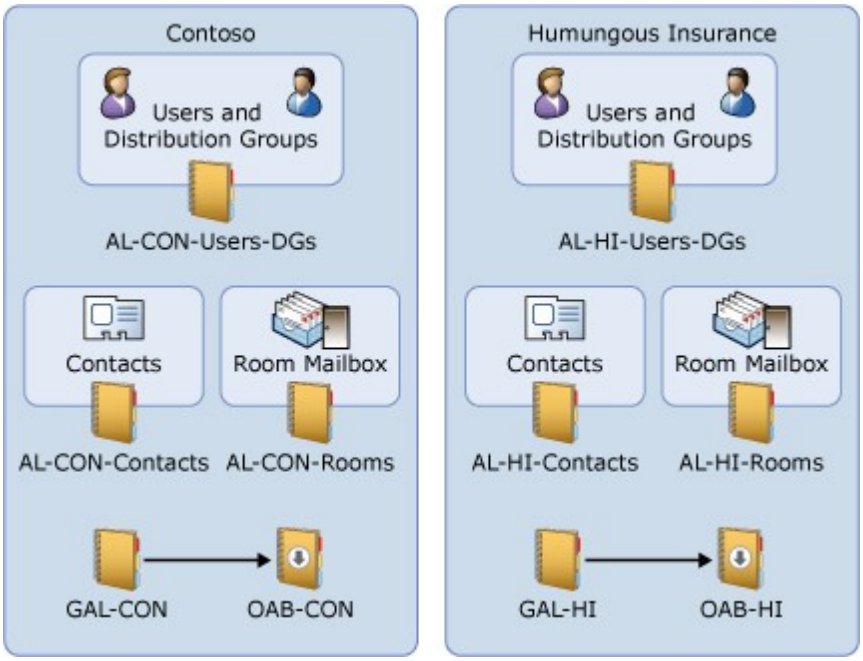
This scenario is applicable to companies that have separate agencies, divisions, or departments that are:

- Within the same Exchange organization.
- Don't share employees.
- Don't share a common reporting chain.

In addition, the agencies, divisions, or departments don't have any special security or privacy concerns.

In this scenario, two ABPs are created with the following settings:

- Employees who view the GAL or distribution group membership can see only recipients within their company.
- There are no distribution groups that span across both companies.



The following table lists the address lists, GALs, room lists, and OABs that are included in the ABPs for Contoso and Humongous Insurance. The ABP components were created by using the *CustomAttribute15* parameter to group the objects. Because the two companies are separate without any interaction between them, they don't share any address lists.

ABP component	Contoso	Humongous Insurance
Address lists	AL_CON_Groups AL_CON_Users_DGs AL_CON_Contacts	AL_HI_Groups AL_HI_Users_DGs AL_HI_Contacts
GAL	GAL_CON	GAL_HI
Room list	AL_CON_Rooms	AL_HI_Rooms
OAB	OAB_CON	OAB_HI

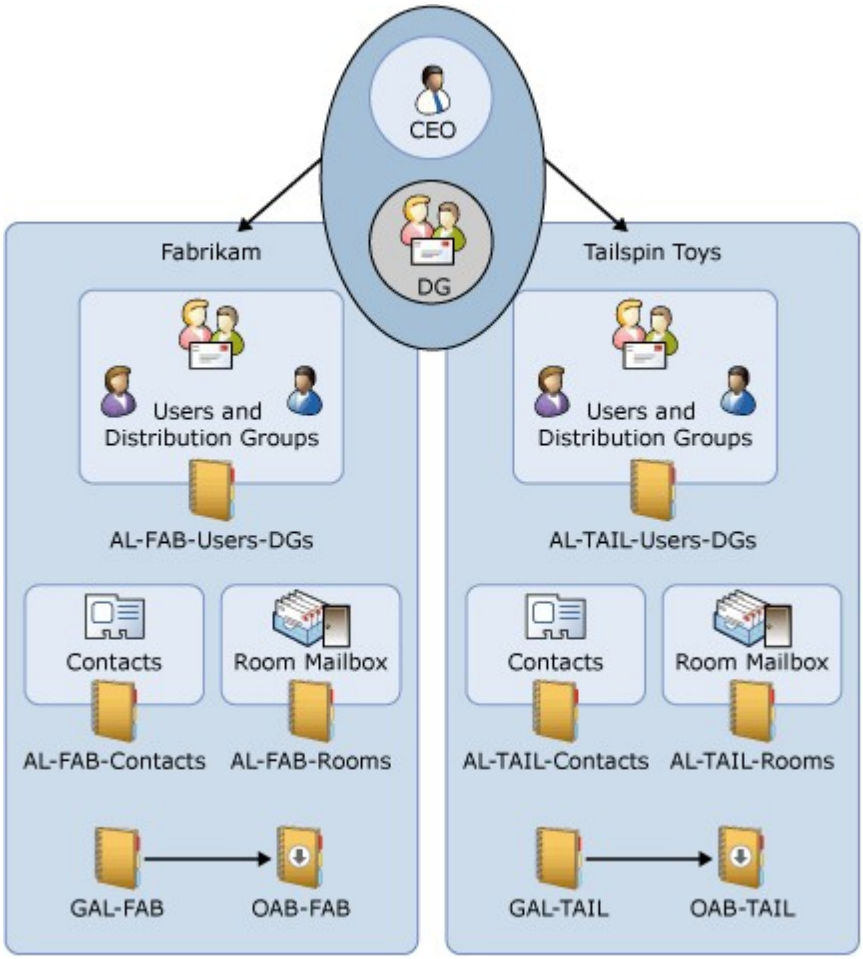
Scenario 2: Two Companies Sharing a CEO

This scenario is applicable to companies that are:

- Within the same Exchange organization.
- Share the same CEO.
- Don't share employees.

In this scenario, three ABPs are created with the following settings:

- Employees who view the GAL or distribution group membership can see only recipients within their company.
- In each company, there is a distribution group named SeniorLeaders, which includes the senior leaders of that company and the shared CEO.
- Employees who view the CEO's group membership can see only groups within their company.
- Three ABPs are created: Fabrikam, Tailspin Toys, and CEO.



ABP component	Fabrikam	Tailspin Toys	CEO
Address lists	AL_FAB_Users_DGs AL_FAB_Contacts	AL_TAIL_Users_DGs AL_TAIL_Contacts	AL_FAB_Users_DGs AL_FAB_Contacts AL_TAIL_Users_DGs AL_TAIL_Contacts
GAL	GAL_FAB	GAL_TAIL	Default GAL
Room list	AL_FAB_Rooms	AL_TAIL_Rooms	Default All Rooms
OAB	OAB_FAB	OAB_TAIL	Default OAB

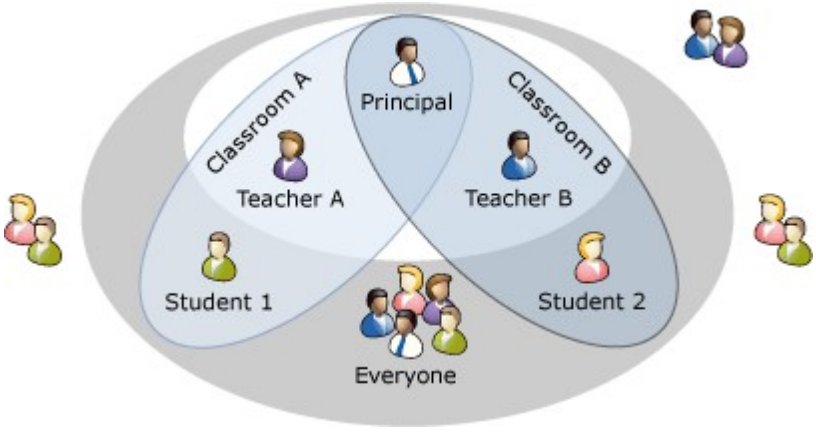
When the CEO is added to the distribution groups in each company and falls within the scope of each company's ABP, the CEO becomes visible to each company. The CEO is visible in both the Fabrikam and Tailspin Toys GALs and can create distribution groups that span both companies. However members of the distribution group can view only members that are within their own company.

Scenario 3: Education

This scenario is applicable to schools or universities where a division of classrooms is necessary to ensure the privacy of the students.

In this scenario, ABPs are created with the following settings:

- Students can view only other students in their classroom, their teacher, and the principal.
- Teachers can view only students in their classroom, all teachers, and the principal.
- Distribution groups are created for each classroom's parents and the faculty.



	Students_ClassA	Teachers_ClassA	Principal
Address Lists	AL_ClassA AL_Principal	AL_ClassA AL_AllTeachers AL_AllGroups AL_Principal	AL_ClassA AL_ClassB AL_AllTeachers AL_AllStudents AL_AllGroups
Global address list	GAL_StudentsClassA	GAL_TeachersClassA	GAL_Everyone
Room address list	AL_BlankRoom	AL_BlankRoom	Default All Rooms
Offline address book	OAB_StudentsClassA	OAB_TeachersClassA	Default OAB

General Deployment Steps

This section provides the general steps for deploying ABPs in your organization, including how to migrate from Exchange 2007 address list segmentation.

Migrating from Address List Segmentation to ABPs

If you're currently using Exchange 2007 address list segmentation (per the instructions in the white paper Configuring Virtual Organizations and Address List Segregation in Exchange 2007) and you want to migrate to ABPs, follow the steps outlined in Migrate to Exchange 2010 Address Book Policies from Exchange 2007 Address List Segregation. This procedure requires some downtime for your organization so be sure plan accordingly.

New Deployment of ABPs

If you aren't using Exchange 2007 address list segmentation, follow the steps listed in this section to deploy ABPs in your organization.

The following steps apply to Scenario 2: Two Companies Sharing a CEO. In this scenario, Fabrikam and Tailspin Toys are separate companies that share a CEO and senior leadership team. This scenario requires three ABPs:

- ABP_FAB
- ABP_TAIL

- ABP_CEO

Step 1: Divide your virtual organizations
You'll need to develop a way to divide your organization into virtual organizations. When making this division, we recommend using the Custom Attribute properties on the mailboxes, contacts, and groups instead of the precanned conditional attributes (such as **Company**, **Department**, or **State/Province**). Using Custom Attributes instead of precanned attributes includes the following benefits:

- Not all recipient types have precanned conditional attributes in Active Directory. For example, the Active Directory objects **Distribution Group** and **Dynamic Distribution Group** don't support the **Company**, **Department**, or **State/Province** attributes.
- Not all precanned conditional attributes are exposed in cmdlets for some recipients. For example, the *Company*, *Department*, and *StateOrProvince* parameters aren't available in the cmdlets for mail users, contacts, distribution groups, and mail-enabled public folders.
- Multiple cmdlets are required to segment recipients when you use precanned conditional attributes. For example, to set the *Company*, *Department*, or *StateOrProvince* parameters for a user mailbox, you must run the **Set-User** cmdlet after you run the **New-Mailbox** or **Set-Mailbox** cmdlets. However, the *CustomAttribute* parameters are exposed in the **Set-*** cmdlets for each recipient type, so there's no need to also run the **Set-User** cmdlet.
- Custom Attribute properties are explicitly reserved to customize an organization and are controlled entirely by organization administrators.

To learn more about custom attributes, see Understanding Custom Attributes.

Another best practice to consider when dividing your organization is to use company identifiers in the names of distribution groups and dynamic distribution groups. One method for doing this is to use group naming policies. These policies allow you to specify that a prefix, a suffix, or both be applied to distribution group names. This is helpful when dividing your organization because you can use these policies to specify a suffix or prefix based on user attributes such as the creator of the distribution group's **Company**, **State/Province**, **Department**, and Custom Attribute properties. This is especially important if you allow users to create their own distribution groups. For more information, see Create a Distribution Group Naming Policy.

Note:
Because group naming policies don't apply to dynamic distribution groups, you must manually apply a naming policy.

Step 2: Create the address lists, room list, GALs, and OABs
When you create the address lists and GALs, don't use the *IncludedRecipient* and *ConditionalX* parameters, such as *ConditionalCompany* and *ConditionalCustomAttribute5*. Instead, we recommend that you use recipient filters. To learn more about recipient filters, see Creating Filters in Recipient Commands.

Note:
All procedure in this section use Shell commands because you can't use the EMC to create recipient filters.

Create the address lists

When you create the ABP, you include multiple address lists based on how you want your users to view the lists in Outlook or Outlook Web App. This scenario requires four address lists:

- AL_FAB_Users_DGs
- AL_FAB_Contacts
- AL_TAIL_Users_DGs
- AL_TAIL_Contacts

This example creates the address list AL_TAIL_Users_DGs. The address list contains all users and distribution groups where *CustomAttribute15* equals `TAIL`.

```
New-AddressList -Name "AL_TAIL_Users_DGs" -RecipientFilter {((RecipientType -eq '
```

The above command would then be run to create the remaining address lists: AL_FAB_Users_DGs, AL_FAB_Contacts, and AL_TAIL_Contacts.

For detailed syntax and parameter information, see New-AddressList.

To learn more about creating address lists by using recipient filters, see Create an Address List By Using Recipient Filters.

Create the room lists

This scenario requires three room lists:

- AL_FAB_Rooms
- AL_TAIL_Rooms
- Default All Rooms (created by default)

ABPs must contain a room list. If your organization doesn't have resource mailboxes (such as room or equipment mailboxes), we recommend that you create a blank room list. The following example creates the blank room list AL_BlankRoom.

```
New-AddressList -Name AL_BlankRoom -RecipientFilter ((Alias -ne $null) -and ((Rec
```

However, in this scenario, Fabrikam and Tailspin Toys both have room mailboxes. This example creates the room list for Tailspin Toys by using a recipient filter where *CustomAttribute15* equals `TAIL`.

```
New-AddressList -Name AL_TAIL_Rooms -RecipientFilter {(Alias -ne $null) -and (Cus
```

The above command would then be run to create the room list for Fabrikam (AL_FAB_Rooms).

For detailed syntax and parameter information, see New-AddressList.

Create the GALs

This scenario requires three GALs:

- GAL_FAB
- GAL_TAIL
- Default GAL (created by default)

The GAL used in an ABP must be a superset of the address lists. Don’t create a GAL with fewer objects than exists in any or all of the address lists in the ABP.

This example creates the GAL for Tailspin Toys. It includes all the recipients that exist in the address lists and room list.

```
New-GlobalAddressList -Name "GAL_TAIL" -RecipientFilter {(CustomAttribute15 -eq "
```

The above command would then be run to create the GAL for Fabrikam (GAL_FAB).

For detailed syntax and parameter information, see New-GlobalAddressList.

Create the OABs

This scenario requires three GALs:

- OAB_FAB

- OAB_TAIL
- Default OAB (created by default)

When using the **New-OfflineAddressBook** or **Set-OfflineAddressBook** to create the OAB, include the appropriate address lists or GAL in the *AddressLists* parameter to make sure no entry is unexpectedly missed. For example, if you want to customize the set of lists a user will see when viewing the OAB, or if you simply want to reduce the OAB's download size, you can use the *AddressLists* parameter to specify the address lists available to the OAB. However, if you want users to see the full set of GAL entries in OAB, make sure you include the GAL in the *AddressLists* parameter.

This example creates the OAB for Tailspin Toys. The entire GAL (GAL_TAIL) is included in the OAB..

```
New-OfflineAddressBook -Name "OAB_TAIL" -AddressLists "GAL_TAIL"
```

The above command would then be run to create the OAB for Fabrikam (OAB_FAB).

For detailed syntax and parameter information, see New-OfflineAddressBook.

Step 3: Create the ABPs
After all the required lists are created, you can create the ABPs.

This example creates the ABP for Tailspin Toys.

```
New-AddressBookPolicy -Name "ABP_TAIL" -AddressLists "AL_TAIL_Users_DGs","AL_TAIL
```

The above command would then be run to create the ABPs for Fabrikam (ABP_FAB) and the organization's CEO (ABP_CEO).

For detailed syntax and parameter information, see New-AddressBookPolicy.

Step 4: Assign the ABPs to mailboxes
Assigning the ABPs to users is the last step in the process. ABPs take effect when a user's application connects to the Microsoft Exchange Address Book service on the Client Access server. Users who are already connected to Outlook or Outlook Web App when the ABP is applied to their account will have to close and then restart the client application before they can see their new address lists and GAL.

This example assigns the address book policy ABP_TAIL to all mailboxes where *CustomAttribute15* equals TAIL.

```
Get-Mailbox -resultsize unlimited | where {$_.CustomAttribute15 -eq "TAIL"}| Set-
```

For more details, see Assign an Address Book Policy to a Mail User.

1.8.1.3.1 Migrate to Exchange 2010 Address Book Policies from Exchange 2007 Address List Segregation

Migrate to Exchange 2010 Address Book Policies from Exchange 2007 Address List Segregation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The instructions in this topic will walk you through the steps required to migrate from Exchange 2007 ACL-based global address list (GAL) segmentation (also known as GAL

segregation) to Exchange 2010 Service Pack 2 (SP2) address book policies (ABPs).

Important:
Several procedures in this topic will impact users. As a result, scheduled downtime is often required.

Prerequisites

- Although not a specific prerequisite, it's highly recommended that you review the considerations and best practices in Understanding Address Book Policies before performing the procedures in this topic.
- The procedures in this topic assume that you followed the steps in the white paper Configuring Virtual Organizations and Address List Segregation in Exchange 2007 to configure your Exchange 2007 organization.
- If you followed the steps in the white paper listed above to implement GAL segmentation in your Exchange 2010 organization, you are officially in an unsupported state. To successfully perform the procedures in this topic, you must first return your organization to a supported state.
- Most of the code and Shell examples in this document use **Contoso** as the Active Directory domain name and the Exchange organization name, and **Fabrikam**, and **Tailspin Toys** as the sub-organization names. Be sure to change the name of the Exchange organization, domain, and sub-organizations to match your configuration.
- You will need the scripts that you used to segment the virtual organizations in Exchange 2007.

Setting Up the Scenario

In this scenario, Tailspin Toys and Fabrikam are subsidiaries of the parent company Contoso.

Step1: Prepare to install Exchange 2010 SP2 in an existing Exchange 2007 organization that has configured GAL segmentation (downtime required)

If your organization is using Exchange 2007 GAL segmentation, installing Exchange 2010 will fail because using GAL segmentation required you to remove all the default settings and permissions from the default GAL.

1. On a domain controller in the Exchange 2007 organization, run the following command at the command prompt to allow access to the default GAL.

```
DSACLS "CN=Default Global Address List,CN=All Global Address Lists,CN=
```

2. On a domain controller that has Windows PowerShell installed or on an Exchange server using the Exchange Management Shell, run the following commands to reconfigure the default settings on the GAL.

Note:
After you complete this step, Outlook 2007 users will be able to see the default GAL. However, Outlook Web App users won't be able to see the default GAL because Outlook Web App uses the `QueryBaseDN` attribute to query the GAL.

```
$container = "CN=Default Global Address List,CN=All Global Address Lis
```

You will receive the following warning and output:

```
WARNING: Appropriate ACE is already present on object "CN=Default Glob
Identity             User                 Deny  Inherited Rights
--------             ----                 ----  --------- ------
\Default Global A... NT AUTHORITY\Auth... False False     Open-Address
\Default Global A... NT AUTHORITY\Auth... False False     ReadProperty
\Default Global A... NT AUTHORITY\Auth... False False     ListObject,
\Default Global A... NT AUTHORITY\Auth... False False     ListChildren
```

Step 2: Install the first Exchange 2010 server

For detailed instructions, see Upgrade from Exchange 2007 Client Access

Step 3: Secure the default GAL

After you install Exchange 2010 SP2, you can remove the address lists that are created during installation and then secure the default GAL again. After you complete this step, you can continue to install additional Exchange 2010 SP2 servers in your organization. For more information, see Understanding Upgrade from Exchange 2007 to Exchange 2010.

1. (Optional) On an Exchange 2010 server, use the Shell to remove the newly created address lists.

```
Remove-AddressList "All Contacts"
Remove-AddressList "All Groups"
Remove-AddressList "All Users"
Remove-AddressList "Public Folders"
```

   For more detail, see Remove an Address List.

2. On an Exchange 2010 server, use the Shell to secure the GAL based on the instructions in the white paper Configuring Virtual Organizations and Address List Segregation in Exchange 2007.

```
Get-GlobalAddressList "Default Global Address List" | Add-ADPermission
```

3. To verify that the commands were successful, run the following commands.

```
$galContainer = "CN=All Global Address Lists,CN=Address Lists Containe
Get-ADPermission $galContainer -user "authenticated users"
```

   The output of this command should resemble the following:

```
Identity             User                 Deny  Inherited Rights
--------             ----                 ----  --------- ------
All Global Addres... NT AUTHORITY\Auth... False False     GenericRead
All Global Addres... NT AUTHORITY\Auth... False False     Open-Address
All Global Addres... NT AUTHORITY\Auth... False True      ListChildren
All Global Addres... NT AUTHORITY\Auth... True  True      ReadProperty
```

Step 4: Switchover to Exchange 2010 servers (downtime required)

Before moving any mailboxes to Exchange 2010 SP2 servers, you must switchover external URL names. This requires configuring Outlook Anywhere, Outlook Web App, Exchange Web Services (EWS), Exchange Control Panel (ECP), AutoDiscover, and offline address books (OABs) to use Exchange 2010 servers instead of Exchange 2007 servers. There are many steps in this process, and you should refer to the information in Exchange 2007 - Planning Roadmap for Upgrade and Coexistence for more detail.

Note:

The following steps outline only the key procedures in the overall process and explain what each of them accomplishes. You may need to run some of these commands on each

server in your organization (some only once), and most will result in some period of downtime. Therefore, it's strongly recommended that you spend adequate time testing your entire switchover process to ensure minimal impact to your clients.

1. Use the Shell to move all OAB generation to an Exchange 2010 Mailbox server. Moving the OAB generation to Exchange 2010 SP2 servers allows OABs to use GALs and not just address lists as sources for the OAB content.

```
Get-OfflineAddressBook | Move-OfflineAddressBook -Server "MBX01_Ex2010
```

   For more detail, see Move the Offline Address Book Generation to Another Server.
2. Set the virtual directory for the OAB to include an Exchange 2010 virtual organization. This will distribute copies of the OABs to the Exchange 2010 servers.
   This example ensures both the Exchange 2007 and Exchange 2010 servers have copies of all OABs.

```
Get-OfflineAddressBook | Set-OfflineAddressBook -virtualdirectories "C
```

   For more detail, see Configure Offline Address Book Distribution Properties.
3. Before any mailboxes can be moved to Exchange 2010, you must route all incoming Outlook Anywhere traffic through Exchange 2010.
   This example enables Outlook Anywhere on an Exchange 2010 server and disables it on an Exchange 2007 server.

```
Enable-OutlookAnywhere -Server:CAS1_Ex2010SP2 -ExternalHostname:mail.c
Disable-OutlookAnywhere  -Server:CAS1_Ex2007
```

   For more detail, see the following topics:
   - Enable Outlook Anywhere
   - Disable Outlook Anywhere
4. To allow AutoDiscover to properly return URLs from Exchange 2010 servers, you must configure Outlook Web App, Exchange ActiveSync, EWS, and ECP on all Exchange 2010 servers to have valid external URL properties for the virtual directories.
   The following examples assume that mail.contoso.com is the external name used to access the Exchange 2010 servers.

```
Set-ActiveSyncVirtualDirectory -Identity 'CAS1_Ex2010SP2\Microsoft-Ser
Set-WebServicesVirtualDirectory  -Identity 'CAS1_Ex2010SP2\EWS*' -Exte
Set-OWAVirtualDirectory -Identity 'CAS1_Ex2010SP2\OWA*' -ExternalURL h
Set-EcpVirtualDirectory -Identity 'CAS1_Ex2010SP2\ECP*' -ExternalURL h
```

   For more detail about how to configure the above settings, see the following topics:
   - Configure Exchange ActiveSync Autodiscover Settings
   - Configure Exchange Services for the Autodiscover Service
   - View or Configure Outlook Web App Virtual Directories
   - Configure ECP Virtual Directory Properties
5. To allow Exchange 2010 to redirect Outlook Web App and EWS requests back to Exchange 2007 for those users with mailboxes on Exchange 2007 servers, you need to configure the Outlook Web App and EWS external URL for 2007 to use legacy.contoso.com. This namespace is the external name used to access the Exchange 2007 servers.

```
Set-WebServicesVirtualDirectory -Identity 'CAS1_Ex2007\EWS*' -External
Set-OWAVirtualDirectory -Identity 'CAS1_Ex2007\OWA*' -ExternalURL http
```

6. To allow Exchange 2010 to proxy all incoming Exchange ActiveSync connections to Exchange 2007, clear the 2007 external URL for Exchange ActiveSync.

```
Set-ActiveSyncVirtualDirectory -Identity 'CAS1_Ex2007\Microsoft-Server
```

7. The final step in the process is to change the public DNS so that mail.contoso.com (in the example we provided) and autodiscover.contoso.com resolve to Exchange 2010, and the legacy.contoso.com DNS record resolves to Exchange 2007. All client

connections will go through Exchange 2010, and then Exchange 2010 will either redirect (in the case of Outlook Web App), proxy (in the case of Exchange ActiveSync), or provide version-specific URLs (in the case of EWS) to clients via AutoDiscover.

Step 5: Create ABPs that mirror the Exchange 2007 address list segmentation ACLs

The next step is to figure out what address lists, GALs, and OABs the virtual organizations have access to using GAL segmentation, and then create an ABP for each virtual organization that mirrors them.

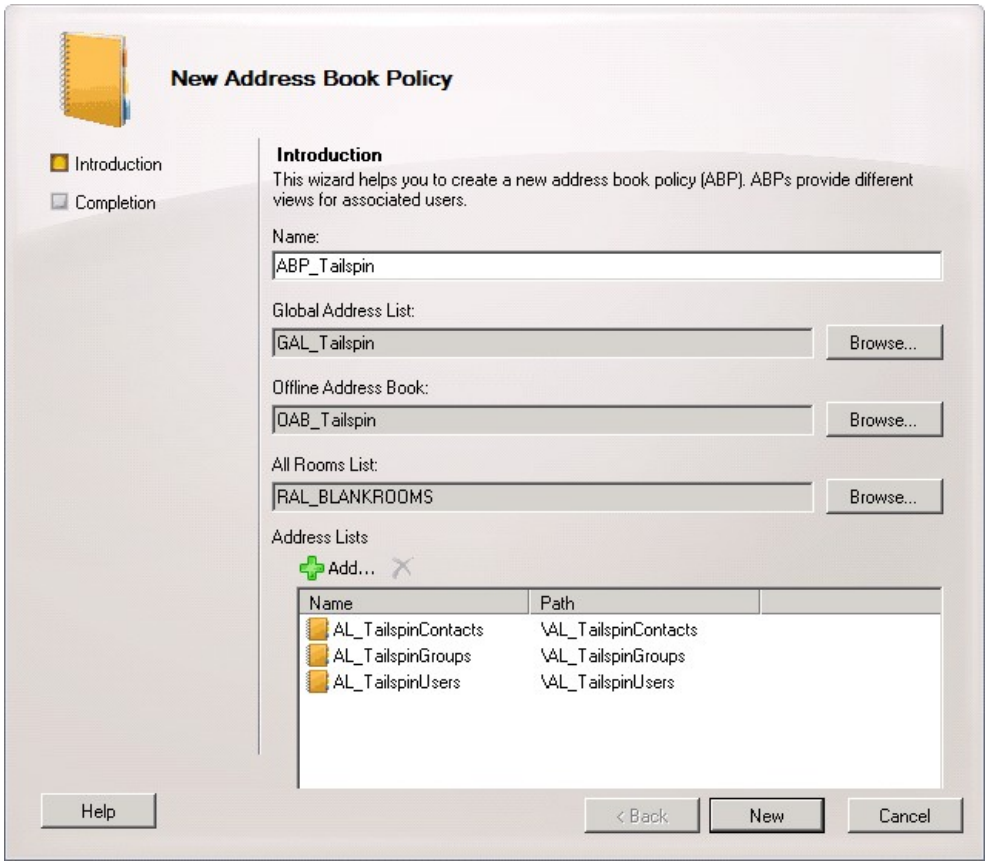
1. If you used the steps in Configuring Virtual Organizations and Address List Segregation in Exchange 2007 to set up your Exchange 2007 organization, you created scripts that segmented your virtual organizations. View those scripts that you used to create the virtual organizations in Exchange 2007 to determine the GAL, address lists, and OAB for each virtual organization. For each virtual organization, you should find one GAL, at least one address list, and one OAB.

   Note:
   ABPs must have a room list. If you don't use room lists in your organization, create a blank room address list and then use that address list when configuring the ABP or set the room list property in the ABP to use the same address list you specify for the GAL.

   For example, when viewing the script used to segment the child company Tailspin Toys, the following information is located:
   - Tailspin Toys users are all contained in a security group called Tailspin_SG.
   - The security group Tailspin_SG grants users read/open access to the following:

Address Lists	GAL	OAB
AL_TailspinUsers AL_TailspinGroups AL_TailspingContacts	GAL_Tailspin	OAB_Tailspin

   - Tailspin Toys doesn't have a room address list.
2. Create an ABP that matches the Tailspin Toys organization.
3. For example, if you use the Exchange Management Console to create the ABP in, input the following information in the New Address Book Policy wizard:



If you use the Shell to create the ABP, run the following command.

```
New-AddressBookPolicy -Name 'ABP_Tailspin' -GlobalAddressList '\GAL_Ta
```

For more detail, see Create an Address Book Policy.

4. Follow the above instructions for each of your virtual organizations. For example, Fabrikam.

Step 6: Move mailboxes from Exchange 2007 servers to Exchange 2010 servers (downtime required)

In moving mailboxes to the Exchange 2010 servers, you will be switching over from using the ACLs to using ABPs.

Note:

We recommend that you create a script that performs this procedure in one step.

1. Move the mailboxes using the **MoveRequest** cmdlets. For more information, see Create a Local Move Request.
2. Assign the ABP to moved mailboxes. For more information, see Assign an Address Book Policy to a Mailbox User (EPW).
3. Clear the QueryBaseDN from the user object. This can be done directly via the Adsiedit.msc console or by using a multi-step process from the Shell. This example shows how to clear the QueryBaseDN by using the Shell.

```
$user = ([ADSI]"LDAP://CN=Bob,CN=Users,DC=Contoso,DC=com").psbase
$user.Properties["msExchQueryBaseDN"].Value=$null
$user.CommitChanges()
```

4. Remove the OAB setting from the mailbox.
   This example removes the OAB from John's mailbox:

```
Set-Mailbox -Identity John -OfflineAddressBook $null
```

After the mailboxes are moved and all of the other settings have been configured, users using Outlook will get the following error and they will be required to close and restart Outlook: "The Microsoft Exchange Administrator has made a change that requires you to quit and restart Outlook."

Step 7: What's next?

So, after you've moved all of your mailboxes to Exchange 2010 SP2 and all of the mailboxes are running on ABPs with your ACLs decommissioned, you can start following the standard Exchange guidance for removing the Exchange 2007 organization.

Removing and Modifying Exchange 2007

How to Remove an Exchange 2007 Organization

If you get stuck, this Microsoft Knowledge Base article may help:

How to Remove Exchange 2007 from a computer

1.8.1.4 Understanding Calendar Repair

Understanding Calendar Repair

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-15*

The *Calendar Repair Assistant* is a configurable mailbox assistant that runs within the Microsoft Exchange Mailbox Assistants service on Microsoft Exchange Server 2010 Mailbox servers. The Calendar Repair Assistant detects and corrects inconsistencies with single and recurring meeting items for mailboxes located on that Mailbox server. As a result, recipients won't miss meeting announcements or have unreliable meeting information.

By default, the CRA is not set to run automatically. To configure the CRA to run and repair calendar inconsistencies, use the **set-mailboxserver** cmdlet in the Exchange Management Shell to set the work cycle and work cycle checkpoint. The Exchange Management Console cannot be used to configure calendar repair log settings.

Contents

Looking for management tasks related to calendars? See Managing Calendars.

Calendar Repair Assistant Tasks

The Calendar Repair Assistant performs the following functions:

1. **Detects inconsistencies** The Calendar Repair Assistant uses the organizer's copy of the calendar item as a master copy for all meeting items. The assistant compares the attendee's calendar item with the organizer's calendar item for inconsistencies. The only exception to this rule is when the assistant compares the attendee's and organizer's response status. The assistant assumes that the attendee's response status is the correct one, and, if necessary, updates the organizer's tracking information.
2. **Determines if inconsistencies were intentional** If an inconsistency is detected, the Calendar Repair Assistant determines whether the attendee intentionally introduced the inconsistency. For example, an attendee can introduce an inconsistency by deleting the meeting request and not notifying the organizer. If the assistant determines that the attendee didn't introduce the inconsistency, it corrects the problem. If the assistant can't determine if the inconsistency was intentional, it performs no further action.
3. **Corrects inconsistencies** The Calendar Repair Assistant corrects inconsistencies on the Mailbox server on which it runs. However, if the organizer's mailbox is on a different server than the attendee's mailbox, the assistant reads from other Exchange 2010 Mailbox servers to compare the calendar items. The assistant doesn't overwrite the recipient's calendar information. Instead, it merges the information so data isn't lost. In addition, the repair update messages are moved to the recipient's Deleted Items folder. For more information about the inconsistencies detected and repaired, see Conflict Detection and Resolution later in this topic.
4. **Sends a calendar repair update message if a correction was made** Calendar repair update messages are sent to users whose calendar items were updated by the Calendar Repair Assistant. Instead of sending the message to the user's Inbox, the assistant sends the message to the user's Deleted Items folder. By doing so, a record of the repair is kept in the mailbox without causing user confusion. If the user is experiencing calendar inconsistencies, you can advise the user to look in the Deleted Items folder for troubleshooting purposes. The assistant only sends repair update messages if the issue is fixed.

For more information about configuring the Calendar Repair Assistant, see Managing Calendars.

Return to top

Conflict Detection and Resolution

The Calendar Repair Assistant detects and corrects the conflicts described in the following table.

Calendar Repair Assistant conflict resolution

Conflict	Resolution
An attendee accepted the organizer's meeting request or recurring meeting request, but the meeting isn't on the attendee's calendar.	The assistant checks the attendee's record in the mailbox database and finds that the attendee deleted the calendar item without sending a response. If the assistant can't determine that the meeting item was intentionally deleted by the attendee, the assistant creates the meeting request again. If the assistant determines that the attendee intentionally deleted the meeting request,

	no further action is taken.
An attendee is missing an occurrence or exception within a recurring meeting series.	The assistant checks the organizer's copy for a deleted occurrence or exception and finds that the attendee deleted the meeting request without sending a response. If the assistant can't determine that the meeting item was intentionally deleted by the attendee, the assistant creates the meeting request again. If the assistant determines that the attendee intentionally deleted the occurrence or exception, no further action is taken.
An attendee's response status for the meeting doesn't match the status on the organizer's calendar item.	The assistant updates the organizer's tracking status with the status on the attendee's calendar item.
Attendees have the meeting on their calendars, but the organizer doesn't have those attendees listed in the attendee list.	The assistant adds the attendees to the organizer's list of attendees. **Note:** If the meeting request was sent to a distribution group with more than 200 members, the Calendar Repair Assistant won't add the attendees to the organizer's attendee list.
An attendee is listed on some of the organizer's recurring meetings, but the attendee's recurrence pattern doesn't match the organizer's recurrence pattern.	The assistant replaces the attendee's recurrence pattern with the organizer's recurrence pattern.
The location of an attendee's meeting doesn't match the location recorded in the organizer's calendar item.	If the attendee intentionally changed the meeting location, no action is taken. If the assistant can't determine that the location was intentionally changed by the attendee, the attendee's calendar item is appended with the meeting location on the organizer's calendar item.
An attendee's start or end time is different from that of the organizer's start or end time.	If the assistant determines that the attendee intentionally changed the time, no further action is taken. If the assistant determines that the conflict was unintentional, the start or end time is changed if either time differentiates more than two hours from the organizer's start or end time.
The organizer or attendee has multiple meetings that have the same MAPI property identifier: LIL_GLOBAL_OBJID.	The assistant compares all the duplicates and performs the following steps to correct the inconsistency: 1. Checks the sequence numbers of all the duplicates. The duplicate with the highest sequence number is kept. The other meeting items are deleted. 2. If the assistant can't determine which item to keep based on the sequence number, it checks the **OwnerCriticalChangeTime** property. If one of the duplicates is the most recent copy, it keeps that duplicate item. The other meeting items are deleted. 3. If the assistant can't determine which

	item to keep based on the most recent copy, it checks the **LastModifiedTime** property. If one of the duplicates has the last modified time, the assistant keeps that duplicate item. The other meeting items are deleted. 4. If the assistant can't determine which item to keep based on the last modified time, it keeps the first calendar item returned by the database when querying for duplicate meetings. The other meeting items are deleted.
An attendee has a single or recurring meeting on his or her calendar, but the organizer doesn't have this item on his or her calendar.	The assistant checks whether the organizer intentionally deleted the meeting. If the organizer intentionally deleted the meeting, the assistant sends a cancellation to the attendees. If the assistant determines that the organizer didn't intentionally delete the meeting, the meeting is added back to the organizer's calendar. If the assistant can't determine the organizer's intent, no action is performed.

Return to top

Calendar Repair Log

Every time the Calendar Repair Assistant changes a calendar item on a user's mailbox, it writes the change to a calendar repair log (.log) file. The output of this .log file doesn't reveal personal data, such as the body of the message or attachments. The file only contains the minimum information to identify the meeting that was repaired and what repair actions were taken. Each time the assistant runs, one calendar repair log file is created for every mailbox. By default, calendar repair logging is enabled.

The calendar repair log is configurable and can be turned on or off for a server or user. For more information, see Managing Calendars.

The default calendar repair log path is *<Exchange Installation Path>*\v14\Logging\Calendar Repair Assistant.

The log files are created with the following naming convention:

CRAYYYYMMDDHH-X.Alias.log

- *CRA* = Calendar Repair Assistant prefix
- *YYYY* = year
- *MM* = month
- *DD* = day
- *HH* = hour
- *X* = instance
- *Alias* = mailbox alias

For example, the following repair log file indicates that a repair was made on Tony's mailbox on April 18, 2010, at 15:00 (3:00 P.M.), and that the repair was the third one made within that hour:

CRA2010041815-3.tony.log

Return to top

Client Application Experience

The Calendar Repair Assistant can't access the same data for all client applications. As a result, users may get a different experience depending on which client application they use to review mail. Therefore, the assistant may not be able to determine if the action made by the user was intentional. As previously stated, the assistant corrects conflicts only if it can successfully determine that the attendee didn't intentionally introduce the conflict. If the assistant can't make this determination, no further action is taken.

The following table lists the different end-user calendaring tasks that could result in a calendar conflict. Based on which client application was used, the Calendar Repair Assistant can determine the user's intent.

Calendaring tasks

Scenario	Client application	Property recorded
Organizer opens the calendar item and modifies its properties.	• Microsoft Office Outlook Web App • Client applications that use Exchange Web Services • Mobile client applications that use Microsoft Exchange ActiveSync	**ModifiedStartTime** **ModifiedEndTime** **ModifiedLocation**
Organizer drags the meeting in his or her calendar view to a different time.	• Outlook Web App • Client applications that use Exchange Web Services **Note:** This scenario isn't supported for client applications that use Exchange ActiveSync.	**ModifiedStartTime** **ModifiedEndTime**
Attendee responds as either accepted or tentatively accepted with or without sending a response message to the organizer.	• Outlook Web App • Client applications that use Exchange Web Services • Mobile client applications that use Exchange ActiveSync	**RespondedAccepted** **RespondedTentative**
Attendee declines a meeting request with or without sending a response message to the organizer.	• Outlook Web App • Client applications that use Exchange Web Services • Mobile client applications that use Exchange ActiveSync	**DeletedWithNoResponse** **RespondedDeclined**
Attendee declines an instance of a recurring meeting request with or without sending a response message to the organizer.	• Outlook Web App • Client applications that use Exchange Web Services • Mobile client applications that use Exchange ActiveSync	**DeletedExceptionWithNoResponse** **RespondedExceptionDecline**
Organizer cancels a meeting.	• Outlook Web App • Client applications that use Exchange Web Services • Mobile client applications that use Exchange	**MeetingExceptionCanceled**

	ActiveSync	

Return to top

1.8.1.5 Understanding E-Mail Address Policies

Understanding E-Mail Address Policies

Exchange Server 2010 > Mailbox > Understanding Mailbox >

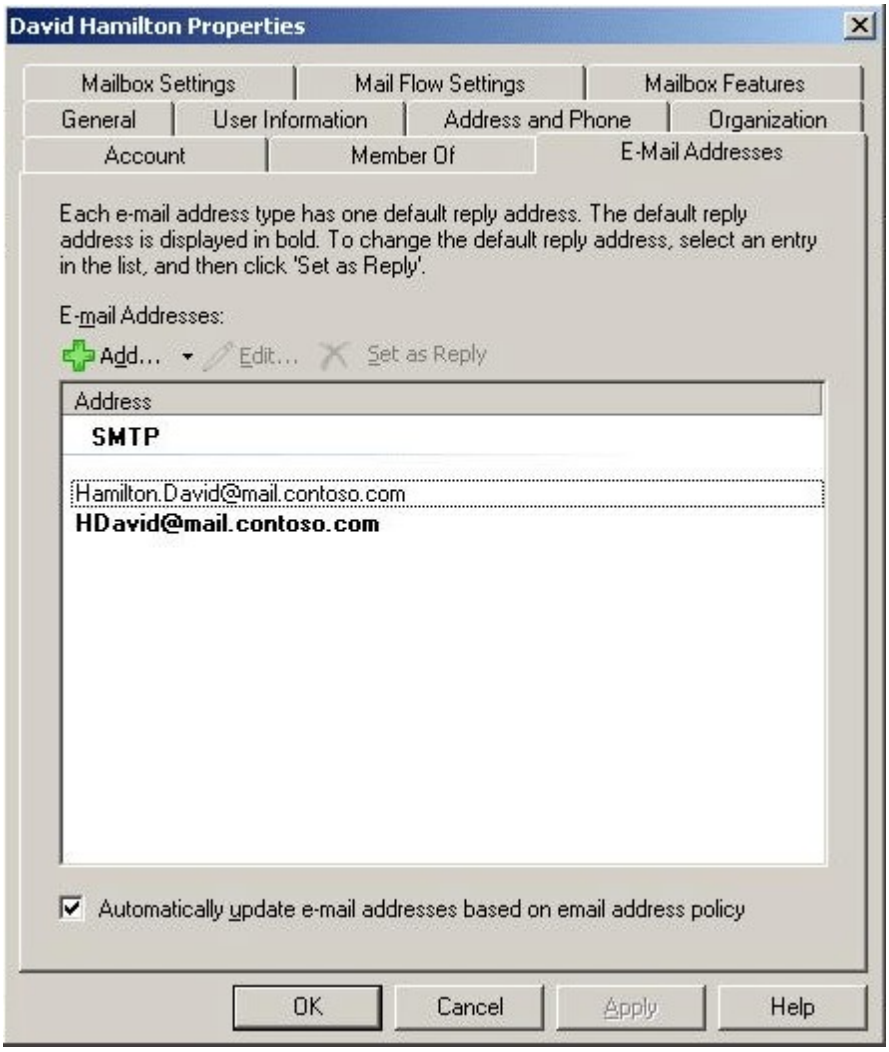
Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Recipients (which include users, resources, contacts, and groups) are any mail-enabled object in Active Directory to which Microsoft Exchange can deliver or route messages. For a recipient to send or receive e-mail messages, the recipient must have an e-mail address. E-mail address policies generate the primary and secondary e-mail addresses for your recipients so they can receive and send e-mail.

By default, Exchange contains an e-mail address policy for every mail-enabled user. This default policy specifies the recipient's alias as the local part of the e-mail address and uses the default accepted domain. The local part of an e-mail address is the name that appears before the at sign (@). However, you can change how your recipients' e-mail addresses will display. For example, you can specify that your recipients' e-mail addresses display as *firstname*.*lastname*@contoso.com.

Furthermore, if you want to specify additional e-mail addresses for all recipients or just a subset, you can modify the default policy or create additional policies. For example, the following figure illustrates a configuration in which the recipient David Hamilton can receive e-mail messages addressed to hdavid@mail.contoso.com and hamilton.david@mail.contoso.com.



Looking for management tasks related to e-mail address policies? See Managing E-Mail Address Policies.

Behaviors of Recipient Policies

Exchange applies a policy to all recipients that match the recipient filtering criteria:

- The recipient policy functionality is divided into two features: e-mail address policies and accepted domains.

  Note:
  A detailed discussion about accepted domains is outside the scope of this topic. For information about accepted domains, see Understanding Accepted Domains.

- When you run the **Update-EmailAddressPolicy** cmdlet in the Exchange Management Shell, the recipient object is updated with the e-mail address policy. For detailed syntax and parameter information, see Update-EmailAddressPolicy.
- Each time a recipient object is modified and saved, Exchange enforces the correct application of the e-mail address criteria and settings. When an e-mail address policy is modified and saved, all associated recipients are updated with the change. In addition, if a recipient object is modified, that recipient's e-mail address policy membership is reevaluated and enforced.

Creating E-Mail Address Policies

When creating an e-mail address policy, you can use the following e-mail address types:

- **Precanned SMTP e-mail address**. *Precanned* SMTP e-mail addresses are commonly used e-mail address types provided for you.
- **Custom SMTP e-mail address**. If you don't want to use one of the precanned SMTP e-mail addresses, you can specify a custom SMTP e-mail address. When creating a custom SMTP e-mail address, you can use the variables in the following table to specify alternate values for the local part of the e-mail address.

Custom SMTP e-mail address

Variable	Value
%g	Given name (first name)
%i	Middle initial
%s	Surname (last name)
%d	Display name
%m	Exchange alias
%*x*s	Uses the first *x* letters of the surname. For example, if *x* = 2, the first two letters of the surname are used.
%*x*g	Uses the first *x* letters of the given name. For example, if *x* = 2, the first two letters of the given name are used.

- **Non-SMTP e-mail address**. The following types of non-SMTP e-mail addresses are supported:
  - EX (Legacy DN Proxy Address Prefix DisplayName)
  - X.500
  - X.400
  - MSMail
  - CcMail
  - Lotus Notes
  - Novell GroupWise
  - Exchange Unified Messaging proxy address (EUM proxy address)

Important:
In Exchange, all non-SMTP e-mail addresses are considered custom addresses. Exchange doesn't provide unique dialog boxes or property pages for X.400, GroupWise, or Lotus Notes e-mail address types. If you add a non-SMTP custom e-mail address, you must have the appropriate dynamic-link library (DLL) files. If you don't provide the appropriate DLL files, you won't be able to create a customized e-mail address policy. The following error will be logged in Event Viewer: "The e-mail address description object in the Microsoft Exchange directory for the 'SADF' address type on 'i386' machines are missing."

For detailed instructions about how to create an e-mail address policy, see the following topics:

- Create an E-Mail Address Policy
- Create an E-Mail Address Policy By Using Recipient Filters

1.8.1.6 Understanding the Exchange 2010 Store

Understanding the Exchange 2010 Store

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-27*

The Exchange store is a storage platform that provides a single repository for managing multiple types of information in one infrastructure. The Exchange store (store.exe) is the core data storage repository for Microsoft Exchange Server 2010.

Contents

Databases in Editions of Exchange 2010

Exchange 2010 is available in two server editions: Standard Edition and Enterprise Edition. Exchange 2010 Standard Edition is designed to meet the messaging and collaboration needs of small and medium corporations, and it may also be appropriate for specific server roles or branch offices. Exchange 2010 Enterprise Edition is designed for large enterprises.

Exchange 2010 Standard Edition supports up to five databases. Exchange 2010 Enterprise Edition supports up to 100 databases.

Logical Components of the Exchange Store

The primary components of the Exchange store are mailbox databases and public folder databases. These components can reside on a single server, or they can be distributed across multiple servers.

Mailbox databases contain the data, data definitions, indexes, checksums, flags, and other information that comprise mailboxes in Exchange 2010. Mailbox databases hold data that's private to an individual user and contain mailbox folders generated when a mailbox is created for that user. A mailbox database is stored as an Exchange database (.edb) file.

Public folder databases contain the data, data definitions, indexes, checksums, flags, and

other information that comprise any public folders in your Exchange organization.

In Exchange 2010, you manage public folders by using the Exchange Management Shell. (You can also perform a limited number of public folder database management tasks in the Exchange Management Console.) For more information about managing public folders, see Managing Public Folders and Understanding Public Folders.

Return to top

File Structure of the Exchange Store

You manage the Exchange store by working with its logical components, such as databases. However, Exchange 2010 stores data in a specialized set of data files, such as Exchange database (.edb) files, transaction log (.log) files, and checkpoint (.chk) files. Unless you're backing up or restoring data, you rarely interact with these files directly. The following table describes each of these files in more detail.

File structure of Exchange store

Data file	Description
Exchange database (.edb)	These files are the repository for mailbox data. They're accessed by the Extensible Storage Engine (ESE) directly and have a B-tree structure designed for quick access. This enables users to access any page of data within one input/output (I/O) cycle, which is a four-fold increase compared to Microsoft Exchange Server 2007. Exchange databases are composed of multiple B-trees, with ancillary trees that work with the main tree by holding indexing and views.
Transaction log (.log)	These files are the repository for database operations such as creating or modifying a message. Committed operations are later written to the database itself (in an .edb file). This approach guarantees that all complete and incomplete transactions are logged to maintain data integrity in case of a service interruption. Each database has its own set of transaction logs.
Checkpoint (.chk)	These files are the repository for data that indicates when an operation is successfully saved to the database on the hard disk. Exchange 2010 uses .chk files so an instance of the ESE can automatically replay log files into an inconsistent database when recovering from a service interruption, starting with the next unwritten operation. The .chk files are placed in the same log location as the .log files.

Return to top

Understanding Transaction Logging

Exchange transaction logging is a robust recovery mechanism of the ESE designed to reliably restore an Exchange database to a consistent state after any sudden stop of the database. The logging mechanism is also used when restoring online backups. This section describes the details of Exchange 2010 transaction logging and includes a brief description of circular logging.

Exchange Transaction Logging

Before changes are made to an Exchange database file, Exchange writes the changes to a transaction log file. After a change is safely logged, it can then be written to the database file. It's common for these changes to become available to end users just after the changes are secured to the transaction log, but before the changes are written to the database file.

Exchange employs a sophisticated internal memory management system tuned for high performance, which efficiently manages the caching of dozens of gigabytes (GB) of database pages. Physically writing changes to the database file is a low-priority task during normal operation.

If a database suddenly stops, cached changes aren't lost just because the memory cache was destroyed. When the database restarts, Exchange scans the log files, and reconstructs and applies any changes not yet written to the database file. This process is called replaying log files. The database is structured so that Exchange can determine whether any operation in any log file has already been applied to the database, needs to be applied to the database, or doesn't belong to the database.

Rather than write all log information to a single large file, Exchange uses a series of log files, each exactly one megabyte (MB), or 1,024 kilobytes (KB), in size. When a log file is full, Exchange closes it and renames it with a sequential number. The first log filled ends with the name E*nn*00000001.log. The *nn* refers to a two-digit number known as the base name or log prefix.

Log files for each database are distinguished by file names with numbered prefixes (for example, E00, E01, E02, or E03). The log file currently open for a database is named E*nn*.log. It doesn't have a sequence number until it has been filled and closed.

The checkpoint file (E*nn*.chk) tracks how far Exchange has progressed in writing logged information to the database files. There's a checkpoint file for each log stream, and a separate log stream for each database.

Log files are numbered in a hexadecimal manner, so the log file after E0000000009.log is E000000000A.log, and not E0000000010.log. You can convert log file sequence numbers to their decimal values by using the Windows Calculator (Calc.exe) application in **Scientific** mode. To do this, run Calc.exe, and then from the **View** menu, click **Scientific**.

To view the decimal sequence number for a specific log file, you can examine its header by using the Exchange Server Database Utilities (Eseutil.exe) tool. The first 4-KB page of each log file contains header information that describes and identifies the log file and the databases it belongs to. The command **Eseutil /ml [log file name]** displays the header information.

If you use the wrong switch for displaying a header (for example, by using **/ml** with a database header instead of **/mh)**, an error is displayed or the header information displayed may be garbled or incorrect.

You can't view the header of a database while it's mounted. You also can't view the header of the current log file (E*nn*.log) while any database is mounted. Exchange holds the current log file open as long as one database is using it. However, you can view the checkpoint file header while databases are mounted. Exchange updates the checkpoint file every thirty seconds, and its header is viewable except during the moment when an update is occurring.

As an Exchange administrator, it's valuable to understand Exchange file headers. If you understand file headers, you can determine which database and log files belong together and which files are needed for successful recovery.

In the following log file header example, note the first four lines.

```
Base name: e00
Log file: e00.log
lGeneration: 11 (0xB)
Checkpoint: (0xB,7DC,6F)
```

These log file header lines show that this log file is the current log file because the log file name doesn't have a sequence number. The `lGeneration` line shows that when the log is filled and closed, its sequence number is `B`, corresponding to the decimal value 11. The base name is `e00`, and therefore the final log file name will be E000000000B.log.

The `Checkpoint` value in the previous header example isn't actually read from the log file header, but it's displayed as if it were. Eseutil.exe reads the `Checkpoint` value directly from E*nn*.chk, so you don't have to enter a separate command to learn where the checkpoint file is. If the checkpoint file has been destroyed, the `Checkpoint` value reads `NOT AVAILABLE`. In this case, the checkpoint is in the current log file (`0xB`), and the numbers `7DC` and `6F` indicate how far into the log file the checkpoint is. Note that you seldom have a practical need for this information.

If the checkpoint file is destroyed, Exchange can still recover and replay log files appropriately. But to do so, Exchange begins scanning log files, beginning with the oldest file available, instead of starting at the checkpoint log. Exchange skips data that has already been applied to the database and works sequentially through the logs until data that must be applied is encountered.

Typically, it takes only one or two seconds for Exchange to scan a log file that has already been applied to the database. If there are operations in a log file that must be written to the database, it can take anywhere from 10 seconds to several minutes to apply them. On average, a log file's contents can be written to the database in 30 seconds or less.

When an Exchange database shuts down normally, all outstanding data is written to the database files. After normal shutdown, the database file set is considered consistent, and Exchange detaches it from its log stream. This means that the database files are now self-contained (up to date). The transaction logs aren't required to start the database files.

You can tell whether a database has been shut down cleanly by running the command **Eseutil /mh** and examining the file headers.

With all databases disconnected and in a Clean Shutdown state, all log files can be safely deleted without affecting the databases. If you were then to delete all log files, Exchange would generate a new sequence of logs starting with E*nn*00000001.log. You could move the database files to a different server that has existing log files, and the databases would attach themselves to a different log stream.

Note:

Although you can delete the log files after all databases have been shut down, doing so affects your ability to restore older backups and roll forward. The current database no longer needs the existing log files, but they may be necessary if you must restore an older database.

If a database is in a Dirty Shutdown state, all existing transaction logs from the checkpoint forward must be present before you can mount the database again. If these logs are unavailable, you must repair the database by running the command **Eseutil /p** to make the database consistent and ready to start.

Caution:
If you have to repair a database, some data will be lost. Data loss is frequently minimal; however, it may be catastrophic. After running **Eseutil /p** on a database, you should run **Eseutil/ d** to defragment the database. This operation discards and rebuilds all database indexes and space trees.

In addition to allowing Exchange to recover reliably from an unexpected database stop, transaction logging is also essential to making and restoring online backups. For more information about making and restoring online backups, see Understanding Backup, Restore and Disaster Recovery.

Return to top

Circular Logging

You can configure Exchange to save disk space by enabling circular logging. Circular logging allows Exchange to overwrite transaction log files after the data that the log files contain is committed to the database. However, if circular logging is enabled, you can recover data only up until the last full backup. For example, you can enable circular logging when using Exchange native data protection, in which you don't make backups. To prevent log buildup, you need to enable circular logging.

In the standard transaction logging used by Exchange 2010, each database transaction is written to a log file and then to the database. When a log file reaches one MB in size, it's renamed, and a new log file is created. Over time, this results in a set of log files. If Exchange stops unexpectedly, you can recover the transactions by replaying the data from these log files into the database. Circular logging overwrites and reuses the first log file after the data it contains has been written to the database.

In Exchange 2010, circular logging is disabled by default. By enabling it, you reduce drive storage space requirements. However, without a complete set of transaction log files, you can't recover any data more recent than the last full backup. In a normal production environment, circular logging isn't recommended.

For information about how to enable and disable circular logging, see Configure Mailbox Database Properties.

Return to top

Extensible Storage Engine

Exchange mailbox databases and the queue on Hub Transport servers and Edge Transport servers utilize the ESE database. ESE is a multiuser, indexed sequential access method (ISAM) table manager with full data manipulation language (DML) and data definition language (DDL) capability. ESE allows applications to store records and create indexes to access those records in different ways. For more information about ESE, see Extensible Storage Engine Architecture. For improvements in Exchange 2010 ESE, see New Exchange Core Store Functionality.

Return to top

Store Health

The Exchange store can detect and correct several scenarios that can cause the store to become unhealthy. The Exchange store can handle poison mailboxes and thread time-outs, use report and alert features to signal an unhealthy Exchange store state, and detect and repair mailbox database and public folder database issues.

Poison Mailbox Detection and Correction

A single mailbox with corrupted data (logical or physical) may in some cases cause the Exchange store to fail, and deny service to all mailboxes hosted by the server. Similarly, a poison mailbox could also cause the Exchange store to repeatedly fail. This section describes the actions the Exchange store takes to detect and cut off poison mailboxes.

Isolating the Poison Mailbox

There are several types of events for which the Exchange store tags a mailbox as a potential threat:

- If a thread doing work for that mailbox fails
- If there are more than five threads in that mailbox that haven't made progress for a long time

A mailbox that's a potential threat is tagged, along with a count of how many times it has been tagged. This information is stored in the registry. The Exchange store also keeps timestamp information about when the mailbox was identified as a potential threat.

During a database mount, the Exchange store reads the time that the mailboxes were identified as potential threats. If more than two hours has elapsed, the registry key for the mailbox is deleted. The advantage of keeping this information in the registry is that in a high availability environment, it's replicated by the cluster database. Even during an Exchange store failover, the other computers have this information. The registry path used for isolating the poison mailbox is **HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server Name>\Private-{db guid}\QuarantinedMailboxes\{mailbox guid}**. The keys for this path are **CrashCount** and **LastCrashTime**.

The settings for how many failures lead to quarantining a mailbox as well as how long a mailbox should stay quarantined are stored in the **MailboxQuarantineCrashThreshold** and **MailboxQuarantineDurationInSeconds** keys in the registry path **HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server Name>\Private-{db guid}\QuarantinedMailboxes**.

The default values for these keys are three failures for **MailboxQuarantineCrashThreshold** and 21,600 seconds (six hours) for **MailboxQuarantineDurationInSeconds**.

Acting on the Poison Mailbox

By default, if a mailbox is identified as causing a failure or deadlock three times within two hours, the Exchange store tags it as quarantined in the registry. No access is allowed to the mailbox unless the OPEN_AS_ADMIN flag is passed. None of the Exchange processes (for example, content indexing or the Mailbox assistants) are allowed to log on. The **QuarantineState** and **QuarantineTime** registry keys keep track of whether the mailbox is quarantined. If the mailbox hasn't caused any failures in the last two hours and isn't quarantined, the registry path for the mailbox is cleaned up by the Exchange store. If a mailbox has been quarantined for longer than the **MailboxQuarantineDurationInSeconds** value since it's **LastCrashTime** value, it's released from quarantine automatically.

Resetting the Quarantined Mailbox

When the cause of the poison mailbox has been identified and corrected, the registry key for the quarantined mailbox should be reset manually by deleting it. However, if this manual step is forgotten, the Exchange store automatically resets quarantined mailboxes six hours after the quarantined flag was set. If the issue isn't debugged and fixed within that time period, this may lead to another set of failures before the mailbox or message is quarantined again.

Note:

The database hosting the mailbox needs to be remounted, or the Exchange store restarted, for the reset of the quarantined mailbox to take effect.

The time period for resetting quarantined mailboxes can be controlled by the registry key **HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server Name>\Private-{db guid}\QuarantinedMailboxes\MailboxQuarantineDurationInSeconds**.

Reporting and Alerts

You can use the Get-MailboxStatistics cmdlet to report the quarantined state of a mailbox. The Exchange store has a Performance Monitor counter for the number of quarantined mailboxes. The counter name is MSExchangeIS Mailbox\Quarantined Mailbox Count.

The Exchange store also writes an event whenever it quarantines a mailbox, with details about which mailbox and what time. The event 10018 identifies a quarantined mailbox.

Return to top

Database Repair

In Exchange 2010 Service Pack 1 (SP1), you can use the New-MailboxRepairRequest cmdlet to detect and repair mailbox corruptions. You can run this cmdlet against a specific mailbox or against a mailbox database. While this task is running, mailbox access is disrupted for the mailbox being repaired. If you run this cmdlet against a mailbox database, only access to the mailbox being repaired is disrupted. All other mailboxes in the database remain operational. For more information, see Create a Mailbox Repair Request.

The **New-MailboxRepairRequest** cmdlet detects and repairs the following types of mailbox corruptions:

- Search folder corruptions (using the `SearchFolder` value of the *CorruptionType* parameter)
- Aggregate counts on folders that aren't reflecting correct values (using the `AggregateCounts` value of the *CorruptionType* parameter)
- Views on folders that aren't returning the correct content (using the `FolderView` value of the *CorruptionType* parameter)
- Provisioned folders incorrectly pointing to parent folders that aren't provisioned (using the `ProvisionedFolder` value of the *CorruptionType* parameter)

After you run the **New-MailboxRepairRequest** cmdlet, you can use Event Viewer to view the details of the request. For more information, see View Mailbox Repair Request Entries in Event Viewer.

You can also use the New-PublicFolderDatabaseRepairRequest cmdlet to detect and fix replication issues in the public folder database. Public folders in the public folder database can still be accessed while the request is running. However, access isn't available to the public folder currently being repaired. For more information, see Create a Public Folder Database Repair Request.

Return to top

Time-Out Detection and Reporting

Another indication of an unhealthy Exchange store is that threads are either deadlocked or otherwise not making any progress. If there are more than five threads on a single mailbox, ten threads on a single database, or twenty threads on a single server that hasn't made progress in one minute, a time-out is reported on the server. The performance counter that indicates detected time-outs is MSExchangeIS\ RPC Request Timeout Detected.

The Exchange store also writes the following events to the server:

- 10025, which reports a time-out on the Exchange server
- 10026, which reports a time-out on the database
- 10027, which reports a time-out on an individual mailbox

If the time-out is detected on a single mailbox, the mailbox is considered potentially poison, and is handled similar to a failure by increasing the **CrashCount** key. This makes it susceptible to being quarantined.

Return to top

Low Disk Space on Database Logs or Database Drives

When the Exchange store detects that the space available on a log or database drive is below 1 GB, it cuts off all transport delivery to that database. This is to prevent a disk running out of space. When a disk runs out of space, the database can't be mounted or debugged. The database space also can't be reclaimed. This is a self-protecting mechanism that only occurs if you don't react to the space issue warnings from your monitoring infrastructure.

When the disk space goes above 1.5 GB, the Exchange store allows deliveries to continue. The following performance counters indicate this behavior:

- MSExchangeIS Mailbox\ Delivery Blocked: Low Database Space
- MSExchangeIS Mailbox\ Delivery Blocked: Low Log Space

The Exchange store also writes the following events to the server:

- 10014, which indicates low disk space on the log
- 10015, which indicates low disk space on the database

If you encounter low disk space issues, you can perform the following actions to correct the issue:

- Delete content from mailboxes. Specifically, you can delete messages from the Deleted Items and Sent Items folders.
- Purge items from the Recoverable Items folder. For details, see Clean Up the Recoverable Items Folder.
- Run database maintenance. For details, see Maintain Mailbox Databases.
- Purge transaction logs. For details, see Understanding High Availability Factors.
- Enable circular logging. For details, see Configure Mailbox Database Properties.
- Change the database path to a hard disk drive that has more space. For details, see Move the Mailbox Database Path for a Mailbox Database Copy.

Return to top

Exchange Store Limits

In Exchange 2010, connection and usage limits are placed on the Exchange store to prevent a single application or a single user from using all the available connections to the Exchange store. If a single user or application uses all the connections, other users or applications won't be able to access the Exchange store, which can result in downtime.

For more information, see Exchange Store Limits.

Return to top

Exchange Store Limits

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-08*

In Microsoft Exchange Server 2010, connection and usage limits have been placed on the Exchange store to prevent a single application or a single user from using all the available connections to the Exchange store. If a single user or application is allowed to use all of the connections, other users or applications cannot be able to access the Exchange store, which could result in downtime.

Note:

For any connections made by accounts that have administrative privileges, the session limits have been increased to 64,000 maximum sessions per server.

Contents

Terminology

Knowledge of the following terms will help you understand the types of connections referenced in this topic.

Sessions

Sessions represent the connections used by services and client applications, such as Microsoft Outlook, to connect to the Exchange store. Services and clients can have multiple sessions at a particular time. The terms *connections* and *sessions* can be used interchangeably.

Threads

Threads represent concurrently executing requests to the Exchange store. For example, if a user opens a folder in Outlook, Outlook executes a request to the Exchange store on behalf of the user. That executing request is a single thread.

For example, 75 users being logged on to a server at the same time is equal to 75 sessions. However, out of those 75 sessions, only 5 of those sessions could be making requests through threads.

Return to top

Session Limits

The following table lists the types of client connections to the Exchange store and the limits based on those connections. If you want to modify the session limits, see "Configure Session Limits" immediately following the table.

The types of connections are as follows:

- **Max concurrent threads per server** Specifies the maximum number of

concurrent threads that an Exchange service can execute on a Mailbox server.

- **Max sessions per server** Specifies the maximum number of sessions that an Exchange service can have open at one time on a Mailbox server.
- **Max user sessions per server** Specifies the maximum number of sessions for a particular protocol for a single user.

Client type	Max concurrent threads per server	Max sessions per server	Default number of user sessions per server
Admin	50	10,000	Not applicable
Availability service	50	10,000	16
Content indexing	50	10,000	Not applicable
Exchange ActiveSync	Not applicable	Not applicable	16
Exchange Web Services	Not applicable	Not applicable	16
Management	Not applicable	Not applicable	16
MAPI on the Middle Tier (MoMT)	Not applicable	Not applicable	32
MSExchangeMailboxAssistants: Events	50	10,000	Not applicable
MSExchangeMailboxAssistants: Timed	50	10,000	Not applicable
MSExchange Remote Procedure Call	Not applicable	Not applicable	16
Microsoft Office Outlook Web App	Not applicable	Not applicable	16
POP3 and IMAP4	Not applicable	Not applicable	16
Transport	50	10,000	Not applicable
Unified Messaging	Not applicable	Not applicable	16
Others	Not applicable	Not applicable	16

Configure Session Limits

You can modify the default session limits.

Note:

If you want to modify the session limits, you need to modify them on all Mailbox servers within any database availability groups (DAGs). If you don't make the same changes on all servers, the results will be inconsistent. To increase the session limit on the Client Access server, the RCAMaxConcurrency value must be increased on the throttling policy. For more information, see Set-ThrottlingPolicy.

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

1. Start Registry Editor (regedit).
2. Navigate to the following registry subkey:
   \\HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services

\MSExchangeIS\ParametersSystem.

3. Right-click **ParametersSystem**, point to **New**, and then click **DWORD (32-bit) Value.**
   The new value is created in the result pane.
4. Rename the key to one of the following values, and then press Enter:
   - **Maximum Allowed Sessions Per User** This limit specifies the maximum allowable sessions per user.
   - **Maximum Allowed Service Sessions Per User** This limit specifies the maximum allowed service sessions per user.
   - **Maximum Allowed Exchange Sessions Per Service** This limit specifies the maximum allowed Exchange sessions per service. The default value is 10,000, and the Maximum value is 65536.
   - **Maximum Allowed Concurrent Exchange Sessions Per Service** This limit specifies the maximum allowed concurrent Exchange sessions per service.
   - **Disable Session Limit** This limit disables session limits. Set the value to **0** to turn off session limits. Set the value to **1** to turn on session limits.
5. Right-click the newly created key, and then click **Modify**.
6. In the **Value data** box, type the number of objects to which you want to limit this entry, and then click **OK**. Use the preceding table to view the default settings.

Return to top

Open Item Limits

Open item limits are limits placed on the number of items that can be opened by a single mailbox in a single session. However, a user can have multiple sessions opened simultaneously. For example, if a user has two sessions opened, the user could open 1,000 folders.

If you want to modify these limits, see "Configure Open Item Limits" immediately following the table.

Item type	Registry object type	Max opened per session
ACL View	objtACLView	50
Attachment	objtAttachment	500
Attachment View	objtAttachmentView	500
Cstream	objtCStream	50
Folder	objtFolder	500
Folder View	objtFolderView	500
FX Destination Stream	objtFXDstStrm	50
FX Source Stream	objtFXSrcStrm	50
Message	objtMessage	250
Message View	objtMessageView	500
Notification	objtNotify	500,000
Rule View	objtRulesView	50
Stream	objtStream	250

Configure Open Item Limits

You can limit the maximum number of resources that a MAPI client can use simultaneously.

Note:

If you want to modify the open item limits, you need to modify them on all Mailbox servers within any DAGs and client access arrays. If you don't make the same changes on all servers, the results will be inconsistent.

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

1. Start Registry Editor (regedit).
2. Navigate to the following registry subkey:
   \\HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services \MSExchangeIS\ParametersSystem
3. Right-click **ParametersSystem**, point to **New**, and then click **Key**.
   A new key is created in the console tree.
4. Rename the key **MaxObjsPerMapiSession**, and then press Enter.
5. Right-click **MaxObjsPerMapiSession**, point to **New**, and then click **DWORD (32-bit) Value**.
   The new value is created in the result pane.
6. Rename the key to <*Object_type*>, where <*Object_type*> is the name of the registry object type that you're modifying. For example, to modify the number of messages that can be opened, use *objtMessage*. Press Enter.
7. Right-click the newly created key, and then click **Modify**.
8. In the **Value data** box, type the number of objects that you want to limit this entry to, and then click **OK**. For example, type **350** to increase the value for the object.
9. Restart the Microsoft Exchange Information Store service.

Return to top

Item Size Limits

Item size limits are the limits placed on items within a user's mailbox.

Item size limits are configurable by using the *MaxSendSize* and *MaxReceiveSize* parameters on the following cmdlets:

- Set-Mailbox
- Set-RemoteMailbox
- Set-MailUser
- Set-MailContact

Item type	Limit
Message (saved)	Maximum size of the SendLimit, ReceiveLimit
Message (sent)	Maximum size of the SendLimit
Attachments	Maximum number of attachments per message = 1,024

Return to top

Understanding Database Maintenance

See Also

Mailbox > Understanding Mailbox > Understanding the Exchange 2010 Store >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-08-24*

Architectural changes that were made to the database engine in Microsoft Exchange Server 2010 significantly improve its performance and robustness. However, these architectural changes also change the behavior of database maintenance tasks from earlier versions of Exchange Server. This topic describes the database maintenance tasks that must be routinely performed against Exchange Server 2010 databases.

All the tasks that are described in this topic are collectively known as background database maintenance.

Database Compaction

Database compaction must be completed to free up unused space in the database file. Database compaction does not return that unused space to the file system. Instead, it frees pages in the database by compacting records into the fewest possible number of pages, and reduces the I/O that is required to access the pages. To do this, the ESE database engine uses the database metadata, which is the information that describes tables in the database. For each table, the ESE database engine examines every page in the table, and tries to move the records to logically ordered pages.

Database compaction is important because it reduces the time associated with backing up the database file, and it helps maintain a predictable database file size. This is important to accurately determine server/storage size.

Database compaction was redesigned for Exchange Server 2010. Most significantly, the operation now gives preference to data contiguity over the amount of compaction. In earlier versions of Exchange Server, the focus was greater on space compaction. This resulted in pages that were always in random order after the process reordered records into free space across pages. In combination with the store schema architecture, this random reordering meant that any request to pull a set of data (such as downloading items inside a folder) always resulted in random I/O. In Exchange Server 2010, random I/O is reduced by keeping records in order on the pages.

Also in earlier versions of Exchange Server, database compaction operations were performed during the online maintenance window. In Exchange 2010, database compaction is now a background process that runs continuously.

Database Defragmentation

Database defragmentation (also known as OLD v2 and B+ tree defragmentation) is a new maintenance task in Exchange Server 2010. Database defragmentation is important to maintain efficient utilization of disk resources over time (i.e., make the I/O more sequential instead of random) and to maintain the compactness of tables that are marked as sequential.

Database defragmentation is a background process that analyzes the database continuously as operations are performed, and then triggers asynchronous work when it is necessary. The process monitors all tables for free pages. If a table reaches a threshold at which a significantly high percentage of the total B+ Tree page count is free, the free pages are returned to the root. The process also works to maintain contiguity throughout a table set with sequential space hints (a table that was created with a known sequential usage pattern). If database defragmentation sees a scan/pre-read on a sequential table, and if the records are not stored on sequential pages within the table, the process defragments that section of the table by moving all the affected pages to a new extent in the B+ tree. You can use performance counters to see the low level of active work performed by database defragmentation when a steady state is reached.

Database defragmentation has the following controls to regulate how it completes tasks:

- **The max number of outstanding tasks** This keeps database defragmentation from doing too much work during the first pass if a very large change has occurred in the database.
  A latency throttle of 100ms When the system is overloaded, database defragmentation will delay defragmentation work. Delayed work is completed the next time that the database follows that same operational pattern and the system has more resources.

Online database scanning (Database Checksumming)

Online database scanning (also known as database checksumming) is the process by which the database is read in large chunks, and every page is examined for physical page corruption. The main purpose of checksumming is to detect physical corruption and lost flushes that may not be detected by transactional operations (stale pages).

Note:

In Exchange Server 2007 and earlier versions, the checksumming operations occurred during the backup process. However, this caused a problem for replicated databases because only the copy that was being backed up was checksummed. If the passive copy was backed up, the active copy was not being checksummed. To resolve this issue, a new optional online maintenance task named Online Maintenance Checksum was added to Exchange Server 2007 Service Pack 1 (SP1). For more information, see How to Configure Online Maintenance Database Scanning in Exchange 2007 SP1 and SP2.

In Exchange 2010, online database scanning checksums the database and performs post Exchange 2010 Store crash operations. Space can leak because of crashes. Online database scanning finds and recovers lost space. The system in Exchange 2010 is designed with the expectation that every database is fully scanned one time every seven days. A warning event is fired if a database is not completely scanned in this timeframe. In Exchange 2010, there are now two modes to run online database scanning on active database copies:

- Run as the last task in the scheduled Mailbox Database Maintenance process: You can configure how long it runs by changing the Mailbox Database Maintenance schedule. You can use this option for smaller databases that are less than 1 terabyte and that require less time to be completely scanned.
- Run the default behavior in the background 24 hours a day, seven days a week: This option works well for all database sizes, but we recommend this for large database sizes (1-2 TB). Exchange scans the database no more than one time per day. This read I/O is 100 percent sequential (which makes it easy on the disk), and equates to a scanning rate of about 5 megabytes (MB)/sec on most systems.

Note:

- The Shell, EMC, and JetStress refer to database checksumming as

background database maintenance. To enable database checksumming in the EMC, select the **Enable background database maintenance (24 X 7 ESE scanning)** check box in **Properties**.
- To enable database checksumming in the shell, enter the following cmdlet: **Set-MailboxDatabase -Identity MDB1 -BackgroundDatabaseMaintenance $true**
- To enable database checksumming in Jetstress 2010, select the **Run background database maintenance** check box on the **Select Test Type** page.

Page Patching

Page patching replaces corrupted pages with healthy copies. Corrupted page detection is a function of database checksumming. In addition, corrupted pages are detected at run time when the page is stored in the database cache. Page patching works against highly available (HA) database copies. How a corrupted page is repaired depends on whether the HA database copy is active or passive.

Page patching process on active database copies

- A corrupted page(s) is detected.
- A marker is written into the active log file. This marker indicates the corrupted page number. It also indicates that the page requires replacement.
- An entry is added to the page patch request list.
- The active log file is closed.
- The Replication service sends the log file to passive database copies.
- The Replication service on a target Mailbox server receives the sent log file and inspects it.
- The Information Store on the target server replays the log file, and replays up to marker, retrieves its healthy version of the page, invokes Replay Service callback, and then ships the page to the source Mailbox server.
- The source Mailbox server receives the healthy version of the page, confirms that an entry exists in the page patch request list, and then writes the page to the log buffer. Correspondingly, the page is inserted into the database cache.
- The corresponding entry in the page patch request list is removed.
- At this point, the database is considered patched. (At some later point, the checkpoint will advance, the database cache will be flushed, and the corrupted page on disk will be overwritten.)
- Any other copy of this page (received from another passive copy) will be silently dropped. This is because no corresponding entry exists in the page patch request list.

Page patching process on passive database copies

- On the Mailbox server on which the corrupted pages are detected, log replay is paused for the affected database copy.
- The replication service coordinates with the Mailbox server that is hosting the active database copy, and it retrieves the corrupted pages and the required log range from the active copy's database header.
- The Mailbox server updates the database header for the affected database copy, and it inserts the new required log range.
- The Mailbox server notifies the Mailbox server that is hosting the active database copy about which log files it requires.
- The Mailbox server receives the required log files, and it inspects them.
- The Mailbox server injects the healthy versions of the database pages it retrieved from the active database copy. The pages are written to the log buffer. Correspondingly, the page is inserted into the database cache.
- The Mailbox server resumes log replay.

Page Zeroing

Database Page Zeroing is a security measure by which deleted pages in the database are overwritten with a pattern (zeroed). This makes discovering the data much more difficult.

In Exchange Server 2007 and earlier versions, page zeroing operations occur during the streaming backup process. Because they occur during the streaming backup process, page zeroing does not cause the generation of log files. This raises an issue for replicated databases because the passive copies never have their pages zeroed. Also, the active copies have their pages zeroed if a streaming backup is finished. In Exchange Server 2007 SP1, we introduced a new optional online maintenance task to address this issue: Zero Database Pages during Checksum. When Zero Database Pages during Checksum is enabled, this task zeroes out pages during the online maintenance window, and then logs the changes. The changes are then replicated to the passive copies.

However, in the Exchange Server 2007 SP1 implementation, the zeroing process occurs during a scheduled maintenance window. This creates a delay between the time that a page is deleted and the time that it is zeroed. Therefore, the page zeroing task becomes a runtime event that operates continuously in Exchange Server 2010 SP1. Typically, the task now zeroes out pages at transaction time when a hard delete occurs.

In addition, database pages can be scrubbed during the online checksum process. The pages targeted in this case are as follows:

- Deleted records that couldn't be scrubbed during runtime because of dropped tasks (if the system is too overloaded) or because the store crashed before the tasks got to scrub the data.
- Deleted tables and secondary indices. When these are deleted, we do not scrub their contents. Therefore, online checksum detects that these pages don't belong to any valid object any longer and it scrubs the pages.

For more information about page zeroing in Exchange 2010, see Understanding Exchange 2010 Page Zeroing.

Use performance counters to track the background maintenance tasks

In Exchange Server 2010, events are not recorded for the defragmentation and compaction maintenance tasks. However, you can use performance counters to track the background maintenance tasks. The following table describes the performance counters to use under the **MSExchange Database ==> Instances** object.

Counter	Description
Database Maintenance Duration	The number of seconds that have passed since the maintenance started for this database. If the value is 0, maintenance has been finished for the day.
Database Maintenance Pages Bad Checksums	The number of non-correctable page checksums encountered during a database maintenance pass
Defragmentation Tasks	The count of background database defragmentation tasks that are currently running
Defragmentation Tasks Completed/sec	The rate at which background database defragmentation tasks are being finished

The following table describes the page zeroing counters to use under the **MSExchange Database** object:

Counter	Description
Database Maintenance Pages Zeroed	Indicates the number of pages zeroed by the database engine since the performance counter was invoked
Database Maintenance Pages Zeroed/sec	Indicates the rate at which pages are zeroed by the database engine

White space

In a database, you can have thousands of tables. You can have at least one table for every folder in every mailbox. The messages tables, folders tables, and attachments tables represent 90 percent of the space that is used in the database. These tables have the greatest percentage of free space (also known as white space) in the database.

To determine how much white space exists in a database, and reclaim the white space, follow these steps:

1. Unmount the database.
2. Complete a space dump by using the Exchange Server Database Utilities (Eseutil) tool together with the */MS* switch. For more information about how to do this, see How to Run Eseutil /M in File Dump Mode.
   At the end of the dump file is a line similar to the following:

   ```
   ------------------------------------------------------------------------
   253
   ```

   This is a summation of the total number of pages that are available in all the tables. Multiply this value by 32K to determine the true amount of white space in the database.

Note:
For an example of the Eseutil dump file, see Determining the True Amount of Space in an Exchange Database.

After you determine how much white space is in a database, you may also want to reclaim the white space.

If you encounter a database that has a significant amount of white space, and you do not expect that the typical operations will reclaim the space, we recommend the following steps:

1. Create a new database and its associated database copies.
2. Move all mailboxes to the new database.
3. Delete the original database and its associated database copies.

See Also

Concepts

New Exchange Core Store Functionality
Understanding the Exchange 2010 Store

Other Resources

Microsoft Exchange Server Jetstress 2010

Understanding the Impact of Named Property and Replica Identifier Limits on Exchange Databases

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-01-08*

Microsoft uses the Messaging API (MAPI) to connect different messaging transport components. The MAPI specification presents most objects as properties. To identify these properties, MAPI uses identifiers, known as property identifiers or PropIDs.

Property identifiers are a set of hexadecimal values that range from 1 to 0xFFFF. This provides sufficient values for 65,534 properties. These properties are divided into the following groups, known as ranges:

- **Transmittable properties** –Properties that Exchange can send together with a message
- **Internal properties** - Properties that can be set only by Exchange
- **Non-transmittable properties** – Properties that are not delivered outside the organization when Exchange delivers a message

The properties in these ranges are known as standard properties. Standard MAPI properties have fixed IDs, and represent all properties that are below 0x8000.

There is one additional range, which is the largest of the groups and which represents all properties that are at 0x8000 and above. The properties in this range are known as *named properties*. Named properties provide a way for vendors to extend the standard MAPI property set by adding their own properties.

Named properties fall into the following main categories:

- Properties that have numbers for names – These named properties are used by such programs as Microsoft Outlook, and are generally defined in a source file.
- Properties that have string values for names - These named properties are known as "String Named Properties." In addition to a name, each of these properties has an associated GUID. This lets developers divide named properties into property sets.

Because named properties do not have specific IDs assigned to them, MAPI provides a facility to dynamically create unique IDs for named properties and to maintain a persistent mapping between a named property and its unique ID. However, the dynamic creation of these IDs means that the property IDs for named properties can vary from computer to computer.

The Microsoft Exchange Information Store service maintains a table of named properties for each mailbox. Messages that are sent over the Internet are transferred in a format that is known as Message/RFC822. This is a text format that includes messages in plain text together with headers that contain a set of key-and-value pairs. RFC822 includes support for a set of properties that are called X-headers. When the transport service processes a message that contains custom information, the transport service contacts the information store service to register named properties for X-headers.

Note:

Any subsequent messages that include the same X-header do not cause Exchange to register additional named properties.

Exchange stores these named properties together with the messages that contain the

related X-header. Microsoft uses the extensible namespace PS_INTERNET_HEADERS to group the X-headers from messages that were received over the Internet.

Named Properties Limits

The following list summarizes some important points about named properties:

- X-headers are fields in Message/RFC822 messages that hold certain important values.
- Named properties is the method that Exchange uses to reserve an ID for a particular value.
- After a named property has been allocated, it may not be deallocated. The property remains reserved for the particular name and GUID combination.

Because there are a fixed number of named properties available, Exchange uses a quota system to track the number of allocated named properties. In this system, the information store service warns you when available named property IDs are close to becoming exhausted. When a second threshold is reached, the information store service stops allocating named property IDs.

Named Property Exhaustion

Although many programs use named properties, Outlook uses the majority of them. When named property IDs are exhausted, Outlook cannot map a named property. In this scenario, you may experience symptoms that resemble the following:

- Event IDs 9666 and 9667 are logged in the Application log. For more information, see Events 9666, 9667, 9668, and 9669 Received When Named Properties or Replica Identifiers Are Depleted for An Exchange Database.
- Messages that contain properties that cannot be mapped are not delivered. When you examine the message tracking information for an affected message, the information resembles the following:

  ```
  550 5.2.0 STOREDRV.Deliver: The Microsoft Exchange Information Store service reported an error. The following information should help identify the cause of this error:
  MapiExceptionNamedPropsQuotaExceeded: 16.18969
  ```

- When an add-in that adds named properties or X-headers to messages is installed in Outlook, certain messages may not be sent to other users in the organization. In this scenario, the sending user receives a non-delivery report (NDR) that resembles the following:

  ```
  The message reached the recipient's e-mail system, but delivery was refused. Attempt to resend the message. If it still fails, contact your system administrator.
  ```

To recover named properties in Microsoft Exchange Server 2010, use the **New-MoveRequest** cmdlet together with the *DoNotPreserveMailboxSignature* parameter. For more information, see New-MoveRequest.

Note:

Doing this depletes the named property IDs by retaining only named properties that exist on at least one message in the mailbox. If all named properties still exist on any message, none will be reclaimed.

Property Changes in Exchange 2010

Exchange Server 2010 includes improvements to address issues that may occur in

Microsoft Exchange Server 2007. In Exchange 2010, named property resources are moved to the mailbox level instead of the database level. For more information about the property change issues that may occur in Exchange 2007, see Understanding the Impact of Named Property and Replica Identifier Limits on Exchange Databases.

For More Information

For more information about managing databases, see Managing Storage Groups and Databases.

1.8.1.7 Understanding Exchange Search

Understanding Exchange Search

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-29*

With increasing mailbox sizes and increasing amounts of data being stored in mailboxes in the form of messages and attachments, it's crucial for users to be able to quickly search and locate the messages they need. In Microsoft Exchange Server 2010, you can provision personal archives for your users, helping you reduce or eliminate the use of .pst files. This results in more mailbox data being stored by a user, and it makes searching across the user's primary and archive mailboxes an important productivity tool.

In Exchange 2010, authorized users can use Multi-Mailbox Search to perform mailbox searches across the entire Exchange 2010 organization for complying with electronic discovery (eDiscovery) requests, regulatory audits, or internal investigations. Multi-Mailbox Search also uses the content indexes created by Exchange Search.

Exchange Search is different from full-text indexing available in Exchange Server 2003. Improvements were made to performance, content indexing, and search. New items are indexed almost immediately after they're created or delivered to the mailbox, providing users with a fast, stable, and more reliable way of searching mailbox data. In Exchange 2010 and Exchange Server 2007, content indexing is enabled by default on all mailbox databases, and there's no initial setup or configuration required.

Note:
Exchange Search doesn't index public folder databases.

Contents

Exchange Search and Localization

Exchange Search and Database Availability Groups

Content Indexing

When Exchange Search services are started, Exchange Search determines the search status of all mailbox databases on the Mailbox server. If a mailbox database is mounted and enabled for search, Exchange Search assigns it one of following status values:

- **New** When the status of a mailbox database is New, Exchange Search creates a content index catalog for the database. After it's created, Exchange Search changes the status of the database to Crawling.
- **Crawling** When the status of a mailbox is Crawling, Exchange Search indexes mailboxes in the database. The status remains Crawling until all mailboxes in the database have been indexed. After all mailboxes in the databases have been indexed, Exchange Search changes the status of the database to Notification.
- **Notification** After the initial crawl has occurred on a database, Exchange Search is notified by the Exchange store of new events such as message creation, delivery, or deletion. Events are added to the notification queue to be indexed. This happens quickly, so the content index is never more than a few minutes out of date. New messages delivered to a mailbox are indexed within a few seconds of delivery.

Return to top

Exchange Search Performance

Exchange Search offers significant performance improvements compared to full-text indexing in Exchange 2003. The search model has changed from a crawl mode to an always up-to-date mode. Several improvements were made to optimize system resources such as CPU, memory, disk input/output (I/O), and disk space required for indexes. These performance improvements result in over 35x improvement in indexing speed. Although a full crawl of the database is much faster, it can use a significant amount of resources on a Mailbox server, depending on the size of the mailbox database. During more intensive phases, this can disrupt mail flow. Because delivery of mail should take precedence over content indexing, a new throttling feature in Exchange Search automatically throttles indexing for a particular mailbox database or set, reducing disk I/O and CPU utilization.

Return to top

Exchange Search Clients

Exchange Search provides a service that's consumed by search clients. These clients include Microsoft Outlook, Microsoft Office Outlook Web App, Windows Mobile, the Multi-Mailbox Search feature in Exchange 2010, and Exchange Web Services.

In Outlook 2010 and Office Outlook 2007, Outlook profiles used to configure Outlook features on users' computers can be configured to use Cached Exchange Mode. When Outlook is connected to Exchange in an *online mode* and accesses the Exchange mailbox, changes such as creation of mailbox items, new mail delivery, and deletion of mailbox items takes place on the Mailbox server. In Cached Exchange Mode, Outlook creates a local replica of the Exchange mailbox on the user's computer. This replica is stored in an .ost file in the user's profile. Changes to mailbox items happen in the local replica, which is

then synchronized with the Exchange mailbox. For details about Cached Exchange Mode, see About Cached Exchange Mode.

In Cached Exchange Mode, Outlook uses Windows Search, a component built-in in Windows 7 and Windows Vista. Windows Search performs content indexing and provides search functionality to Outlook. Interfacing with a local content indexing and search service provides Outlook users running in Cached Exchange Mode a more efficient way to search their mailbox. In addition to indexing e-mail in the offline store, Windows Search also indexes other data residing in the file system. For details about Windows Search, see Windows Search.

Outlook 2010 and Outlook 2007 provide your users an easily accessible **Instant Search** box located on top of the message list pane, so that users can quickly search mailbox content. Additionally, using the Advanced Find feature, users can create more complex search queries using a number of fields and parameters.

Return to top

Advanced Query Syntax

With increasing number of e-mail messages received by users, larger mailboxes, and the resulting information overload, the ability to quickly search messages enhances user productivity, and boosts satisfaction with e-mail. Using Advanced Query Syntax (AQS), users can quickly create advanced search queries and find the messages they need. AQS search queries can be entered directly in the **Instant Search** box in Outlook.

For example, to search messages sent by user April Stewart that have attachments and contain the word Contoso in the subject field, a user can use the following search query: `From:"April Stewart" HasAttachments:true Subject:Contoso`. To further narrow it to unread messages, the user can add the following keyword and value: `unread:true`. To further narrow it to messages sent by April last month, the user can add the following keyword and value: `Sent:lastmonth`.

AQS is supported by both Exchange Search on the server and by Windows Search on the desktop. Search queries using AQS work in Outlook 2010 and Outlook 2007 in online and cached modes. In Exchange 2010, users can also use AQS queries in Outlook Web App and Windows Mobile. Exchange Search clients such as Multi-Mailbox Search also support AQS search queries.

Outlook 2010 and Outlook 2007 support a large number of AQS keywords. Additionally, Exchange Search also supports the keywords shown in the following table.

Exchange Search keywords

Property	Example	Search results
Attachments	attachment:annualreport.pptx	Messages that have an attachment named annualreport.pptx. The use of attachment:annualreport or attachment:annual* returns the same results as using the full name of the attachment.
Cc	cc:paul shen cc:pauls	Messages with Paul Shen in the Cc field.

	cc:pauls@contoso.com	
From	from:bharat suneja from:bsuneja from:bsuneja@contoso.com	Messages sent by Bharat Suneja.
Keywords in retention policy	retentionpolicy:business critical	Messages that have the Business Critical retention tag applied.
Date when messages expire according to policy	expires:4/1/2010	Messages that expire on April 1, 2010.
Sent	sent:yesterday	All messages sent yesterday.
Subject	Subject:"patent filing"	All messages where the phrase "patent filing" appears in the Subject field.
To	to:"ben smith" to:bsmith to:besmith@contoso.com	Messages that have Ben Smith in the To field.

Return to top

Exchange Search and Attachments

Exchange Search indexes text content contained in e-mail attachments. Support for different file formats is provided using search filters. Exchange Setup installs a number of search filters by default, providing support for indexing many popular file formats, including Microsoft Office files. For a list of search filters installed by Exchange Setup, see Default Filters for Exchange Search. You can install additional search filters for file formats that you want Exchange Search to index. Search filters for different file formats are available from many partners and third parties. The following applies to indexing:

- **Unsearchable items** When Exchange Search can't index a file because a search filter for the file format isn't installed on the Mailbox server, the item is treated as an unsearchable item. An item may also be marked as unsearchable due to other reasons. You can retrieve a list of unsearchable items per mailbox, mailbox database, or mailbox server, using the **Get-FailedContentIndexDocuments** cmdlet. For details, see Diagnose Exchange Search Issues. You can also include unsearchable items when you perform a discovery search using Multi-Mailbox Search.
- **Safe list** Certain file types are considered to have no content that can be indexed by Exchange Search. These file types are added to a safe list by creating a null filter value in the registry. Exchange Setup creates a null filter registry value for several file types. Mailbox items containing these file types aren't returned in the list of unsearchable items. For a list of default search filters and default null filter entries, see Default Filters for Exchange Search.
- **Encrypted items** Messages encrypted using S/MIME aren't indexed by Exchange Search. Encrypted messages are returned as unsearchable items if you use the Get-FailedContentIndexDocuments cmdlet.
- **IRM-protected items** Messages protected using Information Rights Management (IRM) are indexed by Exchange Search and included in search results. Messages must be protected by using an Active Directory Rights

Management Services (AD RMS) server in the same Active Directory forest as the Exchange 2010 Mailbox server. For details, see Information Rights Management.

Note:
In Cached Exchange Mode, attachments are also indexed by Windows Search. Windows Search uses search filters installed on the user's computer.

Return to top

Improvements Over Exchange Server 2003 Content Indexing

The search functionality in Exchange 2003 (content indexing) is replaced with Exchange Search in Exchange 2010. Exchange Search provides the following feature and functionality improvements over content indexing:

- Utilization of system resources such as CPU, memory, disk I/O, and disk space required for its indexes is improved, which significantly increases overall performance.
- New messages are typically indexed within 10 seconds of arrival, and query results are returned within seconds.
- Exchange Search is automatically enabled upon installation and doesn't require any configuration.
- Attachments can now be indexed. Several attachment types are supported, including Microsoft Office documents, text attachments, and HTML attachments.
- Indexing is automatically withheld for a specific mailbox database, which reduces the disk I/O load. Also, indexing is automatically withheld for the entire Mailbox server, which reduces both disk I/O and CPU utilization for Exchange Search.
- There is an easily accessible search bar in Outlook Web App and query builder support in Outlook 2010 and Outlook 2007.

Return to top

Difference Between Exchange Search and Exchange Store Search

Exchange Search allows you to quickly search text in messages through the use of pre-built indexes. Exchange store search is based on a sequential scan of all the messages in the search scope instead of using the pre-built indexes The following table compares some of the differences between Exchange Search and Exchange store search.

Exchange Search vs. Exchange store search

Exchange Search	Exchange store search
Faster	Slower
Searches the content index created by crawling the mailbox database	Searches the store
Indexes new items within seconds of creation or delivery to a mailbox	May not return newer items
Uses words, phrases, and sentences, ignores punctuation and spaces, not case-	Searches stream of bytes, finds only exact matches

sensitive	
Supports only prefix searches, doesn't support substring matches	Supports substring matches
Searches attachments using available search filters	Doesn't search within attachments
Can search messages in different languages	Not language-aware

Return to top

Exchange Search and Localization

Localization support for Exchange Search is limited to scenarios in which the client locale matches the message locale (which must also match the language used in the message body). Exchange Search doesn't support instances where a single message has multiple languages embedded in the body or where the client locale is different from the message locale.

To get consistent results for localized searches, the following must be true:

- An e-mail message must be written in a single language and that language must match the locale of the message.
- The search expression must be in a single language.
- The language must match the locale of the client computer, as identified by the connection to the server.

Return to top

Exchange Search and Database Availability Groups

In organizations that have a database availability group (DAG), during the seeding process, DAG members with a passive mailbox database copy replicate the content index catalog from the DAG member that has the active mailbox database copy. The content index is typically 10 percent the size of the mailbox database. After initial seeding, the server with the passive database copy gets message data from the server with the active database and performs content indexing locally. The bandwidth used for copying message content for indexing is in addition to the bandwidth used for replication of transaction logs. When planning a high availability deployment, you must consider the bandwidth used by Exchange Search.

The Exchange 2010 Mailbox Server Role Requirements Calculator includes content indexing considerations when calculating the bandwidth required for content indexing in a DAG. For more information about the calculator, including a link to download the calculator, see the Exchange Server Team Blog article Exchange 2010 Mailbox Server Role Requirements Calculator.

To learn more about DAGs, see Understanding Database Availability Groups.

1.8.1.8 Understanding Hierarchical Address Books

Understanding Hierarchical Address Books

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

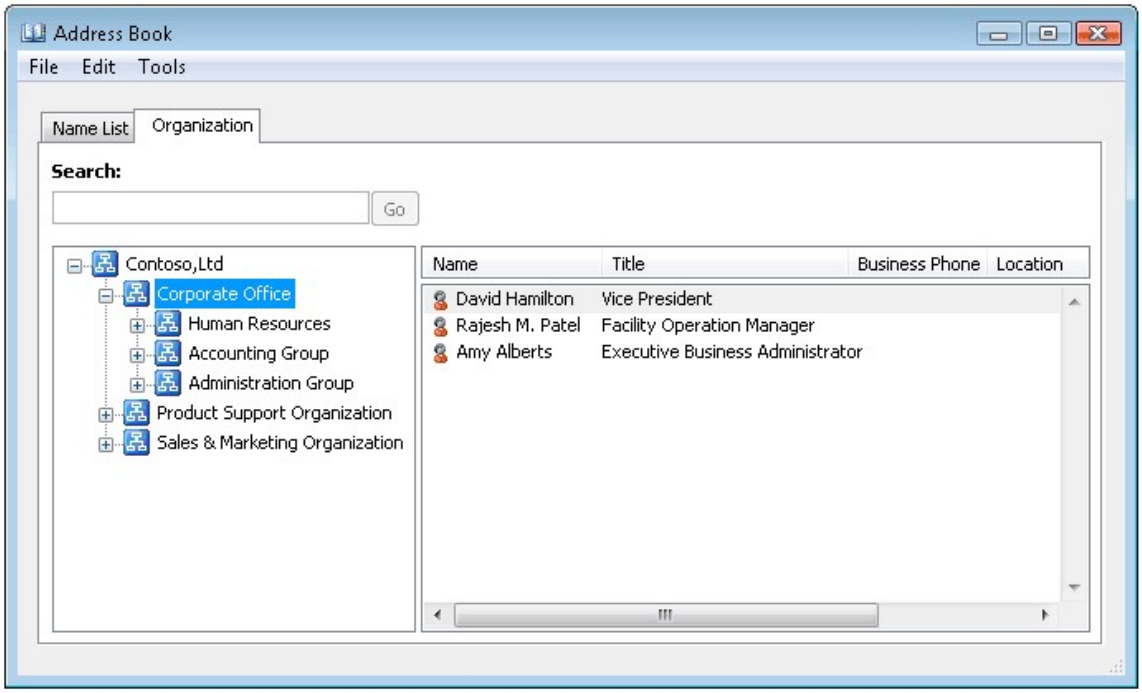
Topic Last Modified: *2010-09-30*

The hierarchical address book (HAB) is a feature in Microsoft Exchange Server 2010 and the Microsoft Outlook 2010 address book that enables end users to browse for recipients in their Exchange organization using an organizational hierarchy. In most Exchange 2010 deployments, users are limited to the default global address list (GAL) and its associated recipient properties. Additionally, the structure of the GAL often doesn't accurately reflect the management or seniority relationships among recipients in your organization. Being able to customize an HAB that maps to your organization's unique business structure provides your users with an efficient method for locating internal recipients.

Using Hierarchical Address Books

In an HAB, your root organization (for example, Contoso, Ltd) is used as the top-level tier. Under this top-level tier, you can add several child tiers to create a customized HAB that's segmented by division, department, or any other organizational tier you want to specify. The following figure illustrates an HAB for Contoso, Ltd with the following structure:

- The top-level tier represents the root organization Contoso, Ltd.
- The second-level child tiers represent the business divisions within Contoso, Ltd: Corporate Office, Product Support Organization, and Sales & Marketing Organization.
- The third-level child tiers represent departments within the Corporate Office division: Human Resources, Accounting Group, and Administration Group.



You can provide an additional level of hierarchical structure by using the *SeniorityIndex* parameter. When creating an HAB, use the *SeniorityIndex* parameter to rank individual recipients or organizational groups by seniority within these organizational tiers. This

ranking specifies the order in which the recipients or groups are displayed in the HAB. For example, in the preceding example, the *SeniorityIndex* parameter for the recipients in the Corporate Office division is set to the following:

- 100 for David Hamilton
- 50 for Rajesh M. Patel
- 25 for Amy Alberts

Note:

If the *SeniorityIndex* parameter isn't set or is equal for two or more users, the HAB sorting order uses the *PhoneticDisplayName* parameter value to list the users in ascending alphabetical order. If the *PhoneticDisplayName* parameter value isn't set, the HAB sorting order defaults to the *DisplayName* parameter value and lists the users in ascending alphabetical order.

Configuring Hierarchical Address Books

Detailed instructions for creating HABs are included in the topic Configure Hierarchical Address Books. The general steps are as follows:

1. Create a distribution group that will be used for the root organization (top-level tier). If desired, you can use an existing organizational unit in your Exchange forest for the distribution group.
2. Create distribution groups for the child tiers and designate them as members of the HAB. Modify the *SeniorityIndex* parameter of these groups so they're listed in the proper hierarchical order within the root organization.
3. Add organization members. Modify the *SeniorityIndex* parameter of the members so they're listed in the proper hierarchical order within the child tiers.
4. For accessibility purposes, you can use the *PhoneticDisplayName* parameter, which specifies a phonetic pronunciation of the *DisplayName* parameter. To learn more about the *PhoneticDisplayName* parameter and speech recognition, see Understanding Automatic Speech Recognition Directory Lookups.

1.8.1.9 Understanding Mailbox Import and Export Requests

Understanding Mailbox Import and Export Requests

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Microsoft Exchange Server 2010 Service Pack 1 (SP1) introduces a new method for importing and exporting mailboxes. Using the **MailboxImportRequest** or **MailboxExportRequest** cmdlet sets, you can import data from or export data to .pst files. After you initiate a mailbox import or export request, the process is completed asynchronously by the Microsoft Exchange Mailbox Replication service (MRS). MRS resides on all Exchange 2010 Client Access servers and is the service responsible for moving mailboxes, importing and exporting .pst files, and restoring disabled and soft-deleted mailboxes.

For information about how to perform mailbox import and export requests, see Managing Mailbox Import and Export Requests.

Contents

Reasons to Import or Export Mailbox Data

There are several reasons why you may want to import or export mailbox data:

- **Satisfy compliance requirements** You can export mailbox content to a .pst file for legal discovery purposes. After the export is complete, you can import the content to a mailbox used specifically for compliance purposes.
- **Create a point-in-time snapshot of a mailbox** By creating a snapshot of specific mailboxes, you avoid having to retain an entire backup set for a mailbox database.
- **Move a user's .pst file into his or her mailbox or personal archive** Microsoft Outlook users can save their e-mail locally as .pst files. Using the New-MailboxImportRequest cmdlet, you can move data from a user's .pst file to his or her mailbox or personal archive. This is an easy method for transferring e-mail from a user's local computer to Exchange servers. To learn more, see Understanding Personal Archives.

Return to top

Limitations to Importing and Exporting Mailbox Data in Previous Versions of Exchange

Exchange Server 2007 and the release to manufacturing (RTM) version of Exchange 2010 use the **Import-Mailbox** and **Export-Mailbox** cmdlets to import and export .pst files. There are limitations to using these cmdlets:

- You must install Outlook on an Exchange server dedicated to importing and exporting mailbox data. As a result, you must purchase both an Exchange and an Outlook license solely for this purpose.
- The .pst file must reside on the server dedicated to importing and exporting mailbox data.
- The import or export operation is performed by the related cmdlet, and content in the .pst file moves through the dedicated server. Therefore, you can't shut down the session until the import or export is complete.

Return to top

Advantages to Using Import and Export Requests

The following are advantages to using import and export requests in Exchange 2010 SP1:

- A .pst provider is included in Exchange 2010 SP1 that can read and write .pst files.
- Import and export requests are asynchronous. The process is performed by MRS, which takes advantage of the queuing and throttling frameworks.
- The .pst files can be imported directly to a user's personal archive.
- Multiple .pst files can be imported or exported at the same time.
- Import and export cmdlets can be run against any Exchange 2010 SP1 server in your organization.
- The .pst files can reside on any shared network drive accessible by your Exchange servers.
- The following types of .pst files are supported by Exchange 2010 SP1:
  - Unicode and ANSI files created by Office Outlook 2003
  - Unicode files created by Office Outlook 2007 and Outlook 2010
  - Unicode files created by the Exchange 2010 SP1 New-MailboxExportRequest cmdlet
  - ANSI files created by the Exchange Server Mailbox Merge wizard (ExMerge)

Return to top

Permissions

You must have the correct permissions to import or export mailbox data. By default, none of the role groups include the Mailbox Import Export role. You must add the Mailbox Import Export role to a role group. If you try to run the import or export cmdlets without the correct permissions, you receive an error stating that the cmdlet doesn't exist.

For details, see Add the Mailbox Import Export Role to a Role Group.

Note:

After you add the Mailbox Import Export role to a role group, you must restart the Exchange Management Shell.

Return to top

Considerations

Before you import or export mailbox data, consider the following:

- To import or export mailbox data, a network shared folder accessible by your Exchange servers must be set up. You must also grant read/write permissions to the Exchange Trusted Subsystem group so that group can access the network share where you import and export mailbox data. If you don't grant this permission, you receive an error message stating that Exchange is unable to establish a connection to the target mailbox.
- The maximum .pst file size supported by Outlook is 50 gigabytes (GB). Therefore, we recommend that you don't import a .pst file larger than 50 GB. You can create multiple .pst files for mailboxes larger than 50 GB by specifying specific folders to include or exclude or by using a content filter.
- Import and export requests are performed by MRS, which also processes move requests and mailbox restore requests. All requests are queued and throttled by MRS. To learn more, see Throttling the Mailbox Replication Service.
- Importing and exporting mailbox data may take several hours depending on

file size, network bandwidth, and MRS throttling.
- Data can't be imported to a public folder or public folder database.

Return to top

Importing Mailbox Data

Use the **MailboxImportRequest** cmdlet set to import data from a .pst file to a mailbox or personal archive. The following is a list of options you can specify when importing mailbox data from a .pst file:

Note:
The mailbox to which you import the data must exist. You can't import data to a user account that doesn't have a mailbox.

- You can import data to a different user account than the one from which it was exported. For example, you can export data from john@contoso.com and import it to legaldiscovery@contoso.com.
- You can import items to only the user's personal archive by specifying the *IsArchive* parameter.
- If associated folder messages exist in the .pst file, you can import them using the *AssociatedMessagesCopyOption* parameter. Associated messages contain hidden data with information about rules, views, and forms. If they exist in the .pst file, all messages from the transport dumpster are imported.
- You can include or exclude specific folders using the *IncludeFolders* or *ExcludeFolders* parameter.
- You can exclude the Recoverable Items folder using the *ExcludeDumpster* parameter. By default, an import request includes the user's Recoverable Items folder if it's present in the .pst file.

MailboxImportRequest Cmdlet Set

Use the following cmdlets for mailbox import requests.

Cmdlet	Description	Topic
New-MailboxImportRequest	Start the process of importing a .pst file to a mailbox or personal archive. You can create more than one import request per mailbox. Each request must have a unique name.	Create a Mailbox Import Request
Set-MailboxImportRequest	Change import request options after the request is created or recover from a failed request.	Configure Mailbox Import Request Properties
Suspend-MailboxImportRequest	Suspend an import request any time after the request is created but before the request reaches the status of Completed.	Suspend a Mailbox Import Request
Resume-MailboxImportRequest	Resume an import request that's suspended or failed.	Resume a Mailbox Import Request
Remove-MailboxImportRequest	Remove fully or partially completed import requests. Completed import requests aren't automatically cleared.	Remove a Mailbox Import Request

	You must use this cmdlet to remove them.	
Get-MailboxImportRequest	View general information about an import request.	View Mailbox Import Request Properties
Get-MailboxImportRequestStatistics	View detailed information about an import request.	View Mailbox Import Request Properties

Return to top

Exporting Mailbox Data

Use the **MailboxExportRequest** cmdlet set to export mailbox data to a .pst file. You can export one mailbox or several mailboxes, but only one request is written to each .pst file at a time. The following is a list of options you can specify when exporting mailbox data to a .pst file:

- You can export personal archive data using the *IsArchive* parameter.
- You can filter the messages that are exported using the *ContentFilter* parameter. You can filter by message content, attachment, senders, recipients, Inbox category, importance, message type, message size, and when the message was sent, received, or expired. For more information, see Filterable Properties for the -ContentFilter Parameter.
- You can specify folders to include or exclude using the *IncludeFolders* or *ExcludeFolders* parameter. If exporting data from an Exchange 2010 mailbox, you can also exclude the Recoverable Items folder using the *ExcludeDumpster* parameter.
- You can export associated messages using the *AssociatedMessagesCopyOption* parameter. Associated messages contain hidden data with information about rules, views, and forms. By default, associated items aren't copied to the .pst file.

MailboxExportRequest Cmdlet Set

Use the following cmdlets for mailbox export requests.

Cmdlet	Description	Topic
New-MailboxExportRequest	Start the process of exporting data from a primary mailbox or personal archive to a .pst file. You can create more than one export request per mailbox. Each request must have a unique name.	Create a Mailbox Export Request
Set-MailboxExportRequest	Change export request options after the request is created or recover from a failed request.	Configure Mailbox Export Request Properties
Suspend-MailboxExportRequest	Suspend an export request any time after the request is created but before the request reaches the status of Completed.	Suspend a Mailbox Export Request
Resume-	Resume an export request	Resume a Mailbox Export

MailboxExportRequest	that's suspended or failed.	Request
Remove-MailboxExportRequest	Remove fully or partially completed export requests. Completed export requests aren't automatically cleared. You must use this cmdlet to remove them.	Remove a Mailbox Export Request
Get-MailboxExportRequest	View general information about an export request.	View Mailbox Export Request Properties
Get-MailboxExportRequestStatistics	View detailed information about an export request.	View Mailbox Export Request Properties

Return to top

1.8.1.10 Understanding Move Requests

Understanding Move Requests

Exchange Server 2010 > Mailbox > Understanding Mailbox >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-28*

When you move a mailbox, you're moving it from a *source mailbox database* to a *target mailbox database*. The target mailbox database can be on the same server, on a different server, in a different domain, in a different Active Directory site, or in another forest.

Note:
This topic doesn't cover moving mailboxes to or from Microsoft Office Outlook Web App.

Contents

Personal Archives

Shared Mailboxes and Resource Mailboxes

Mailbox Moves During Server Failures

Client Experience

Looking for management tasks related to move requests? See Managing Move Requests.

Cautions

When moving mailboxes, consider the following:

- You can't use the Exchange System Manager or Active Directory Users and Computers to move mailboxes from Microsoft Exchange Server 2003 to Exchange Server 2010.
- You can't use the **Move-Mailbox** cmdlet in Exchange Server 2007 to move mailboxes from Exchange 2007 to Exchange 2010.
- When you move mailboxes, users won't be able to view their message tracking information.

Return to top

Changes in Exchange 2010 SP1

The following changes were made to move request functionality in Exchange 2010 Service Pack 1 (SP1):

- Exchange 2010 SP1 now *soft deletes* the mailbox on the source database, so that you can recover the mailbox in the event of a Mailbox server failover or data loss. You can restore a soft-deleted mailbox by using the **MailboxRestoreRequest** cmdlet set. To learn more, see Soft-Deleted Mailboxes later in this topic.

  Note:
  Soft-deleted mailboxes require that both the source Mailbox server and the Client Access server performing the request be running Exchange 2010 SP1.

- The **MoveRequest** cmdlet set has been updated to support moving archives to a separate database.

Return to top

Limitations to Moving Mailboxes in Previous Versions of Exchange

Exchange 2007 uses the **Move-Mailbox** cmdlet to move mailboxes between mailbox databases. There are limitations to using this cmdlet:

- Mailbox moves are offline. While you move a mailbox, which can take several hours, the user can't access the mailbox.
- Moving mailboxes is synchronous. The cmdlet does the actual move, and you can't close the Exchange Management Shell session while the move is being performed.
- The Dumpster folder isn't moved with the mailbox.
- Content indexing doesn't begin until after the move is completed. This results in a poor search experience for users until the indexing is completed.

- Move throttling is manually controlled by administrators.
- Moving mailboxes across forests requires direct access to Active Directory and the mailbox database.

Return to top

Advantages of Move Requests

Move requests are a new feature in Exchange 2010. There are multiple advantages to using move requests:

- Mailbox moves are asynchronous and are performed by the Microsoft Exchange Mailbox Replication service (MRS). To learn more, see Asynchronous Mailbox Moves later in this section.
- Mailboxes are kept online during the asynchronous moves. To learn more, see Online Mailbox Moves later in this section.
- The items in a mailbox's Recoverable Items folder are moved with the mailbox.

  Note:
  The Recoverable Items folder is available only in Exchange 2010. To learn more, see Understanding Recoverable Items.

- As soon as the mailbox move begins, content indexing starts to scan the mailbox so that fast searching is available upon completion of the move.
- You can configure throttling for each MRS instance, each mailbox database, or each Mailbox server.
- Remote mailbox moves work over the Internet by way of the Microsoft Exchange Mailbox Replication Proxy (MRSProxy) service. You don't need to set up a direct back-end server and Active Directory access between the forests.
- Mailbox moves can be managed from any Exchange 2010 server within the organization.
- Mailbox content doesn't move through an administrative computer. For example, in Exchange 2007, when you run the **Move-Mailbox** cmdlet, the data move is managed by the computer on which you run the cmdlet. You can't shut down that session of Exchange until the move completes.
- The mailbox's move history is maintained in the mailbox.

Asynchronous Mailbox Moves

Using the move request cmdlets in Exchange 2010, you can perform an asynchronous move because the cmdlets don't perform the actual move. The move is performed by MRS, a service that runs on all Client Access servers in your Exchange 2010 organization. Using MRS is beneficial because you can manage mailbox moves from any Exchange 2010 server within your organization after the move request is started. For more information, see Microsoft Exchange Mailbox Replication Service later in this topic.

Online Mailbox Moves

In an *online mailbox move*, end users can still access their e-mail accounts during the move. The user is only locked out of the account for a brief time at the end of the process (when the final synchronization occurs). Online mailbox moves are supported between Exchange 2010 databases and between Exchange 2007 SP3 and Exchange 2010 databases. You can perform online mailbox moves across forests or in the same forest. The process for local mailbox moves and remote mailbox moves is different from online moves and is discussed later in this topic.

Return to top

Reasons for Moving Mailboxes

You may need to move mailboxes in the following scenarios:

- **Transition** When you transition an existing Exchange 2007 or Exchange

Server 2003 organization to Exchange 2010, you move mailboxes from the existing Exchange servers to an Exchange 2010 Mailbox server.

- **Realignment** You can move mailboxes for realignment purposes. For example, you may want to move a mailbox from one database to a database that has a larger mailbox size limit.
- **Investigating an issue** If you need to investigate an issue with a mailbox, you can move that mailbox to a different server. For example, you can move all mailboxes that have high activity to another server.
- **Corrupted mailboxes** If you encounter corrupted mailboxes, you can move the mailboxes to a different server or database. The corrupted messages won't be moved.
- **Physical location changes** You can move mailboxes to a server in a different Active Directory site. For example, if a user moves to a different physical location, you can move that user's mailbox to a server closer to the new location.
- **Separation of administrative roles** You may want to separate Exchange administration from Windows operating system account administration. To do this, you can move mailboxes from a single forest into a resource forest scenario. In this scenario, the Exchange mailboxes reside in one forest and their associated Windows user accounts reside in a separate forest.
- **Outsourcing e-mail administration** You may want to outsource the administration of e-mail and retain the administration of Windows user accounts. To do this, you can move mailboxes from a single forest into a resource forest scenario.
- **Integrating e-mail and user account administration** You may want to change from a separated or outsourced e-mail administration model to a model in which e-mail and user accounts can be managed from within the same forest. To do this, you can move mailboxes from a resource forest scenario to a single forest. In this scenario, the Exchange mailboxes and Windows user accounts reside in the same forest.

Return to top

Supported Scenarios for Moving Mailboxes

The following table lists the supported scenarios for moving Exchange mailboxes and includes links to related topics.

Supported scenarios for moving mailboxes

Moving from	Moving to	Supported	Online move supported	Related topic
Exchange 2010	Exchange 2010	Yes	Yes	Managing Move Requests
Exchange 2007 SP3	Exchange 2010	Yes	Yes	Move Mailboxes from Exchange 2007 Servers to Exchange 2010 Servers
Exchange 2007 SP1	Exchange 2010	No	No	Move Mailboxes from Exchange 2007 Servers to Exchange 2010 Servers

Exchange 2003 SP2	Exchange 2010	Yes	No	Move Mailboxes from Exchange 2003 Servers to Exchange 2010 Servers
Exchange 2010	Exchange 2007 SP3	Yes	No	Move Mailboxes from Exchange 2010 Servers to Exchange 2007 Servers
Exchange 2010	Exchange 2003 SP2	Yes	No	Move Mailboxes from Exchange 2010 Servers to Exchange 2003 Servers
Exchange 2000	Exchange 2010	No	No	Not applicable
Exchange 2010	Exchange 2000	No	No	Not applicable

Return to top

Services Used in Move Requests

Move requests are processed by two services:

- Microsoft Exchange Mailbox Replication service (MRS)
- Microsoft Exchange Mailbox Replication Proxy (MRSProxy) service

Microsoft Exchange Mailbox Replication Service

When you use the move request cmdlets to move mailboxes, MRS processes the move process. As stated earlier, MRS resides on an Exchange 2010 Client Access server and is the service that moves mailboxes from the source database to the target database. In Exchange 2007, the mailbox move is performed by the **Move-Mailbox** cmdlet. By using a service as the agent of the move, mailboxes can be moved while simultaneously remaining accessible to users. During the move, you can view, cancel, and manage the move request from any Exchange 2010 server in your organization.

You can start and stop MRS as you would any service. MRS constantly checks for all move requests in its own Active Directory site. In addition, there's a sharing mechanism between all instances of MRS so that no two servers will attempt to perform the same move request.

All MRS instances in an Active Directory site work together so that database and Client Access server throttling is handled across all instances of MRS. MRS throttling is controlled by a configuration file. For more information about how to modify the configuration file, see Throttling the Mailbox Replication Service.

Microsoft Exchange Mailbox Replication Proxy Service

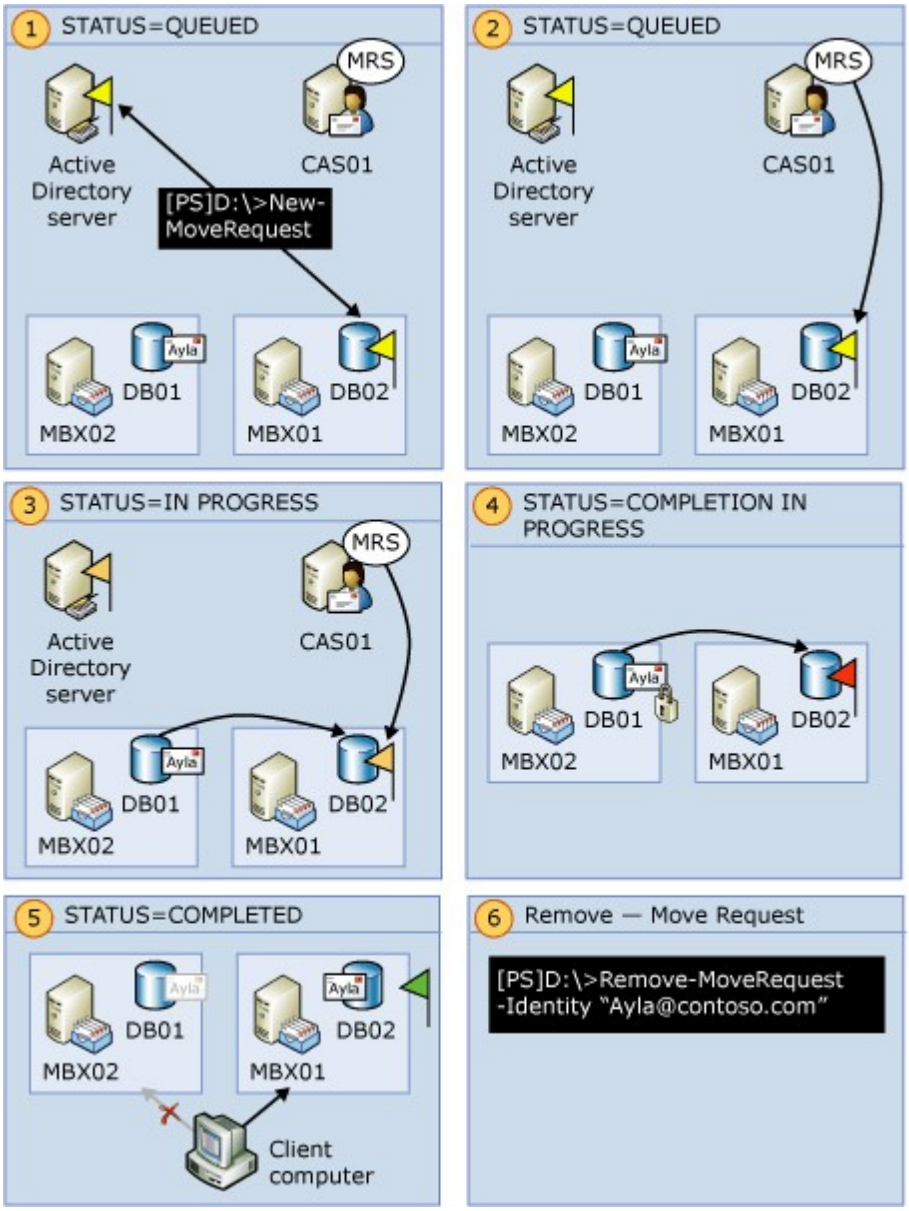
In addition to MRS, the MRSProxy service is installed on every Exchange 2010 Client Access server. MRSProxy helps to facilitate cross-forest move requests and runs on the remote forest's Exchange 2010 Client Access server. However, MRSProxy is disabled by default. You need to turn on the MRSProxy service on the remote forest. We recommend that you enable MRSProxy on all Client Access servers in the remote forest.

For more information, see Start the MRSProxy Service on a Remote Client Access Server.

Return to top

Basic Move Request Process

The following figure illustrates the basic process for local move requests.



In this scenario, Ayla's mailbox will be moved from the source database DB01 on Mailbox server MBX02 to the target database DB02 on Mailbox server MBX01. To do this, you run the following command.

```
New-MoveRequest -Identity Ayla@contoso.com -TargetDatabase "DB02"
```

The following steps describe the basic process for local move requests:

1. The command updates Active Directory, and then places a special message in the system mailbox within that Active Directory site that a move request has been initiated and is set to a status of **Queued**. Information about the move request is stored in two places: the target database's system mailbox and in Active Directory. If the move is an offline move, the mailbox is locked and

can't be accessed until the move reaches a status of **Completed**.

2. All instances of MRS periodically check the system mailbox on every database in its Active Directory site to verify if there are any queued move requests. In this example, the MRS instance on CAS01 finds Ayla's mailbox in the **Queued** status.

   Note:
   The **New-MoveRequest** cmdlet selects an instance of MRS and requests that the service process the move request immediately. If the selected instance of MRS is available, it starts the move immediately. If not, the mailbox remains in the **Queued** status until an MRS instance finds the move request.

3. MRS begins to move the data from DB01 to DB02. MRS updates the mailbox's status in the system mailbox to **In Progress**.
4. When the move is almost finished, Ayla's mailbox is locked for a short time while the final mailbox synchronization is completed. At this point, the move request status changes to **Completion In Progress**.
5. When the move is complete, Ayla's new mailbox on DB02 is activated, and the old mailbox on DB01 is soft deleted. The move request status changes to **Completed**. Depending on Ayla's e-mail client, she may need to log off and log on again to access her mailbox. For more information, see Client Experience later in this topic.
6. The administrator clears the move request information from Active Directory and on the system mailbox on DB02. Until the move request information is cleared, you can't move the mailbox again. For details about how to clear a move request, see Clear or Remove Move Requests.
   A record of the move is kept in Ayla's mailbox and can be accessed by running the Get-MailboxStatistics cmdlet with the *IncludeMoveReport* parameter. For more information, see View Move Request Properties.

Return to top

Remote Mailbox Moves

Remote mailbox moves are also known as cross-forest mailbox moves. Exchange 2010 supports two types of remote mailbox moves:

- **Remote mailbox moves that have Exchange 2010 in both forests** In this scenario, one forest is an Exchange 2010 forest, and the other forest has at least one Exchange 2010 Client Access server. You can use the Exchange Management Console (EMC) or the Exchange Management Shell to perform these mailbox moves. For details, see Create a Remote Move Request That has Exchange 2010 in Both Forests.
- **Remote mailbox moves with a legacy Exchange forest** In this scenario, one forest contains Exchange 2010, and the other forest contains Exchange 2003 SP2, Exchange 2007 SP3, or a combination of both. No Exchange 2010 Client Access server is installed in the legacy forest. You can't use the EMC to perform these mailbox moves. You must use the Shell. For details, see Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010.

Prerequisites for Moving Mailboxes Across Forests

The prerequisites for moving mailboxes across forests are extensive. For details, see Prepare Mailboxes for Cross-Forest Move Requests.

Using the TargetDatabase or the RemoteTargetDatabase Parameters

The New-MoveRequest cmdlet uses the *TargetDatabase* and the *RemoteTargetDatabase* parameters to identify the target database to which you're moving mailboxes.

TargetDatabase Parameter

The *TargetDatabase* parameter specifies the identity of the database to which you're moving the mailbox. Use this parameter to perform local and remote mailbox moves when initiating the move from the target forest. When you initiate the move from the source forest, MRS pulls the mailbox from the source forest to the target forest.

Note:

Using the *TargetDatabase* parameter is optional. If you don't specify this parameter, its usage is implied, and the mailbox provisioning load balancer specifies a target database. If you don't want the load balancer to select a database, either use the *TargetDatabase* parameter or specify the databases you want to exclude from provisioning by setting the *IsExcludedFromProvisioning* parameter to `$true` in the Set-MailboxDatabase cmdlet.

RemoteTargetDatabase Parameter

The *RemoteTargetDatabase* parameter specifies the identity of the target database in the remote forest. Use this parameter for remote mailbox moves only when you need to initiate the move from the source forest. For example, if you're moving a mailbox from an Exchange 2010 server to an Exchange 2007 or Exchange 2003 server, you initiate the move from the Exchange 2010 forest, which is the source forest. When you initiate a move from the source forest, MRS pushes the mailbox from the Exchange 2010 server to the Exchange 2007 or Exchange 2003 server.

This example pushes Tony Smith's mailbox to the remote forest.

```
New-MoveRequest -Identity 'tony@humongousinsurance.com' -RemoteLegacy -RemoteTarg
```

Remote Mailbox Moves with Exchange 2010 in Both Forests

The following describes a remote mailbox move scenario:

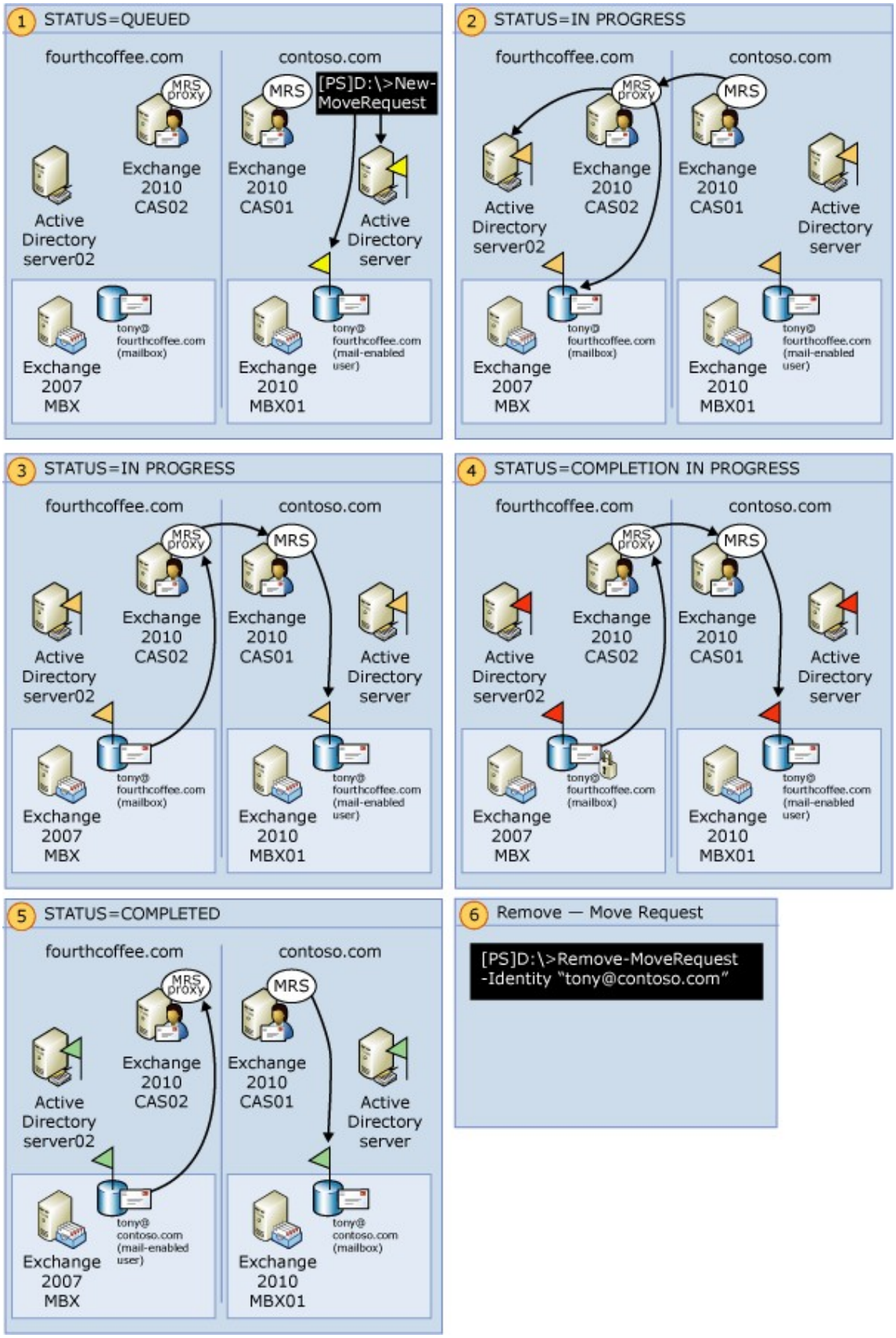
- One forest is an Exchange 2010 forest and the other forest has at least one Exchange 2010 Client Access server.
- MRS and MRSProxy exist on all Exchange 2010 Client Access servers. MRS processes the cross-forest moves.
- The Fourth Coffee and Contoso forests both contain Exchange 2010 Client Access servers, but only Contoso contains Exchange 2010 Mailbox servers. Fourth Coffee contains only Exchange 2007 SP3 Mailbox servers.
- Fourth Coffee contains the mailbox for tony@fourthcoffee.com. Contoso contains a mail-enabled user for tony@fourthcoffee.com that has all the prerequisite settings configured.
- The following command is run from the target forest, Contoso.com.

```
New-MoveRequest -Identity 'tony@fourthcoffee.com' -TargetDatabase DBa
```

Note:

If Tony's mailbox were being moved from an Exchange 2003 server, the move would be offline, and Tony wouldn't be able to access his mailbox until the move was complete.

The following figure illustrates this remote mailbox move scenario.


1 STATUS=QUEUED
fourthcoffee.com
contoso.com
[PS]D:\>New-MoveRequest
MRS proxy
MRS
Exchange 2010 CAS02
Exchange 2010 CAS01
Active Directory server02
Active Directory server
tony@fourthcoffee.com (mailbox)
tony@fourthcoffee.com (mail-enabled user)
Exchange 2007 MBX
Exchange 2010 MBX01
2 STATUS=IN PROGRESS
3 STATUS=IN PROGRESS
4 STATUS=COMPLETION IN PROGRESS
5 STATUS=COMPLETED
tony@contoso.com (mail-enabled user)
tony@contoso.com (mailbox)
6 Remove — Move Request
[PS]D:\>Remove-MoveRequest -Identity "tony@contoso.com"

1. The **New-MoveRequest** cmdlet prompts MRS on the Client Access server in the Contoso forest. The cmdlet updates the Contoso Active Directory information and the system mailbox on the target database. At this point, the move request status is **Queued**.
2. To initiate the move, MRS in the Contoso forest communicates through MRSProxy in the Fourth Coffee forest. MRSProxy then updates the Fourth Coffee Active Directory information and the system mailbox on the remote database. At this point, the status changes to **In Progress**.
3. The MRS server in the Contoso forest pulls Tony's mailbox data from the Mailbox server through the MRSProxy server in Fourth Coffee to the mail-enabled user tony@fourthcoffee.com. At this point, the status is **In Progress**.
4. When the mailbox move is almost complete, MRSProxy locks Tony's mailbox at Fourth Coffee for a short time while final synchronization is completed. At this point, the status is **Completion In Progress**.
5. In the Contoso forest, MRS converts the mail-enabled user tony@fourthcoffee.com to the mailbox tony@contoso.com. In the Fourth Coffee forest, MRSProxy converts the mailbox tony@fourthcoffee.com to the mail-enabled user tony@contoso.com, and the mailbox is soft deleted. At this point, the status is **Completed**. Tony can now access his mailbox in the Contoso forest. Depending on Tony's e-mail client, he may need to log off and log on again to access his mailbox. For more information, see Client Experience later in this topic.
6. The administrator clears the move request information from Active Directory and from the system mailbox. Until the move request information is cleared, you can't move the mailbox again. For details about how to clear a move request, see Clear or Remove Move Requests.
   A record of the move is kept in Tony's mailbox and can be accessed by running the Get-MailboxStatistics cmdlet with the *IncludeMoveReport* parameter.

Note:

If you want to move the mailbox back to the remote forest, you must initiate the move in the Contoso forest. This is because the Contoso Mailbox server is running the latest version of Exchange (in this case, Exchange 2010). In addition, you must use the *RemoteTargetDatabase* parameter when you run the **New-MoveRequest** cmdlet.

Remote Legacy Mailbox Moves

If you're moving mailboxes remotely to or from Exchange 2007 or Exchange 2003 organizations, and those organizations don't contain an Exchange 2010 Client Access server, MRS in the Exchange 2010 forest will directly access the remote legacy database and the remote organization's Active Directory server. When performing a remote legacy move request, you must supply the following information in the command:

- Identity of the mail-enabled user
- *RemoteLegacy* switch
- Fully qualified domain name (FQDN) of the remote global catalog server
- FQDN of the external e-mail address created in the source forest for the mail-enabled user when the move request is complete
- Target database when moving mailboxes to Exchange 2010 or the remote target database when moving mailboxes from Exchange 2010 to the remote legacy database

The following describes a remote legacy mailbox move scenario:

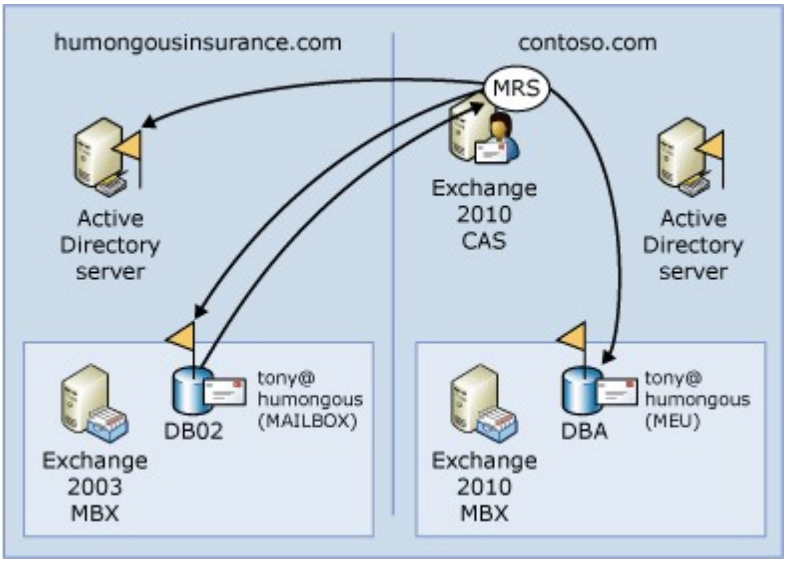
- The legacy forest (Humongous Insurance) doesn't contain an Exchange 2010 Client Access server. This scenario is similar to the remote move request process. However, because the remote legacy forest doesn't have an instance of MRSProxy to connect with, MRS in the Contoso forest connects directly to the Humongous Insurance Active Directory server and system mailbox on the Exchange 2003 mailbox database.
- When you move Exchange 2003 mailboxes to Exchange 2010, the mailbox

move will be offline. During the move, the users won't be able to access their mailboxes. When you move Exchange 2007 SP3 to Exchange 2010 mailboxes, the move will be online, and the users can access their mailboxes during the move.

- The following command is run from the target forest, Contoso.com.

```
New-MoveRequest -Identity 'tony@humongousinsurance.com' -RemoteLegacy
-TargetDatabase DB02  -RemoteGlobalCatalog 'GC01.humongousinsurance.com
```

The following figure illustrates this remote legacy mailbox move scenario.



Return to top

Mailbox Moves Using a Script

The MoveMailbox.ps1 script in Exchange 2010 provides a synchronous mailbox move management experience similar to the Exchange 2007 **Move-Mailbox** cmdlet. By default, scripts are installed at C:\Program Files\Microsoft\Exchange Server\V14\Scripts. For more information, see Move Mailboxes by Using the MoveMailbox.ps1 Script in the Shell.

Note:
You can use this script for local moves only. You can't use this script for cross-forest moves.

MoveMailbox.ps1 performs the following tasks:

1. Creates a local move request.
2. Waits for the mailbox move to complete.
3. Removes the move request after it's complete.

Return to top

Soft-Deleted Mailboxes

When mailboxes are moved from an Exchange 2010 SP1 database to any other database, Exchange doesn't fully delete the mailbox from the source database immediately upon completion of the move. Instead, the mailbox in the source mailbox database is switched to a soft-deleted state. Mailbox data can be accessed during a mailbox restore operation

using the **MailboxRestoreRequest** cmdlet set. The soft-deleted mailboxes are retained in the source database until either the deleted mailbox retention period expires or you use the Remove-StoreMailbox cmdlet to purge the mailbox.

Note:

Soft-deleted mailboxes require that both the source Mailbox server and the Client Access server performing the request be running Exchange 2010 SP1.

To view soft-deleted mailboxes, run the Get-MailboxStatistics cmdlet against a database and look for results that have a **DisconnectReason** property with a value of `SoftDeleted`.

Personal Archives

In the release to manufacturing (RTM) version of Exchange 2010, if a personal archive exists for a mailbox that you want to move, the archive gets moved with the primary mailbox. This is because the personal archive and the primary mailbox must reside on the same mailbox database. Before moving mailboxes that have a personal archive, you should consider the size of the archive. Consider database size and how that size might impact the time the move will take to complete.

In Exchange 2010 SP1, personal archives and mailboxes can exist on separate databases. The move request cmdlets and the move request user interface (UI) in the EMC support moving mailboxes and personal archives together or separately. By default, the primary mailbox and the archive are moved together. For more information about moving an archive and primary mailbox separately, see Create a Local Move Request.

If you're moving mailboxes from an Exchange 2010 server to an Exchange 2007 or Exchange 2003 server, you must first disable the personal archive before you can move the mailbox. For details, see Disable a Personal (On-Premises) or Cloud-Based Archive for a Mailbox.

To learn more about personal archives, see Understanding Personal Archives.

Return to top

Shared Mailboxes and Resource Mailboxes

In addition to the default user mailboxes, you can move shared mailboxes and resource mailboxes. A *shared mailbox* is a mailbox to which multiple users can log on. A *resource mailbox* is a mailbox that represents a type of resource, such as a conference room or video equipment. Resource mailboxes have additional properties in Active Directory that user mailboxes and shared mailboxes don't have, such as capacity.

Exchange 2003 doesn't support resource mailboxes. Instead, you must use shared mailboxes to represent resources. If you move a shared mailbox from Exchange 2003 to Exchange 2010, MRS creates the mailbox as a shared Exchange 2010 mailbox. After you move the mailbox to Exchange 2010, you can convert it to a resource mailbox. For details about how to convert a shared mailbox to a resource mailbox, see Convert a Mailbox.

Return to top

Mailbox Moves During Server Failures

Move requests can handle transient errors. MRS conducts checkpoints every 5 minutes to make sure that the database to which the mailbox being moved is still operational. If MRS finds that the target database isn't operational, MRS will pause for 30 seconds, and then retry the move. If you experience a failover, the move won't fail. Instead, MRS will detect

a database failover, determine the new location of the database, and then restart the move process.

Another error that could occur is if the Client Access server on which MRS is running stops responding. If this happens, the move stops, and one of the other MRS instances will continue the process and complete the move.

For more information, see Troubleshooting Mailbox Moves.

Return to top

Client Experience

The following table lists the different experiences end users will have, based on the version of Exchange that their mailbox is being moved to and from, and based on which client application they're using when the move request begins.

Client experience based on Exchange version and client application

Moving from	Moving to	Client application being used when the move starts	End-user experience
Exchange 2010 or Exchange 2007 SP2	Exchange 2010	Microsoft Outlook 2010, Office Outlook 2007, or Office Outlook 2003	When the move request has a status of **Completion in Progress**, the mailbox will be locked for a short time. When the move is complete, Outlook displays a message notifying the user to close and restart Outlook.
Exchange 2010	Exchange 2010	Outlook Web App	When the move request has a status of **Completion in Progress**, the mailbox is locked for a short time. If users are logged on to Outlook Web App when the mailbox is locked, or if they attempt to log on while the mailbox is locked, they will receive an error stating that the mailbox is being moved, and they won't be able to log on until the move is complete. If users aren't logged on at the time, they won't be aware of the move unless the URL

			that they use to access Outlook Web App changed. If the URL changed, users receive a message similar to the following: "Use the following link to open this mailbox with the best performance: https://mail.contoso.com/owa" When users click the link, they are directed to the new location and can log on using their credentials.
Exchange 2007 SP3	Exchange 2010	Microsoft Outlook Web Access	When the move request has a status of **Completion in Progress**, the mailbox is locked for a short time. If users are logged on to Outlook Web Access when the mailbox is locked, they are automatically logged off and need to log on again to view their mailbox. If users aren't logged on at the time, they won't be aware of the move unless the URL that they use to access Outlook Web Access changed. If it changed, users receive a message similar to the following: "Use the following link to open this mailbox with the best performance: https://mail.contoso.com/owa" When users click the link, they are directed to the new location and can log on using

			their credentials.
Exchange 2010 or Exchange 2007 SP3	Exchange 2010	Outlook Mobile Access	When the move request has a status of **Completion in Progress**, the mailbox is locked for a short time. Users experience an interruption only if the Outlook Web App URL that they use has changed. If the URL has changed, users must modify the URL in their phone's e-mail settings.
Exchange 2010 or Exchange 2007 SP3	Exchange 2010	Third-party client application	When the move request has a status of **Completion in Progress**, the mailbox is locked for a short time. If users are using a third-party client application (such as Eudora), check with the manufacturer to determine whether users need to log off and then log on again after the move request is complete.
Exchange 2003 SP2 or SP3	Exchange 2010	Outlook 2003 and Outlook Web Access	This is an offline move, and users can't access their mailbox during the move request process. However, users can use Outlook to access mail archived locally. User can't use Outlook Web Access during this time. When the move is complete, Outlook displays a message notifying users to close and restart Outlook.
Exchange 2003 SP2	Exchange 2010	Outlook Mobile Access	When the move request has a status of **Completion in Progress**, the mailbox

			is locked for a short time. Users experience an interruption only if the Outlook Web Access URL that they use has changed. If the URL has changed, users must modify the URL in their phone's e-mail settings.
Exchange 2010	Exchange 2007 SP3	Outlook 2007 and Outlook Web Access	This is an offline move, and users can't access their mailbox during the move request process. However, users can use Outlook to access mail archived locally. Users can't use Outlook Web Access during this time. When the move is complete, Outlook displays a message notifying users to close and restart Outlook.
Exchange 2010	Exchange 2003 SP2	Outlook 2003 and Outlook Web Access	This is an offline move, and users can't access their mailbox during the move request process. However, users can use Outlook to access mail archived locally. Users can't use Outlook Web Access during this time. When the move is complete, Outlook displays a message notifying users to close and restart Outlook.

Return to top

1.8.1.11 Understanding Offline Address Books

Understanding Offline Address Books

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-10*

An offline address book (OAB) is a copy of a collection of address lists that has been downloaded so that a Microsoft Outlook user can access the information it contains while disconnected from the server. Microsoft Exchange generates the new OAB files, compresses the files, and then places the files on a local share. Exchange administrators can choose which address lists are made available to users who work offline, and they can also configure the method by which the address books are distributed.

For more information about address lists, see Understanding Address Lists.

Important:

OAB data is produced by the Microsoft Exchange System Attendant service running as Local System. If an administrator uses the security descriptor to prevent users from viewing certain recipients in Active Directory, users who download the OAB will be able to view those hidden recipients. Therefore, to hide a recipient from an address list, you set the *HiddenFromAddressListsEnabled* parameter on the **Set-PublicFolder**, **Set-MailContact**, **Set-MailUser**, **Set-DynamicDistributionGroup**, **Set-Mailbox**, and **Set-DistributionGroups** cmdlets. Alternatively, you can create a new default OAB that doesn't contain the hidden recipients. For more information about how to add or remove address lists from an OAB, see Add or Remove an Address List from an Offline Address Book.

Looking for management tasks related to managing Mailbox servers? See Managing Mailbox Servers.

Contents

Moving OABs Between Exchange Versions

Exchange supports moving OABs only in the following configurations:

- Between servers running Microsoft Exchange Server 2010
- From Exchange 2010 to Exchange Server 2007 servers
- From Exchange 2007 to Exchange 2010 servers
- From Exchange Server 2003 to Exchange 2010 servers

Exchange doesn't support moving OABs from Exchange 2010 to Exchange 2003 servers.

Return to top

Outlook Clients and OAB Version

You can specify the OAB versions that are generated for client download. The following options are available:

- **OAB version 2 (ANSI OAB)** This OAB format is used with both Microsoft Exchange 2000 Server and Exchange Server version 5.5. Exchange 2003 also supports ANSI OABs. The following versions of Outlook supports OAB version 2:
  - Outlook 2010
  - Office Outlook 2007
  - Office Outlook 2003
  - Outlook 2002
  - Outlook 2000
  - Outlook 98
- **OAB version 3 (Unicode OAB)** This OAB is used for Exchange 2003. This OAB has additional information that helps Outlook reduce server remote procedure calls (RPCs). Additionally, the Unicode OAB has new features that are related to sorting rules for different language locales. These features permit the following versions of Outlook to use the correct sorting rule for the language locale with the OAB:
  - Outlook 2010
  - Outlook 2007
  - Outlook 2003
- **OAB version 4 (Unicode OAB)** This OAB was introduced in Exchange 2003 Service Pack 2 (SP2) and is supported by Outlook 2003 (SP2), Outlook 2007, and Outlook 2010. This Unicode OAB allows client computers to receive differential updates rather than full OAB downloads.

Outlook Clients That Use OAB Version 3 and Version 2

For Outlook clients that use OAB version 3 and version 2, if the size of the Changes.oab file is one-eighth (or more) the size of the entire OAB file, Outlook initiates a full OAB download.

For example, Outlook will obtain the size of the compressed Changes.oab files. Outlook will then obtain the total size of all the compressed full OAB files on the server, including the templates. If the size of the Changes.oab files is greater than one-eighth the size of the full OAB files, Outlook will download the full OAB instead of the incremental files.

Minor changes to recipient attributes will cause all recipient information to be included in the Changes.oab file. The following are examples of these minor changes:

- Updating phone numbers to reflect a new area code for a large number of recipients
- Adding an additional proxy address to a large number of recipients

Therefore, changing minimal bytes of information for half of your recipients could create a Changes.oab file that's larger than one-eighth the size of your entire OAB file.

Outlook Clients That Use OAB Version 4

For Outlook 2010, Outlook 2007, and Outlook 2003 SP2 clients that use OAB version 4, if the size of the Changes.oab files is one-half (or more) the size of the entire OAB files, Outlook initiates a full OAB download. For more information about improvements that have been made in OAB version 4, see "Improvements in Exchange 2003 SP2 and Outlook 2003 SP2" in Improvements for Offline Address Books.

Return to top

OAB Distribution Methods

You can choose which address books are made available to users who work offline. When the OAB generation (OABGen) process occurs, Exchange generates new OAB files,

compresses the files, and then places the files on a local share. You can then configure the method by which the address books are distributed. There are two methods by which the OAB is distributed to client computers:

- Web-based distribution
- Public folder distribution

Web-Based Distribution

Web-based distribution is the distribution method by which Outlook 2010 or Outlook 2007 clients that are working offline or through a dial-up connection access the OAB. If you use Web-based distribution, you don't have to use public folders.

With Web-based distribution, after the OAB is generated, the Client Access server replicates the files. Web-based distribution uses HTTPS and Background Intelligent Transfer Service (BITS). For an overview about how BITS works, see About BITS.

Important:

Although Web-based distribution is enabled by default and doesn't require further configuration, we recommend that you enable Secure Sockets Layer (SSL) for the OAB distribution point. For more information, see Require SSL for Offline Address Book Distribution.

There are several advantages to using Web-based distribution, including:

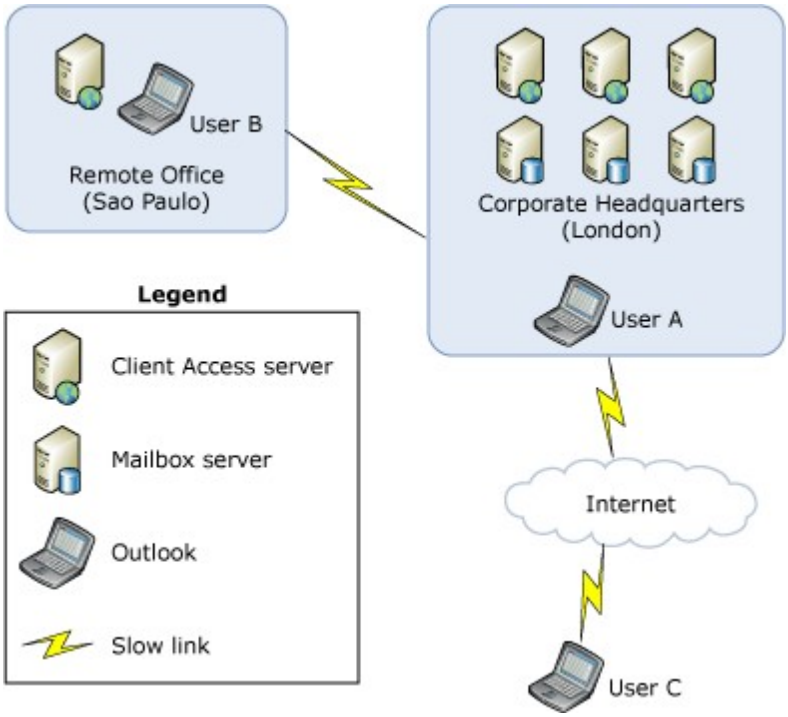
- Support of more concurrent client computers.
- Reduction in bandwidth usage.
- More control over the OAB distribution points. With Web-based distribution, the distribution point is the HTTPS Web address where client computers can download the OAB.

To benefit most from Web-based distribution, client computers must be running Outlook 2010 or Outlook 2007. Organizations that also have client computers running Outlook 2003 or earlier can use both public folder distribution and Web-based distribution. The Outlook 2003 Service Pack 1 (SP1) and earlier clients will still access their OABs by using public folders, while Outlook 2010 or Outlook 2007 clients will take advantage of the new Web-based distribution method.

To function properly, Web-based distribution depends on the following components:

- **OAB generation process** This is the process by which Exchange creates and updates the OAB. To create and update the OAB, the OABGen service runs on the OAB generation server. To support OAB distribution, this server must be an Exchange Mailbox server.
- **Microsoft Exchange File Distribution service** The Microsoft Exchange File Distribution service runs on Client Access servers and is responsible for gathering the OAB and keeping the content synched with the content on the Mailbox server.
- **OAB virtual directory** The OAB virtual directory is the distribution point used by the Web-based distribution method. By default, when Exchange is installed, a new virtual directory named OAB is created in the default internal Web site in Internet Information Services (IIS). If you have client-side users that connect to Outlook from outside your organization's firewall, you can add an external Web site. Alternatively, when you run the **New-OABVirtualDirectory** cmdlet in the Exchange Management Shell, a new virtual directory named OAB is created in the default IIS Web site on the local Exchange Client Access server. For information, see Create an Offline Address Book Virtual Directory.
- **Autodiscover service** This is a feature available in Outlook 2010 or Outlook 2007 and in some mobile devices that automatically configure the clients for access to Exchange. The service runs on a Client Access server and returns the correct OAB URL for a specific client connection. For more information about the Autodiscover service, see Understanding the Autodiscover Service.

The following figure illustrates workflow for the OAB Web-based distribution method. The figure assumes that all client users have the same OAB and that the OAB is distributed to all Client Access servers.



In this figure, a company has offices in London and Sao Paulo. The Mailbox servers for the entire company are in the corporate headquarters in London. Sao Paulo, which is a slow link, has Client Access servers to which the Sao Paulo client users connect to Outlook. In addition, the company has users who work remotely and connect to the corporate network through the Internet.

Before a user connects to a MAPI-based client computer, such as Outlook, the following happens:

1. The OAB is generated on one of the Mailbox servers in the London office.
2. On each of the Client Access servers in London, the Microsoft Exchange File Distribution service copies the new OAB files from the OAB Mailbox server in London.
3. On the Client Access server in Sao Paulo, the Microsoft Exchange File Distribution service copies the files over the slow link from the Mailbox server in London. Depending on the speed of the slow link, the copy process may take from several minutes to several hours. The new OAB isn't made available to client computers until it's completely copied and verified.

Note:
Not all Client Access servers will copy the new OAB at the exact same time. There is a poll interval (the default is 8 hours) that starts copying if there are new differential files. The first poll occurs when the Microsoft Exchange File Distribution service starts. Therefore, unless the Client Access servers were started at the same time, the server polls will be different on each Client Access server.

After all of the Client Access servers have copied the OAB content, there are several scenarios by which the client user will download the OAB:

- **Scenario 1** Onsite user

In this scenario, all actions occur in the London office:

.1.User A, who's located in the London office and whose Outlook is set to Cached Exchange Mode, connects to Outlook.
.2.Outlook connects to the Autodiscover service to obtain the URL to the closest OAB distribution point.
.3.The Autodiscover service returns the URL to one of the Client Access servers in London.
.4.Outlook uses BITS to connect to the URL that was provided by the Autodiscover service.
.5.Outlook downloads the OAB.

- **Scenario 2** Slow link user
  In this scenario, the User B mailbox resides in the London office because there are no Mailbox servers in the Sao Paulo office. Because User B is preparing to leave for a business trip and requires a local copy of the OAB, User B must download the OAB. The User B OAB will be downloaded from the Client Access server that's closest to the Sao Paulo office:
  .1.User B, who's located in the Sao Paulo office, connects to Outlook.
  .2.Outlook connects to the Autodiscover service to obtain the URL to the closest OAB distribution point.
  .3.The Autodiscover service returns the URL to the Client Access server in Sao Paulo.
  .4.Outlook uses BITS to connect to the URL that was provided by the Autodiscover service.
  .5.Outlook downloads the OAB. However, because the Sao Paulo Client Access server copies the OAB to London over a slow link, User B may not get the most recent version of the OAB.
- **Scenario 3** Internet user
  In this scenario, because the user connects using the Internet, Exchange can't locate the Client Access server that's closest to the user's physical location. Therefore, Exchange defaults to a Client Access server that's close to the user's Mailbox server:
  .1.User C, whose Mailbox server is in London, connects to Outlook from the Internet.
  .2.Outlook connects to the Autodiscover service to obtain the URL to the closest OAB distribution point.
  .3.Because the User C mailbox is located on the Mailbox server in London, the Autodiscover service returns the URL to one of the Client Access servers in London.
  .4.Outlook connects to the URL that was provided by the Autodiscover service by using BITS.
  .5.Outlook downloads the OAB.

Public Folder Distribution

Public folder distribution is the distribution method by which Outlook 2003 SP1 or earlier clients that are working offline or through a dial-up connection access the OAB. With public folder distribution, the OAB generation process places the files directly in one of the public folders, and then Exchange store replication copies the data to other public folder distribution points.

With public folder distribution, every request for a full OAB download is served immediately. For example, if a public folder that's serving 10,000 users receives 1,000 requests in one hour, and the OAB size is 5 megabytes (MB), the server will immediately transmit 5 gigabytes (GB) of data. Depending on network speed and available bandwidth, this volume of traffic could potentially overload the network for an extended period.

To prevent this overload, you can set a bandwidth threshold to limit the network bandwidth that results from OAB downloads. This process is called *throttling*.

By default, throttling is turned off. You can activate throttling by adding the following entry to the registry on all public folder servers that host OAB system folders.

Caution:
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem

Type: DWORD

Value: OAB Bandwidth Threshold (KBps)

Value Data: bandwidth threshold setting (Range: 0 to 4194304 (decimal))

The bandwidth threshold setting is in kilobytes per second (KBps) and should be configured with a decimal value. For example, setting the registry key to a decimal value of 5,000 configures the public folder server to use 5,000 KBps as the bandwidth threshold for OAB downloads, which is approximately 40,960 kilobits per second (Kbps), or 40.96 megabits per second (Mbps). After the setting has been added and configured, Exchange will dynamically detect the registry entry and begin enforcing the bandwidth limit without requiring the Microsoft Exchange Information Store service to restart.

Each time an OAB download request occurs, administrative rights on the Exchange server are verified for the requestor. If the security context that's used for the request is the equivalent of the local administrator on the Exchange server, it's assumed that an internal function is requesting the download. In this event, the requestor is allowed to proceed with a full OAB download. However, the bytes that are transmitted to the administrative client are still calculated as part of the average full OAB bytes downloaded. If the requestor doesn't have administrative rights, the average full OAB bytes that are downloaded over the last 10 seconds are determined. If this value is less than the configured threshold, a full OAB download is allowed.

Note:
Setting the registry key to 0 allows a maximum of one client without administrative rights, in 10 second intervals, at a time to download a full OAB.

When setting the OAB download bandwidth threshold, we recommend that you configure thresholds on the individual servers to values that won't cause an overload of the Exchange server's network adapter or the network. If you haven't already gathered and analyzed network and Exchange server performance data, you should do so before you configure the registry entry.

Effects of OAB Downloads on the Network When Using Public Folder Distribution

Because there are several cases that can cause a large number of full OAB downloads, you should understand the effect on bandwidth that a large OAB download has on the network.

The Exchange server can easily handle many download requests for the OAB. As a result, multiple attempts to download a full OAB over a slow link can saturate a network. (All the available bandwidth is being used.) When this happens, there are two significant effects:

- Applications that must use the wide area network (WAN) will perform slowly. This is because they wait for their network requests to traverse the saturated WAN link.
- The actual traffic needed on the WAN increases because individual network requests may time out, resulting in additional requests being made.

When the network becomes saturated, the latency increases, not only the time it takes for each client computer to download the OAB, but the overall duration of the download

process. Normally, this means that the data rate for each client computer is reduced. However, if the latency is too high, RPC packets will time out, causing additional RPC requests for the same data to be retrieved. Also, if an Outlook user attempts to download the OAB and the download is canceled or fails, Outlook deletes the data that has been downloaded and attempts to download the OAB again. As a result, more data is requested, which in turn, increases the overall duration for a large set of OAB downloads.

Outlook downloads the OAB from the Exchange server through a series of RPC packets. Each packet is received and acknowledged, and then the next packet is sent. Based on the latency between Outlook and Exchange, a single Outlook client is limited to how quickly it can receive and acknowledge each packet. Because of this delay, a single Outlook client may not be able to saturate a network link. However, as more Outlook clients begin to download the OAB, the combined download rate of all clients could saturate the link. The link will remain saturated until the full OABs are downloaded.

The relationship is linear in that the larger the latency between the Outlook client and the Exchange server, the fewer packets can be received. Fewer clients are able to download an OAB before a slow link is saturated. The reverse is also true. If latency is low, more clients are needed to saturate a slow link. The number of Outlook clients that can download the OAB simultaneously without saturating the WAN will increase as either network latency decreases or network bandwidth increases.

Return to top

OAB Considerations

As a best practice, whether you use a single OAB or multiple OABs, consider the following factors as you plan and implement your OAB strategy:

- Size of each OAB in your organization. For more information, see "OAB Size Considerations" later in this topic.
- Number of OAB downloads.
- Number and frequency of parent distinguished name changes.
- SMTP address mismatches.
- Overall number of changes made to the directory.

OAB Size Considerations

For some organizations, the OAB is a small file that remote users occasionally download. For these organizations, downloading the OAB is usually not a concern. However, for some large organizations that have large directories, or for organizations that have deployed Outlook 2003 in Cached Exchange Mode, it may be a concern, especially if the organizations have consolidated Exchange servers into a regional data center.

OAB sizes can vary from a few megabytes to a few hundred megabytes. The following factors can affect the size of the OAB:

- Usage of certificates in a company. The more public key infrastructure (PKI) certificates, the larger the OAB. PKI certificates range from 1 kilobyte (KB) to 3 KB. They're the single largest contributor to the OAB size.
- Number of mail recipients in Active Directory.
- Number of distribution groups in Active Directory.
- Information that a company adds to Active Directory for each mailbox-enabled or mail-enabled object. For example, some organizations populate the address properties on each user; others don't.

Return to top

1.8.1.12 Understanding Public Folders

Understanding Public Folders

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-17*

Public folders, introduced in the first version of Microsoft Exchange, are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization. Public folders are hierarchically organized, stored in dedicated databases, and can be replicated between servers running Exchange.

Public folders aren't designed for the following purposes:

- **Archiving data** Public folders aren't designed for archiving data. Users who have mailbox limits sometimes use public folders instead of their personal folders (.pst) files to archive data. This practice isn't recommended because it affects storage on public folder servers and undermines the goal of mailbox limits.
- **Document sharing and collaboration** Public folders aren't designed for document sharing and collaboration. Public folders don't provide versioning or other document management features, such as controlled check-in and check-out functionality, and automatic notifications of content changes.

In Exchange Server 2010, public folders are an optional feature. If all client computers in your organization are running Microsoft Outlook 2010 or Office Outlook 2007, there are no dependencies on public folders for features such as free and busy information and offline address book (OAB) downloads. Instead of using public folders for OAB downloads and free and busy information, in Exchange 2010, these features are serviced by the Autodiscover service, the Microsoft Exchange System Attendant service, and the Microsoft Exchange File Distribution service.

Until all client computers in your organization are running Outlook 2010 or Outlook 2007, you should continue using public folders.

Contents

Public Folder Database Creation During Setup

Computers running Outlook 2003 and earlier or Microsoft Entourage require a public folder database (previously called the public folder store) to connect to Exchange. Therefore, in a pure Exchange 2010 organization, as you install the Mailbox server role on the first server, Setup prompts you with the question: **Do you have any client computers running**

Outlook 2003 and earlier or Entourage in your organization? If the answer is yes, a public folder database is created. If the answer is no, a public folder database isn't created.

When you install the second server, you aren't prompted with the question, and Setup doesn't create a public folder database. Whether a public folder database is needed in the organization is decided only when you install the first server. After that, all public folder databases are optional. If you don't create a public folder database during Setup, you can always create one anytime after Setup is complete. For more information about how to create a public folder database, see Create a Public Folder Database.

In a mixed Exchange organization, Setup doesn't prompt you with the question. In these organizations, to ensure backward compatibility to Exchange versions prior to Exchange Server 2007, a public folder database is created by default. Specifically, because Exchange 2010 is installed in its own administrative group, this public folder database will support legacy Schedule+ free and busy functionality.

For more information about installing Exchange 2010, see Deploying Exchange 2010.

Return to top

Public Folder Trees

The MAPI folder tree is divided into the following subtrees:

- **Default public folders (also known as the IPM_Subtree)** Users can access these folders directly by using client applications such as Outlook.
- **System public folders (also known as the Non_IPM_Subtree)** Users can't access these folders directly by using conventional methods. Client applications such as Outlook use these folders to store information such as free and busy data, OABs, and organizational forms. Other system folders contain configuration information used by custom applications or by Exchange. The public folder tree contains additional system folders, such as the EFORMS REGISTRY folder, that don't exist in general purpose public folder trees. System folders include the following:
  - **EFORMS REGISTRY and Events Root** By default, one content replica of each of these folders resides in the default public folder database on the first Exchange server installed in the first administrative group. This is the location where organizational forms are stored for legacy Outlook clients (clients using an Outlook version earlier than Outlook 2007).
  - **Offline Address Book and Schedule+ Free Busy** The Offline Address Book folder and the Schedule+ Free Busy folder automatically contain a subfolder for each administrative group (or site) in your topology. By default, a content replica of a specific administrative group folder resides on the first server installed in the administrative group. These folders are used to store legacy free and busy information and OAB data for legacy Outlook clients. Legacy Outlook clients don't support the new features in Exchange 2010 or Exchange 2007 that manage free and busy information and OAB data. (These features include the Availability service, the Autodiscover service, and OAB distribution on Client Access servers.)
  - **OWAScratchPad** Each public folder database has an OWAScratchPad folder, which is used to temporarily store attachments that are being accessed by using Microsoft Office Outlook Web App. Don't modify this folder.
  - **StoreEvents** Each public folder database has a StoreEvents folder, which holds registration information for custom Exchange database events. Don't modify this folder.
  - **Other folders** To support internal Exchange database operations, a tree may contain several other system folders, such as schema-root. Don't modify these folders.

Return to top

Public Folder Replication

Public folder databases replicate two types of public folder information:

- **Hierarchy** Properties of the folders and organizational information about the folders (including the tree structure). All public folder databases have a copy of the hierarchy information. For a specific folder, the public folder database can use hierarchy information to identify the following:
  - Permissions on the folder
  - Servers that hold content replicas of the folder
  - Folder's position in the public folder tree (including its parent and child folders, if any)
- **Content** Messages that form the content of the folders. To replicate content, you must configure a folder to replicate its content to a specific public folder database or list of databases. Only the databases that you specify will have copies of the content. A copy of the folder that includes content is called a content replica.

Note:

Public folder content replication isn't controlled by database availability groups (DAGs). You can have public folder databases on servers that have DAGs; however, the public folders will use their own public folder replication methods outside of the DAG.

To learn more about public folder replication, see Understanding Public Folder Replication.

Return to top

Public Folder Referrals

When a client application, such as Outlook, attempts to open an Exchange public folder, the Exchange server determines which folder replica the client application should access. This process is called *public folder referral*. If a replica of the requested content exists on the Exchange server that serves the request, the client application accesses the local replica. If the replica doesn't exist on the local server, Exchange attempts to locate a replica in the same Active Directory site. You can modify the flow of user traffic to allow referrals over certain connectors by specifying a list of referral servers and assigning a routing cost to each server.

For more information about public folder referrals, see Understanding Public Folder Referrals.

Return to top

Mail-Enabled Public Folders

Mail-enabling a public folder provides an extra level of functionality to users. In addition to being able to post messages to the folder, users can send e-mail messages to, and sometimes receive e-mail messages from, the folder. If you're developing custom applications, you can use this feature to move messages or documents into or out of public folders.

A mail-enabled folder is a public folder that has an e-mail address. Depending on how the folder is configured, it may appear in the global address list (GAL). Each mail-enabled folder has an object in Active Directory that stores its e-mail address, address list name, and other mail-related attributes.

Because mail sent to public folders is directed to the public folder database instead of to a mailbox in the mailbox database, Exchange routes e-mail messages by using a method that's slightly different from the method used to route e-mail messages to a regular mailbox.

Return to top

Public Folder Access

In Exchange 2010, the following client applications can access public folders:

- Outlook 2010
- Outlook 2007
- Outlook 2003

For more information about how to create and manage public folders by using Outlook 2007, see Create and share a public folder.

For more information about how to create and manage public folders by using Outlook 2003, see Using Public Folders.

Return to top

Considerations with Mixed Exchange 2010 and Exchange 2007 Organizations

In a mixed Exchange 2010 and Exchange 2007 organization, you need to manage your public folders and public folder databases from Exchange 2010. Exchange 2007 servers don't recognize Exchange 2010 public folder databases due to Active Directory schema changes. The following table describes the expected behaviors when performing certain public folder management tasks on Exchange 2007 servers and Exchange 2010 servers.

Tasks	Exchange 2007 servers	Exchange 2010 servers
Create a public folder database	If any Exchange 2010 mailbox databases are in your organization and don't have the **msExchHomePublicDB** attribute populated, the Exchange 2007 server can't update the Exchange 2010 mailbox database's **msExchHomePublicDB** setting. Although you receive an error message, the public folder database is created. After you create the public folder database, you need to change the default public folder database. You need to perform this procedure from an Exchange 2010 server. For details, see Change the Default Public Folder Database for a Mailbox Database.	Always works.
Remove the default public folder database	If any mailbox databases are pointing to the public folder database that you're trying to remove, you receive an error message advising that you need	Works on both Exchange 2007 and Exchange 2010 servers provided that no mailbox

	to change the default public folder database. To change the default public folder database, perform the following steps: 1. On an Exchange 2010 server, change the default public folder database for the mailbox database. For details, see Change the Default Public Folder Database for a Mailbox Database. 2. On the Exchange 2007 server, remove all replicas of that public folder database. For details, see Remove Multiple Public Folders from a Public Folder Database. 3. On the Exchange 2007 server, remove the public folder database. For details, see Remove Public Folder Databases. **Note:** If the new default public folder database that you're pointing the mailbox databases to is an Exchange 2010 public folder database, see "Set an Exchange 2010 public folder database as the default public folder database for an Exchange 2007 mailbox database" later in this table.	databases have the public folder database that you're trying to remove as the default public folder database.
Remove the last public folder database in the organization	If this is the last Exchange 2007 public folder database in the organization, the **Remove-PublicFolderDatabase** cmdlet needs to update the **msExchFirstInstance** property on the Exchange 2010 public folder database to `$true`. This fails because the object version of the Exchange 2010 object is higher. Run the Remove-PublicFolderDatabase cmdlet from the Exchange 2010 server.	Works on both Exchange 2007 and Exchange 2010 servers provided that no mailbox databases have the public folder database that you're trying to remove as the default public folder database.
Set an Exchange 2010 public folder database as the default public folder database for an Exchange 2007 mailbox database	Changing the default public folder database doesn't work on an Exchange 2007 server if either the mailbox database or the public folder database is an Exchange 2010 database. Because Exchange 2007 servers don't recognize the Exchange 2010 public folder databases, the **Set-MailboxDatabase** cmdlet must be run on an Exchange 2010 server.	Always works and should be used to change the default public folder databases if your public folder database and your mailbox database are associated with different versions of Exchange.

	On the Exchange 2010 server, change the default public folder database for the Exchange 2007 mailbox database. For details, see Change the Default Public Folder Database for a Mailbox Database.	

Return to top

Considerations with Mixed Exchange 2010 and Exchange 2003 Organizations

When you install Exchange 2010 in an Exchange 2003 organization, Setup automatically creates an administrative group and routing group within the Exchange 2003 organization. The Exchange 2010 servers added to your organization are included in the new administrative group and routing group. As previously mentioned, Setup also installs a public folder database on the first Exchange 2010 Mailbox server. In that public folder database, Setup creates a free and busy folder for the new administrative group. The **legacyExchangeDN** property for users whose mailboxes were created on an Exchange 2010 server (and not migrated from Exchange 2003) maps to the Exchange 2010 administrative group name, and therefore also maps to the Free/Busy folder. By default, to facilitate free and busy searches from Outlook 2003 and earlier client users whose mailboxes reside on an Exchange 2003 server, the client users' free and busy information is posted to the Free/Busy public folder.

Management

In a mixed Exchange 2010, Exchange 2007, and Exchange 2003 organization, you can use Exchange System Manager to manage public folders. The following scenarios are supported:

- Exchange System Manager should only connect to the Exchange 2003 public folder database for administration. From there, changes replicate to Exchange 2010.
- In a pure Exchange 2010 environment or a mixed Exchange 2010 and Exchange 2007 organization, you can't reinstall Exchange System Manager to manage public folders. You must use the Exchange Management Shell.
- When verifying hierarchy replication or when viewing the Local Replica Age Limit value on a folder, we recommend using Exchange System Manager for public folders that exist on an Exchange 2003 server and using the Shell for public folders that exist on an Exchange 2010 or Exchange 2007 server.

Outlook Web App

In a mixed Exchange 2010, Exchange 2007, and Exchange 2003 organization, one of the Exchange 2010 and Exchange 2007 Client Access servers has a virtual directory named **/public**. You can fully access public folders from Outlook Web App without having to use the **/public** virtual directory.

Important:
Exchange 2010 Outlook Web App clients can’t view public folders that reside on Exchange 2003 servers.

In addition, the following public folder features are available in Outlook Web App:

- Full access to public folders on Exchange 2010 Mailbox servers without having to keep an Exchange 2003 Mailbox server available for public folder access from Outlook Web App
- Public folder search capabilities

- Web Parts support

Return to top

Updating the Public Folder Hierarchy

If you notice that the public folder hierarchy on one server is different from the public folder hierarchy on other servers, you may want to synchronize the hierarchy. In Exchange 2003 Service Pack 2 (SP2), the **Synchronize Hierarchy** command is used to synchronize the public folder hierarchy on an Exchange 2003 server with the other servers in your organization. In Exchange 2010, the **Update-PublicFolderHierarchy** cmdlet is used to synchronize the public folder hierarchy on the Exchange 2010 server with the rest of the servers in your organization.

Note:

You can't run the **Synchronize Hierarchy** command on an Exchange 2010 server. Similarly, you can't run the **Update-PublicFolderHierarchy** cmdlet on an Exchange 2003 server. However, running either command updates the public folder hierarchy in your entire organization.

For more information, see Update a Public Folder Hierarchy.

Return to top

Public Folder Content Replication

To help stop public folder content replication errors in your organization, you can suspend the replication of public folder content. Suspending replication allows you to reconfigure the public folder hierarchy and replication schedules.

To suspend or resume the replication of public folder content in a mixed organization, on an Exchange 2010 server, run the **Suspend-PublicFolderReplication** cmdlet or the **Resume-PublicFolderReplication** cmdlet in the Shell. Although you run these cmdlets on an Exchange 2010 server, they will suspend or resume the replication of public folder content on all servers in your mixed organization. For information about using the Shell to suspend or resume the replication of public folder content, see the following topics:

- Suspend Public Folder Content Replication
- Resume Public Folder Content Replication

Return to top

Best Practices

This section provides the best practices to consider when performing the following public folder tasks in your Exchange organization:

- Creating public folder databases
- Designing the public folder hierarchy
- Performing nightly maintenance

Creating Public Folder Databases

When you plan how many public folder databases to create in your organization, consider the following best practices:

- For large enterprise topologies where public folders are heavily used, deploy dedicated public folder servers. This best practice stems from the general best practice of dedicating CPU resources and disk resources to isolated server functions.

- Having fewer larger public folder databases scales better and is more easily managed than having several smaller public folder databases. By reducing the number of public folder databases, you can decrease the time required to back up and restore many smaller databases. You also reduce the amount of background replication traffic. Additionally, online maintenance of fewer larger databases is quicker than online maintenance of many smaller databases. Also, it is easier to manage a smaller number of public folder databases from the perspective of applying permissions and content access, and implementing efficient replication and referrals.
  The best practice of having fewer larger public folder databases is especially helpful when you consider your topology from the organization level. However, at the server level, some management and maintenance tasks, such as backup and restore processes, can be more quickly performed if you have several smaller databases. Ultimately, the number of public folder databases that you deploy must address your business requirements. As you determine the number of databases that you want to deploy, you must balance the cost of replication traffic against the costs of database backup, maintenance, and restore times.

Designing the Public Folder Hierarchy

As you design your public folder hierarchy, you must recognize the effect of hierarchy replication in your environment. Deep public folder hierarchies scale better than wide hierarchies. A *deep hierarchy* consists of many vertically nested folders, instead of many higher-level folders. A *wide hierarchy* consists of many higher-level folders with fewer vertically nested subfolders.

For example, consider how 250 folders might be arranged in a specific hierarchy. A wide hierarchy might have 250 direct subfolders under one parent folder. A deep hierarchy might have five top-level folders, each with five direct subfolders. Inside each of those subfolders may be 10 subfolders.

In both these examples, there are 250 folders (5 × 5 × 10 = 250). However, the deep hierarchy offers better performance than the wide hierarchy for the following reasons:

- The way that replication handles folders that have different permissions applied to them is more efficient in deep hierarchies.
- Client computer actions (such as sort, search, and expand) against a folder that has 10 subfolders is much less expensive than a folder that has 250 subfolders.

Although deep hierarchies scale better than wide hierarchies, it's a best practice not to exceed 250 subfolders per folder. Exceeding 250 subfolders likely will cause an unacceptable client experience when a client computer requests access.

A factor to consider as you implement a hierarchy is the effect that permissions have on the experience users have when they want to gain access to public folders. When each public folder subfolder has its own access control list (ACL) entries defined, every time that the Exchange server receives a new public folder replication message, the ACL for the parent public folder must be evaluated to determine which users have rights to view the changes to the parent public folder. If the parent public folder has a large discretionary access control list (DACL) entry, it may take a long time to update the view for each public folder subscriber.

Note:

The DACL for the parent folder consists of the sum of the DACLs of all the public folder subfolders.

You may have many megabytes (MB) of DACL data that must be parsed if the following conditions are true:

- There are many subfolders under a single parent public folder.
- Each of those subfolders has its own ACL defined.

This DACL data must be parsed so that the display can be updated for all the public folder subscribers every time that a public folder replication message is received.

Therefore, we recommend that you arrange your public folder hierarchy according to the user sets that gain access to the parent folders. Additionally, don't implement complex permission models for your public folder hierarchies.

Performing Nightly Maintenance

To make sure that your databases continue to operate efficiently, we recommend that you perform nightly maintenance on mailbox databases and public folder databases. Exchange Mailbox servers automate the tasks based upon the schedule that you set.

Return to top

1.8.1.12.1 Understanding Public Folder Permissions

Understanding Public Folder Permissions

Mailbox > Understanding Mailbox > Understanding Public Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-13*

You can configure public folder permissions for administrators or for users of client programs such as Microsoft Outlook. Public folder permissions consist of various access rights that specify the level of control a client user or administrator has over a public folder or public folder hierarchy.

Looking for management tasks related to public folder permissions? Check out Managing Public Folder Permissions.

Client User Access Rights and Roles

Use the Exchange Management Shell to configure the permissions for users who use client programs such as Outlook to access public folders. Whether you want to manually select the access rights or use predefined roles that contain specific access rights, you'll use the Add-PublicFolderClientPermission cmdlet.

Important:

To make sure users can send e-mail messages to a mail-enabled public folder, the public folder must have at least the CreateItems access right granted to the Anonymous account.

The following is a list of client user access rights (followed by a table that shows the predefined permission roles):

- **ReadItems** The user can read items within the specified public folder.
- **CreateItems** The user can create items within the specified public folder and send e-mail messages to the public folder if it's mail-enabled.
- **EditOwnedItems** The user can edit the items that the user owns in the specified public folder.
- **DeleteOwnedItems** The user can delete items that the user owns in the specified public folder.
- **EditAllItems** The user can edit all items in the specified public folder.
- **DeleteAllItems** The user can delete all items in the specified public folder.
- **CreateSubfolders** The user can create subfolders in the specified public

folder.

- **FolderOwner** The user is the owner of the specified public folder. The user can view and move the public folder, create subfolders, and set permissions for the folder. The user can't read, edit, delete, or create items.
- **FolderContact** The user is the contact for the specified public folder.
- **FolderVisible** The user can view the specified public folder, but can't read or edit items within the specified public folder.

The following table lists the predefined public folder roles and the access rights that are included in each role. The table headers reflect the access rights listed previously in this topic.

Note:
The FolderOwner access right and the Owner role have different permissions as shown in the following table.

Access rights included with each predefined public folder role

Role	CreateItems	ReadItems	CreateSubfolders	FolderOwner	FolderContact	FolderVisible	EditOwnedItems	EditAllItems	DeleteOwnedItems	DeleteAllItems
None						X				
Owner	X	X	X	X	X	X	X	X	X	X
PublishingEditor	X	X	X			X	X	X	X	X
Editor	X	X				X	X	X	X	X
PublishingAuthor	X	X	X			X	X		X	X
Author	X	X				X	X		X	
Non-Editing Author	X	X				X				
Reviewer		X				X				
Contributor	X					X				

Note:
Client users can use Outlook to manage public folder permissions for public folders that reside on a server running Microsoft Exchange Server 2010. For information about how to manage public folder permissions from Microsoft Office Outlook 2007 or Outlook 2010, see Create and Share a Public Folder. For information about how to manage public folder permissions for public folders that reside on Exchange 2010 servers from Office Outlook 2003, see Outlook folder permissions.

Administrator Access Rights

In Exchange 2010, there are two ways to grant administrators the rights to manage public folders:

- Public Folder Management role group
- Add-PublicFolderAdministrativePermission cmdlet

The following table describes the differences between the rights that are granted by the Public Folder Management role group and the rights that are granted by using the **Add-PublicFolderAdministrativePermission** cmdlet.

Administrator access rights differences

Public Folder Management role group	Add-PublicFolderAdministrativePermission cmdlet
The user can create top-level public folders.	The user can't create top-level public folders.
The user is granted the AllExtendedRights permission to public folders and the rights to run the public folder cmdlets.	The user can be granted or denied specific rights to public folders.
The user can administer any top-level public folder, child public folder, and system public folders in the public folder tree. In addition, this user's access rights can't be revoked by using the Remove-PublicFolderAdministrativePermission cmdlet.	The user can be granted the right to administer specific top-level public folders and specific child public folders. However, the user's access rights can be revoked by using the Remove-PublicFolderAdministrativePermission cmdlet.
The Public Folder Management role group is a Role Based Access Control (RBAC) role group that consists of the following roles: • Mail-Enabled Public Folders role • Public Folders role • Public Folder Replication role For more information, see Public Folder Management.	Not applicable

The following list describes the standard set of administrative access rights that can be set on a public folder:

- **None** The administrator doesn't have any rights to modify public folder attributes.
- **ModifyPublicFolderACL** The administrator has the right to modify Client Access server role permissions for the specified folder.
- **ModifyPublicFolderAdminACL** The administrator has the right to modify administrator permissions for the specified public folder.
- **ModifyPublicFolderDeletedItemRetention** The administrator has the right to modify the Public Folder Deleted Item Retention attributes (*RetainDeletedItemsFor*, *UseDatabaseRetentionDefaults*).
- **ModifyPublicFolderExpiry** The administrator has the right to modify the Public Folder Expiration attributes (*AgeLimit*, *UseDatabaseAgeDefaults*).
- **ModifyPublicFolderQuotas** The administrator has the right to modify the Public Folder Quota attributes (*MaxItemSize*, *PostQuota*, *PostWarningQuota*, *UseDatabaseQuotaDefaults*)
- **ModifyPublicFolderReplicaList** The administrator has the right to modify the replica list attribute for the specified public folder (*Replicas*).
- **AdministerInformationStore** The administrator has the right to modify all other public folder properties not defined previously.
- **ViewInformationStore** The administrator has the right to view public folder properties.
- **AllExtendedRights** The administrator has the right to modify all public folder

properties.

Creating Custom Role Groups

In addition to the Public Folder Management role group and the **Add-PublicFolderAdministrativePermission** cmdlet, you can create custom role groups that will allow a user to only perform certain tasks. For example, if you want to allow an administrator to manage public folders and mail-enabled public folders, but not public folder replication, you can create a custom role group that includes only the Mail Enabled Public Folders role and the Public Folders role. For more information about creating role groups, see Create a Role Group.

1.8.1.12.2 Understanding Public Folder Replication

Understanding Public Folder Replication

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

Public folder replication is the process by which public folder content and the public folder hierarchy are replicated across multiple servers for efficiency and fault tolerance purposes. When multiple public folder databases located on separate servers support a single public folder tree, Microsoft Exchange uses public folder replication to keep the databases synchronized. Public folder content exists only in Exchange stores configured to have a replica of a specific folder. Content and hierarchy information are replicated separately. Each public folder database retains a copy of the hierarchy, which includes lists of the other public folder databases that retain content replicas of each folder. Content replicas exist only on the public folder databases that you specify. For more information about how to configure public folder replication, see Configure Public Folder Replication.

Note:

Unlike in Exchange Server 2007, you can't use continuous replication in Exchange Server 2010 to replicate public folders. In Exchange 2010, continuous replication is for mailbox databases only. A public folder database can be hosted on a Mailbox server in a database availability group (DAG), but you must use multiple public folder databases and public folder replication for data redundancy.

Public folder databases replicate two types of public folder information:

- **Hierarchy** Hierarchy replication occurs when the properties of the folders and organizational information about the folders have been modified. All public folder databases have a copy of the hierarchy information. Modifying the following public folder information results in hierarchy replication:
  - Folder name
  - Replica list
  - Folder's position in the public folder tree (including any parent and child folders)
  - Permissions

  Note:

  Hierarchy replication doesn't occur when you change the e-mail addresses for a mail-enabled public folder. The e-mail addresses are stored on the directory object in Active Directory. Only by changing the properties within the public store database does hierarchy replication occur.
- **Content** Content replication occurs when messages are sent to public folders or when data is added. For example, sending e-mail messages to a mail-

enabled public folder or adding an organizational form to a public folder results in content replication. To replicate content, you must configure a folder to replicate its content to a specific public folder database or list of databases. Only the databases that you specify will have copies of the content. A copy of the folder that includes content is called a *content replica*.

Contents

Looking for management tasks related to public folders? See Managing Public Folders.

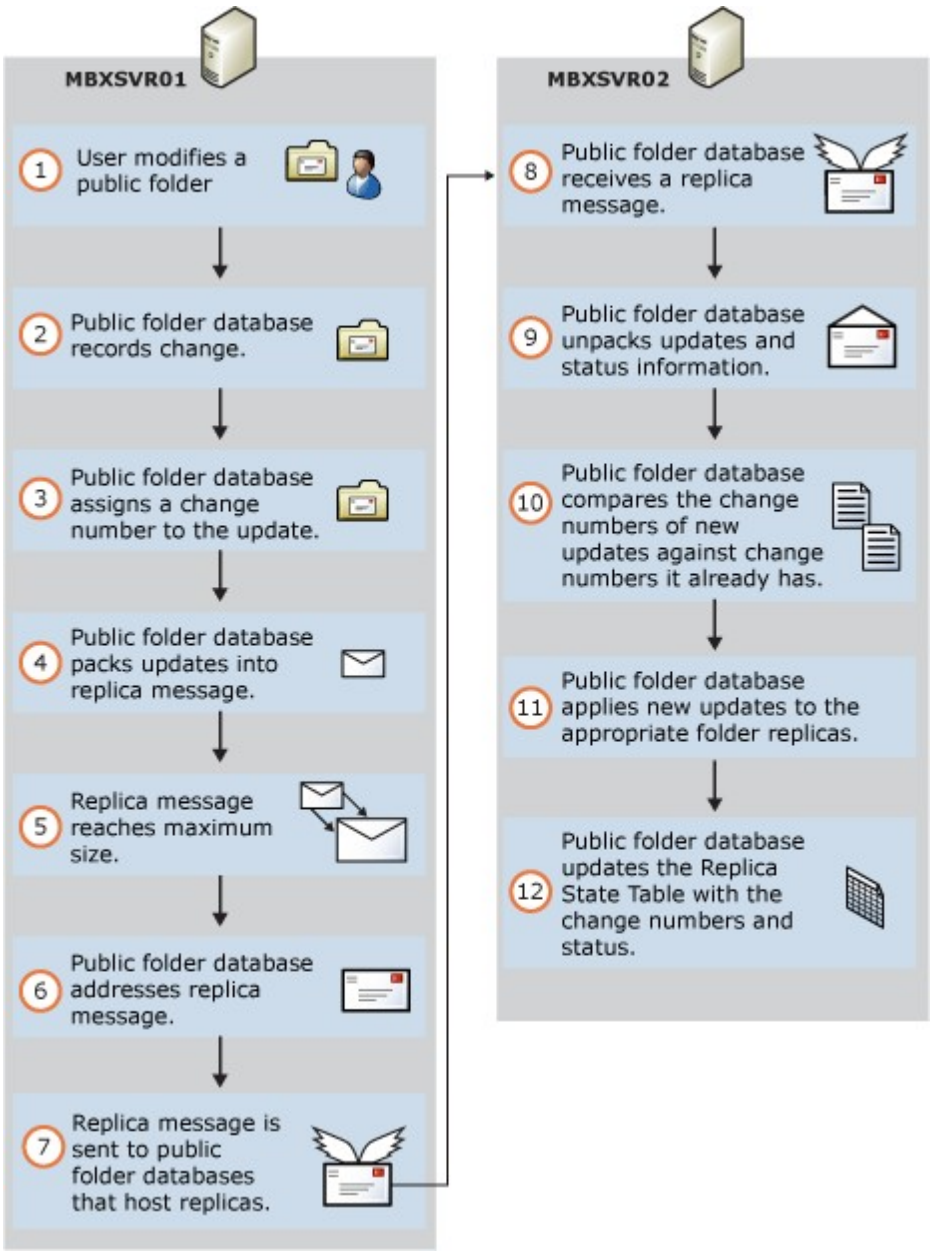
How Public Folder Replication Works

When you modify a public folder or its contents, the public folder database that contains the replica of the public folder that was changed sends a descriptive e-mail message to the other public folder databases that host a replica of the public folder. To reduce traffic on your network, Exchange includes information about multiple changes in one e-mail message. The amount of information included in these messages depends on the size limit you set for replication messages. If any message exceeds the specified size limit, that message is sent as a separate replication message. Exchange routes these replication messages the same way that it routes other e-mail messages.

If you make changes to the public folder hierarchy that affect several folders, the replication process may require considerable network bandwidth. For example, to move public folders from one server to another, you must create replicas on the server to which you want to move the public folders, wait for the hierarchy changes to replicate to the original server, and then wait for the content to replicate to the new replicas. After the replicas are synchronized, you must remove the replicas from the old server. Even removing the replicas from the old server generates network traffic because removing replicas must replicate as a hierarchy change. To learn more about how these changes to the public folder hierarchy can affect your system, see "Status Requests and Status Messages" later in this topic.

Basic Hierarchy and Content Replication Process

The following figure and the explanatory text that follows describe the basic process by which public folder hierarchy and public folder content are replicated.



The details of the process are as follows:

1. A user modifies the public folder.
2. The local public folder database records the change.
3. At the next scheduled replication cycle (which is determined by the replication interval that you set for the public folder database), the public folder database checks the folder properties to determine which other servers contain a replica of that folder. If other replicas exist, the database determines what information must be replicated to them. This information becomes the update to the replicas.
   Public folder replication is object-based. If one property of an object is modified, the entire object must be replicated. Because the database that replicates the change can't assume that all of the receiving replicas are up to date, it must replicate the entire object. The implications for the different types of replication are as follows:
   - **Hierarchy replication** The replication of new hierarchy changes occurs

when a public folder is created or deleted, or when a change is made to the properties of a public folder (such as a change to the replica list, client permissions, description, administrative note, or storage limits).
- **Content replication** If a new message is posted or an existing message is modified, the update includes the entire message and its properties.

4. The public folder database assigns a change number to the update.
   When a folder replicates an update to another server, the change number is included with the update. The receiving server then uses the change number to determine whether the update represents a new change, and whether the server is missing any data.
5. The public folder database packs updates into a replication message. The change numbers of all of the updates in the message are called a *change number set* (CNSet).
   Along with the updates, the public folder database packs information from the folder's entries that are in the replication state table, including the CNSets that were previously applied to the replica. For more information about the replication state table, see "Replication State Table" later in this topic.
6. To reduce mail traffic, the public folder database packs multiple hierarchy updates into a single replication message. Likewise, the database packs multiple content updates for the same folder into a single replication message. However, the database can't pack hierarchy updates into the same replication message as content updates, and each content replication message contains updates for a single folder.
7. The public folder database addresses the replication message to the other public folder databases that host replicas of the updated folder. The database sends the message, along with any other messages that have been packed since the previous replication cycle.
   To deliver replication messages, the public folder database relies on the internal routing components in Exchange. The database doesn't attempt to split replication messages based on topology details. If the contents of a folder are modified and the folder has five other replicas, the database generates a single replication message and addresses it to all five databases that host those replicas. The routing components determine how to route and deliver the message.
8. The public folder database receives the replication message.
9. The receiving public folder database unpacks the update and status information from the replication message.
10. The database compares the change numbers of the new updates to the list of change numbers that it already contains, and then identifies which updates it hasn't previously received.
11. The database applies the new updates to the appropriate folder replicas.
12. For each updated replica, the database updates the replication state table with the change numbers of the current update and the folder status information from the replication message.
    If the information in the replication state table indicates that other CNSets have been applied to other replicas of the folder but not to replicas on this database, the database records the CNSets that are missing in a location called the *backfill array*, and then prepares to send a backfill request. For more information about backfill requests, see "Backfill Requests and Backfill Messages" later in this topic.

Return to top

Replication Messages

The replication process uses the Active Directory attributes of the public folder databases, and not the Active Directory attributes of individual public folders. The Active Directory attributes for individual public folders are used only to send regular e-mail messages to or

from the folders. A public folder database object is configured and maintained automatically and resides in the Configuration container in Active Directory.

Replication messages differ from other e-mail messages in that Exchange treats replication messages as system messages. This means that replication messages aren't bound by the restrictions applied to user e-mail messages (such as size and delivery restrictions).

The following table lists the different types of replication messages that Exchange uses.

Note:
The values listed in parentheses in the following table are the hexadecimal notation of the message types. These notations are used in events and logs. You can use the hexadecimal value to troubleshoot replication issues.

Types of public folder replication messages and when they are used

Message type*	When used
Hierarchy (0x2)	Replicates hierarchy changes from the local public folder database to all other public folder databases that support the same hierarchy. Although Exchange handles hierarchy changes separately from changes to content replicas, it treats the hierarchy as if it was another folder. In some event messages and other operations, Exchange refers to the hierarchy as Folder 1-1.
Content (0x4)	Replicates content changes from one replica to all other content replicas of that folder. A content message only contains information that applies to a single folder.
Backfill request (0x8)	Requests missing data in CNSets from another database. This includes hierarchy and content change numbers.
Backfill response (0x80000002 or 0x80000004)	Sends missing data in CNSets to a database that requested missed updates.
Status (0x10)	Sends the current CNSet of a folder to one or more replicas of that folder. This includes hierarchy and content change numbers.
Status request (0x20)	Requests CNSets to be replicated or status messages to be returned. This includes hierarchy and content change numbers.

Replication State Table

Each public folder database maintains a replication state table to track the status of each replica in the database. The replication state table stores the following information:

- Basic information required to construct updates to each replica.
- Information about the last update to each replica that originated in the local database, including the change number of the update.
- Groups of updates that have been applied to all other known replicas of the folder. Change numbers identify the updates in each group. The set of change numbers for all updates in a group is called a CNSet. Update information is passed from one database to another as part of the replication process.

The following tables provide an example of how replication state tables function. In this example, the public folder databases on Server A and Server B both have replicas of a

folder named Projects. On each server, the replication state table tracks not only the status of the replica on that server, but also the status of the replica on the other server. Using this information, Server A determines whether its replica of Projects folder is synchronized with the replica of the Projects folder on Server B. Server B can likewise track its status relative to Server A.

Sample data from the replication state table for Server A

Replica	Data
Projects folder on Server A (local replica)	Last update sent: A-100
Projects folder on Server B	A-100 received B-50 received

Sample data from the replication state table for Server B

Replica	Data
Projects folder on Server A	A-100 received B-50 received
Projects folder on Server B (local replica)	Last update sent: B-50

By combining the lists of public folder databases that contain content replicas with the information in the replication state table, each public folder database can determine how up to date it is compared to the other public folder databases that support the public folder tree.

Return to top

Backfill Requests and Backfill Messages

Backfilling occurs when a public folder database determines that it hasn't received all the updates for a replicated folder (or for the hierarchy) and must therefore retrieve the missing updates from another public folder database.

To streamline the backfill process, Exchange stores information about missing updates in the backfill array.

The following events may alert a public folder database to missing updates that need to be backfilled:

- The status information in an incoming replication message indicates that the replica on the public folder database that sent the message has updates that are missing on the receiving database. The receiving database identifies the missing change numbers and stores them in its backfill array.
- A public folder database starts for the first time. The new database sends status requests to get information about the other databases in the hierarchy. After the corresponding status messages arrive, the database populates its replication state table and, if necessary, the backfill array. The backfill array may contain entries for both the hierarchy and for any content replicas that the database must host.
- An incoming hierarchy message indicates that a new content replica is to be placed in the public folder database. The new database sends status requests

to get information about content that might be available for this replica in the other databases in the hierarchy. After the corresponding status messages arrive, the database populates the replication state table and, if necessary, the backfill array.

The backfill array stores this information for a specified length of time (called the *backfill time-out*). If the missing updates arrive in subsequent replication messages during this time, they are removed from the backfill array. The following table lists the default backfill time-out values, which depend on where the missing updates exist and whether they were previously requested.

Default time-outs used for backfill requests

Type of request	Content exists on a database in the local Active Directory site	Content exists on a database in a remote Active Directory site
Initial backfill	6 hours	12 hours
First backfill retry	12 hours	24 hours
Subsequent backfill retries	24 hours	48 hours

If the backfill time-out expires, and the updates are still missing, Exchange creates one or more backfill requests and determines which servers to use as backfill sources.

To select servers to use as a backfill source, Exchange first creates a list of all the servers that have replicas of the folder, and then sorts the list according to the following sequence of criteria:

1. Sort according to server status. Servers that are down or unavailable drop to the end of the list.
2. Sort according to preferred backfill server (if any). Exchange checks the public folder database object in Active Directory for a preferred backfill server. This setting is seldom used. In most circumstances, the backfill process operates most efficiently if Exchange selects a backfill server automatically. Most deployments of Exchange don't need a preferred backfill server. Microsoft Customer Service and Support can provide a script that sets a preferred backfill server if your deployment requires it.
3. Sort according to transport cost (lowest to highest). Servers in the same routing group have priority over servers in remote Active Directory sites.
4. Sort according to Exchange version (newest to oldest).
5. Sort according to the number of necessary changes available on the server (largest to smallest). Servers that don't have any of the missing changes are dropped from the list.

If one server doesn't have all the necessary changes, Exchange selects the next server in the sorted list and sends a backfill request to that server as well. This process is repeated until all of the changes are requested.

If the selected server doesn't respond to the backfill request, the database marks that server as unavailable and repeats the selection process. Servers marked as unavailable move to the end of the list.

Status Requests and Status Messages

In addition to the status information in each replication message, Exchange uses status requests and status messages to determine whether public folders must issue backfill requests.

A public folder database sends a status request under the following circumstances:

- The database is notified of a change to the list of databases that hold replicas of a folder. For example, if you add a database to the list or remove a

database from the list, Exchange replicates this change by using hierarchy update messages. In this case, the database sends a status request that requires every database that contains a replica of the folder to respond.
- A new database has started for the first time. In this case, the database requests the status of the public folder hierarchy. The database sends a status request that requires every database that supports the public folder tree to respond.
- A database that has been restored by using Windows Server Backup starts for the first time after the restore completes. In this case, the database requests the status of the public folder hierarchy and all of the folders for which the database contains content replicas. This status request lists two or three databases as required responders. Required responders are databases that support this hierarchy and, according to an internal selection process, are dependable sources of folder content.

To indicate the current state of a particular folder on the sending database, the public folder database sends a status message to another database under the following circumstances:

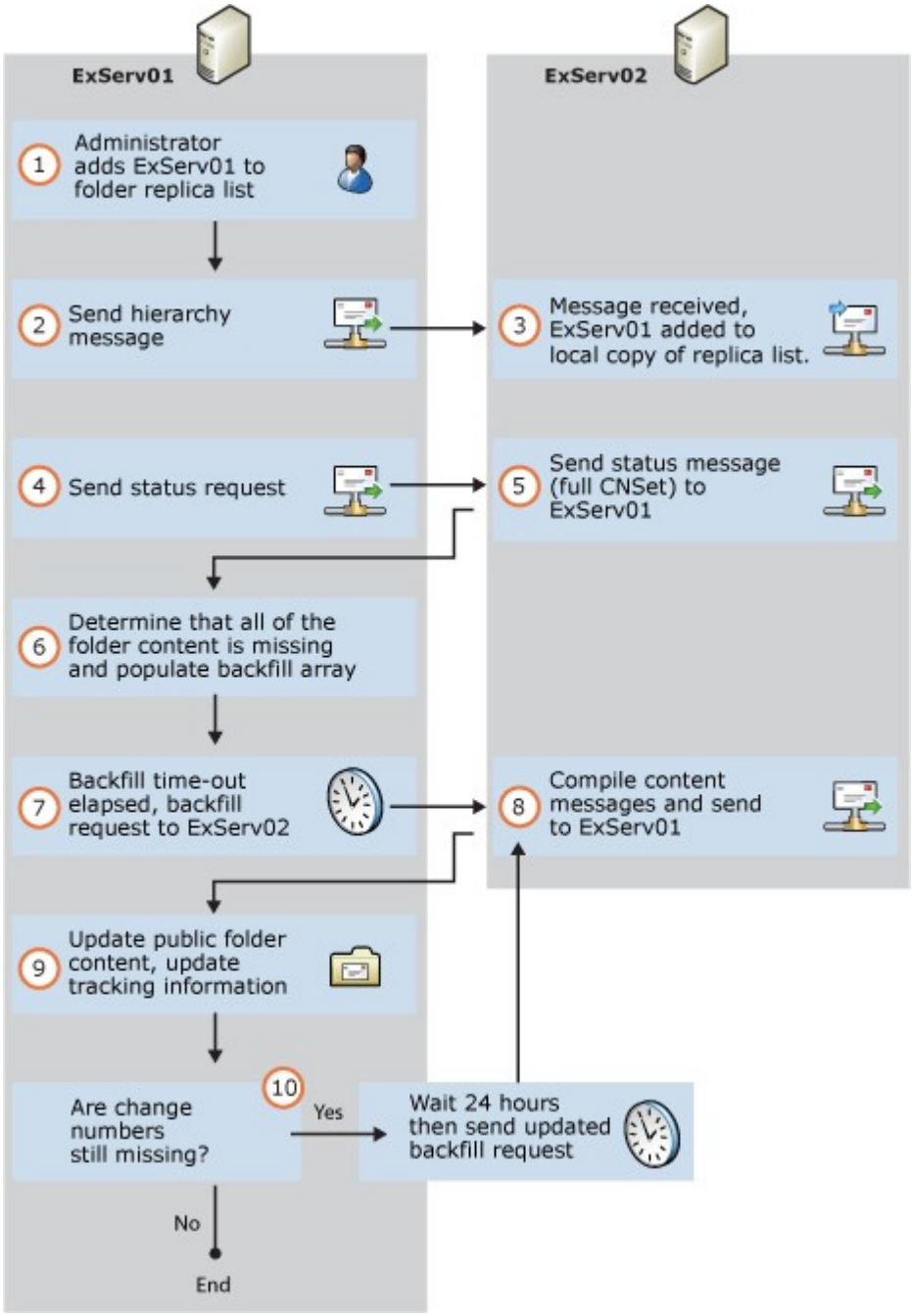
- In response to a status request sent by another database. The status message is sent only to the requesting database and only if the following are true:
  - The database that received the status request is in the requests list of required responders.
  - The replication state table indicates that the database that received the status request has updates that are missing from the database that sent the request.
- If there have been no subsequent updates 24 hours after the most recent update to a folder was received. Each time the database receives an update for a specific folder, the timer is reset to 24 hours. This status message is sent to the other public folder databases that contain replicas of the updated folder.

If a public folder database receives a status message indicating that the sending database has more recent information about the folder, the receiving database creates a backfill request. If the change numbers are shown to be equal (or the change numbers on the receiving server are more recent), no action is taken. For example, when a new public folder database starts for the first time, it sends status request messages to each database that supports the public folder hierarchy. Each database responds with information about the status of the hierarchy (as tracked by that database). The new database uses this information to identify which replicas (if any) it should have. The new database can then send backfill requests as needed to fill in the replica content.

Return to top

Examples of Replication Cycles

The following figure illustrates a simplified two-server scenario that shows the sequence of events that occurs when you add a content replica to a public folder database. This action adds the public folder database to the folder's replica list. Note that the sequence of steps depends on factors such as the timing of the replication intervals and the routing topology.

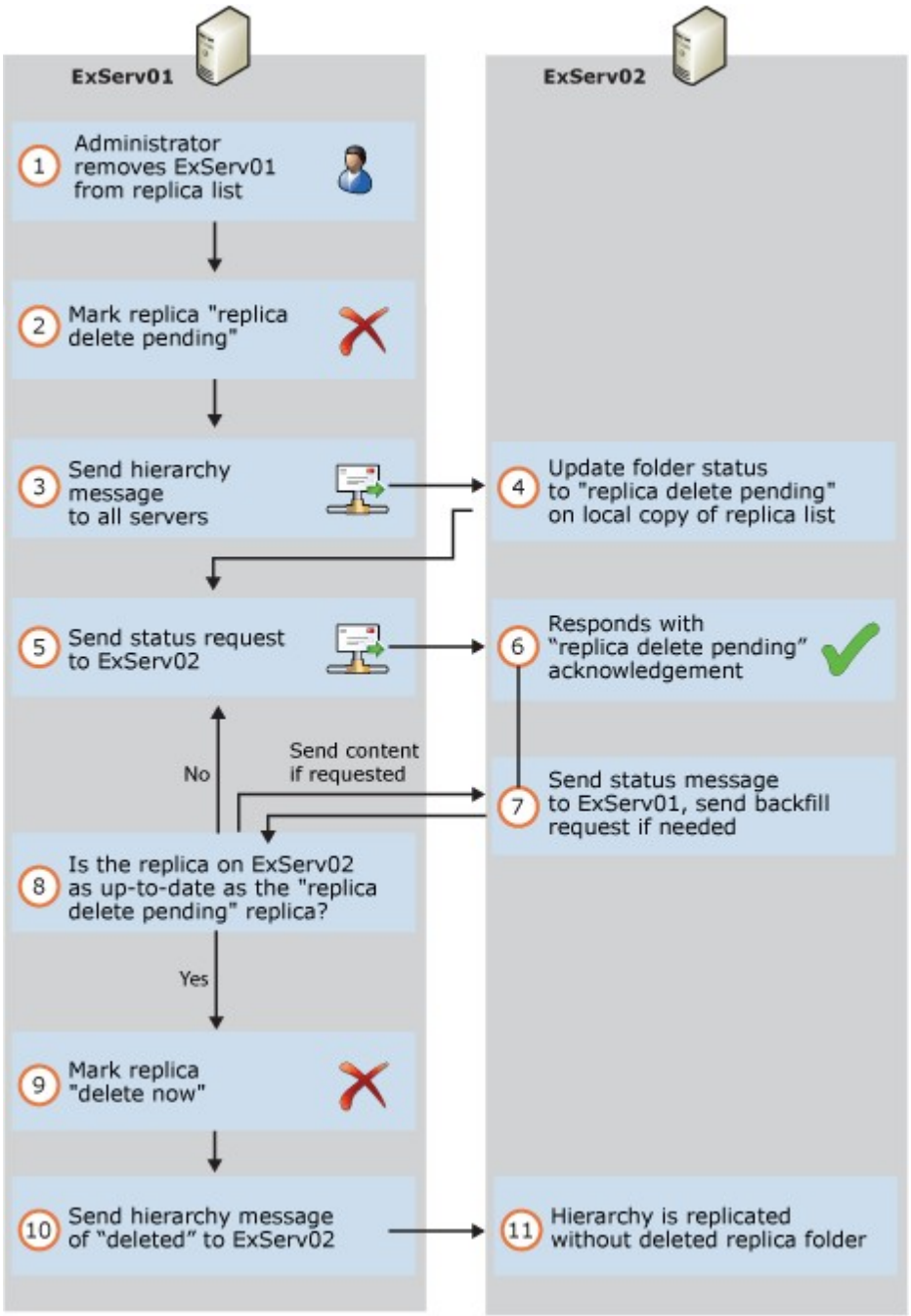


The details of the process are as follows:

1. Working on ExServ01, an administrator adds ExServ01 to a folder's replica list.
2. ExServ01 sends a hierarchy message.
3. ExServ02 adds ExServ01 to the local copy of the folder's replica list.
4. ExServ01 sends a status request to ExServ02.
5. ExServ02 sends a status message to ExServ01 that includes the full CNSet of the folder.
6. ExServ01 determines that all the folder content is missing and records the appropriate entries in the backfill array.
7. If the content is still missing when the backfill time-out elapses, ExServ01 creates a backfill request and sends it to ExServ02.

8. ExServ02 compiles the content messages and sends them to ExServ01.
9. ExServ01 uses the incoming content messages to update the folder content and related tracking information.
10. If change numbers still appear to be missing, ExServ01 waits 24 hours, and then sends an updated backfill request. If a server other than ExServ02 is available, ExServ01 might send the request to that server.

The following figure illustrates a simplified two-server scenario that shows the sequence of events that occur when you remove a replica from a public folder database. (This action removes the public folder database from the folder's replica list.) Note that the sequence of steps depends on factors such as the number of servers in the topology.



The details of the process are as follows:

1. Working on ExServ01, an administrator removes ExServ01 from a folder's replica list.
2. ExServ01 marks its replica (the copy of the folder on ExServ01) as **delete pending**.
   Clients can no longer access the folder by using this database.
3. ExServ01 sends a hierarchy message.
4. ExServ02 updates its copy of the folder's replica list to show that the folder is in the delete pending state on ExServ01.
   ExServ02 no longer refers clients that are looking for this folder to ExServ01.
5. ExServ01 sends a status request to ExServ02.
6. ExServ02 sends a status message to ExServ01. If the replica on ExServ02 isn't up to date, ExServ02 places the appropriate entries in the backfill array. Within five minutes, ExServ02 sends the corresponding backfill request to ExServ01.
7. ExServ01 checks that the folder replica on ExServ02 contains all of the information that the delete pending replica does. If it doesn't, ExServ01 sends the appropriate content updates and returns to Step 5. Otherwise, ExServ01 continues to Step 8.
   This process ensures that as long as other replicas exist, deleting a single replica doesn't result in a loss of content.
8. ExServ01 marks its replica as **delete now**. The next maintenance cycle will remove the replica from ExServ01.
9. ExServ01 sends a hierarchy message.
10. ExServ02 removes ExServ01 from its copy of the folder's replica list.

Return to top

Best Practices for Implementing Replication

Public folder replication in Exchange can be a resource-intensive operation. Replication requires network, CPU, and disk resources to operate. By implementing a solution that enables efficient public folder replication, especially in organizations with heavy public folder usage, you may greatly improve network, CPU, and disk load in your Exchange organization.

Generally, it's a best practice to minimize replication across the organization. By minimizing replication, you minimize the amount of data that travels over your network. Additionally, by minimizing replication, you can help make sure that multiple users are less likely to access different versions of data on multiple replicas. However, you should note that by minimizing replication, you decrease availability of the public folder data because fewer replicas of the folder are available to clients if a public folder database fails. If availability on a large scale is required for data in a specific public folder, you may require more replication.

Return to top

1.8.1.12.3 Understanding Public Folder Referrals

Understanding Public Folder Referrals

Mailbox > Understanding Mailbox > Understanding Public Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-27*

When a user accesses a public folder by using a MAPI client application, such as Microsoft Outlook, the public folder database determines which public folder replica the client should access. This process is called *referral*. If a replica of the requested content exists on the server running Microsoft Exchange that serves the client request, the client accesses the local replica. When a user connects to a public folder database that doesn't contain a copy of the public folder content that the user wants, the user is redirected to another public folder database that has a copy of the content. As illustrated in the following figure, you can create a custom cost list for public folder referral to control this redirect traffic.

Note:

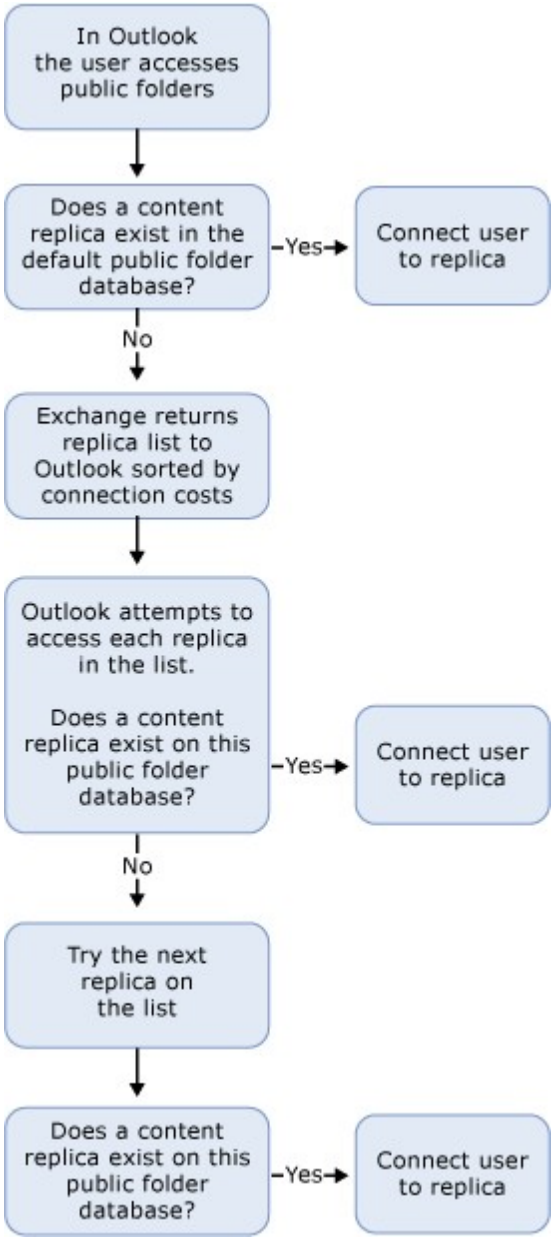
Public folder referrals have an associated *cost number*. The numbers range from 1 through 100. This cost number is used to optimize message flow. Specifically, e-mail messages are routed according to lowest cost number. If two or more routes are available with the same cost, the load is distributed as equally as possible between them. This cost is also used to calculate the most appropriate route that the client application can use to access public folders on remote servers.

Using the default referral configuration, Exchange Server 2010 follows the structure of your organization's Active Directory site to locate an appropriate server. However, to modify the flow of user traffic, Active Directory site administrators can redirect this configuration by specifying whether to allow referrals over certain connectors. For Exchange 2010 servers, you can also specify a list of referral servers and assign routing costs to each server to redirect server traffic. For example, you can limit referrals to a single Active Directory site or only allow referrals between certain servers in each Active Directory site.

Looking for management tasks related to public folders? See Managing Public Folders.

How Referrals Are Determined

When a user connects to Exchange and uses a MAPI client application to request access to a public folder, Exchange locates a content replica of the public folder by using information supplied by the public folder database associated with the user's mailbox database. The public folder database retrieves the replica list of the requested folder and, if necessary, retrieves routing and cost information from Active Directory Sites and Services. Exchange uses the process shown in the following figure to locate a content replica.



The details of the process are as follows:

1. The MAPI client connects to the user's mailbox database to access the user's private folders. The MAPI client also connects to the user's mailbox to retrieve the default public folder database for information about the public folder hierarchy. For more information about how to set the default public folder database, see Change the Default Public Folder Database for a Mailbox Database.
2. The MAPI client attempts to read the content for a specific public folder. Initially, the default public folder database is queried for the content. If that database is a content replica for the folder in question, the process is complete.
3. If there is no replica on the default public folder database, Exchange returns a list of replicas to the client, sorted by that server’s perspective of connection costs to each of the other listed content replicas. Connection costs are determined by querying Active Directory Sites and Services for the

site connector cost information of the other Mailbox servers in the organization on which a public folder database resides. Alternatively, you can specify costs to other servers by providing a custom override list to the public folder database. The list returned to the client doesn't include servers for which the cost is greater than 500.

Note:
Cost information is refreshed once every hour. Therefore, any changes to Active Directory site costs aren't available for up to one hour. In addition, any changes in the public folder custom list, including its initial configuration or complete removal, isn't available for up to one hour. Servers that aren't listed in the custom list of the public folder will never receive referrals from the server that has the custom list.

4. The MAPI clients attempt to access each replica in the list by connecting to the server, attempting to locate the folder, and then attempting to read the folder's content.
5. If a failure occurs, the client attempts to access the next replica server in the list until the client has attempted to access all replica servers in the custom list.

Note:
The MAPI client doesn't refresh its connection unless its current connection is terminated. In other words, if a preferred or low-cost replica can't be reached, the client attempts to access the next replica in the list, which may be expensive to reach. If the low-cost server becomes available, the MAPI client doesn't redirect the connection to the low-cost replica until the user logs off and then logs back on to the MAPI client.

Assigning Cost

Although Exchange administrators can create public folder referrals and site costs, we don't recommend that you do this because the maximum public folder referral cost that Exchange administrators can set for a public folder database is 100. By setting the maximum referral cost for a server to 100, the server may still be used for referrals.

Instead, public folder referrals and site costs should be determined by an administrator who is a member of the Domain Admins group or the Enterprise Admins group in Active Directory. In Active Directory Sites and Services, a user who has Domain Admin or Enterprise Admin permissions can set the public folder referral cost up to 500. This higher cost number helps ensure that a server won't be used for referrals.

Note:
To create efficient public folder referrals, you must understand the structure of your organization's Active Directory site. For more information about routing, Active Directory sites, routing costs, and Send and Receive connectors, see Understanding Message Routing.

For detailed steps about how to configure an Exchange 2010 server to use a specific list of servers and costs for referrals, see Configure Public Folder Referrals.

1.8.1.13 Understanding Quota Messages

Understanding Quota Messages

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-13*

A *quota message* is an e-mail message that's automatically sent by Microsoft Exchange to the owners of a mailbox or a public folder when a size limit (called a *storage quota*) for the mailbox or public folder is exceeded. You can use the New-SystemMessage, Get-SystemMessage, Set-SystemMessage, and Remove-SystemMessage cmdlets in the Exchange Management Shell to view built-in quota messages or to create, view, modify, or remove customized quota messages.

Quota Messages in Exchange 2010 SP1

Exchange 2010 SP1 introduces a flag that controls whether a mailbox is checked to see if its size is equal to or greater than 50% of the **Prohibit send** quota.As a result, if the **Issue Warning** quota is set to a value less than 50% of the **Prohibit send** quota, the warning message associated with the **Issue warning** quota won't be sent to the user. For example, if a mailbox has a size limit of 10 MB, and you set the **Issue warning** quota to 3 MB and the **Prohibit send** quota to 8 MB, the user won't ever receive the warning specified by the **Issue warning** quota because the **Issue warning** quota limit isn't equal to or greater than 50% of the **Prohibit send** quota. Instead, the user will receive only the message associated with the **Prohibit send** quota (in this case, when the user's mailbox size reaches 8 MB).

In addition, the flag is cleared after you run the **Set-MailboxDatabase** cmdlet with the *QuotaNotificationSchedule* parameter. When you run that command, the mailbox won't be checked again until the flag is reset. Flags are reset when a message is saved in the mailbox or when a message is sent to or from the mailbox.At that point if the mailbox size is greater than 50% of the **Prohibit send** quota, the flag is reset and the mailbox is checked at the time specified by the *QuotaNotificationSchedule* parameter.

Storage Quotas

A *storage quota* is a storage size limit for a mailbox or a public folder. You can use the Exchange Management Console (EMC) or the Shell to view or set the storage quotas for all of the mailboxes or public folders in a database. You can also use the EMC or the Shell to set storage quotas on a per-mailbox basis, thereby overriding the storage quotas that are set at the database level. However, storage quotas for individual public folders can be viewed or set only in the Shell.

For more information about viewing and configuring storage quotas, see the following topics:

- Configure Mailbox Database Properties
- Configure Storage Quotas for a Mailbox
- Configure Archive Quotas for a Personal (On-Premises) Archive
- Set-MailboxDatabase
- Set-Mailbox
- Configure Public Folder Properties
- Set-PublicFolderDatabase
- Set-PublicFolder

Quota Messages

By default, Exchange sends a quota message to mailbox or public folder owners when a:

- Mailbox, personal archive, or public folder exceeds its **Issue warning** limit (the lowest storage quota).
- Mailbox exceeds its **Prohibit send** limit or a public folder exceeds its **Prohibit post** limit (the middle storage quota).
- Mailbox exceeds its **Prohibit send and receive** quota or a personal archive

exceeds its archive quota (the highest storage quota).

Quota messages for mailboxes are sent to mailbox owners. If a mailbox is owned by a security group (that is, if it's a shared mailbox), quota messages are sent to the security group. Quota messages for public folders are sent to every public folder owner. Owners of mailboxes and public folders can be users, contacts, or security groups.

Quota messages are sent with high importance and aren't subject to storage quotas. They're always delivered, even if the recipient's mailbox is full.

Exchange can generate quota messages in many languages. For a list of the supported language locales that are available for use with quota messages, see Supported Locales for Use with System Messages.

Quota Message Format

There are seven types of quota messages: four for mailboxes and three for public folders. All quota messages include the following:

- Text **Microsoft Exchange** in the **From** field
- Brief, non-customizable description of the situation in the **Subject** field
- Customizable message in the message body
- Graphical representation of the storage quota and the amount of storage used in the message body (except for mailboxes or public folders of unlimited size)

Default Quota Messages

The following tables list the subject and the default message text for the seven default English quota messages (four for mailboxes and three for public folders). The default message can be customized, but the subject text can't.

Note:

There are no specific archive quota messages. If a user's archive is meeting or exceeding any quotas, they will receive mailbox quota messages.

Mailbox quota and archive quota messages

Event	Subject of message	Default message text
Mailbox of unlimited size exceeds its **Issue warning** quota	Your mailbox is becoming too large	Please reduce your mailbox size. Delete any items you don't need from your mailbox and empty your Deleted Items folder.
Mailbox of limited size exceeds its **Issue warning** quota **Important:** The message associated with the **Issue warning** quota won't be sent to the user unless the value of the quota is greater than 50% of the value specified in the **Prohibit send** quota. For example, if you set the **Prohibit send** quota to 8 MB, you must set the **Issue warning** quota to at least 4 MB. If you don't, the **Issue warning** quota message won't be sent.	Your mailbox is almost full	Please reduce your mailbox size. Delete any items you don't need from your mailbox and empty your Deleted Items folder.

Mailbox of limited size exceeds its **Prohibit send** quota	Your mailbox is full	Your mailbox can no longer send messages. Please reduce your mailbox size. Delete any items you don't need from your mailbox and empty your Deleted Items folder.
Mailbox of limited size exceeds its **Prohibit send and receive** quota	Your mailbox is full	Your mailbox can no longer send or receive messages. Please reduce your mailbox size. Delete any items you don't need from your mailbox and empty your Deleted Items folder.

Public folder quota messages

Event	Subject of message	Default message text
Public folder of unlimited size exceeds its **Issue warning** quota	Your public folder is becoming too large	Please reduce the size of your public folder by deleting any items you don't need.
Public folder of limited size exceeds its **Issue warning** quota	Your public folder is almost full	Please reduce the size of your public folder by deleting any items you don't need.
Public folder of limited size exceeds its **Prohibit post** quota	Your public folder is full	Users can no longer post items to this folder. Please reduce the size of your public folder by deleting any items you don't need.

1.8.1.14 Understanding Recipients

Understanding Recipients

Exchange Server 2010 > Mailbox > Understanding Mailbox >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-24*

The people and resources that send and receive messages are the core of any messaging and collaboration system. In an Exchange organization, these people and resources are referred to as *recipients*. A recipient is any mail-enabled object in Active Directory to which Exchange can deliver or route messages.

Recipient Types

Microsoft Exchange Server 2010 includes several explicit recipient types. Each recipient type is represented by a unique icon in the Exchange Management Console (EMC) and a unique name in the *RecipientTypeDetails* property in the Exchange Management Shell. The use of explicit recipient types has the following benefits:

- At a glance, you can differentiate between various recipient types.
- You can search, sort, and filter by each recipient type.
- You can more easily perform bulk management operations for each recipient

type.
- You can more easily view recipient properties because the EMC uses the recipient types to render different property pages. For example, the resource capacity is displayed for a conference room mailbox, but isn't present for a user mailbox.

The following table lists the available recipient types. All these recipient types are discussed in more detail later in this topic.

Exchange 2010 recipient types

Recipient type	Description
Dynamic distribution group	A distribution group that uses recipient filters and conditions to derive its membership at the time messages are sent.
Equipment mailbox	A resource mailbox that's assigned to a non-location specific resource, such as a portable computer projector, microphone, or a company car. Equipment mailboxes can be included as resources in meeting requests, providing a simple and efficient way of utilizing resources for your users.
Legacy mailbox	A mailbox that resides on a server running Exchange Server 2003.
Linked mailbox	A mailbox that's assigned to an individual user in a separate, trusted forest.
Mail contact	A mail-enabled Active Directory contact that contains information about people or organizations that exist outside the Exchange organization. Each mail contact has an external e-mail address. All messages sent to the mail contact are routed to this external e-mail address.
Mail forest contact	A mail contact that represents a recipient object from another forest. Mail forest contacts are typically created by Microsoft Identity Integration Server (MIIS) synchronization. **Important:** Mail forest contacts are read-only recipient objects that are updated only through MIIS or similar custom synchronization. You can't use the EMC or the Shell to remove or modify a mail forest contact.
Mail user	A mail-enabled Active Directory user that represents a user outside the Exchange organization. Each mail user has an external e-mail address. All messages sent to the mail user are routed to this external e-mail address. A mail user is similar to a mail contact, except that a mail user has Active Directory logon credentials and can access resources.

Mail-enabled non-universal group	A mail-enabled Active Directory global or local group object. Mail-enabled non-universal groups were discontinued in Exchange Server 2007 and can exist only if they were migrated from Exchange 2003 or earlier versions of Exchange. You can't use Exchange 2010 to create non-universal distribution groups.
Mail-enabled public folder	An Exchange public folder that's configured to receive messages.
Mail-enabled universal distribution group	A mail-enabled Active Directory distribution group object that can be used only to distribute messages to a group of recipients.
Mail-enabled universal security group	A mail-enabled Active Directory security group object that can be used to grant access permissions to resources in Active Directory and can also be used to distribute messages.
Microsoft Exchange recipient	A special recipient object that provides a unified and well-known message sender that differentiates system-generated messages from other messages. It replaces the System Administrator sender used for system-generated messages in earlier versions of Exchange. To learn more, see Understanding the Microsoft Exchange Recipient.
Room mailbox	A resource mailbox that's assigned to a meeting location, such as a conference room, auditorium, or training room. Room mailboxes can be included as resources in meeting requests, providing a simple and efficient way of organizing meetings for your users.
Shared mailbox	A mailbox that's not primarily associated with a single user and is generally configured to allow logon access for multiple users.
User mailbox	A mailbox that's assigned to an individual user in your Exchange organization. It typically contains messages, calendar items, contacts, tasks, documents, and other important business data.
Remote mailbox	New in Exchange 2010, a remote mailbox consists of a mail-enabled user that exists in the on-premises Active Directory and an associated mailbox that exists in the cloud-based service.
Linked user	New in Exchange 2010, a linked user is a user that resides in one forest while their mailbox resides in another forest.

Mailboxes

Mailboxes are the most common recipient type used by information workers in an Exchange organization. Each mailbox is associated with an Active Directory user account.

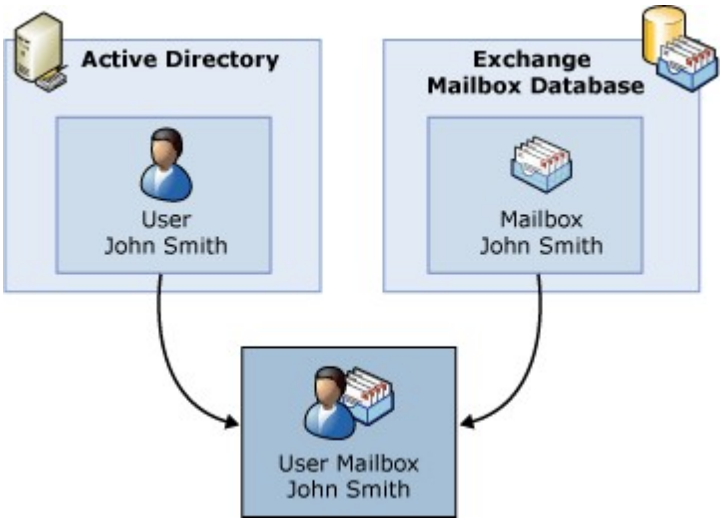
The user can use the mailbox to send and receive messages, and to store messages, appointments, tasks, notes, and documents. Mailboxes are the primary messaging and collaboration tool for the users in your Exchange organization.

Mailbox Components

Each mailbox consists of an Active Directory user and the mailbox data that's stored in the Exchange mailbox database (as shown in the following figure). All configuration data for the mailbox is stored in the Exchange attributes of the Active Directory user object. The mailbox database contains the actual data that's in the mailbox associated with the user account.

Important:

When you create a mailbox for a new or existing user, the Exchange attributes required for a mailbox are added to the user object in Active Directory. The associated mailbox data isn't created until the mailbox either receives a message or the user logs on to it.



Warning:

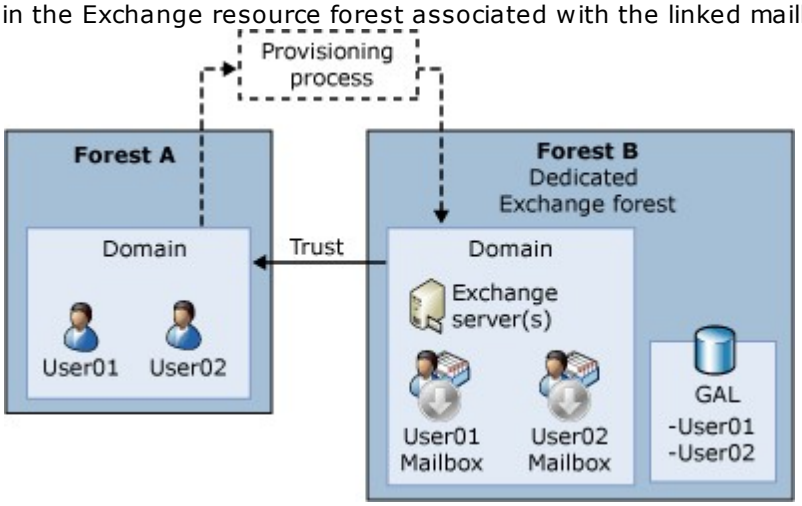
If you remove a mailbox, the mailbox data stored in the Exchange mailbox database is marked for deletion and the associated user account is also deleted from Active Directory. To retain the user account and delete only the mailbox data, you must disable the mailbox.

Mailbox Types

Exchange 2010 supports the following mailbox types:

- **User mailboxes** User mailboxes are assigned to individual users in your Exchange organization. User mailboxes provide your users with a rich collaboration platform. They can send and receive messages, manage their contacts, schedule meetings, and maintain a task list. Users can also have voice mail messages delivered to their mailboxes. User mailboxes are the most commonly used mailbox type and are typically the mailbox type assigned to users in your organization.
- **Linked mailboxes** Linked mailboxes are mailboxes that are accessed by users in a separate, trusted forest. Linked mailboxes may be necessary for organizations that deploy Exchange in a resource forest. The resource forest scenario allows an organization to centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests.
  As stated earlier, every mailbox must have a user account associated with it. However, the user account that accesses the linked mailbox doesn't exist in the forest where Exchange is deployed. Therefore, a disabled user account that exists in the same forest as Exchange is associated with each linked mailbox. The following figure illustrates the relationship between the linked user account used to access the linked mailbox and the disabled user account

in the Exchange resource forest associated with the linked mailbox.



- **Remote mailboxes** When you create a remote mailbox, the mail-enabled user is created in your on-premises Active Directory. Directory synchronization, if it's configured, automatically synchronizes this new user object to the cloud-based service, which then converts it to a user mailbox. You can create remote mailboxes as regular user mailboxes or as resource mailboxes for meeting rooms and equipment.
- **Shared mailboxes** Shared mailboxes aren't primarily associated with individual users and are generally configured to allow logon access for multiple users.
  Although it's possible to grant additional users the logon rights to any mailbox type, shared mailboxes are dedicated for this functionality. The Active Directory user associated with a shared mailbox must be a disabled account. After you create a shared mailbox, you must grant permissions to all users that require access to the shared mailbox.

  Important:

  You can only use the Shell to manage shared mailboxes. Management tasks include creating, removing, enabling, and disabling. After you create a shared mailbox, you can use the EMC for some tasks such as viewing, modifying, or moving the shared mailboxes. We recommend that you use resource mailboxes or Microsoft SharePoint Portal Server portals for collaboration instead of shared mailboxes. To learn more about converting a shared mailbox to a resource mailbox, see Convert a Mailbox.
- **Legacy mailboxes** Legacy mailboxes are mailboxes that reside on servers running Exchange 2003. You can manage legacy mailboxes by using the EMC or the Shell. However, not all Exchange 2010 features will apply to these mailboxes.
- **Resource mailboxes** Resource mailboxes are special mailboxes designed to be used for scheduling resources. Like all mailbox types, a resource mailbox has an associated Active Directory user account, but it must be a disabled account. The following are the resource mailbox types:
  - **Room mailboxes** These are resource mailboxes that are assigned to meeting locations, such as conference rooms, auditoriums, and training rooms.
  - **Equipment mailboxes** These are resource mailboxes that are assigned to non-location specific resources, such as portable computer projectors, microphones, or company cars.

  You can include both types of resource mailboxes in meeting requests, providing a simple and efficient way to utilize resources for your users. You can configure resource mailboxes to automatically process incoming meeting requests based on the resource booking policies that are defined by the resource owners. For example, you can configure a conference room to

automatically accept incoming meeting requests except recurring meetings, which can be subject to approval by the resource owner. To learn more about using resource mailboxes, see Managing Resource Mailboxes and Scheduling.

System Mailboxes

System mailboxes are created by Exchange in the root domain of the Active Directory forest during installation. Users or administrators can't log on to these mailboxes. System mailboxes are created for Exchange 2010 features such as message approval and Multi-Mailbox Search. This table lists information about system mailboxes as they're displayed in Active Directory.

Mailbox	Common name (CN)
Discovery	SystemMailbox {e0dc1c29-89c3-4034-b678-e6c29d823ed9}
Message Approval	SystemMailbox {1f05a927-*xxxx*- *xxxx* - *xxxx* -*xxxxxxxxxxxx*} where *x* is a randomly assigned number
Federated E-mail	FederatedEmail 4c1f4d8b-8179-4148-93bf-00a95fa1e042

If you want to decommission the last Exchange 2010 Mailbox server in your organization, you should first disable these system mailboxes by using the Disable-Mailbox cmdlet. When you decommission a Mailbox server that contains these system mailboxes, you should move them to another Mailbox server to make sure that you don't lose functionality.

Planning for Mailboxes

Mailboxes are created in mailbox databases on Exchange servers that have the Mailbox server role installed. To help provide a reliable and effective platform for your mailbox users, detailed planning for the deployment of Mailbox servers and databases is essential. To learn more about planning for Mailbox servers and databases, see the following topics:

- Planning Roadmap for New Deployments
- Exchange 2003 - Planning Roadmap for Upgrade and Coexistence
- Exchange 2007 - Planning Roadmap for Upgrade and Coexistence
- Managing Mailbox Databases
- Managing Mailbox Servers

Distribution Groups

Distribution groups are mail-enabled Active Directory group objects that are primarily used for distributing messages to multiple recipients. Any recipient type can be a member of a distribution group.

Important:
Note the terminology differences between Active Directory and Exchange 2010. In Active Directory, a distribution group refers to any group that doesn't have a security context, whether it's mail-enabled or not. In Exchange 2010, all mail-enabled groups are referred to as distribution groups, whether they have a security context or not.

Exchange supports the following types of distribution groups:

- **Mail-enabled universal distribution groups** These are Active Directory distribution group objects that are mail-enabled. They can be used only to distribute messages to a group of recipients.
- **Mail-enabled universal security groups** These are Active Directory security group objects that are mail-enabled. They can be used to grant access permissions to resources in Active Directory and can also be used to distribute

messages.

- **Mail-enabled non-universal groups** These are Active Directory global or local group objects that are mail-enabled. You can create or mail-enable only universal distribution groups. You may have mail-enabled groups that were migrated from previous versions of Exchange that aren't universal groups. These groups can still be managed by using the EMC or the Shell.

Note:
To convert a domain-local or a global group to a universal group, you can use the Set-Group cmdlet in the Shell.

For more information about the changes from Exchange Server 2007 to Exchange Server 2010 that affect group management, see the Distribution Groups section in the "New Mailbox and Recipient Functionality" topic.

Dynamic Distribution Groups

Dynamic distribution groups are distribution groups whose membership is based on specific recipient filters rather than a defined set of recipients.

Unlike regular distribution groups, the membership list for dynamic distribution groups is calculated each time a message is sent to them, based on the filters and conditions that you specify. When an e-mail message is sent to a dynamic distribution group, it's delivered to all recipients in the organization that match the criteria defined for that dynamic distribution group.

Important:
A dynamic distribution group includes any recipient in Active Directory that has attributes that match the group's filter at the time a message is sent. If a recipient's properties are modified to match the group's filter, that recipient could inadvertently become a group member and start receiving messages that are sent to the dynamic distribution group. Well-defined, consistent account provisioning processes can reduce the chances of this issue occurring.

To help you create recipient filters for dynamic distribution groups, you can use precanned filters. A *precanned filter* is a commonly used filter that you can use to meet a variety of recipient-filtering criteria. You can use these filters to specify the recipient types that you want to include in a dynamic distribution group. In addition, you can also specify a list of conditions that the recipients must meet. You can create precanned conditions based on the following properties:

- Custom attributes 1–15
- State or province
- Company
- Department

You can also specify conditions based on recipient properties other than those previously listed. To do this, you must use the Shell to create a custom query for the dynamic distribution group. Keep in mind that the filter and condition settings for dynamic distribution groups that have custom recipient filters can be managed only by using the Shell. For an example of how to create a dynamic distribution group by using a custom query, see Create a Dynamic Distribution Group.

Note:
In the EMC, you use the **Distribution Group** node under **Recipient Configuration** to manage dynamic distribution groups. There isn't a separate node for dynamic distribution groups.

Mail Contacts

Mail contacts typically contain information about people or organizations that exist outside your Exchange organization. Mail contacts can appear in the global address list (GAL) and other address lists, and can be added as members to distribution groups. Each contact has an external e-mail address, and all e-mail messages that are sent to a contact are

automatically forwarded to that address. Contacts are ideal for representing people external to your Exchange organization who don't need access to any internal resources. The following are mail contact types:

- **Mail contacts** These are mail-enabled Active Directory contacts that contain information about people or organizations that exist outside your Exchange organization.
- **Mail forest contacts** These represent recipient objects from another forest. These contacts are typically created by MIIS synchronization. Mail forest contacts are read-only recipient objects that can be updated or removed only by means of synchronization. You can't use Exchange management interfaces to modify or remove a mail forest contact.

Mail Users

Mail users are similar to mail contacts. Both have external e-mail addresses, both contain information about people outside your Exchange organization, and both can be displayed in the GAL and other address lists. However, unlike a mail contact, mail users have Active Directory logon credentials and can access resources to which they are granted permission.

If a person external to your organization requires access to resources on your network, you should create a mail user instead of a mail contact. For example, you may want to create mail users for short-term consultants who require access to your server infrastructure, but who will use their own external e-mail addresses.

Another scenario is to create mail users in your organization for users who you don't want to maintain an Exchange mailbox. For example, after an acquisition, the acquired company may maintain their separate messaging infrastructure, but may also need access to resources on your network. For those users, you may want to create mail users instead of mailbox users.

Note:

In the EMC, you use the **Mail Contact** node under **Recipient Configuration** to manage mail users. There isn't a separate node for mail users.

Mail-Enabled Public Folders

Public folders are intended to serve as a repository for information shared among many users. Mail-enabling a public folder provides an extra level of functionality to users. In addition to being able to post messages to the folder, users can send e-mail messages to, and sometimes receive e-mail messages from, the public folder. Each mail-enabled folder has an object in Active Directory that stores its e-mail address, address book name, and other mail-related attributes.

You can manage public folders by using either the Shell or the Public Folder Management Console. To access the Public Folder Management Console, click the **Toolbox** node in the EMC. For more information about managing mail-enabled public folders, see Configure Public Folder Properties.

Microsoft Exchange Recipient

The Microsoft Exchange recipient is a special recipient object that provides a unified and well-known message sender that differentiates system-generated messages from other messages. It replaces the System Administrator sender that was used for system-generated messages in earlier versions of Exchange.

The Microsoft Exchange recipient isn't a typical recipient object, such as a mailbox, mail user, or mail contact, and it isn't managed by using the typical recipient tools. However, you can use the Set-OrganizationConfig cmdlet in the Shell to configure the Microsoft Exchange recipient.

To learn more about the Microsoft Exchange recipient, see Understanding the Microsoft Exchange Recipient.

Note:
When system-generated messages are sent to an external sender, the Microsoft Exchange recipient isn't used as the sender of the message. Instead, the e-mail address specified by the *ExternalPostmasterAddress* parameter in the Set-TransportConfig cmdlet is used. For more information about the external postmaster address, see Configure the External Postmaster Address.

1.8.1.14.1 Understanding Automatic Mailbox Distribution

Understanding Automatic Mailbox Distribution

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-07*

When you create or move a mailbox, or mail-enable an existing user, that mailbox needs to be stored in a mailbox database. In previous versions of Microsoft Exchange, you needed to specify the mailbox database when you performed one of those operations. With Microsoft Exchange Server 2010, you have the option of letting Exchange choose the database for you using automatic mailbox distribution.

With automatic mailbox distribution, Exchange looks at the mailbox databases in your organization, excludes databases that aren't suitable using criteria discussed later in this topic, and then randomly chooses a database where the mailbox should be located. This process randomly distributes mailboxes across all of the suitable mailbox databases in your organization.

Automatic distribution is used when you don't specify the *Database* parameter on the **New-Mailbox** and **Enable-Mailbox** cmdlets or the *TargetDatabase* parameter on the **New-MoveRequest** cmdlet.

Note:
Automatic mailbox distribution is performed only when a mailbox is created on an Exchange 2010 server, moved to an Exchange 2010 server, or when a user is mail-enabled. The **New-Mailbox**, **New-MoveRequest**, and **Enable-Mailbox** cmdlets must be run from a server running Exchange 2010. Exchange doesn't redistribute mailboxes to distribute load across databases automatically based on server load.

The following process is used to find a suitable mailbox database where a new or moved mailbox should be located:

1. Exchange retrieves a list of all mailbox databases in the Exchange 2010 organization.
2. Any mailbox database that's marked for exclusion from the distribution process is removed from the available list of databases. You can control which databases are excluded. For more information, see Exclude Databases from Automatic Distribution later in this topic.
3. Any mailbox database that's outside of the database management scopes applied to the administrator performing the operation is removed from the list of available databases. For more information, see Database Scopes later in this topic.
4. Any mailbox database that's outside of the local Active Directory site where the operation is being performed is removed from the list of available databases.
5. From the remaining list of mailbox databases, Exchange chooses a database randomly. If the database is online and healthy, the database is used by Exchange. If it's offline or not healthy, another database is chosen at

random. If no online or healthy databases are found, the operation fails with an error.

The process of selecting a mailbox database is performed by the Mailbox Resources Management Agent cmdlet extension agent. The `Mailbox Resources Management Agent` is one of several cmdlet extension agents that extend the functionality of running cmdlets. For more information about cmdlet extension agents, see Understanding Cmdlet Extension Agents.

If you never want mailboxes to be distributed automatically, you can disable the `Mailbox Resources Management Agent`. When you disable the agent, the change is applied to the entire Exchange 2010 organization. For more information about how to disable cmdlet extension agents, see Disable a Cmdlet Extension Agent.

Exclude Databases from Automatic Distribution

By default, all online and healthy mailbox databases on Exchange 2010 servers in the local Active Directory site can be chosen by automatic mailbox distribution to store a new or moved mailbox. However, you might want to exclude some databases from the distribution process for various reasons. For example, you may designate a mailbox database as a journaling database in which only mailboxes you manually specify should be located. Or you might want to temporarily remove a database from rotation to perform scheduled maintenance. Exchange 2010 gives you the option to either permanently or temporarily exclude databases from the exclusion process.

Every Exchange 2010 mailbox database has the two following properties that can be set using the **Set-MailboxDatabase** cmdlet:

- **IsExcludedFromProvisioning** Use this property if you want to indicate that the database should be permanently excluded from automatic mailbox distribution.
- **IsSuspendedFromProvisioning** Use this property if you want to indicate that the database should be temporarily excluded from automatic mailbox distribution.

Both properties have two valid values, `$True` and `$False`. The default value for each is `$False`. The property you choose is purely for your information. Setting either property to `$True` has the same result of excluding the database from the automatic distribution process. Both properties must be set to `$False` for a mailbox database to be included in the automatic distribution process.

Exchange 2010 provides these two properties for excluding a mailbox database from automatic distribution so that you can easily identify the databases that have been permanently excluded from automatic distribution and which have been temporarily excluded.

To set a mailbox database as permanently excluded from automatic distribution, use the following command:

```
Set-MailboxDatabase <database name> -IsExcludedFromProvisioning $True
```

To set a mailbox database as temporarily excluded from automatic distribution, use the following command:

```
Set-MailboxDatabase <database name> -IsSuspendedFromProvisioning $True
```

When a mailbox database is excluded from automatic distribution, the only way to create a mailbox in, or move a mailbox to, the database is to use the *Database* parameter on the

New-Mailbox and **Enable-Mailbox** cmdlets or the *TargetDatabase* parameter on the **New-MoveRequest** cmdlet.

If you want to make an excluded mailbox database available for selection in the automatic distribution process, set both properties to `$False`.

Database Scopes

Database management scopes are an additional level of control over the automatic mailbox distribution process that's been added to Microsoft Exchange Server 2010 Service Pack 1 (SP1). If a mailbox database is online and healthy, it's in the local Active Directory site, and it isn't excluded from the automatic distribution process, Exchange 2010 SP1 checks to see if the mailbox database is included in the database scope applied to the administrator running the cmdlet. If it's included in the database scope, it's included in the list of databases available to that administrator.

Database scopes are part of the Role Based Access Control (RBAC) permissions model. For more information about RBAC and database scopes, see the following topics:

- Understanding Role Based Access Control
- Understanding Management Role Scopes

Database scopes can be useful if you have many mailbox databases in your local Active Directory site that are available to automatic distribution, but you want to limit which databases can be used by certain sets of administrators. For example, your Exchange 2010 SP1 servers may serve several agencies but you only want to allow each agency to create or move mailboxes to mailbox databases that are allocated to them.

By default, all administrators in an Exchange 2010 SP1 organization can see all of the mailbox databases in the organization. To limit the databases that they can see, and therefore limit the databases they can potentially create mailboxes in or move mailboxes to, you must do the following:

1. Create a custom database management scope using the **New-ManagementScope** cmdlet that includes only the mailbox databases you want the administrator to use.
2. Associate the new database scope with a management role assignment in one of the following ways:
   - Add the new database scope to an existing management role assignment using the *CustomConfigWriteScope* parameter on the **Set-ManagementRoleAssignment** cmdlet. The database scope is now applied to the management role group, universal security group (USG), or user assigned the role assignment.
   - Create a management role assignment using the **New-ManagementRoleAssignment** cmdlet and use the *CustomConfigWriteScope* parameter to specify the new database scope. You can create a role assignment between a management role and a role group, USG, or user.
3. If you created a role assignment to a role group or USG, add users to the role group or USG so that the role assignment and database scope are applied to the users.
4. If applicable, remove the user (or users who are members of role groups or USGs you created in the preceding steps) you assigned the new role assignment to from any other role groups or USGs that might be assigned a database scope that contains databases you don't want them to access.
5. Verify that the administrators have access only to the databases they should have access to.

After you complete these steps, the administrators that are assigned role assignments with the database scopes you created will only be able to create mailboxes in or move mailboxes to the databases you specified.

For more information about how to use database scopes to limit which mailbox databases are available to administrators, see Control Automatic Mailbox Distribution Using Database Scopes.

1.8.1.14.2 Understanding Custom Attributes

Understanding Custom Attributes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-14*

Microsoft Exchange Server 2010 and Exchange Server 2007 include 15 extension attributes. You can use these attributes to add information about a recipient, such as an employee ID, organizational unit (OU), or some other custom value for which there isn't an existing attribute. These custom attributes are labeled in Active Directory as **ms-Exch-Extension-Attribute1** through **ms-Exch-Extension-Attribute15**. In the Exchange Management Shell, the corresponding parameters are *CustomAttribute1* through *CustomAttribute15*. These attributes aren't used by any Exchange components. They can be used to store Active Directory data without having to extend the Active Directory schema.

In Exchange Server 2003 and earlier, if you wanted to store this information in Active Directory, you had to create an attribute by extending the Active Directory schema. Schema extension requires planning, procuring object identifiers (OIDs) for new attributes, and testing the extension process in a test environment before you implement it in a production environment. In Exchange 2010 and Exchange 2007, user-defined Active Directory schema extensions can't be used in recipient filters used by address lists, e-mail address policies, and dynamic distribution groups.

Important:

In Exchange 2003, you can create user-defined Active Directory schema extensions. However, in Exchange 2010, you can't use Exchange 2003 user-defined schema extensions as filterable properties. If your organization has user-defined schema extensions, we recommend that you use the 15 custom attributes defined by Exchange 2010 for each recipient. However, if the 15 custom attributes defined by Exchange don't meet the needs of your organization, we recommend that you don't upgrade objects that use user-defined schema extensions.

Contents

Advantages of Custom Attributes

Some of the advantages of using custom attributes include:

- You avoid extending the Active Directory schema.
- The attributes are created by Exchange Setup.
- You can use the Exchange Management Console (EMC) or the Exchange

Management Shell to manage the attributes. You don't need to build custom controls or write scripts to populate and display these attributes.
- The attributes are filterable properties that can be used in the *Filter* parameter with recipient cmdlets such as **Get-Mailbox**. They can also used in the EMC and the Shell to create filters for e-mail address policies, address lists, and dynamic distribution groups.

Return to top

Custom Attribute Examples

In many Exchange deployments, creating an e-mail address policy for all recipients in an OU is a common scenario. The OU isn't a filterable property that can be used in the *RecipientFilter* parameter of an e-mail address policy or an address list.

Note:
Dynamic distribution groups have an additional parameter that you can use to restrict it to recipients in a particular OU or container.

If the recipients in that OU don't share any common properties that you can filter by, such as department or location, you can populate one of the custom attributes with a common value, as shown in this example.

```
Get-Mailbox -OrganizationalUnit Sales | Set-Mailbox CustomAttribute1 "SalesOU"
```

Now you can create an e-mail address policy for all recipients that have the *CustomAttribute1* property that equals SalesOU, as shown in this example.

```
New-EmailAddressPolicy -Name "Sales" -RecipientFilter { CustomAttribute1 -eq "Sal
```

Return to top

Custom Attribute Example with the ConditionalCustomAttributes Parameter

When creating dynamic distribution groups, e-mail address policies, or address lists, you don't need to use the *RecipeintFilter* parameter to specify custom attributes. You can use the *ConditionalCustomAttribute1* to *ConditionalCustomAttribute15* parameters instead. You can create a dynamic distribution group based on the recipients whose CustomAttribute1 is set to SalesOU, as shown in this example.

```
New-DynamicDistributionGroup -Name "Sales Users and Contacts" -IncludedRecipients
```

Note:
You must use the *IncludedRecipients* parameter if you use a *Conditional* parameter. In addition, you can't use *Conditional* parameters if you use the *RecipientFilter* parameter. If you want to include additional filters to create your dynamic distribution group, e-mail address policies, or address lists, you should use the *RecipientFilter* parameter.

Return to top

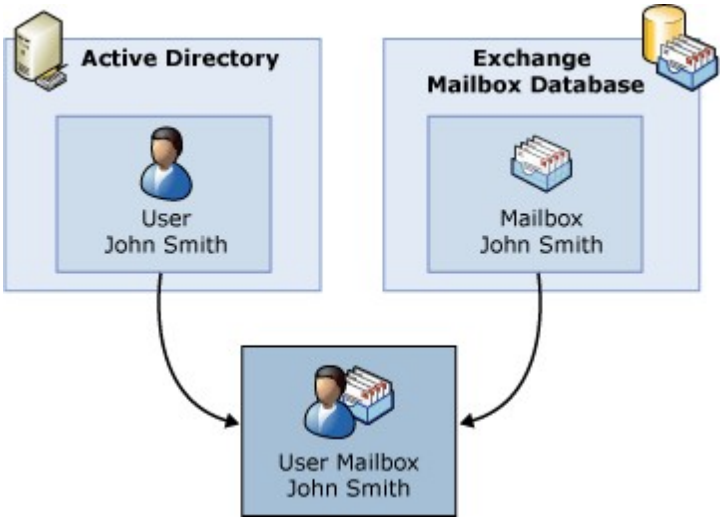
Understanding Disconnected Mailboxes

[This topic is in progress.]

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Each mailbox consists of an Active Directory user and the mailbox data stored in the Exchange mailbox database. (The following figure shows the components of a mailbox.) All configuration data for a mailbox is stored in the Exchange attributes of the Active Directory user object. The mailbox database contains the mail data that's in the mailbox associated with the user account.



A disconnected mailbox is a mailbox object in the mailbox database that isn't associated with an Active Directory user account. There are two types of disconnected mailboxes:

- **Disabled mailboxes** When a mailbox is disconnected or removed by using the **Disable-Mailbox** or **Remove-Mailbox** cmdlet, Exchange retains the deleted mailbox and the mailbox is switched to a disabled state. With disabled mailboxes, you can recover mailbox data without having to restore the entire mailbox database. Disabled mailboxes are retained in the mailbox database until the deleted mailbox retention period expires or until the mailbox is permanently deleted.
- **Soft-deleted mailboxes** When mailboxes are moved from a Microsoft Exchange Server 2010 Service Pack 1 (SP1) database to any other database, Exchange doesn't fully delete the mailbox from the source database upon completion of the move. Instead, the mailbox in the source mailbox database is switched to a *soft-deleted* state. With soft-deleted mailboxes, you can use the **MailboxRestoreRequest** cmdlet set to access mailbox data during a mailbox restore operation. Soft-deleted mailboxes are retained in the source database until either the deleted mailbox retention period expires or until the **Remove-StoreMailbox** cmdlet is used to purge the mailbox. For more information, see Restore a Soft-Deleted Mailbox.

For more information and detailed steps about how to manage disconnected mailboxes, see Managing Disconnected Mailboxes.

Working with Disabled Mailboxes

There are three operations you can perform on a disabled mailbox:

- Connect it to an existing user account in Active Directory
- Restore it to a new or existing user account in Active Directory
- Permanently delete it from the Exchange mailbox database

During the time a disabled mailbox is retained in the Exchange mailbox database, you can connect it to an existing Active Directory user account that isn't associated with another mailbox. Scenarios in which you may want to connect or restore a disabled mailbox include the following:

- You disabled a mailbox and now want to reconnect the mailbox to an Active Directory user account.
- You removed a mailbox by using the Remove-Mailbox cmdlet without the *Permanent* or *StoreMailboxIdentity* parameters and now want to reconnect the mailbox to a different Active Directory user account.
- You want to convert a user mailbox to a linked mailbox associated with a user account external to the forest in which your Exchange organization exists. The resource forest scenario is an example of when you would want to associate a mailbox with an external account. In a resource forest scenario, user objects in the Exchange forest have mailboxes, but the user objects are disabled for logon. You must associate these mailbox objects in the Exchange forest with enabled user objects in the external accounts forest.

Connecting or Restoring Disabled Mailboxes

In Exchange 2010 SP1, there are two methods by which you can reconnect a disabled mailbox. In the first method, you can still use the **Connect-Mailbox** cmdlet in the Exchange Management Shell or the Connect Mailbox wizard in the Exchange Management Console (EMC) to connect a disabled mailbox. This method was introduced in Exchange 2007. The Connect Mailbox wizard is available from the action pane when you select the **Disconnected Mailbox** node under **Recipient Configuration**.

The second method to reconnect a disabled mailbox uses the *MailboxRestoreRequest* cmdlet set in the Shell. This cmdlet set uses the Mailbox Replication Service (MRS) to reconnect the mailbox. You can't use the EMC to perform this process.

After you reconnect a mailbox to an existing Active Directory user account, that user account becomes the owner of the mailbox and has full access to any content within the mailbox.

For detailed instructions about how to connect disabled mailboxes, see Connect or Restore a Disabled Mailbox

Permanently Deleting a Disabled Mailbox

As stated previously, Exchange retains disabled mailboxes in the mailbox database based on the deleted mailbox retention settings configured for that mailbox database. After the specified retention period, a disabled mailbox is permanently deleted from the Exchange mailbox database. However, you can also permanently delete a disabled mailbox at any time by using one of the following two methods:

- You can use the Remove-Mailbox cmdlet in the Shell. To do this, you need to set the *Permanent* parameter to `$true` when you run the command.
  If you want to permanently delete the data within the mailbox database for a previously disabled mailbox, you must use the *StoreMailboxIdentity* parameter with the **Remove-Mailbox** cmdlet. You can use the Get-MailboxStatistics cmdlet to determine the value you need to supply to the *StoreMailboxIdentity* parameter for a disconnected mailbox. For an example of this scenario, see the third code example in the reference topic Remove-Mailbox.
- You can use the Remove-StoreMailbox cmdlet to purge a mailbox and all of its

message content from the mailbox database. This results in permanent data loss for the mailbox being purged. You can only run this cmdlet against disconnected mailboxes. For more information, see Permanently Delete a Disconnected Mailbox.

Working with Soft-Deleted Mailboxes

A soft-deleted mailbox is created when the mailbox is moved from one Exchange Server 2010 SP1 mailbox database to any other mailbox database. Exchange doesn't fully delete the mailbox from the source database after a move in case an error occurs causing the mailbox on the destination database to fail. You can always restore the source mailbox and try again. Exchange will retain the soft-deleted mailbox for the retention period.

There are two operations that you can perform on soft-deleted mailboxes:

1. You can restore the soft-deleted mailbox to an existing active directory user.
2. You can permanently delete the soft-deleted mailbox.

Restoring a Soft-Deleted Mailbox

Permanently Deleting a Soft-Deleted Mailbox

Working with Disconnected Personal Archives

Personal archives become disconnected when they are disabled. Similar to disabled mailboxes, a disconnected personal archive can be connected by using the **Connect-Mailbox** cmdlet with the *Archive* parameter.

The primary mailbox and the personal archive share the same legacy distinguished name (DN), so you must connect the personal archive to the same user mailbox that it was previously connected to. You can't connect the personal archive to a different user mailbox.

There are two operations that you can perform on disconnected personal archives:

- Connect it to an existing mailbox in Active Directory
- Permanently delete it from the Exchange mailbox database

Connecting Disconnected Personal Archives

A disconnected personal archive is retained in the mailbox database for a specified amount of time. By default, Exchange retains the disconnected personal archives for 30 days. During this time, you can recover the personal archive by associating it with an existing mailbox.

Note:

If you disable a personal archive for a user mailbox and then enable a personal archive for that same user, that user mailbox will get a new personal archive. You must use the **Connect-Mailbox** cmdlet to connect a disabled personal archive to an existing mailbox.

For more information, see Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive.

Permanently Deleting a Disabled Personal Archive

Exchange retains disconnected personal archives based on the deleted mailbox retention settings configured for the mailbox database. The default retention period is 30 days. After the specified retention period, a disconnected personal archive is permanently deleted from the mailbox database.

You can also permanently delete a disconnected mailbox at any time by using the

Remove-Mailbox cmdlet with the *Archive* switch in the Shell. To do this, you need to set the *Permanent* parameter to `$true` when you run the command.

1.8.1.14.4 Understanding the Microsoft Exchange Recipient

Understanding the Microsoft Exchange Recipient

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-27*

This topic describes the configuration and management of the Microsoft Exchange recipient. The *Microsoft Exchange recipient* is a special Microsoft Exchange Server 2010 recipient object that provides a unified and well-known message sender that differentiates system-generated messages from other messages. The Microsoft Exchange recipient is functionally equivalent to an internal postmaster. The Microsoft Exchange recipient replaces the System Administrator sender that was used for system-generated messages in earlier versions of Exchange. Messages from the Microsoft Exchange recipient display **Microsoft Exchange** as the sender. The types of messages sent by the Microsoft Exchange recipient include:

- DSN messages
- Journal reports
- Quota messages
- Agent-generated messages

Contents

Configuring the Microsoft Exchange Recipient

Unlike a mailbox, mail user, or mail contact, the Microsoft Exchange recipient isn't a typical recipient object. The Microsoft Exchange recipient isn't managed by using the typical recipient tools found in the Exchange Management Console (EMC) or the Exchange Management Shell. However, you can use the Set-OrganizationConfig cmdlet in the Shell to perform the following configuration tasks:

- Allow or prevent the application of the default e-mail address policy to the Microsoft Exchange recipient. By default, the default mail address policy is applied to the Microsoft Exchange recipient.
- Configure a recipient object to receive messages that are sent to the Microsoft Exchange recipient. By default, no recipient is configured to receive messages that are sent to the Microsoft Exchange recipient.
- Configure the e-mail addresses of the Microsoft Exchange recipient. This includes specifying a primary SMTP address.

Microsoft Exchange Recipient Parameters

The following table describes the **Set-OrganizationConfig** parameters used to configure

the Microsoft Exchange recipient.

Microsoft Exchange recipient parameters in Set-OrganizationConfig

Parameter	Default value	Description
MicrosoftExchangeRecipientEmailAddresses	MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@<*Accepted Domain*>. The <*Accepted Domain*> placeholder represents an accepted domain that's used in an e-mail address policy. For every accepted domain that's used in an e-mail address policy, there's a corresponding e-mail address.	The *MicrosoftExchangeRecipientEmailAddresses* parameter specifies one or more e-mail addresses for the Microsoft Exchange recipient. All valid Exchange 2010 e-mail address types may be used. You can specify multiple values for this parameter as a comma-delimited list. If the *MicrosoftExchangeRecipientEmailAddressPolicyEnabled* parameter is set to `$true`, the e-mail addresses are automatically generated by the default e-mail address policy, and you can't use the *MicrosoftExchangeRecipientEmailAddresses* parameter. E-mail addresses that you specify by using the *MicrosoftExchangeRecipientEmailAddresses* parameter replace any existing e-mail addresses that are already configured.
MicrosoftExchangeRecipientEmailAddressPolicyEnabled	`$true`	The *MicrosoftExchangeRecipientEmailAddressPolicyEnabled* parameter specifies whether the default e-mail address policy is automatically applied to the Microsoft Exchange recipient. The default value is `$true`. If this parameter is set to `$true`, Exchange 2010 automatically adds new e-mail addresses to the Microsoft Exchange recipient when e-mail address policies are added or modified in the Exchange organization. If this parameter is set to `$false`, you must manually add new e-mail addresses to the Microsoft Exchange recipient when e-mail address policies are added or modified. If you change the value of the *MicrosoftExchangeRecipientEmailAddressPolicyEnabled* parameter from `$false` to `$true`, any e-mail addresses that you defined by using the *MicrosoftExchangeRecipientEmailAddresses* parameter are preserved. However, the value of the *MicrosoftExchangeRecipientPrimarySmtpAddress parameter* reverts to

		MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@<*Accepted Domain in Highest Priority E-mail Address Policy*>.
MicrosoftExchangeRecipientPrimarySmtpAddress	MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@<*Accepted Domain in Highest Priority E-mail Address Policy*>	The *MicrosoftExchangeRecipientPrimarySmtpAddress* parameter specifies the primary return SMTP e-mail address for the Microsoft Exchange recipient. If the *MicrosoftExchangeRecipientEmailAddressPolicyEnabled* parameter is set to `$true`, you can't use the *MicrosoftExchangeRecipientPrimarySmtpAddress* parameter. If you modify the value of the *MicrosoftExchangeRecipientPrimarySmtpAddress* parameter, the value is automatically added to the list of e-mail addresses that are defined in the *MicrosoftExchangeRecipientEmailAddresses* parameter. The *MicrosoftExchangeRecipientPrimarySmtpAddress* parameter is meaningful only if the Microsoft Exchange recipient has more than one defined SMTP e-mail address. If the *MicrosoftExchangeRecipientEmailAddresses* parameter has only one defined SMTP e-mail address, the value of the *MicrosoftExchangeRecipientPrimarySmtpAddress* parameter and the *MicrosoftExchangeRecipientEmailAddresses* parameter are the same.
MicrosoftExchangeRecipientReplyRecipient	`$null`	The *MicrosoftExchangeRecipientReplyRecipient* parameter specifies the recipient that should receive messages that are sent to the Microsoft Exchange recipient. Typically, you would configure a mailbox to receive the messages that are sent to the Microsoft Exchange recipient. This parameter can take any of the following values for the specified recipient: • Distinguished name (DN) • Canonical name • GUID • Name • Display name • Alias

		• Exchange DN • Primary SMTP e-mail address If you don't configure a recipient for the Microsoft Exchange recipient, messages that are sent to the Microsoft Exchange recipient are discarded.

Internal and External Delivery of System Messages

The Microsoft Exchange recipient is used as the sender for system-generated messages sent to internal message senders. An internal sender is a recipient object that exists inside the Exchange organization. Specifically, the domain part of the primary SMTP e-mail address of the recipient object must be defined in the list of accepted domains for the Exchange organization.

When system-generated messages are sent to an external sender, the Microsoft Exchange recipient isn't used as the sender of the message. Instead, the e-mail address that's specified by the *ExternalPostmasterAddress* parameter in the Set-TransportConfig cmdlet is used. For more information, see Configure the External Postmaster Address.

However, under certain circumstances, the Microsoft Exchange recipient could be exposed to external recipients. These circumstances include but aren't limited to the following:

- Alternative recipients
- Externally forwarded meeting requests
- External out-of-office notifications
- Journal reports

Microsoft Exchange Recipient in Cross-Forest Scenarios

There's only one Microsoft Exchange recipient in an Exchange organization. Exchange 2010 determines that a message is sent from the Microsoft Exchange recipient by comparing the e-mail address of the message sender to the list of e-mail addresses that are defined by the *MicrosoftExchangeRecipientEmailAddresses* parameter. If Exchange 2010 determines that the sender is the Microsoft Exchange recipient, any messages from the sender are exempt from any configured message size limits that may exist in the Exchange organization.

However, in a cross-forest scenario, each forest has its own Microsoft Exchange recipient and its own message size limits. When messages are sent from the Microsoft Exchange recipient in the source forest, the target forest treats the sender as it would any other unauthenticated, external recipient. Even though the message is a system-generated message from the source forest, the message is still subject to any message size limits that are configured in the target forest.

To make sure that each forest can recognize messages that are sent from the Microsoft Exchange recipient in the other forest, you can configure the Microsoft Exchange recipient in each forest with an additional e-mail address that matches the primary e-mail address of the Microsoft Exchange recipient in the other forest. With this configuration, each forest can recognize messages that are sent from the Microsoft Exchange recipient in the other forest. This configuration correctly exempts messages that are sent from the Microsoft

Exchange recipient in both forests from any message size limits.

However, this configuration introduces issues if either forest allows messages to be sent to the Microsoft Exchange recipient by using the *MicrosoftExchangeRecipientReplyRecipient* parameter. Because the Microsoft Exchange recipient in each forest is configured by using the e-mail addresses of the Microsoft Exchange recipients of both forests, any messages that are sent to the Microsoft Exchange recipient will never leave the local forest from which the messages are sent. The messages will be sent to the recipient that's specified by the *MicrosoftExchangeRecipientReplyRecipient* parameter in the local forest. If one administrator is responsible for the messaging administration of both forests, that administrator can read the messages that are sent to the Microsoft Exchange recipient in both forests. However, if different administrators are responsible for each forest, the administrator of one forest can't manage the messages that are incorrectly sent to the Microsoft Exchange recipient in the other forest.

For more information about how to administer Exchange 2010 in cross-forest scenarios, see "Understanding Multiple Forest Administration" in Deploy Multiple Forest Topologies.

1.8.1.14.5 Understanding Recipient Restrictions

Understanding Recipient Restrictions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-02-01*

You can configure restrictions on the recipients in your organization. These restrictions allow you to use recipients consistent with your organization's policies.

Looking for management tasks related to managing Mailbox servers? See Managing Mailbox Servers.

Contents

Message Size Restrictions

Restrictions on the size of a message are the most commonly used restrictions in any messaging system. Setting a maximum message size prevents your messaging system, or the underlying network infrastructure, from being overwhelmed.

Depending on what you want to do, you can configure message size restrictions for several components. For example, you can restrict the total size of a message or the size of the individual message components (such as the message header, attachments, or the

number of recipients).

Although you can also specify whether message size restrictions are applied to your entire Microsoft Exchange Server 2010 organization or to a specific connector or user object, this section focuses only on message size restrictions that you can apply to recipients. For a complete list of message size restrictions that you can configure in an Exchange 2010 organization, see Understanding Message Size Limits.

When configuring message size restrictions for individual recipients, it's important to consider other message size restrictions that may exist in your organization. For example, assume that the Hub Transport servers in your organization are configured to restrict message size to 10 megabytes (MB). In this case, for a mail contact that has external addresses, you should set the maximum receive size to be no larger than 10 MB. Although a sender in your organization will be able to submit a message larger than 10 MB to this mail contact, the message would be rejected by the Hub Transport server. To learn more about how different message size restrictions affect each other and the order of precedence, see Understanding Message Size Limits.

Message Size Restrictions for All Recipient Types

Exchange 2010 can deliver or route messages to all recipients. Therefore, you can set a maximum receiving message size limit for any recipient type in your Exchange organization. If a sender attempts to send a message that's larger than the specified size, the message is returned to the sender with a descriptive error message.

In the Exchange Management Console (EMC), you set the maximum receiving message size by using the **Mail Flow Settings** tab of the recipient's properties. In the Exchange Management Shell, use the *MaxReceiveSize* parameter of the appropriate **Set-** cmdlet. For an example about how to configure receiving message size restrictions for a recipient, see Configure Message Size Limits for a Mailbox or a Mail-Enabled Public Folder.

Message Size Restrictions Specific to Mailboxes and Mail-Enabled Public Folders

Mailboxes and mail-enabled public folders are the only recipient types that can submit messages to your Exchange messaging system. Therefore, in addition to setting receiving message size restrictions, you can also set sending message size restrictions.

In the EMC, you set the maximum sending message size of a mailbox by using the **Mail Flow Settings** tab of the mailbox properties. In the Shell, use the *MaxSendSize* parameter of the **Set-Mailbox** and **Set-MailPublicFolder** cmdlets. For an example about how to configure sending message size restrictions for mailboxes and mail-enabled public folders, see Configure Message Size Limits for a Mailbox or a Mail-Enabled Public Folder.

Important:

If you implement sending message size restrictions for your mailbox users, you should also make sure that your Client Access servers are configured to accept client requests that are equal to or larger than the sending message size limit that you configured. Microsoft Office Outlook Web App uses ASP.NET and is thereby affected by the ASP.NET configuration. ASP.NET has a setting, **maxRequestLength**, which determines the maximum amount of data that the Web browser can submit to the Client Access server. If this limit is lower than the sending message size restriction, your users may receive a confusing error. To learn more about managing the maximum message size in Outlook Web App, see Configure Maximum Message Size in Outlook Web App.

Public Folder Management Console

The Public Folder Management Console is a Microsoft Management Console (MMC) 3.0-based interface that provides Exchange administrators with a graphical user interface (GUI) to create, configure, and manage public folders. You can also configure message size restrictions for a mail-enabled public folder by using the **Message Size Restrictions** option on the **Mail Flow Settings** tab of the public folder properties in the Public Folder Management Console. To learn more about the Public Folder Management Console, see

Using the Public Folder Management Console.

Return to top

Message Delivery Restrictions

With Exchange 2010, you can place restrictions on how messages are delivered to individual recipients. Message delivery restrictions apply to all recipient types and can be useful for controlling access to specific recipients in your Exchange 2010 organization. For example, several organizations specify that only a small set of users can send messages to large distribution groups.

You can configure the following message delivery restrictions for a recipient:

- **Accept messages from a specific list of senders** If you specify a list of senders from which to accept messages, the recipient will receive messages only from those senders. By default, all recipients are configured to accept messages from all senders.
  Use this restriction for recipients for which you want only a small number of authorized senders to be able to send messages. For example, you may want to configure a distribution group that contains all the employees in your organization to accept messages from only specific employees in the Human Resources department who are responsible for company-wide communications. Another scenario where you can use this restriction is for mail contacts that represent suppliers for a retail organization. You may want to configure each of these mail contacts to accept messages from only the buyers who work directly with those suppliers.
- **Reject messages from a specific list of senders** If you specify a list of senders from which to reject messages, the recipient will reject messages from those senders. By default, all recipients are configured not to reject messages from any senders.

  Note:
  This restriction overrides the **Accept messages from a specific list of senders** restriction. If a sender is listed in both lists, any messages sent by that sender will be rejected.

  Use this restriction to block specific users from sending messages to specific recipients. For an example about how this restriction is useful, consider the following scenario. You create a distribution group called All Employees. You configure that distribution group to accept messages from only those senders that are a member of the Human Resources distribution group. However, the Human Resources distribution group also includes mailboxes for interns whom you don't want to allow access to the All Employees distribution group. Therefore, to prevent the intern mailboxes from sending messages to the All Employees distribution group, you can specify the intern mailboxes when configuring the **Reject messages from a specific list of senders** restriction for the All Employees group.
- **Require that all senders are authenticated** If you configure a recipient to require that all senders are authenticated, any messages from senders that don't have valid logon credentials in your organization will be rejected. By default, only new distribution groups and dynamic distribution groups are configured to require all senders to be authenticated.

  Note:
  In previous versions of Exchange, by default, no recipients were configured to require all senders to be authenticated. Therefore, any distribution groups that you migrate from a previous version of Exchange won't have this restriction configured.

  Use this restriction to specify that recipients receive messages only from internal senders that have been successfully authenticated. For example, to

prevent messages that originate outside of your Exchange organization from being delivered to distribution groups that are used for internal communications, you can configure these groups to require sender authentication.

For details about how to configure message delivery restrictions for a recipient, see Configure Message Delivery Restrictions.

Return to top

Maximum Recipients per Message Restrictions

It can take a significant amount of time for a Hub Transport server to route messages that are addressed to a large number of recipients. As a result, this may affect the performance of the Hub Transport server, which could impact the overall message delivery in your Exchange organization.

To eliminate this risk, you can restrict the number of recipients that are allowed per message. Although you can configure this restriction at the mailbox level, you can also configure it at a higher level, such as the organization level, connector level (only for Receive connectors), and Hub Transport server level. Generally, it's a best practice to configure this setting at a higher level and use the mailbox-level configuration only for exceptions. For more information about the different levels at which you can configure this restriction, as well as a list of default values, see Understanding Message Size Limits.

For details about how to configure maximum recipients per message restrictions for a mailbox, see Restrict the Number of Recipients per Message.

Return to top

Mailbox Size Restrictions

You can configure storage quotas for mailboxes. By using storage quotas, you can control the size of mailboxes and manage the growth of mailbox databases. For detailed steps about how to configure storage quotas for a mailbox, see Configure Storage Quotas for a Mailbox.

Note:

You can also configure storage quotas at the mailbox database level. The quotas that you configure for a mailbox database apply to all mailboxes in that database, unless the mailbox is configured not to use mailbox database defaults. Generally, it's a best practice to configure storage quotas at the mailbox database level and use the mailbox level configuration only for exceptions. For detailed steps about how to configure storage quotas for a mailbox database, see Configure Mailbox Database Properties.

Because storage quotas have a direct impact on your storage capacity planning, you must plan your storage quotas carefully. Storage quotas, number of mailboxes per mailbox database, and the storage subsystem that hosts each mailbox database are all factors that you should consider when planning your deployment.

Before deploying Unified Messaging (UM) in your Exchange organization, you must review any existing storage quotas you've configured. Because Windows Media Audio (WMA) and waveform audio (.wav) files are attached to each voice message, voice messages may be larger than e-mail messages. As a result, voice messages may cause user mailboxes to exceed their quota more quickly than e-mail messages that don't include attachments. To learn more about the impact of Unified Messaging on storage quotas, see Understanding

Storage Quotas and Voice Mail.

Return to top

Public Folder Size Restrictions

Similar to mailboxes, you can configure storage quotas for your mail-enabled public folders. By using storage quotas, you can control the size of mail-enabled public folders and manage the growth of public folder databases.

In addition to storage quotas, you can also define age limits for your public folders. If you specify an age limit for a public folder, any items in that public folder that exceed the age limit without having been modified are removed automatically from that public folder. This provides administrators with an additional option for controlling the growth of their public folder databases. For detailed steps about how to configure storage quotas and age limits for public folders, see Configure Public Folder Properties.

Note:

Storage quotas and age limits also apply to public folders that aren't mail-enabled.

Return to top

1.8.1.14.6 Understanding Recipient Scope

Understanding Recipient Scope

Mailbox > Understanding Mailbox > Understanding Recipients >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-20*

You manage recipients by using the Exchange Management Console (EMC) and the Exchange Management Shell. These management interfaces provide the flexibility to view and manage recipients that are stored at various levels of an Active Directory hierarchy.

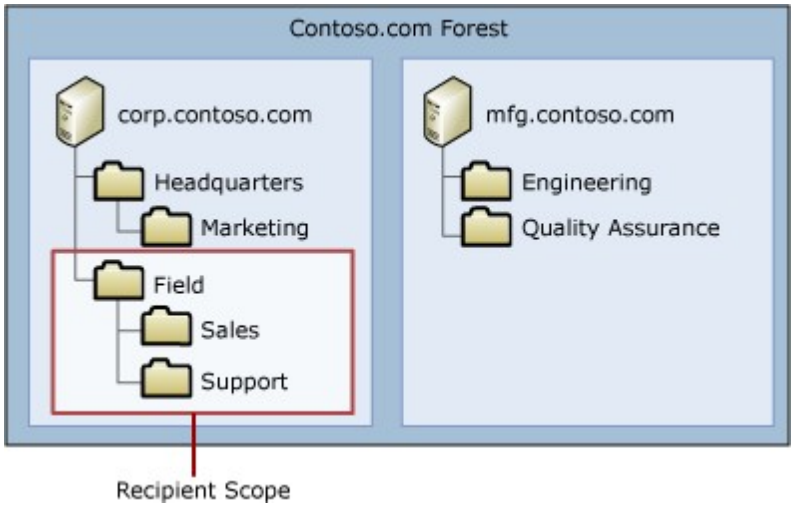
Microsoft Exchange Server 2010 management interfaces do this by using a concept called the *recipient scope*. Recipient scope refers to the specified portion of the Active Directory hierarchy that the EMC and the Shell will use for recipient management. When you set the recipient scope to a specific location within Active Directory, you can view and manage all recipients stored in that location and all the containers under it. For example, if you set the recipient scope to a domain, the Exchange management interface you're using lets you view and manage all recipients that are stored in all organizational units (OUs) within that domain.

Note:

The recipient scope is simply a view of Active Directory and has no security context. You can access and manage only the objects and containers to which your user account has been granted permission, regardless of the recipient scope setting.

Setting the recipient scope does more than limit the number of recipients returned. When you set the recipient scope, the management interface you are using operates within the recipient scope that you specified. When performing recipient management tasks, the management interface can view only the portion of Active Directory that you set as the recipient scope. For example, assume that your company has the Active Directory

structure shown in the following figure. If you set the recipient scope to the **Field** OU of the corp.contoso.com domain, the Exchange management interface can view only the portion of Active Directory that's highlighted in the following figure.



The recipient scope applies to the *first class* recipient objects. First class recipient objects refer to all mailboxes, mail contacts, mail users, distribution groups, and dynamic distribution groups.

Important:

The properties of first class recipient objects aren't bound by the recipient scope. For example, when adding members to a distribution group, you can select any recipient in the forest, regardless of the recipient scope. Similarly, when configuring the manager of a mailbox user, you can select any mail-enabled user or contact in the forest.

Looking for management tasks related to managing Mailbox servers? See Managing Mailbox Servers.

Recommendations for Working with Recipient Scope

The following are some recommendations for working with recipient scope:

- In large organizations, recipients may be spread across multiple domains or OUs. In these cases, setting a recipient scope that focuses on the specific set of recipients you're managing may reduce the number of recipients that are returned, thereby improving the performance of the Exchange management interfaces.
- Set the recipient scope to the entire forest only when performing specific tasks that apply to all recipients in the forest. When the recipient scope is set to the entire forest, the management interfaces use a global catalog server to access Active Directory. The recipient information that's displayed in the interfaces is dependent on the replication latencies of Active Directory. As a result, the information that's displayed may not be entirely up to date. Likewise, any updates made through the interfaces may not take effect until Active Directory replicates the changes.
  Furthermore, if you have a large Active Directory deployment with recipients spread across multiple domains, using a forest-wide recipient scope can reduce the performance of the management interfaces due to the sheer number of recipients returned.
- If you have a complex Active Directory replication topology, or if you have high

replication latency, specify the global catalog that's most up to date when setting the recipient scope to the entire forest.
- If you use a specific domain controller on which all updates to Active Directory are made, you can specify that domain controller as the preferred recipient domain controller when setting the recipient scope. For example, if you have an account provisioning system that works with a specific domain controller, you can specify that domain controller as the preferred recipient domain controller.

Setting the Recipient Scope

Exchange 2010 management interfaces always start with the recipient scope at the domain level. The default setting for the recipient scope is always set to the domain of the computer that's running the management interface. Neither the user account that's being used nor the Exchange servers being managed has bearing on the default value of the recipient scope.

To illustrate this point, consider a scenario where the organization contoso.com has an Active Directory forest with three domains: contoso.com (which contains all computer accounts), users.contoso.com (which contains all user accounts), and exchange.contoso.com (which contains the Exchange servers). To administer an Exchange server in exchange.contoso.com, an administrator logs on to a computer in contoso.com with a user account in users.contoso.com. When the administrator opens the EMC or the Shell, by default, the recipient scope is set to contoso.com.

Depending on the task you need to accomplish, you can change the recipient scope to a different location in Active Directory. You can set the recipient scope to a single OU, to the top level of an OU hierarchy, to a domain, or even to the entire forest.

Recipient Scope in the EMC

Changing the recipient scope in the EMC changes the set of recipients that are displayed in the result pane of the **Recipient Configuration** node. The dialog boxes that you use to select recipients or OUs (located on various wizard pages) also work within the same scope. For example, if you're mail-enabling an existing contact, the **Select Contact** dialog box in the New Mail Contact wizard displays only the contacts within the recipient scope that aren't already mail-enabled.

Note:

The Microsoft Management Console (MMC) saves any changes you make to a snap-in as preferences in your user profile on the administrator computer. The recipient scope setting is also saved as one of your preferences. As a result, the next time you start the EMC on the same computer, the default setting of the recipient scope is overwritten by the scope last specified. However, if you use another computer or a different user account to run the EMC, you will need to adjust the recipient scope again.

To modify the recipient scope in the EMC, select the **Recipient Configuration** node, and then click **Modify Recipient Scope** in the action pane. For more information about changing the recipient scope in the EMC, see Change the Recipient Scope.

Recipient Scope in the Shell

Because you must manually type all values in the Shell, it's important that you keep the recipient scope in mind as you manage recipients. If you make references to objects that are outside the recipient scope, you may receive errors. For example, if you try to create a new distribution group in an OU that isn't within the recipient scope you specified, you will receive the error, "Organizational unit *<OU name>* wasn't found. Please make sure you have typed it correctly".

You can view or modify the recipient scope by using the Set-AdServerSettings cmdlet.

When you change the recipient scope in the Shell, you change the set of recipients that

are returned for the **Get-** cmdlets of the recipient. The recipient scope is accessible by using the **Set-AdServerSettings** cmdlet.

Note:
The default scope isn't retained when you close the Shell. The Shell resets to the default domain-level recipient scope the next time that the Shell is opened.

1.8.1.15 Understanding Recoverable Items

Understanding Recoverable Items

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-14*

To protect from accidental or malicious deletion and to facilitate discovery efforts commonly undertaken before or during litigation or investigations, Microsoft Exchange Server 2010 introduces the Recoverable Items folder. The Recoverable Items folder replaces the feature known as the dumpster in Exchange Server 2007. The Recoverable Items folder is used by the following Exchange features:

- Deleted item retention
- Single item recovery
- Litigation hold
- Mailbox audit logging

Contents

Terminology

Knowledge of the following terms will help you understand the content in this topic.

Delete
: Describes when an item is deleted from any folder and placed in the Deleted Items default folder.

Soft delete
: Describes when an item is deleted from the Deleted Items default folder and placed in the Recoverable Items folder. Additionally describes when a Microsoft Outlook user deletes an item by pressing Shift+Delete, which bypasses the Deleted Items folder and places the item directly in the Recoverable Items folder.

Hard delete
: Describes when an item is marked to be purged from the mailbox database. This is also known as a *store hard delete*.

Return to top

Recoverable Items Folder

To better meet customers' legal compliance requirements, the dumpster is reinvented as

the Recoverable Items folder in Exchange 2010. The Recoverable Items folder resides in the non-IPM subtree of each mailbox. The non-IPM subtree is a storage area within the mailbox that contains operational data about the mailbox. This subtree isn't visible to users using Outlook, Microsoft Office Outlook Web App, or other e-mail clients.

This architectural change provides the following key benefits:

- When a mailbox is moved to another mailbox database, the Recoverable Items folder moves with it.
- The Recoverable Items folder is indexed by Exchange Search and can be discovered using Multi-Mailbox Search.
- The Recoverable Items folder has its own storage quota.
- Exchange can prevent data from being purged from the Recoverable Items folder.
- Exchange can track edits of certain content.

The Recoverable Items folder contains the following subfolders:

- **Deletions** This subfolder contains all items deleted from the Deleted Items folder. (In Outlook, you can soft delete an item by pressing Shift+Delete.) This subfolder is exposed to users through the Recover Deleted Items feature in Outlook and Outlook Web App.
- **Versions** If either litigation hold or single item recovery is enabled, this subfolder contains the original and modified copies of the deleted items. This folder isn't visible to end users.
- **Purges** If either litigation hold or single item recovery is enabled, this subfolder contains all items that are hard deleted. This folder isn't visible to end users.
- **Audits** If mailbox audit logging is enabled for a mailbox, this subfolder contains the audit log entries. To learn more about mailbox audit logging, see Understanding Mailbox Audit Logging.

Deleted Item Retention

An item is considered to be soft deleted in the following cases:

- A user deletes an item or empties all items from the Deleted Items folder.
- A user presses Shift+Delete to delete an item from any other mailbox folder.

Soft-deleted items are moved to the Deletions subfolder of the Recoverable Items folder. This provides an additional layer of protection so users can recover deleted items without requiring Help desk intervention. Users can use the Recover Deleted Items feature in Outlook or Outlook Web App to recover a deleted item. Users can also use this feature to permanently delete an item.

Items remain in the Deletions subfolder until the deleted item retention period is reached. The default deleted item retention period for a mailbox database is 14 days. You can modify this period for a mailbox database or for a specific mailbox. In addition to a deleted item retention period, the Recoverable Items folder is also subject to quotas. To learn more, see Recoverable Items Mailbox Quotas later in this topic.

After the deleted item retention period elapses, the item is moved to the Purges folder and is no longer visible to the user. When the Managed Folder Assistant processes the mailbox, items in the Purges subfolder are purged from the mailbox database.

Single Item Recovery

If an item is removed from the Deletions subfolder, either using the Recover Deleted Items feature or by an automated process such as the Managed Folder Assistant, the item can't be recovered by the user. In previous versions of Exchange, recovering these items required the administrator to restore the mailbox database or a mailbox from backup copies. This process generally delayed recovery by minutes or hours, depending on the backup mechanism used.

Exchange 2010 introduces *single item recovery*, a feature you can use to recover items without having to restore the mailbox databases using backup media. This results in considerably shorter recovery periods. When the Managed Folder Assistant processes the Recoverable Items folder for a mailbox that has single item recovery enabled, any item in the Purges subfolder isn't purged if the deleted item retention period hasn't elapsed for that item. Additionally, if the user changes certain properties of an item in any mailbox folder, a copy of the item is made before the modification is written to the Exchange store. The copy is stored in the Versions subfolder by a process known as *copy-on-write page protection*. You can recover different versions of a modified item until the deleted item retention period elapses.

The following table lists the contents of and actions that can be performed in the Recoverable Items folder if single item recovery is enabled.

Recoverable Items folder and single item recovery

State of single item recovery	Recoverable Items folder contains soft-deleted items	Recoverable Items folder contains modified and hard-deleted items	Users can purge items from the Recoverable Items folder	Managed Folder Assistant automatically purges items from the Recoverable Items folder
Enabled	Yes	Yes	No	Yes. By default, all items are purged after 14 days, with the exception of calendar items, which are purged after 120 days.
Disabled	Yes	No	Yes	Yes. By default, all items are purged after 14 days, with the exception of calendar items, which are purged after 120 days. If the Recoverable Items warning quota is reached before the deleted item retention period elapses, messages are deleted in first in, first out (FIFO) order.

Single item recovery isn't enabled by default for new mailboxes or mailboxes moved from a previous version of Exchange. You must use the Exchange Management Shell to enable single item recovery for a mailbox, and then configure or modify the deleted item retention period. To learn more about how to enable single item recovery for a mailbox and to perform single item recovery of deleted items, see the following topics:

- Enable Single Item Recovery for a Mailbox
- Perform Single Item Recovery

Litigation Hold

Exchange 2010 introduces Multi-Mailbox Search, a feature that administrators or records managers can use with delegated Discovery Management permissions to perform discovery searches of mailbox content. Exchange 2010 also introduces litigation hold, which you can use to preserve items in user mailboxes and protect the items from deletion by users or automated processes.

Placing a mailbox on litigation hold stops the Managed Folder Assistant from automatically purging messages from the Purges subfolder. Additionally, copy-on-write page protection is also enabled for the mailbox. Copy-on-write page protection creates a copy of the original item before any modifications are written to the Exchange store. After the mailbox is removed from litigation hold, the Managed Folder Assistant resumes automated purging.

The following table lists the contents of and actions that can be performed in the Recoverable Items folder if litigation hold is enabled.

Recoverable Items folder and litigation hold

State of litigation hold	Recoverable Items folder contains soft-deleted items	Recoverable Items folder contains modified and hard-deleted items	Users can purge items from the Recoverable Items folder	Managed Folder Assistant automatically purges items from the Recoverable Items folder
Enabled	Yes	Yes	No	No
Disabled	Yes	No	Yes	Yes

To learn more about Multi-Mailbox Search and litigation hold, see the following topics:

- Understanding Multi-Mailbox Search
- Understanding Litigation Hold

Copy-on-Write Page Protection and Modified Items

If a user who is placed on litigation hold (or has single item recovery enabled) modifies specific properties of a mailbox item, a copy of the original mailbox item is created before the changed item is written. The original copy is saved in the Versions subfolder. This process is known as copy-on-write page protection. Copy-on-write page protection applies to items residing in any mailbox folder. The Versions subfolder isn't visible to users.

The following table lists the message properties that trigger copy-on-write page protection.

Properties that trigger copy-on-write page protection

Item type	Properties that trigger copy-on-write page protection
Messages (IPM.Note*) Posts (IPM.Post*)	• Subject • Body • Attachments • Senders and recipients • Sent and received dates
Items other than messages and posts	Any change to a visible property, except the following: • Item location (when an item is moved between folders) • Item status change (read or unread)

	• Changes to a retention tag applied to an item
Items in the Drafts default folder	None. Items in the Drafts folder are exempt from copy-on-write page protection.

Important:
In Exchange 2010 Service Pack 1 (SP1), copy-on-write page protection doesn't save a version of the meeting when a meeting organizer receives responses from attendees and the meeting's tracking information is updated. Also, changes to RSS feeds aren't captured by copy-on-write page protection.

When litigation hold is removed from a mailbox and single item recovery is disabled, copies of modified items stored in the Versions folder are removed.

Return to top

Recoverable Items Mailbox Quotas

When an item is moved to the Recoverable Items folder, its size is deducted from the mailbox quota and added to the size of the Recoverable Items folder. In Exchange 2010, mailbox databases have a configurable Recoverable Items warning quota (*soft limit*) of 20 gigabytes (GB) and a Recoverable Items quota (*hard limit*) of 30 GB. By default, these limits are inherited by all mailboxes in the database. However, you can configure individual mailboxes with different quotas. To learn more, see Configure Deleted Item Retention and Recoverable Items Quotas.

When the Recoverable Items folder for a mailbox reaches the Recoverable Items quota, no more items can be stored in the folder. This impacts mailbox functionality in the following ways:

- Mailbox users can't delete items.
- The Managed Folder Assistant can't delete items based on retention tag or managed folder settings.
- For mailboxes that have single item recovery or litigation hold enabled, the copy-on-write page protection process can't maintain versions of items edited by the user.
- For mailboxes that have mailbox audit logging enabled, no mailbox audit log entries can be saved in the Audits subfolder.

For mailboxes that aren't placed on litigation hold, the Managed Folder Assistant automatically purges items from the Recoverable Items folder when the deleted item retention period elapses. If the folder reaches the Recoverable Items warning quota, the assistant automatically purges items in FIFO order.

When the Recoverable Items folder reaches the soft and hard limit defaults, you are notified by means of an event log and a Microsoft System Center Operations Manager alert. This alert fires when the Recoverable Items folder first reaches the soft and hard limit defaults, and then once daily afterward.

The following table lists the events logged when the Recoverable Items folder reaches the soft and hard limit defaults.

Recoverable Items quota warnings and errors

Event ID	Type	Source	Message
10024	Warning	MSExchangeIS Mailbox Store	The mailbox for *<mailbox user>* (*GUID*) has exceeded

			the Recoverable Items Warning Quota. Please remove items from Recoverable Items or increase the Recoverable Items Warning Quota and Recoverable Items Quota. If the Recoverable Items Quota is exceeded, the user will be unable to delete items from the mailbox.
10023	Error	MSExchangeIS Mailbox Store	The mailbox for *<mailbox user>* (*GUID*) has exceeded the maximum Recoverable Items Quota. Items cannot be deleted from this mailbox. The mailbox owner should be notified about the condition of the mailbox as soon as possible. Please remove items from Recoverable Items or increase the Recoverable Items Quota to restore functionality.
10023	Warning	MSExchangeMailboxAssistants	The mailbox:*<mailbox user>* Recoverable Items size has exceeded the warning quota limit. Items were deleted from Recoverable Items folders to prevent mailbox outage. Recoverable Items Warning Quota: 20 GB (21,474,836,480 bytes) Original Recoverable Items size: 21475005311 Current Recoverable Items size: 21474823820 Folder stats: - Folders processed: RecoverableItemsRoot, RecoverableItemsVer

			sions, RecoverableItemsPurges, RecoverableItemsDeletions - Original folder sizes: 21391661934, 55190914, 1987247, 26157788 (item counts: 276828, 400, 84, 646) - Current folder sizes: 21391480443, 55190914, 1987247, 26157788 (item counts: 276817, 400, 84, 646)

If the mailbox is placed on litigation hold, copy-on-write page protection can't maintain versions of modified items. To maintain versions of modified items, you must reduce the size of the Recoverable Items folder. You can use the Search-Mailbox cmdlet to copy messages from the Recoverable Items folder of a mailbox to a discovery mailbox, and then delete the items from the mailbox. Alternatively, you can also raise the Recoverable Items quota for the mailbox. For details, see Clean Up the Recoverable Items Folder.

Return to top

1.8.2 Permissions to Manage Mailbox Servers

Permissions to Manage Mailbox Servers

Exchange Server 2010 > Mailbox >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-12*

Mailbox Permissions

Allow Mailbox Access

Manage Send As Permissions for a Mailbox

Manage Full Access Permissions

Managing Public Folder Permissions

1.8.2.1 Allow Mailbox Access

Allow Mailbox Access

Exchange Server 2010 > Mailbox > Permissions to Manage Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to grant Full Access permission for a mailbox or Receive As permission for a mailbox database.

When you grant a user Full Access permission to a mailbox, that user has full access to only the mailbox for which the permissions are applied. With Full Access permission, the user can open and read the contents of the mailbox.

Important:

In Exchange 2010 Service Pack 1 (SP1), Outlook 2007 and Outlook 2010 clients automatically map to any mailbox to which a user has Full Access permissions. If a user is granted Full Access permissions to another user's mailbox or to a shared mailbox, Autodiscover automatically loads all mailboxes to which the user has full access. If the user has full access to a large number of mailboxes, performance issues may occur when starting Outlook. For example, in some Exchange organizations, administrators have full access to all the mailboxes in the organization. In this case, upon starting, Outlook attempts to open all mailboxes in the organization. Users can't control this behavior and have no way to turn it off.

However, the user can't send mail as that mailbox without additional permissions. For information about granting Send As permission, see Manage Send As Permissions for a Mailbox.

When you grant a user Receive As permission to a mailbox database, that user can log on to all mailboxes within that database, but can't send mail from those mailboxes. For example, you may want to grant access to the mailbox database for mobile access or for legal review.

Full Access or Receive As permissions aren't granted until the Microsoft Exchange Information Store service caches the permissions and updates the cache. To grant the permissions immediately, stop and then restart the Microsoft Exchange Information Store service.

Use the EMC to grant Full Access permission for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox for which you want to grant Full Access permission.
3. In the action pane, under the mailbox name, click **Manage Full Access Permission**. The Manage Full Access Permission wizard opens.
4. On the **Manage Full Access Permission** page, click **Add**.
5. In **Select User or Group**, select the user to which you want to grant Full Access permission, and then click **OK**.
6. Click **Manage**.
7. On the **Completion** page, the **Summary** states whether Full Access permission was successfully granted. The summary also displays the Shell command used to grant Full Access permission.
8. Click **Finish**.

Use the Shell to grant Full Access permission for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

This example grants the user Ayla Kol Full Access permission to Chris Ashton's mailbox.

```
Add-MailboxPermission "Chris Ashton" -User "Ayla Kol" -AccessRights FullAccess
```

For detailed syntax and parameter information, see Add-MailboxPermission.

Use the Shell to grant Receive As permission for a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to grant Receive As permission for a mailbox database.

This example grants the user Ayla Kol Receive As permission for mailboxes on mailbox database DB01. Ayla will be able to log on to every mailbox on that database.

```
Add-ADPermission -Identity "DB01" -User "Ayla" -ExtendedRights Receive-As
```

For detailed syntax and parameter information, see Add-ADPermission.

1.8.2.2 Manage Send As Permissions for a Mailbox

Manage Send As Permissions for a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use Send As permissions to configure a mailbox so that users other than the mailbox owner can use that mailbox to send messages. After this permission is granted, any messages that are sent from the mailbox will appear as if they were sent by the mailbox owner.

The Send As permission isn't granted until after replication has occurred. Replication times depend on your Exchange and network configuration. To grant the permission immediately, stop and then restart the Microsoft Exchange Information Store service.

Also, before you perform this procedure, be aware that you cannot send e-mail messages on behalf of a mailbox if the mailbox is hidden from address lists. When sending a message, Exchange requires that an e-mail address is resolved in the **From** field. In the case where a message is sent on behalf of a mailbox that is hidden from address lists, the SMTP address is interpreted as an address that isn't from your organization (known as a *foreign address*) and is rejected. For information about how to change your mailbox settings, see Configure User and Resource Mailbox Properties.

In Outlook, users will receive the following errors when attempting to send a message on behalf of a mailbox that is hidden from address lists:

- **Online mode** When users press **Send**, they will receive the following error: "You do not have permission to send on behalf of the specified user."

- **Cached Exchange Mode** Outlook initially sends the message, but users will receive a non-delivery report (NDR) containing the following message: "You are not allowed to send this message because you are trying to send on behalf of another user without permission to do so. Please verify that you are sending on behalf of the correct sender, or ask your system administrator to help you get the required permission."

Looking for other management tasks related to mailbox permissions? Check out Permissions to Manage Mailbox Servers.

What Do You Want to Do?

- Use the EMC to manage Send As permissions for a mailbox
- Use the Shell to manage Send As permissions for a mailbox

Use the EMC to manage Send As permissions for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send As permissions" entry in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select a recipient. You can manage Send As permission for the following recipient types:
   - Discovery mailboxes
   - User mailboxes
   - Resource mailboxes
3. In the action pane, click **Manage Send As Permission**.
4. On the **Manage Send As Permission** page, select the users or groups to which you want to grant the Send As permission or from which you want to remove the permission.
   - **Add** Click this button to open the **Select User or Group** dialog box. Use this dialog box to select the users or groups to which you want to grant the Send As permission.
   -  Select a user or group, and then click this button to remove the Send As permission from that user or group.
5. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** close the wizard.

Use the Shell to manage Send As permissions for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send As permissions" entry in the Mailbox Permissions topic.

Use the **Add-ADPermission** cmdlet to manage Send As permissions for a mailbox. When you use the **Add-ADPermission** cmdlet, you must specify the name of the mailbox on

which the Send As permission should be added and the mailbox that should be granted the permission. Because the **Add-ADPermission** cmdlet controls many permissions, you must also specify the Send As permission with the *ExtendedRights* parameter. For example, to add the Send As permission to contoso\kim on the user mailbox John Simpson, use the following command:

```
Add-ADPermission "John Simpson" -User "Domain\User" -Extendedrights "Send As"
```

For detailed syntax and parameter information, see Add-ADPermission.

1.8.2.3 Manage Full Access Permissions

Manage Full Access Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-12*

Use the Manage Full Access Permission wizard to grant Full Access permissions to users or groups for a selected mailbox. You can also use this wizard to remove Full Access permissions from users or groups.

When you grant the Full Access permission to another user for a mailbox, that user becomes able to log on to the mailbox and access its entire contents.

Important:

In Microsoft Exchange Server 2010 Service Pack 1 (SP1), Outlook 2010 and Outlook 2007 clients automatically map to any mailbox to which a user has Full Access permissions. If a user is granted Full Access permissions to another user's mailbox or to a shared mailbox, Autodiscover automatically loads all mailboxes to which the user has full access. If the user has full access to a large number of mailboxes, performance issues may occur when starting Outlook. For example, in some Exchange organizations, administrators have full access to all the mailboxes in the organization. In this case, upon starting, Outlook tries to open all mailboxes in the organization.
In Microsoft Exchange Server 2010, users can't control this behavior and can't turn it off.
In Microsoft Exchange Server 2010 Service Pack 2 (SP2), administrators can turn off the auto-mapping feature. For more information, see the third Exchange Management Shell example in this topic or read Disable Outlook Auto-Mapping with Full Access Mailboxes.

Granting Full Access permissions doesn't grant the right to send mail as the selected mailbox. To grant Send As permissions, see the following topics:

- Manage Send As Permissions for a Mailbox
- Manage Send As Permissions for Mail-Enabled Public Folders

Looking for other management tasks related to mailbox permissions? Check out Permissions to Manage Mailbox Servers.

What Do You Want to Do?

- Use the EMC to manage full access permissions for a mailbox
- Use the Shell to manage full access permissions for a mailbox

Use the EMC to manage full access

permissions for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select a recipient. You can manage Full Access permissions for the following recipient types:
   - Discovery mailboxes
   - User mailboxes
   - Resource mailboxes
3. In the action pane, click **Manage Full Access Permission**.
4. On the **Manage Full Access Permission** page, select the users or groups to which you want to grant the Full Access permission or from which you want to remove the permission. Select one of the following options:
   - **Add** Click this button to open the **Select User or Group** dialog box. Use this dialog box to select the users or groups to which you want to grant the Full Access permission.
   -  Select a user or group, and then click this button to remove the Full Access permission from that user or group.

   Important:

   By default, every mailbox has the security principal **NT AUTHORITY\SELF** listed. This security principal represents the mailbox owner. If you revoke the Full Access permission from this security principal, the mailbox owner is no longer able to log on to the mailbox.
5. On the **Completion** page, verify whether the command was completed successfully.
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task was not completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** close the wizard.

Use the Shell to manage full access permissions for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

This example grants Raymond Sam Full Access permissions to Terry Adams' mailbox.

```
Add-MailboxPermission -Identity "Terry Adams" -User RaySam -AccessRights Fullacce
```

This example removes Jim Hance's Full Access permissions to Ayla Kol's mailbox.

```
Remove-MailboxPermission -Identity Ayla -User 'JHance' -AccessRights FullAccess -
```

This example grants Mark Steele Full Access permissions to Jeroen Cool's mailbox and disables the auto-mapping feature.

```
Add-MailboxPermission -Identity JeroenC -User 'Mark Steele' -AccessRights FullAcc
```

For detailed syntax and parameter information, see Add-MailboxPermission.

1.8.2.4 Disable Outlook Auto-Mapping with Full Access Mailboxes

Disable Outlook Auto-Mapping with Full Access Mailboxes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-16*

In Exchange 2010 Service Pack 1 (SP1) Exchange introduced a feature that allows Outlook 2007 and Outlook 2010 clients to automatically map to any mailbox to which a user has Full Access permissions. If a user is granted Full Access permissions to another user's mailbox or to a shared mailbox, Outlook automatically loads all mailboxes to which the user has full access.

To accomplish this, Exchange populates the msExchDelegateListLink attribute in Active Directory to locate mailboxes for which the user has Full Access permission, and then provides this information to the Autodiscover service. Autodiscover then populates the `AlternateMailbox` attribute with the information necessary for Outlook to open the full access mailboxes. If the user has Full Access permissions to several mailboxes, performance issues may occur when starting Outlook. In Exchange 2010 SP1, there was no way to turn this feature off. However, in Exchange 2010 SP2, you can use the Shell to disable this feature.

Looking for other management tasks related to mailbox permissions? Check out Permissions to Manage Mailbox Servers

Use the Shell to disable auto-mapping

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

Note:
You can't' use the EMC to disable auto-mapping.

This example grants the user Mark Steele full access permission to Jeroen Cool's mailbox and disables the auto-mapping feature.

```
Add-MailboxPermission -Identity JeroenC -User 'Mark Steele' -AccessRight FullAcce
```

This example removes auto-mapping on an existing shared mailbox and removes the auto-mapping behavior for users who have already been granted Full Access permissions.

```
$FixAutoMapping = Get-MailboxPermission sharedmailbox |where {$_AccessRights -eq
$FixAutoMapping | Remove-MailboxPermission
$FixAutoMapping | ForEach {Add-MailboxPermission -Identity $_.Identity -User $_.U
```

For detailed syntax and parameter information, see the following topics:

- Remove-MailboxPermission
- Get-MailboxPermission
- Add-MailboxPermission

1.8.2.5 Managing Public Folder Permissions

Managing Public Folder Permissions

Exchange Server 2010 > Mailbox > Permissions to Manage Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-14*

1.8.2.5.1 Add Administrative Permissions for Users to Access Public Folders

Add Administrative Permissions for Users to Access Public Folders

Mailbox > Permissions to Manage Mailbox Servers > Managing Public Folder Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

There are two methods by which a user is granted the permissions to administer public folders:

- Public Folder Management role group
  Adding the user to the Public Folder Management role group is similar to assigning the Public Folder Administrator role in Exchange 2007. It grants the user all the permissions necessary for managing public folders.
- **PublicFolderAdminstrativePermission** cmdlet set
  Using these cmdlets is more granular and gives you the ability to specify the scope for the user in the organization by modifying the database's access control lists (ACLs).

Looking for other management tasks related to public folder permissions? Check out Managing Public Folder Permissions.

Use the Shell to add a user to the Public

Folder Management role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to add a user to the Public Folder Management role group.

This example adds the user Tony to the Public Folder Management role group.

```
Add-RoleGroupMember -Identity "Public Folder Management" -Member Tony
```

For detailed syntax and parameter information, see Add-RoleGroupMember.

Use the Shell to add administrative permissions for a user to access a specific public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder administrative permissions" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to add administrative permissions for a user to access a specific public folder.

Note:
Adding permissions to a specific folder also requires that the user has the correct Role Based Access Control (RBAC) permissions assigned so that they can access the public folder cmdlets.

This example adds AllExtendedRights permissions for the user Chris to access the public folder Marketing and all the public folders under it.

```
Add-PublicFolderAdministrativePermission -Identity "\Marketing" -User "Chris" -Ac
```

For detailed syntax and parameter information, see Add-PublicFolderAdministrativePermission.

1.8.2.5.2 Manage Send As Permissions for Mail-Enabled Public Folders

Manage Send As Permissions for Mail-Enabled Public Folders

Mailbox > Permissions to Manage Mailbox Servers > Managing Public Folder Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the Send As permission to configure a mail-enabled public folder so that users other than the public folder owner can use that mail-enabled public folder to send messages.

The Send As permission isn't granted until after replication has occurred. Replication times

depend on your Exchange and network configuration. To grant the permission immediately, stop and then restart the Microsoft Exchange Information Store service.

Also, before you perform this procedure, be aware that you cannot send e-mail messages on behalf of a mail-enabled public folder if the folder is hidden from address lists. When sending a message, Exchange requires that an e-mail address is resolved in the **From** field. In the case where a message is sent on behalf of a mail-enabled public folder that is hidden from address lists, , the SMTP address is interpreted as an address that is not from your organization (known as a *foreign address*) and is rejected. For more information about how to change public folder settings, see Configure Public Folder Properties.

In Outlook, users will receive the following errors when attempting to send a message on behalf of a mailbox that is hidden from address lists:

- **Online mode** When users press **Send**, they will receive the following error: "You do not have permission to send on behalf of the specified user."
- **Cached Exchange Mode** Outlook initially sends the message, but users will receive a non-delivery report (NDR) containing the following message: "You are not allowed to send this message because you are trying to send on behalf of another user without permission to do so. Please verify that you are sending on behalf of the correct sender, or ask your system administrator to help you get the required permission."

Looking for other tasks related to public folders? Check out Managing Public Folders.

What Do You Want to Do?

- Use the Public Folder Management Console to manage Send As permissions for a mailbox
- Use the Shell to manage Send As permissions for a mailbox

Use the Public Folder Management Console to manage Send As permissions for a mail-enabled public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send As permissions" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the Public Folder Management Console tree, expand **Default Public Folders**, and then click the parent public folder of the public folder you want to configure.
4. In the result pane, select the public folder, and then, in the action pane, click **Manage Send As Permission**.
5. On the **Manage Send As Permission** page, select the users or groups to which you want to grant the Send As permission or from which you want to remove the permission.
   - **Add** Click this button to open the **Select User or Group** dialog box. Use this dialog box to select the users or groups to which you want to grant the Send As permission, click **OK** and then click **Manage**.
   -  Select a user or group, and then click this button to remove the Send As permission from that user or group. After you've removed the user or group, click **Manage**.
6. On the **Completion** page, review the following, and then click **Finish** to close

the wizard:

- A status of **Completed** indicates that the wizard completed the task successfully.
- A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

7. Click **Finish** close the wizard.

Use the Shell to manage Send As permissions for a mail-enabled public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Send As permissions" entry in the Mailbox Permissions topic.

Use the **Add-ADPermission** cmdlet to manage Send As permissions for a mail-enabled public folder. When you use the **Add-ADPermission** cmdlet, you must specify the name of the public folder on which the Send As permission should be added and the public folder that should be granted the permission. Because the **Add-ADPermission** cmdlet controls many permissions, you must also specify the Send As permission with the *ExtendedRights* parameter. For example, to add the Send As permission to contoso\kim on the public folder Sales, use the following command:

```
Add-ADPermission Sales -User contoso\kim -Extendedrights "Send As"
```


1.8.2.5.3 Remove Public Folder Administrative Permissions

Remove Public Folder Administrative Permissions

Mailbox > Permissions to Manage Mailbox Servers > Managing Public Folder Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic shows you how to use the Exchange Management Shell to remove public folder administrative permissions from a user.

Note:

You can't use the **Remove-PublicFolderAdministrativePermission** cmdlet to remove the rights of a member of the Public Folder Management role group. You must use the **Remove-RoleGroupMember** cmdlet.

There are two methods by which a user is granted the permissions to administer public folders:

- Public Folder Management role group
  Adding the user to the Public Folder Management role group is similar to assigning the Public Folder Administrator role in Exchange 2007. It grants the user all the permissions necessary for managing public folders.
- **PublicFolderAdminstrativePermission** cmdlet set
  Using these cmdlets is more granular and gives you the ability to specify the scope for the user in the organization by modifying the database's access control lists (ACLs).

Looking for other management tasks related to public folder permissions? Check out

Managing Public Folder Permissions.

Use the Shell to remove a user from the Public Folder Management role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to remove a user from the Public Folder Management role group.

This example removes the user Chris from the Public Folder Management role group.

```
Remove-RoleGroupMember -Identity "Public Folder Management" -Member Chris
```

For detailed syntax and parameter information, see Remove-RoleGroupMember.

Use the Shell to remove administrative permissions for a user to access a specific public folder or public folder hierarchy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder administrative permissions" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to remove administrative permissions for a user to access a specific public folder or public folder hierarchy.

This example removes all administrative permissions to the entire public folder tree from the user Kim.

```
Remove-PublicFolderAdministrativePermission -Identity "\" -User "Kim" -AccessRigh
```

A warning appears asking if you're sure you want to perform this action. Type **Y** to confirm.

For detailed syntax and parameter information, see Remove-PublicFolderAdministrativePermission.

1.8.2.5.4 View Public Folder Administrative Permission Settings

View Public Folder Administrative Permission Settings

Mailbox > Permissions to Manage Mailbox Servers > Managing Public Folder Permissions >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

There are two methods by which a user is granted the permissions to administer public folders:

- Public Folder Management role group
  Adding the user to the Public Folder Management role group is similar to assigning the Public Folder Administrator role in Exchange 2007. It grants the user all the permissions necessary for managing public folders.
- **PublicFolderAdminstrativePermission** cmdlet set
  Using these cmdlets is more granular and gives you the ability to specify the scope for the user in the organization by modifying the database's access control lists (ACLs).

Looking for other management tasks related to public folder permissions? Check out Managing Public Folder Permissions.

Use the Shell to view members of the Public Folder Management role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to view members of the Public Folder Management role group.

This example returns the members of the Public Folder Management role group.

```
Get-RoleGroupMember -Identity "Public Folder Management"
```

Note:
By default, a maximum of 1,000 role group members are displayed. If you want to display more, you must use the *ResultSize* parameter to override the maximum number of members that are returned. You can type either an integer value or the value `unlimited`. The value `unlimited` returns all members of the role group.

For detailed syntax and parameter information, see Get-RoleGroupMember.

Use the Shell to view information about administrative permissions for a public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder administrative permissions" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to view information about administrative permissions for a public folder.

This example returns the user David's access rights for the public folder Marketing.

```
Get-PublicFolderAdministrativePermission -Identity "\Marketing" -User "David"
```

This example returns the administrative access rights sorted by user for the public folder Sales.

```
Get-PublicFolderAdministrativePermission -Identity "\Sales" | Format-List User,Ac
```

For detailed syntax and parameter information, see Get-

PublicFolderAdministrativePermission.

1.8.2.5.5 Use the Public Folder Management Console to Manage Public Folder Settings

Use the Public Folder Management Console to Manage Public Folder Settings

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the Manage Public Folder Settings wizard to manage public folder settings for the selected public folder and subfolders. The wizard also allows you to add, remove, and modify client permissions.

Looking for other management tasks related to public folder permissions? Check out Managing Public Folder Permissions.

What Do You Want to Do?

- Add or modify public folder permissions for a client user
- Remove public folder permissions for a client user
- Overwrite child public folder settings with the parent public folder settings

Add or modify public folder permissions for a client user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the public folder tree of the Public Folder Management Console, expand **Default Public Folders**, and then click the parent public folder of the public folder you want to configure.
4. In the result pane, click the public folder you want to configure.
5. In the action pane, click **Manage Settings**.
6. On the **Introduction** page, view or modify the following settings:
   - **Current root folder** This read-only field displays the path and the public folder you're modifying.
   - **Update client permissions** Click this button to update the client access permissions for this public folder.
   - **Apply client permission changes to this folder and all its subfolders** Select this check box if you want the changes that you make to the selected public folder to apply to all of the child public folders. This option is available only if the public folder you're modifying has one or more child public folders.
   - **Overwrite settings** Click this button if you want to override the settings of the child public folders with the selected parent public folder's settings. You can overwrite the age limits, keep per-user read/unread state, replicas, and replication schedule. This option is available only if the public folder you're modifying has one or more child public folders. If you select

this option, see Overwrite child public folder settings with the parent public folder settings later in this topic for details.

7. On the **Specify Action** page, you can specify whether you want to add or remove client user permissions:
   - **Add users** Click this button to add users and set their permissions. If users already have permission to this folder or a child folder, that permission will be replaced with new permissions.
   - **Remove Users** Click this button to remove users from folders to which they have permissions. If you select this option, see Remove public folder permissions for a client user later in this topic for details.

8. On the **Assign Permissions** page, you can grant users access to public folders. Complete the following fields:
   - **Add** Click this button to add a user to whom you want to assign permissions.
   - **Permission Level** Use this list and the associated check boxes to assign permissions to the selected user. For more information about the permissions and the level of access that each one grants, see the "Client User Access Rights and Roles" section of Understanding Public Folder Permissions.

     Note:
     The **Custom** permission level isn't listed in the **Permission Level** list. You can create a custom role by selecting or clearing the access right check boxes.

9. On the **Add Users** page, review your configuration settings. Click **Add** to add the user. Click **Back** to make configuration changes. Exchange will remove any existing permissions and then create the permissions for the user.

10. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
11. Click **Finish** to close the wizard.

Remove public folder permissions for a client user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the public folder tree of the Public Folder Management Console, expand **Default Public Folders**, and then click the parent public folder of the public folder you want to configure.
4. In the result pane, click the public folder you want to configure.
5. In the action pane, click **Manage Settings**.
6. On the **Introduction** page, complete the following fields:
   - **Update client permissions** Click this button to update the client access permissions for this public folder.
   - **Apply client permission changes to this folder and all its subfolders** Select this check box if you want the changes that you make to the

selected public folder to apply to all of the child public folders. This option is available only if the public folder you're modifying has one or more child public folders.

7. On the **Specify Action** page, click **Remove users** to remove users from folders to which they have permissions, and then click **Next**.

8. On the **Select Users** page, you can select users from whom you want to remove their permissions. Click **Add** to select the user you want to remove, and then click **Next**.
9. On the **Remove Users** page, review your configuration settings. Click **Remove** to remove the user's permissions. Click **Back** to make configuration changes. Exchange will remove any existing permissions from the user.
10. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
11. Click **Finish** to close the wizard.

Overwrite child public folder settings with the parent public folder settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the public folder tree of the Public Folder Management Console, expand **Default Public Folders**, and then click the parent public folder of the public folder you want to configure.
4. In the result pane, click the public folder you want to configure.
5. In the action pane, click **Manage Settings**.
6. On the **Introduction** page, click **Overwrite Settings** to override the child public folder settings with the selected parent public folder settings. You can overwrite the age limits, keep per-user read/unread state, replicas, and replication schedule. This option is available only if the public folder that you're modifying has one or more child public folders.

7. On the **Select Settings** page, select the settings to overwrite. For more information about the settings you can configure, see Configure Public Folder Properties.
    - **Age limits** Select this check box to copy the selected public folder's age limits to the child public folders.
    - **Keep per user read/unread state** Select this check box to copy the selected public folder's per-user read/unread settings to the child public folders. This setting allows users to see if a public folder message has been read or unread in Microsoft Outlook.
    - **Replicas** Select this check box to copy the selected public folder's replica settings to the child public folders.
    - **Replication schedule** Select this check box to copy the selected public folder's replication schedule to the child public folders.
8. On the **Overwrite Settings** page, review your configuration settings. Click **Overwrite** to overwrite the child public folder settings with the selected public folder. Click **Back** to make configuration changes.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:

- A status of **Completed** indicates that the wizard completed the task successfully.
- A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

10. Click **Finish** to close the wizard.

1.8.2.5.6 Add Permissions for Client Users to Access Public Folder Content

Add Permissions for Client Users to Access Public Folder Content

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When adding client permissions, you can either use predefined permission roles (which consist of specific access rights) or you can customize permissions by manually applying the available access rights. To specify the permissions for the client user, you can use the Public Folder Management Console, the **Add-PublicFolderClientPermission** cmdlet, or the **AddUsersToPFRecursive.ps1** user management script.

Note:

If a client user already has a specific access right to a public folder, you can't add the same access right again. Therefore, if you use the **AddUsersToPFRecursive.ps1** script, and the user already has one of the access rights that you're trying to grant, a warning will appear stating that the current access rights will be removed before new access rights are granted.

Looking for other management tasks related to public folder permissions? Check out Managing Public Folder Permissions.

Use the Public Folder Management Console to add public folder permissions for a client user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the public folder tree of the Public Folder Management Console, expand **Default Public Folders**, and then click the parent public folder of the public folder you want to configure.
4. In the result pane, click the public folder you want to configure.
5. In the action pane, click **Manage Settings**.
6. On the **Introduction** page, complete the following fields:
   - **Update client permissions** Click this button to update the client access permissions for this public folder.
   - **Apply client permission changes to this folder and all its subfolders** Select this check box if you want the changes that you make to the selected public folder to apply to all of the child public folders. This option is

available only if the public folder you're modifying has one or more child public folders.

7. On the **Specify Action** page, click **Remove users** to remove users from folders to which they have permissions, and then click **Next**.
8. On the **Select Users** page, you can select users from whom you want to remove their permissions. Click **Add** to select the user you want to remove, and then click **Next**.
9. On the **Remove Users** page, review your configuration settings. Click **Remove** to remove the user's permissions. Click **Back** to make configuration changes. Exchange will remove any existing permissions from the user.
10. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
11. Click **Finish** to close the wizard.

Use the Shell to add public folder permissions for a client user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to add public folder permissions for a client user.

This example adds Publishing Editor permissions for the user Kim to access the public folder West Coast.

```
Add-PublicFolderClientPermission -Identity "\Marketing\West Coast" -AccessRights
```

For detailed syntax and parameter information, see Add-PublicFolderClientPermission.

Use the AddUsersToPFRecursive.ps1 script to add client access rights to a public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

This example adds Reviewer permissions for the user David to access the top-level public folder Sales and all of the public folders under it.

```
AddUsersToPFRecursive.ps1 -TopPublicFolder "\Sales" -User "David" -Permission Rev
```

For more information about how to use public folder management scripts, see Scripts for Managing Public Folders in the Exchange Management Shell.

Remove or Replace Public Folder Client Permissions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When removing public folder permissions, you can either use predefined permission roles (which consist of specific access rights) or manually remove the available access rights. To remove the permissions from the client user, you can use the Public Folder Management Console, the **Remove-PublicFolderClientPermission** cmdlet, or the **RemoveUserFromPFRecursive.ps1** user management script.

To replace the users or permissions, use the following scripts:

- **ReplaceUserWithUserOnPFRecursive.ps1** This script replaces a user with a new user in the client permissions list for a public folder and any folders that exist within it. Existing permissions for the first user are retained. Public folders that don't contain permissions for the user aren't modified.
- **ReplaceUserPermissionOnPFRecursive.ps1** This script replaces a user's permissions to a public folder and any folders that exist under it with a new set of permissions. Public folders that don't contain permissions for the user aren't modified.

Looking for other management tasks related to public folders? Check out Managing Public Folders or Managing Public Folder Permissions.

Use the Public Folder Management Console to remove a client user's permissions to public folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the public folder tree of the Public Folder Management Console, expand **Default Public Folders**, and then click the parent public folder of the public folder you want to configure.
4. In the result pane, click the public folder you want to configure.
5. In the action pane, click **Manage Settings**.
6. On the **Introduction** page, complete the following fields:
   - **Update client permissions** Click this button to update the client access permissions for this public folder.
   - **Apply client permission changes to this folder and all its subfolders** Select this check box if you want the changes that you make to the selected public folder to apply to all of the child public folders. This option is available only if the public folder you're modifying has one or more child public folders.
7. On the **Specify Action** page, click **Remove users** to remove users from folders to which they have permissions, and then click **Next**.
8. On the **Select Users** page, you can select users from whom you want to remove their permissions. Click **Add** to select the user you want to remove, and then click **Next**.
9. On the **Remove Users** page, review your configuration settings. Click

Remove to remove the user's permissions. Click **Back** to make configuration changes. Exchange will remove any existing permissions from the user.

10. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
11. Click **Finish** to close the wizard.

Use the Shell to remove a client user's permissions to public folder items

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to remove a client user's permissions to public folder items.

This example removes the user David's permissions to create items in the public folder Oregon.

```
Remove-PublicFolderClientPermission -Identity "Sales\West Coast\Oregon" -User Dav
```

For detailed syntax and parameter information, see Remove-PublicFolderClientPermission.

Use the RemoveUserFromPFRecursive.ps1 script to remove a client user's permissions to access public folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

This example removes the user David's permissions to access the public folder Oregon and all folders under it.

```
RemoveUserFromPFRecursive.ps1 -Server "SERVER01" -TopPublicFolder -"\Sales\Oregon
```

For more information about using the RemoveUserFromPFRecursive.ps1 script, see Scripts for Managing Public Folders in the Exchange Management Shell.

Use the ReplaceUserWithUserOnPFRecursive.ps1 script to replace a user with a new user in the client permissions list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

Using the script to replace public folder permissions saves you time because you only have to run the script once. If you were to use cmdlets to perform this task, you would have to perform multiple steps to accomplish the same task.

This example replaces the user David with the user Kim as a person who can access the items in the public folder Sales and all folders under it.

```
ReplaceUserWithUserOnPFRecursive.ps1 -TopPublicFolder "\Sales" -UserOld "David" -
```

For more information about using the ReplaceUserWithUserOnPFRecursive.ps1 script, see Scripts for Managing Public Folders in the Exchange Management Shell.

Use the ReplaceUserPermissionOnPFRecursive.ps1 script to replace client permissions with a new set of permissions

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

Using the script to replace public folder permissions saves you time because you only have to run the script once. If you were to use cmdlets to perform this task, you would have to perform multiple steps to accomplish the same task.

This example replaces the user Kim's current permission to access the public folder Marketing and all folders under it with the Publishing Editor permissions.

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "SERVER01" -TopPublicFolder "\Mark
```

For more information about using the ReplaceUserPermissionOnPFRecursive.ps1 script, see Scripts for Managing Public Folders in the Exchange Management Shell.

1.8.2.5.8 View Public Folder Client Permissions Settings

View Public Folder Client Permissions Settings

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic shows you how to use the Exchange Management Shell to view information about the client access permissions to a public folder.

Note:

You can't use the Exchange Management Console (EMC) to perform this procedure.

Use the Shell to view client access permissions

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

This example returns the entire list of the client access permissions for the public folder Marketing.

```
Get-PublicFolderClientPermission -Identity "\Marketing" | fl
```

This example returns the user David's client access permissions to the public folder East Coast.

```
Get-PublicFolderClientPermission -Identity "\Marketing\EastCoast" -User David
```

For detailed syntax and parameter information, see Get-PublicFolderClientPermission.

1.8.3 Managing Mailbox Servers

Managing Mailbox Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-11*

Change the Recipient Scope

Configure Mailbox Server Properties

Creating Filters in Recipient Commands

Configure Message Delivery Restrictions

Managing Address Lists

Managing Automatic Replies

Managing Calendars

Managing Details Templates

Managing Distribution Groups

Managing E-Mail Address Policies

Managing Exchange Search

Managing Hierarchical Address Books

Managing Mail Contacts and Mail Users

Managing Mailbox Databases

Managing Mailbox Import and Export Requests

Managing Repair Requests

Managing Meeting Items

Managing Move Requests

Managing Offline Address Books

Managing Public Folders

Managing Recoverable Items

Managing Resource Mailboxes and Scheduling

Managing User Mailboxes

Modify the Maximum Number of Recipients to Display in the Result Pane

View Logon Statistics

1.8.3.1 Change the Recipient Scope

Change the Recipient Scope

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Recipient scope is the specified portion of Active Directory hierarchy that the Exchange Management Console (EMC) and the Exchange Management Shell uses for recipient management. When you set the recipient scope to a specific location within Active Directory, you can view and manage all recipients stored in that location, including all the containers under it.

The EMC and Shell always start with the recipient scope at the domain-level of the computer that is running the management interface. Neither the user account that's being used nor the Exchange servers being managed has bearing on the default value of the recipient scope.

When you change the recipient scope of the EMC, you change the set of recipients that are displayed in the result pane of the **Recipient Configuration** node. The dialog boxes that you use to select recipients or OUs (located on various wizard pages) also work within the same scope. For example, if you're mail-enabling an existing contact, the **Select Contact** dialog box in the **New Mail Contact** wizard displays only the contacts within the recipient scope that are not already mail-enabled.

Note:

The Microsoft Management Console (MMC) saves any changes you make to a snap-in as preferences in your user profile on the administrator computer. The recipient scope setting is also saved as one of your preferences. As a result, the next time you start the EMC on the same computer, the default setting of the recipient scope is now the scope that you last specified. However, if you use another computer or a different user account to run the EMC, you'll need to adjust the recipient scope again.

When you change the recipient scope in the Shell, you change the set of recipients that are returned for the **Get-** cmdlets of the recipient. The recipient scope is accessible by using the **Set-ADServerSettings** cmdlet.

Note:

The default scope is not retained when you close the Shell. The Shell resets to the default domain-level recipient scope the next time that the Shell is opened.

What Do You Want to Do?

Use the EMC to change the recipient scope

Use the Shell to change the recipient scope

Use the EMC to change the recipient scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Active Directory Domain Services server settings" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **Modify Recipient Scope**.
3. In **Recipient Scope** dialog box, select one of the following options:
   - **View all recipients in forest** Click this button to work with all recipients in the forest. To use a specific global catalog server, select the **Global Catalog** check box and then click **Browse**. In **Select Global Catalog**, select the global catalog server that you want to use. If you don't specify a global catalog server, Exchange automatically selects an available one.
   - **View all recipients in specified organizational unit** Click this button to work with all recipients in a specific organizational unit (OU) and all OUs under it. Click **Browse,** and then, in **Select Organizational Unit**, select the OU that you want to use.

     To use a specific domain controller, select the **Recipient Domain Controller** check box. If you don't specify a recipient domain controller, Exchange automatically selects an available one.
4. Click **OK**.

Use the Shell to change the recipient scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Active Directory Domain Services server settings" entry in the Exchange and Shell Infrastructure Permissions topic.

This example sets the recipient scope to the Marketing Users OU in the contoso.com domain for the current session.

```
Set-AdServerSettings -RecipientViewRoot "contoso.com/Marketing Users"
```

This example sets the scope of the current session to the entire forest and designates gc1.contoso.com as the preferred global catalog server.

```
Set-AdServerSettings -ViewEntireForest $true -PreferredGlobalCatalog gc1.contoso.
```

For detailed syntax and parameter reference, see Get-AdServerSettings.

1.8.3.2 Configure Mailbox Server Properties

Configure Mailbox Server Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

To configure the Mailbox servers in your organization, you can either use the **Mailbox** node in the Exchange Management Console (EMC) or the **Set-MailboxServer** cmdlet in the Exchange Management Shell.

What Do You Want to Do?

- Use the EMC to configure Mailbox server properties
- Use the Shell to configure Mailbox server properties

Use the EMC to configure Mailbox server properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox server configuration" entry in the Mailbox Permissions topic.

1. In the console tree, select the forest you want, and then navigate to **Server Configuration** > **Mailbox**.
2. In the result pane, select the server you want to configure.
3. In the action pane, under the server name, click **Properties**.
4. On the **General** tab, you can view general information about the server:
   - **Version** This field displays the version of Exchange installed on the server.
   - **Edition** This field displays the Exchange Server edition. The edition is either Standard Edition or Enterprise Edition.
   - **Role(s)** This field displays the Exchange server roles installed on the server.
   - **Product ID** This field displays the product ID for the Exchange server. If you haven't yet entered the product key for the server, the product ID displayed is **Unlicensed**. To license an unlicensed version of Exchange, see Enter Product Key.
   - **Modified** This field displays the last date and time that a configuration change was made on this server.
5. On the **System Settings** tab, view the domain controller servers and global catalog servers. You can also enable an error reporting feature:
   - **Domain controller servers being used by Exchange** This read-only box displays a list of domain controller servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.
   - **Global catalog servers being used by Exchange** This read-only box displays a list of global catalog servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.
   - **Automatically send fatal service error report to Microsoft** Select this check box if you want to enable the error reporting feature and automatically send an error report to Microsoft in the event of a fatal error.

If you enable the error reporting feature, information about fatal service errors is sent to Microsoft over encrypted channels. The information is used to improve Microsoft products. When this feature is enabled and the issue reported has a known solution, the server receives feedback from Microsoft. This feedback contains a link to information that may help resolve the problem.

6. On the **Customer Feedback Options** tab, you can enroll the selected server into the Customer Experience Improvement Program. For more information, see Opt-in or Opt-out of the Customer Experience Improvement Program.

7. On the **Messaging Records Management** tab, configure the schedule for the Managed Folder Assistant. The Managed Folder Assistant is an Exchange Mailbox Assistant that places the managed folders that you have created into users' mailboxes and applies managed content settings to managed folders. When the Managed Folder Assistant is running, it processes all the mailboxes on a server. If the Managed Folder Assistant doesn't finish processing the mailboxes on the server in the time that you specified, it automatically resumes processing where it left off the next time it runs. There is one Managed Folder Assistant for each server. To learn more, see Configure the Managed Folder Assistant.
   - **Schedule the Managed Folder Assistant** Use this box to schedule the Managed Folder Assistant or to prevent it from running. The following options are available:
     Use Custom Schedule Select this option to configure the Managed Folder Assistant to run at specified times. If you select **UseCustom Schedule**, you must also click **Customize** to set a schedule. There is no default schedule.
     Never Run Select this option to prevent the Managed Folder Assistant from running.
   - **Customize** Click this button to open the **Schedule** dialog box and set a schedule for the Managed Folder Assistant. To set the schedule, click the time grid in the dialog box. The Managed Folder Assistant runs during the time slots that you select, which are marked in blue. You can select the same time slot every day by clicking a column header for a specific time slot. You can select an entire day by clicking the name of that day.
     The default time slot for the grid is one hour. For finer control, you can change the schedule grid to 15 minute intervals by clicking **15 Minutes**. Scheduled intervals must be at least 15 minutes apart.

Use the Shell to configure Mailbox server properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox server configuration" entry in the Mailbox Permissions topic.

This example sets the server override list to HubServer01, HubServer02, and HubServer03

```
Set-MailboxServer -Identity Server1 -SubmissionServerOverrideList HubServer01,Hub
```

This example sets the maximum size of the messaging records management (MRM) log directory to 1 GB.

```
Set-MailboxServer -Identity Exchange01 -LogDirectorySizeLimitForManagedFolders "1
```

This example sets the maximum size of the MRM log files to 20 MB.

```
Set-MailboxServer -Identity Exchange01 -LogFileSizeLimitForManagedFolders "20 MB"
```

For detailed syntax and parameter information, see Set-MailboxServer.

For More Information

Overview of the Mailbox Server Role

Managing Mailbox Servers

1.8.3.3 Creating Filters in Recipient Commands

Creating Filters in Recipient Commands

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-28*

You can use several Exchange Management Shell commands to filter a set of recipients. You can create the following types of filters in an Exchange command:

- Precanned filters
- Custom filters using the *RecipientFilter* parameter
- Custom filters using the *Filter* parameter
- Custom filters using the *ContentFilter* parameter

In Microsoft Exchange Server 2003 and earlier versions, LDAP filtering syntax is used to create custom address lists, global address lists (GALs), e-mail address policies, and distribution groups. In Exchange Server 2007 and Exchange Server 2010, the OPATH filtering syntax replaces the LDAP filtering syntax. Exchange supports existing LDAP filters, but you can't edit them. Before you can change an LDAP filter, you must upgrade it to an OPATH filter. For more information, see Upgrade Custom LDAP Filters to OPATH Filters.

Contents

Precanned Filters

A *precanned filter* is a commonly used Exchange filter that you can use to meet a variety of recipient-filtering criteria for creating dynamic distribution groups, e-mail address policies, address lists, or GALs. With precanned filters, you can either use Exchange Management Shell or a wizard in the Exchange Management Console (EMC). Using precanned filters,

you can do the following:

- Determine the scope of recipients.
- Add conditional filtering based on properties such as company, department, and state or region.
- Add custom attributes for recipients. For more information, see Understanding Custom Attributes.

The following parameters are considered precanned filters:

- *IncludedRecipients*
- *ConditionalCompany*
- *ConditionalDepartment*
- *ConditionalStateOrProvince*
- *ConditionalCustomAttribute1*–15.

Precanned filters are available for the following cmdlets:

- New-DynamicDistributionGroup
- Set-DynamicDistributionGroup
- New-EmailAddressPolicy
- Set-EmailAddressPolicy
- New-AddressList
- Set-AddressList
- New-GlobalAddressList
- Set-GlobalAddressList

Example

This example describes using precanned filters in the Shell to create a dynamic distribution group. The syntax in this example is similar but not identical to the syntax you would use to create an e-mail address policy, address list, or GAL. When creating a precanned filter, you should ask the following questions:

- From which organizational unit (OU) do you want to include recipients? (This question corresponds to the *RecipientContainer* parameter.)

  Note:

  Selecting the OU for this purpose applies only when creating dynamic distribution groups, and not when creating e-mail address policies, address lists, or GALs.

- What type of recipients do you want to include? (This question corresponds to the *IncludedRecipients* parameter.)
- What additional conditions do you want to include in the filter? (This question corresponds to the *ConditionalCompany*, *ConditionalDepartment*, *ConditionalStateOrProvince*, and *ConditionalCustomAttribute* parameters.)

This example creates the dynamic distribution group Contoso Finance for user mailboxes in the OU Contoso.com/Users and specifies the condition to include only recipients who have the **Department** attribute defined as Finance and the **Company** attribute defined as Contoso.

```
New-DynamicDistributionGroup -Name "Contoso Finance" -OrganizationalUnit Contoso.
```

This example displays the properties of this new dynamic distribution group.

```
Get-DynamicDistributionGroup -Identity "Contoso Finance" | Format-List *Recipient
```

Return to top

Custom Filters Using the RecipientFilter

Parameter

If precanned filters don't meet your needs for creating or modifying dynamic distribution groups, e-mail address policies, and address lists, you can create a custom filter by using the *RecipientFilter* parameter.

The recipient filter parameter is available for the following cmdlets:

- New-DynamicDistributionGroup
- Set-DynamicDistributionGroup
- New-EmailAddressPolicy
- Set-EmailAddressPolicy
- New-AddressList
- Set-AddressList
- New-GlobalAddressList
- Set-GlobalAddressList

For more information about the filterable properties you can use with the *RecipientFilter* parameter, see Filterable Properties for the -RecipientFilter Parameter.

Example

The following example uses the *RecipientFilter* parameter to create a dynamic distribution group. The syntax in this example is similar but not identical to the syntax you use to create an e-mail address policy, address list, or GAL.

This example uses custom filters to create a dynamic distribution group for user mailboxes that have the **Company** attribute defined as Contoso and the **Office** attribute defined as North Building.

```
New-DynamicDistributionGroup -Name AllContosoNorth -OrganizationalUnit contoso.co
```

Return to top

Custom Filters Using the Filter Parameter

You can use the *Filter* parameter to filter the results of a command to specify which objects to retrieve. For example, instead of retrieving all users or groups, you can specify a set of users or groups by using a filter string. This type of filter doesn't modify any configuration or attributes of objects. It only modifies the set of objects that the command returns.

Using the *Filter* parameter to modify command results is known as *server-side filtering*. Server-side filtering submits the command and the filter to the server for processing. The Shell also supports client-side filtering, in which the command retrieves all objects from the server and then applies the filter in the local console window. To perform client-side filtering, use the **Where-Object** cmdlet. For more information about server-side and client-side filtering, see "How to Filter Data" in Working with Command Output.

To find the filterable properties for cmdlets that have the *Filter* parameter, you can run the **Get** command against an object and format the output by pipelining the **Format-List** parameter. Most of the returned values will be available for use in the *Filter* parameter. The following example returns a detailed list for the mailbox Ayla.

```
Get-Mailbox -Identity Ayla | Format-List
```

The *Filter* parameter is available for the following cmdlets:

- Get-ActiveSyncDevice
- Get-ActiveSyncDeviceClass
- Get-CASMailbox

- Get-Contact
- Get-DistributionGroup
- Get-DynamicDistributionGroup
- Get-Group
- Get-Mailbox
- Get-MailContact
- Get-MailPublicFolder
- Get-MailUser
- Get-Message
- Get-Queue
- Get-Recipient
- Get-RemoteMailbox
- Get-RoleGroup
- Get-SecurityPrincipal
- Get-StoreUsageStatistics
- Get-ThrottlingPolicyAssociation
- Get-UMMailbox
- Get-User
- Remove-Message
- Resume-Message
- Resume-Queue
- Retry-Queue
- Suspend-Message
- Suspend-Queue

For more information about the filterable properties you can use with the *Filter* parameter, see Filterable Properties for the -Filter Parameter.

Example

This example uses the *Filter* parameter to return information about users whose title contains the word "manager".

```
Get-User -Filter {Title -like '*Manager*'}
```

Return to top

Custom Filters Using the ContentFilter Parameter

You can use the *ContentFilter* parameter to select specific message content to export when using the New-MailboxExportRequest cmdlet. If the command finds a message that contains the match to the content filter, it exports the message to a .pst file.

Example

This example creates an export request that searches Ayla's mailbox for messages where the body contains the phrase "company prospectus". If that phrase is found, the command exports all messages with that phrase to a .pst file.

```
New-MailboxExportRequest -Mailbox Ayla -ContentFilter {Body -like "*company prosp
```

For more information about the filterable properties you can use with the *ContentFilter* parameter, see Filterable Properties for the -ContentFilter Parameter.

Return to top

Additional OPATH Syntax Information

When creating your own custom filters, be aware of the following:

- Use braces { } around the entire OPATH syntax string with the *Filter* or *RecipientFilter* parameter.
- Include the hyphen before all operators. The most common operators include:
  - **-and**
  - **-or**
  - **-not**
  - **-eq** (equals)
  - **-ne** (not equal)
  - **-lt** (less than)
  - **-gt** (greater than)
  - **-like** (string comparison)
  - **-notlike** (string comparison)
- Many of the properties for the *RecipientFilter* and *Filter* parameters accept wildcard characters. If you use a wildcard character, use the **like** operator instead of the **eq** operator. The **like** operator is used to find pattern matches in rich types, such as strings, whereas the **eq** operator is used to find an exact match.
- Run the following commands to get information about operators you can use:
  - `Help about_logical_operator`
  - `Help about_comparison_operator`
- You can use most properties of recipient types to create filter strings. For information about filterable properties you can use with a specific cmdlet, see the cmdlet reference topics in Exchange Management Shell.

Return to top

1.8.3.3.1 Filterable Properties for the -Filter Parameter

Filterable Properties for the -Filter Parameter

Mailbox > Managing Mailbox Servers > Creating Filters in Recipient Commands >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-07*

This topic lists the filterable properties for the *-Filter* parameter in Microsoft Exchange Server 2010.

Use the *-Filter* parameter to return the objects from a **Get-** command in a filtered list. For example, if you want the **Get-Contact** cmdlet to return a subset of all of the contacts in your Microsoft Exchange organization, you would use the *-Filter* parameter. The subset of objects that is returned is based on specific properties.

The *-Filter* parameter is used in the following cmdlets:

- Get-AcceptedDomain
- Get-ActiveSyncDevice
- Get-ActiveSyncDeviceAccessRule
- Get-ActiveSyncDeviceClass
- Get-ActiveSyncMailboxPolicy
- Get-ActiveSyncOrganizationSettings
- Get-ActiveSyncVirtualDirectory

- Get-AdminAuditLogConfig
- Get-AddressList
- Get-AddressRewriteEntry
- Get-AdSite
- Get-AdSiteLink
- Get-AttachmentFilterEntry
- Get-AttachmentFilterListConfig
- Get-AutodiscoverVirtualDirectory
- Get-AvailabilityAddressSpace
- Get-AvailabilityConfig
- Get-CalendarDiagnosticLog
- Get-CASMailbox
- Get-CASMailboxPlan
- Get-ClientAccessArray
- Get-ClientAccessServer
- Get-CmdletExtensionAgent
- Get-Contact
- Get-ContentFilterConfig
- Get-DatabaseAvailabilityGroup
- Get-DeliveryAgentConnector
- Get-DetailsTemplate
- Get-DistributionGroup
- Get-DistributionGroupMember
- Get-DomainController
- Get-DynamicDistributionGroup
- Get-EcpVirtualDirectory
- Get-EdgeSubscription
- Get-EdgeSyncServiceConfig
- Get-ExchangeAssistanceConfig
- Get-EmailAddressPolicy
- Get-ExchangeServer
- Get-FederatedOrganizationIdentifier
- Get-FederationTrust
- Get-ForeignConnector
- Get-GlobalAddressList
- Get-Group
- Get-IMAPSettings
- Get-IPAllowListConfig
- Get-IPAllowListProvider
- Get-IPAllowListProvidersConfig
- Get-IPBlockListConfig
- Get-IPBlockListProvider
- Get-IPBlockListProvidersConfig
- Get-IRMConfiguration
- **Get-LinkedUser**
- Get-ManagedContentSettings
- Get-ManagedFolder
- Get-ManagedFolderMailboxPolicy
- Get-ManagementRole
- Get-ManagementRoleAssignment
- Get-ManagementRoleEntry
- Get-ManagementScope
- Get-Mailbox
- Get-MailboxAuditBypassAssociation
- Get-MailboxDatabase
- Get-MailboxServer

- Get-MailContact
- Get-MailPublicFolder
- Get-MailUser
- Get-MessageClassification
- Get-MoveRequest
- Get-OABVirtualDirectory
- Get-OfflineAddressBook
- Get-OrganizationConfig
- Get-OrganizationRelationship
- Get-OrganizationalUnit
- Get-OutlookAnywhere
- Get-OutlookProvider
- Get-OwaMailboxPolicy
- Get-OwaVirtualDirectory
- **Get-PerimeterConfig**
- Get-POPSettings
- Get-PowerShellVirtualDirectory
- Get-PublicFolderDatabase
- Get-ReceiveConnector
- Get-RecipientFilterConfig
- Get-RemoteDomain
- Get-RemoteMailbox
- Get-RetentionPolicy
- Get-RetentionPolicyTag
- Get-RoleGroup
- Get-RoleGroupMember
- Get-RoutingGroupConnector
- Get-RpcClientAccess
- Get-Recipient
- Get-RecipientEnforcementProvisioningPolicy
- Get-ResourceConfig
- Get-RetentionPolicy
- Get-RoleAssignmentPolicy
- **Get-RMSTrustedPublishingDomain**
- Get-SecurityPrincipal
- Get-SendConnector
- Get-SenderFilterConfig
- Get-SenderIdConfig
- Get-SenderReputationConfig
- Get-SharingPolicy
- Get-SystemMessage
- Get-ThrottlingPolicy
- Get-ThrottlingPolicyAssociation
- Get-TransportConfig
- Get-TransportServer
- Get-Trust
- Get-UMAutoAttendant
- Get-UMDialplan
- Get-UMHuntGroup
- Get-UMIPGateway
- Get-UMMailbox
- Get-UMMailboxPIN
- Get-UMMailboxPolicy
- Get-UMServer
- Get-User
- Get-WebServicesVirtualDirectory

- Get-X400AuthoritativeDomain

Looking for management tasks related to creating filters? See Creating Filters in Recipient Commands.

Common Filterable Properties

The following table contains the common filterable properties for the *-Filter* parameter. This table lists the name of the property, the Lightweight Directory Access Protocol (LDAP) display name, a description of the property, the possible values that the property can take, and each of the cmdlets that accept this property for the *-Filter* parameter. You can use the LDAP display name to convert your Exchange Server 2003 or earlier LDAP filters into Exchange 2010 Opath filters. For more information about how to convert LDAP filters to Exchange 2010 Opath filters, see Upgrade Custom LDAP Filters to OPATH Filters.

Note:

Not all filterable properties have an LDAP display name. The properties that do not have an LDAP display name are not Active Directory directory service properties. They are properties that are calculated by Exchange.

Note:

Many of the properties for the *-Filter* parameter accept wildcard characters. If you use a wildcard character, use the *-like* operator instead of the *-eq* operator. The *-like* operator is used to find pattern matches in rich types, such as strings, whereas the *-eq* operator is used to find an exact match.

Property name	LDAP display name	Description	Value	Cmdlets that accept this property
AcceptMessagesOnlyFrom	*authOrig*	This property contains the mailbox users and mail-enabled contacts that can send e-mail messages to this distribution group.	• Distinguished name (DN) • Canonical name • Globally unique identifier (GUID) • Name • Display name • Alias • Exchange DN • Primary Simple Mail Transfer Protocol (SMTP) address	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-RemoteMailbox

				Get-UmMailboxPin
AcceptMessagesOnlyFromDLMembers	*dLMemSubmitPerms*	This property contains the distribution groups that are allowed to send e-mail messages to this distribution group.	• DN • Canonical name • GUID • Name • Display name • Alias • Exchange DN • Primary SMTP address	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DynamicDistributionGroup Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-RemoteMailbox Get-UmMailboxPin
ActiveSyncAllowedDeviceIDs	*msExchMobileAllowedDeviceIds*	This property contains a list of device IDs that are allowed to synchronize with the mailbox.	Device IDs	Get-CASMailbox Get-UmMailboxPin
ActiveSyncDebugLogging	*msExchMobileDebugLogging*	This property specifies whether error logging is enabled for mobile devices.	• String • Wildcard character accepted	Get-CASMailbox Get-CASMailboxPlan Get-UmMailboxPin
ActiveSyncEnabled	Not applicable	This property specifies	• Boolean • $true or $false	Get-CalendarDiagn

		whether Exchange ActiveSync is enabled for the mailbox		osticLog Get-CASMailbox Get-CASMailboxPlan Get-UmMailboxPin
ActiveSyncMailboxPolicy	*msExchMobileMailboxPolicyLink*	This property contains the name of the Exchange ActiveSync mailbox policy for the mailbox.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-CASMailbox Get-CASMailboxPlan Get-DistributionGroupMember Get-UmMailboxPin Get-Recipient Get-RoleGroupMember
AddressListMembership	*showInAddressBook*	This property contains the address lists and global address list (GAL) of which the recipient is a member.	DN	Get-DistributionGroupMember Get-Recipient
Alias	*mailNickname*	This property contains the alias (the generic name used to identify a mail account) of the recipient. The alias can be a combination of characters that are separated by	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroup Get-DistributionGroupMember Get-

		periods without intervening spaces.		DynamicDistributionGroup Get-Group Get-LinkedUser Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-PublicFolderDatabase Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-SecurityPrincipal Get-UmMailboxPin Get-User
AllowUMCallsFromNonUsers	*msExchUMListInDirectorySearch*	This property specifies whether to exclude the mailbox from directory searches.	• 0 or None • 1 or SearchEnabled	Get-CalendarDiagnosticLog Get-Contact Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan

				Get-User
AssistantName	*msExchAssistantName*	This property contains the assistant name of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
City	*L*	This property contains the city name of the recipient.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember Get-UMMailboxPin Get-User
Company	*Company*	This property contains the company name of the recipient.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember

				Get-UMMailboxPin Get-User
CountryOrRegion	Not applicable	This property contains the country or region in which the recipient resides.	• Country/Region • You can locate valid *CountryOrRegion* values on the **Address and Phone** tab in the recipient's properties.	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember Get-UMMailboxpin Get-User
CustomAttribute1	*extensionAttribute1*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser

				Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute2	*extensionAttribute2*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-

				UMMailboxPin
CustomAttribute3	*extensionAttribute3*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute4	*extensionAttribute4*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember

		distribution group, or distribution group.		Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute5	*extensionAttribute5*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolde

				r Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute6	*extensionAttribute6*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMem

				ber Get-UMMailboxPin
CustomAttribute7	*extensionAttribute7*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute8	*extensionAttribute8*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-

		enabled public folder, dynamic distribution group, or distribution group.		DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute9	*extensionAttribute9*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan

				Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute10	*extensionAttribute10*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox

				Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute11	*extensionAttribute11*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute12	*extensionAttribute12*	This property contains a custom attribute that you can add to a mailbox, mail	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup

		contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.		Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute13	*extensionAttribute13*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-

				MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute14	*extensionAttribute14*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-

				RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
CustomAttribute15	*extensionAttribute15*	This property contains a custom attribute that you can add to a mailbox, mail contact, mail user, mail-enabled public folder, dynamic distribution group, or distribution group.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
Database	*homeMDB*	This property contains the mailbox database.	DN	Get-CalendarDiagnosticLog Get-Contact

				Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Group Get-LinkedUser Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-SecurityPrincipal Get-UMMailboxPin Get-User
Department	*department*	This property contains the department of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-

				DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember Get-UMMailboxPin Get-User
DisplayName	*displayName*	This property contains the ambiguous name resolution (ANR) search for the display name of the recipient.	• String • Wildcard character accepted	Get-AddressList Get-CalendarDiagnosticLog Get-CASMailbox Get-CASMailboxplan Get-Contact Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Group Get-LinkedUser Get-Mailbox Get-MailContact Get-MailboxDatabase

				Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-MessageClassification Get-MoveRequest Get-PublicfFolderDatabase Get-Recipient Get-RemoteMailbox Get-RoleGroup Get-RoleGroupMember Get-SecurityPrincipal Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan Get-User
DistinguishedName	*distinguishedName*	This property contains the DN of the recipients for which you are filtering.	DN	Get-AcceptedDomain Get-ActivesyncDevice Get-ActiveSyncDeviceAccessRule Get-ActivesyncDevi

				ceClass Get-ActivesyncMailboxPolicy Get-ActiveSyncOrganizationSettings Get-ActivesyncVirtualDirectory Get-AdminAuditLogConfig Get-AddressList Get-AddressRewriteEntry Get-ADSite Get-ADSiteLink Get-AttachmentFilterEntry Get-AttachmentFilterListConfig Get-AutodiscoverVirtualDirectory Get-AvailabilityAddressSpace Get-AvailabilityConfig Get-CalendarDiagnosticLog Get-CASMailbox Get-

				CASMailboxPlan Get-ClientAccessArray Get-ClientAccessServer Get-CmdletExtensionAgent Get-Contact Get-ContentFilterConfig Get-DatabaseAvailabilityGroup Get-DeliveryAgentConnector Get-DetailsTemplate Get-DistributionGroup Get-DistributionGroupMember Get-DomainController Get-DynamicDistributionGroup Get-ECPVirtualDirectory Get-EdgeSubscription Get-

				EdgeSyncServiceConfig Get-ExchangeAssistanceConfig Get-EmailAddressPolicy Get-ExchangeServer Get-FederatedOrganizationIdentifier Get-FederationTrust Get-ForeignConnector Get-GlobalAddressList Get-Group Get-IMAPSettings Get-IPAllowListConfig Get-IPAllowListProvider Get-IPAllowListProvidersConfig Get-IPBlockListConfig Get-IPBlockListProvider Get-

				IPBlockListProvidersConfig Get-IRMConfiguration Get-LinkedUser Get-ManagedContentSettings Get-ManagedFolder Get-ManagedFolderMailboxPolicy Get-ManagementRole Get-ManagementRoleAssignment Get-ManagementRoleEntry Get-ManagementScope Get-Mailbox Get-MailboxAuditBypassAssociation Get-MailboxDatabase Get-MailboxServer Get-MailContact Get-MailPublicFolder

				Get-MailUser Get-MessageClassification Get-MoveRequest Get-OABVirtualDirectory Get-OfflineAddressBook Get-OrganizationConfig Get-OrganizationRelationship Get-OrganizationalUnit Get-OutlookAnywhere Get-OutlookProvider Get-OWAMailboxPolicy Get-OWAVirtualDirectory Get-PerimeterConfig Get-POPSettings Get-PowershellVirtualDirectory Get-PublicFolderDa

				tabase Get-ReceiveConnector Get-RecipientFilterConfig Get-RemoteDomain Get-RemoteMailbox Get-RetentionPolicy Get-RetentionPolicyTag Get-RoleGroup Get-RoleGroupMember Get-RoutingGroupConnector Get-RPCClientAccess Get-Recipient Get-RecipientEnforcementProvisioningPolicy Get-ResourceConfig Get-RetentionPolicy Get-RoleAssignmentPolicy Get-

				RMSTrustedPublishingDomain Get-SecurityPrincipal Get-SendConnector Get-SenderFilterConfig Get-SenderIDConfig Get-SenderReputationConfig Get-SharingPolicy Get-SystemMessage Get-ThrottlingPolicy Get-ThrottlingPolicyAssociation Get-TransportConfig Get-TransportServer Get-Trust Get-UMAutoattendant Get-UMDialPlan Get-UMHuntgroup Get-

				UMIPGateway Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan Get-UMMailboxPolicy Get-UMServer Get-User Get-WebServicesVirtualDirectory Get-x400AuthoritativeDomain
EmailAddresses	*proxyAddresses*	This property contains the e-mail addresses of this recipient. All Exchange 2007 e-mail address types are valid. Separate multiple values with commas.	• E-mail address • Wildcard character accepted	Get-CalendarDiagnosticLog Get-CASMailbox Get-Contact Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Group Get-LinkedUser Get-Mailbox Get-MailContact Get-MailboxPlan

				Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-PublicFolderDatabase Get-Recipient Get-RoleGroupMember Get-RemoteMailbox Get-SecurityPrincipal Get-UMMailbox Get-UMMailboxPin Get-User
EmailAddressPolicyEnabled	Not applicable	This property contains the control for applying e-mail address policies to this recipient.	• Boolean • $true or $false	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailContact

				Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxpin
ExchangeGuid	*msExchMailboxGuid*	This property contains the GUID for the identity of the mailbox.	GUID	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-Mailuser Get-MoveRequest Get-RemoteMailbox Get-UMMailboxPin
ExchangeVersion	*msExchVersion*	This property contains the earliest version of Exchange that you can use to manage the returned object.	String	Get-AcceptedDomain Get-ActivesyncDevice Get-ActiveSyncDeviceAccessRule Get-ActivesyncDeviceClass Get-ActivesyncMail

				boxPolicy Get-ActiveSyncOrganizationSettings Get-ActivesyncVirtualDirectory Get-AdminAuditLogConfig Get-AddressList Get-AddressRewriteEntry Get-ADSite Get-ADSiteLink Get-AttachmentFilterEntry Get-AttachmentFilterListConfig Get-AutodiscoverVirtualDirectory Get-AvailabilityAddressSpace Get-AvailabilityConfig Get-CalendarDiagnosticLog Get-CASMailbox Get-CASMailboxPlan Get-

				ClientAccessArray Get-ClientAccessServer Get-CmdletExtensionAgent Get-Contact Get-ContentFilterConfig Get-DatabaseAvailabilityGroup Get-DeliveryAgentConnector Get-DetailsTemplate Get-DistributionGroup Get-DistributionGroupMember Get-DomainController Get-DynamicDistributionGroup Get-ECPVirtualDirectory Get-EdgeSubscription Get-EdgeSyncServiceConfig Get-

				ExchangeAssistanceConfig Get-EmailAddressPolicy Get-ExchangeServer Get-FederatedOrganizationIdentifier Get-FederationTrust Get-ForeignConnector Get-GlobalAddressList Get-Group Get-IMAPSettings Get-IPAllowListConfig Get-IPAllowListProvider Get-IPAllowListProvidersConfig Get-IPBlockListConfig Get-IPBlockListProvider Get-IPBlockListProvidersConfig Get-

				IRMConfiguration Get-LinkedUser Get-ManagedContentSettings Get-ManagedFolder Get-ManagedFolderMailboxPolicy Get-ManagementRole Get-ManagementRoleAssignment Get-ManagementRoleEntry Get-ManagementScope Get-Mailbox Get-MailboxAuditBypassAssociation Get-MailboxDatabase Get-MailboxServer Get-MailContact Get-MailPublicFolder Get-MailUser Get-

				MessageClassification Get-MoveRequest Get-OABVirtualDirectory Get-OfflineAddressBook Get-OrganizationConfig Get-OrganizationRelationship Get-OrganizationalUnit Get-OutlookAnywhere Get-OutlookProvider Get-OWAMailboxPolicy Get-OWAVirtualDirectory Get-PerimeterConfig Get-POPSettings Get-PowershellVirtualDirectory Get-PublicFolderDatabase Get-

				ReceiveConnector Get-RecipientFilterConfig Get-RemoteDomain Get-RemoteMailbox Get-RetentionPolicy Get-RetentionPolicyTag Get-RoleGroup Get-RoleGroupMember Get-RoutingGroupConnector Get-RPCClientAccess Get-Recipient Get-RecipientEnforcementProvisioningPolicy Get-ResourceConfig Get-RetentionPolicy Get-RoleAssignmentPolicy Get-RMSTrustedPublishingDomain

				Get-SecurityPrincipal Get-SendConnector Get-SenderFilterConfig Get-SenderIDConfig Get-SenderReputationConfig Get-SharingPolicy Get-SystemMessage Get-ThrottlingPolicy Get-ThrottlingPolicyAssociation Get-TransportConfig Get-TransportServer Get-Trust Get-UMAutoattendant Get-UMDialPlan Get-UMHuntgroup Get-UMIPGateway Get-UMMailbox

				Get-UMMailboxPin Get-UMMailboxPlan Get-UMMailboxPolicy Get-UMServer Get-User Get-WebServicesVirtualDirectory Get-x400AuthoritativeDomain
ExpansionServer	*msExchExpansionServerName*	This property contains the name of the Exchange server on which to expand the distribution group or dynamic distribution group.	Server name	Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Recipient Get-RoleGroupMember
ExternalEmailAddress	*targetAddress*	This property contains the external e-mail address. E-mail messages sent to the mail-enabled user are sent to this external address.	• E-mail address • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroupMember Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient

				Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
ExternalOofOptions	*msExchExternalOOFOptions*	This property contains the option for sending an out-of-office message to external senders.	• InternalOnly • External	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin
Fax	*facsimileTelephoneNumber*	This property contains the fax number of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
FirstName	*givenName*	This property contains the ANR search for the first name of the recipient.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember Get-UMMailboxpin

				Get-User
ForwardingAddress	*altRecipient*	This property contains the forwarding address to which messages are sent.	Existing SMTP address	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-MailPublicFolder Get-MailUser Get-RemoteMailbox Get-UMMailboxPin
GrantSendOnBehalfTo	*publicDelegates*	This property contains the DN of other mailboxes that can send messages on behalf of this recipient.	DN	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DynamicDistributionGroup Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-RemoteMailbox Get-UMMailboxPin

GroupType	*groupType*	This property contains the group type in Active Directory.	• DomainLocal • SecurityEnabled • Global • Universal • BuiltinLocal	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Group Get-LinkedUser Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroup Get-RoleGroupMember Get-SecurityPrincipal Get-UMMailboxPin Get-User

Guid	*objectGuid*	This property contains the GUID for the identity of the Active Directory object.	GUID	Get-AcceptedDomain Get-ActivesyncDevice Get-ActiveSyncDeviceAccessRule Get-ActivesyncDeviceClass Get-ActivesyncMailboxPolicy Get-ActiveSyncOrganizationSettings Get-ActivesyncVirtualDirectory Get-AdminAuditLogConfig Get-AddressList Get-AddressRewriteEntry Get-ADSite Get-ADSiteLink Get-AttachmentFilterEntry Get-AttachmentFilterListConfig Get-AutodiscoverVirtualDirectory Get-AvailabilityAddressSpace

				Get-AvailabilityConfig Get-CalendarDiagnosticLog Get-CASMailbox Get-CASMailboxPlan Get-ClientAccessArray Get-ClientAccessServer Get-CmdletExtensionAgent Get-Contact Get-ContentFilterConfig Get-DatabaseAvailabilityGroup Get-DeliveryAgentConnector Get-DetailsTemplate Get-DistributionGroup Get-DistributionGroupMember Get-DomainController Get-

				DynamicDistributionGroup Get-ECPVirtualDirectory Get-EdgeSubscription Get-EdgeSyncServiceConfig Get-ExchangeAssistanceConfig Get-EmailAddressPolicy Get-ExchangeServer Get-FederatedOrganizationIdentifier Get-FederationTrust Get-ForeignConnector Get-GlobalAddressList Get-Group Get-IMAPSettings Get-IPAllowListConfig Get-IPAllowListProvider Get-

				IPAllowListProvidersConfig Get-IPBlockListConfig Get-IPBlockListProvider Get-IPBlockListProvidersConfig Get-IRMConfiguration Get-LinkedUser Get-ManagedContentSettings Get-ManagedFolder Get-ManagedFolderMailboxPolicy Get-ManagementRole Get-ManagementRoleAssignment Get-ManagementRoleEntry Get-ManagementScope Get-Mailbox Get-MailboxAuditBypassAssociation Get-

				MailboxDatabase Get-MailboxServer Get-MailContact Get-MailPublicFolder Get-MailUser Get-MessageClassification Get-MoveRequest Get-OABVirtualDirectory Get-OfflineAddressBook Get-OrganizationConfig Get-OrganizationRelationship Get-OrganizationalUnit Get-OutlookAnywhere Get-OutlookProvider Get-OWAMailboxPolicy Get-OWAVirtualDirectory

				Get-PerimeterConfig Get-POPSettings Get-PowershellVirtualDirectory Get-PublicFolderDatabase Get-ReceiveConnector Get-RecipientFilterConfig Get-RemoteDomain Get-RemoteMailbox Get-RetentionPolicy Get-RetentionPolicyTag Get-RoleGroup Get-RoleGroupMember Get-RoutingGroupConnector Get-RPCClientAccess Get-Recipient Get-RecipientEnforcementProvisioningPolicy

				Get-ResourceConfig Get-RetentionPolicy Get-RoleAssignmentPolicy Get-RMSTrustedPublishingDomain Get-SecurityPrincipal Get-SendConnector Get-SenderFilterConfig Get-SenderIDConfig Get-SenderReputationConfig Get-SharingPolicy Get-SystemMessage Get-ThrottlingPolicy Get-ThrottlingPolicyAssociation Get-TransportConfig Get-TransportServer

				Get-Trust Get-UMAutoattendant Get-UMDialPlan Get-UMHuntgroup Get-UMIPGateway Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan Get-UMMailboxPolicy Get-UMServer Get-User Get-WebServicesVirtualDirectory Get-x400AuthoritativeDomain
HiddenFromAddressListsEnabled	*msExchHideFromAddressLists*	This property specifies whether the user is visible in the address list.	• Boolean • $true or $false	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailContact

				Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
HomePhone	*homePhone*	This property contains the home phone number of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-User Get-UMMailboxPin Get-User
IncludedRecipients	Not applicable	This property contains the recipient types that are used to build the dynamic distribution group.	• AllRecipients • MailboxUsers • Resources • MailContacts • MailGroups • Mail Users • None	Get-DynamicDistributionGroup
Initials	*initials*	This property contains the initials for the name of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-

				LinkedUser Get-UMMailboxPin Get-User
IsLinked	Not applicable	This property specifies whether a folder is linked to a master folder.	• Boolean • $true or $false	Get-CalendarDiagnosticLog Get-LinkedUser Get-Mailbox Get-MailboxPlan Get-UMMailboxpin Get-User
IsMailboxEnabled	Not applicable	This property specifies whether a mailbox is mailbox-enabled.	• Boolean • $true or $false	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin
IsResource	Not applicable	This property specifies whether a mailbox is a resource mailbox.	• Boolean • $true or $false	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin
IsShared	Not applicable	This property specifies whether a resource mailbox is shared.	• Boolean • $true or $false	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin

IssueWarningQuota	*mDBStorageQuota*	This property contains the mailbox size at which a warning message is sent to the user.	Unlimited or integer	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxDatabase Get-MailboxPlan Get-OrganizationConfig Get-PublicFolderDatabase Get-UMMailboxPin
LanguagesRaw	*msExchUserCulture*	This property contains the language preference for this mailbox.	An acceptable value for this parameter is a combination of an International Organization for Standardization (ISO) 639 two-letter lowercase culture code that is associated with a language and an ISO 3166 two-letter uppercase subculture code that is associated with a country or region. For example, United States English is represented as `en-us`. To learn more about culture codes and for a full list of acceptable values, see CultureInfo Class in the MSDN Library.	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin
LastName	*sn*	This property contains the ANR search for the last name of the recipient.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser

				Get-Recipient Get-RoleGroupMember Get-UMMailboxPin Get-User
ManagedBy	*managedBy*	This property contains the DN of the user or contact that manages this group.	DN	Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Group Get-Recipient Get-RoleGroup Get-RoleGroupMember
ManagedFolderMailboxPolicy	*msExchMailboxTemplateLink*	This property contains the managed folder mailbox policy that controls messaging records management (MRM) for the mailbox.	• Name • GUID • DN	Get-CalendarDiagnosticLog Get-DistributionGroupMember Get-Mailbox Get-MailboxPlan Get-Recipient Get-RoleGroupMember Get-UMMailboxPin
Manager	*manager*	This property contains the manager of	• String • Wildcard character accepted	Get-CalendarDiagnosticLog

		the recipient.		Get-Contact Get-DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember Get-UMMailboxPin Get-User
MaxBlockedSenders	*msExchMaxBlockedSenders*	This property contains the maximum number of senders that can be included in the Blocked Senders list.	Integer	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin
MaxReceiveSize	*delivContLength*	This property contains the maximum size of messages that this recipient can receive.	Unlimited or integer	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DynamicDistributionGroup Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-

				MoveRequest Get-RemoteMailbox Get-TransportConfig Get-UMMailboxPin
MaxSafeSenders	*msExchMaxSafeSenders*	This property contains the maximum number of senders that can be included in the Safe Senders list.	Integer	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin
MaxSendSize	*submissionContLength*	This property contains the maximum size of messages that this recipient can send.	Unlimited or integer	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DynamicDistributionGroup Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-RemoteMailbox Get-TransportConfig

				Get-UMMailboxPin
MemberOfGroup	*memberOf*	This property contains the groups of which the recipient is a member.	String	Get-CalendarDiagnosticLog Get-CASMailbox Get-Contact Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Group Get-LinkedUser Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailUser Get-MailPublicFolder Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailbox Get-UMMailboxPin

				Get-UMMailboxPlan Get-User
MobilePhone	*mobile*	This property contains the mobile phone number of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
Name	*name*	This property contains the name of the recipient.	String	Get-AcceptedDomain Get-ActivesyncDevice Get-ActiveSyncDeviceAccessRule Get-ActivesyncDeviceClass Get-ActivesyncMailboxPolicy Get-ActiveSyncOrganizationSettings Get-ActivesyncVirtualDirectory Get-AdminAuditLogConfig Get-AddressList Get-AddressRewriteEntry

				Get-ADSite Get-ADSiteLink Get-AttachmentFilterEntry Get-AttachmentFilterListConfig Get-AutodiscoverVirtualDirectory Get-AvailabilityAddressSpace Get-AvailabilityConfig Get-CalendarDiagnosticLog Get-CASMailbox Get-CASMailboxPlan Get-ClientAccessArray Get-ClientAccessServer Get-CmdletExtensionAgent Get-Contact Get-ContentFilterConfig Get-DatabaseAvailabilityGroup Get-

				DeliveryAgentConnector Get-DetailsTemplate Get-DistributionGroup Get-DistributionGroupMember Get-DomainController Get-DynamicDistributionGroup Get-ECPVirtualDirectory Get-EdgeSubscription Get-EdgeSyncServiceConfig Get-ExchangeAssistanceConfig Get-EmailAddressPolicy Get-ExchangeServer Get-FederatedOrganizationIdentifier Get-FederationTrust Get-ForeignConnec

				tor Get-GlobalAddressList Get-Group Get-IMAPSettings Get-IPAllowListConfig Get-IPAllowListProvider Get-IPAllowListProvidersConfig Get-IPBlockListConfig Get-IPBlockListProvider Get-IPBlockListProvidersConfig Get-IRMConfiguration Get-LinkedUser Get-ManagedContentSettings Get-ManagedFolder Get-ManagedFolderMailboxPolicy Get-ManagementRole

				Get-ManagementRoleAssignment Get-ManagementRoleEntry Get-ManagementScope Get-Mailbox Get-MailboxAuditBypassAssociation Get-MailboxDatabase Get-MailboxServer Get-MailContact Get-MailPublicFolder Get-MailUser Get-MessageClassification Get-MoveRequest Get-OABVirtualDirectory Get-OfflineAddressBook Get-OrganizationConfig Get-OrganizationRelationship

				Get-OrganizationalUnit Get-OutlookAnywhere Get-OutlookProvider Get-OWAMailboxPolicy Get-OWAVirtualDirectory Get-PerimeterConfig Get-POPSettings Get-PowershellVirtualDirectory Get-PublicFolderDatabase Get-ReceiveConnector Get-RecipientFilterConfig Get-RemoteDomain Get-RemoteMailbox Get-RetentionPolicy Get-RetentionPolicyTag Get-RoleGroup

				Get-RoleGroupMember Get-RoutingGroupConnector Get-RPCClientAccess Get-Recipient Get-RecipientEnforcementProvisioningPolicy Get-ResourceConfig Get-RetentionPolicy Get-RoleAssignmentPolicy Get-RMSTrustedPublishingDomain Get-SecurityPrincipal Get-SendConnector Get-SenderFilterConfig Get-SenderIDConfig Get-SenderReputationConfig Get-SharingPolicy

				Get-SystemMessage Get-ThrottlingPolicy Get-ThrottlingPolicyAssociation Get-TransportConfig Get-TransportServer Get-Trust Get-UMAutoattendant Get-UMDialPlan Get-UMHuntgroup Get-UMIPGateway Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan Get-UMMailboxPolicy Get-UMServer Get-User Get-WebServicesVirtualDirectory Get-x400AuthoritativeDomain

Notes	*info*	This property contains specific comments about the recipient.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Group Get-LinkedUser Get-RoleGroupMember Get-Recipient Get-UMMailboxPin Get-User
Office	*physicalDeliveryOfficeName*	This property contains the office of the recipient.	String	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser Get-Mailbox Get-MailboxPlan Get-Recipient Get-RoleGroupMember Get-UMMailboxPin Get-User

OfflineAddressBook	*msExchUseOAB*	This property contains the offline address book (OAB) that is associated with this mailbox.	• Name • GUID • DN	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxDatabase Get-MailboxPlan Get-UMMailboxPin
OperatorNumber	*msExchUMOperatorNumber*	This property contains the string of digits for the personal operator.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan
OtherFax	*otherFacsimileTelephoneNumber*	This property contains the additional fax number of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
OtherHomePhone	*otherHomePhone*	This property contains the additional home phone number of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
OtherTelephone	*otherTelephone*	This property contains the additional telephone	• String • Wildcard character accepted	Get-CalendarDiagnosticLog

		number of the user or contact.		Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
Pager	*pager*	This property contains the pager number of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
Phone	*telephoneNumber*	This property contains the phone number of the recipient.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember Get-UMMailboxPin Get-User
PhoneticDisplayName	*msDS-PhoneticDisplayName*	This property contains a phonetic pronunciation of the *DisplayName* property. UM uses this property for Automatic	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DynamicDistributionGroup Get-Group

		Speech Recognition.		Get-LinkedUser Get-MailPublicFolder Get-UMMailboxPin Get-User
PoliciesExcluded	*msExchPoliciesExcluded*	This property contains the GUIDs of any policies that are excluded.	GUID	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin
PostalCode	*postalCode*	This property	• String • Wildcard	Get-CalendarDiagn

		contains the postal code of the user or contact.	character accepted	osticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember Get-UMMailboxPin Get-User
PostOfficeBox	*postOfficeBox*	This property contains the post office box number of the user or contact.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
PrimarySmtpAddress	Not applicable	This property contains the primary SMTP address, which is the e-mail address that external users will see when they receive a message from this recipient.	SMTP address	Get-CalendarDiagnosticLog Get-CASMailbox Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Mailbox Get-MailboxPlan

				Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailbox Get-UMMailboxPin
ProhibitSendQuota	*mDBOverQuotaLimit*	This property contains the mailbox size at which the user associated with this mailbox can no longer send messages.	Unlimited or integer	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxDatabase Get-MailboxPlan Get-UMMailboxPin
ProhibitSendReceiveQuota	*mDBOverHardQuotaLimit*	This property contains the mailbox size at which the user associated with this mailbox can no longer send or receive messages.	Unlimited or integer	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxDatabase Get-MailboxPlan Get-UMMailboxPin

PublicFolderContacts	*pFContacts*	This property contains the contacts for the public folder.	Multiple DNs	Get-MailPublicFolder
PublicFolderType	*msExchPFTreeType*	This property specifies the public folder type.	• GeneralPurpose • MAPI • Network News Transfer Protocol (NNTP) • NotSpecified	Get-MailPublicFolder
RecipientFilter	*msExchQueryFilter*	This property contains the recipient filter that has been applied.	String	Get-AddressList Get-DynamicDistributionGroup Get-EmailAddressPolicy Get-GlobalAddressList
RecipientLimits	*msExchRecipLimit*	This property contains the maximum number of recipients per message to which this mailbox can send.	Unlimited or integer	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailUser Get-RemoteMailbox Get-UMMailboxPin
RecipientType	Not applicable	This property specifies the recipient type.	• UserMailbox • MailUser • MailContact • MailUniversalDistributionGroup • MailUniversalSecurityGroup • MailNonUniversalGroup • DynamicDistributionGroup • PublicFolder	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroup Get-DistributionGroupMember

				Get-DynamicDistributionGroup Get-Group Get-LinkedUser Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-UMMailboxPin Get-User
RecipientTypeDetails	Not applicable	This property specifies the recipient subtype.	• ConferenceRoomMailbox • EquipmentMailbox • LegacyMailbox • LinkedMailbox • UserMailbox • MailContact • DynamicDistributionGroup • MailForestContact • MailNonUniversalGroup • MailUniversalDistributionGroup • MailUniversalSecurityGroup	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroup Get-DistributionGroupMember Get-DynamicDistributionGroup Get-Group

			• MailUser • PublicFolder • SharedMailbox	Get-LinkedUser Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MailPublicFolder Get-MoveRequest Get-Recipient Get-RemoteMailbox Get-RoleGroupMember Get-SecurityPrincipal Get-UMMailboxPin Get-User
RejectMessagesFrom	*unauthOrig*	This property contains the recipients from whom messages will be rejected by this recipient.	• DN • Canonical name • GUID • Name • Display name • Alias • Exchange DN • Primary SMTP address	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DynamicDistributionGroup Get-Mailbox Get-MailboxPlan

				Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-RemoteMailbox Get-UMMailboxPin
RejectMessagesFromDLMembers	*dLMemRejectPerms*	This property specifies the distribution groups from which this recipient will reject messages.	• DN • Canonical name • GUID • Name • Display name • Alias • Exchange DN • Primary SMTP address	Get-CalendarDiagnosticLog Get-DistributionGroup Get-DynamicDistributionGroup Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-RemoteMailbox Get-UMMailboxPin
ResourceCapacity	*msExchResourceCapacity*	This property contains the capacity of this resource mailbox.	Non-negative integer	Get-CalendarDiagnosticLog Get-Mailbox

				Get-MailboxPlan Get-UMMailboxPin
ResourceCustom	Not applicable	This property contains custom properties for this resource mailbox.	Custom property defined by **Set-ResourceConfig**	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin
RetainDeletedItemsFor	*garbageCollPeriod*	This property contains the length of time to keep deleted items.	Time span: *dd.hh:mm:ss* where *dd* = days, *hh* = hours, *mm* = minutes, and *ss* = seconds	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-MailUser Get-RemoteMailbox Get-UMMailboxPin
RulesQuota	*msExchMDBRulesQuota*	This property contains the limit for the size of rules for this mailbox.	String	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin
SamAccountName	*SamAccountName*	This property contains the logon name that is used to support client computers and servers running older versions of the operating system, such as Microsoft	String	Get-CalendarDiagnosticLog Get-CASMailbox Get-DistributionGroup Get-

		Windows NT 4.0, Windows 98, Windows 95, and LAN Manager.		DistributionGroupMember Get-Group Get-LinkedUser Get-Mailbox Get-MailboxPlan Get-MailUser Get-Recipient Get-RemoteMailbox Get-RoleGroup Get-RoleGroupMember Get-UMMailbox Get-UMMailboxPin Get-User
SendOofMessageToOriginatorEnabled	*oOFReplyToOriginator*	This property specifies whether out-of-office messages from distribution group members are sent to the message sender.	• Boolean • $true or $false	Get-DistributionGroup Get-DynamicDistributionGroup
ServerName	Not applicable	This property contains the name of the server on which the object resides	Server name	Get-CalendarDiagnosticLog Get-CASMailbox Get-DistributionGroupMember Get-Mailbox

				Get-MailboxPlan Get-Recipient Get-RoleGroupMember Get-UMMailbox Get-UMMailboxPin
SimpleDisplayName	*displayNamePrintable*	This property contains an alternative display name of the object when only a limited set of characters is permitted.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group Get-LlinkedUser Get-Mailbox Get-MailContact Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-RemoteMailbox Get-UMMailboxPin

				Get-User
StateOrProvince	*st*	This property contains the state or province information that is defined for this recipient.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember Get-UMMailboxPin Get-User
StreetAddress	*streetAddress*	This property contains the street address that is defined for the user or contact.	String	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
TelephoneAssistant	*telephoneAssistant*	This property contains the telephone number of the contact's assistant.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-LinkedUser Get-UMMailboxPin Get-User
Title	*title*	This property contains the title of the recipient.	String	Get-CalendarDiagnosticLog Get-Contact

				Get-DistributionGroupMember Get-LinkedUser Get-Recipient Get-RoleGroupMember Get-UMMailboxPin Get-User
UMDtmfMap	*msExchUMDtmfMap*	This property contains a user-defined dual tone multi-frequency (DTMF) map for the UM-enabled user. DTMF is also referred to as *touch-tone*.	• String • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-LinkedUser Get-Mailbox Get-MailboxPlan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-RemoteMailbox Get-UMMailbox Get-UMMailboxPin

				Get-User
UMEnabled	Not applicable	This property specifies whether UM is enabled for this mailbox.	• Boolean • $true or $false	Get-CalendarDiagnosticLog Get-DistributionGroupMember Get-Mailbox Get-MailboxPlan Get-Recipient Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan
UMMailboxPolicy	*msExchUMTemplateLink*	This property contains the UM mailbox policy for the mailbox. You use UM mailbox policies to set UM settings for UM-enabled users, such as personal identification number (PIN) policies and dialing restrictions.	String	Get-CalendarDiagnosticLog Get-DistributionGroupMember Get-Recipient Get-RoleGroupMember Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan
UMRecipientDialPlanId	*msExchUMRecipientDialPlanLink*	This property contains the dial plan identifier for the mailbox, user, or contact.	DN	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroupMember Get-LinkedUser

				Get-Recipient Get-RoleGroupMember Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan Get-User
UseDatabaseQuotaDefaults	*mDBUseDefaults*	This property specifies whether the mailbox uses the quota attributes for the mailbox database in which this mailbox resides. The quota attributes are: ProhibitSendQuota, ProhibitSendReceiveQuota, IssueWarningQuota, and RulesQuota.	• Boolean • $true or $false	Get-CalendarDiagnosticLog Get-Mailbox Get-MailboxPlan Get-UMMailboxPin
UserPrincipalName	*userPrincipalName*	This property contains the UPN for this recipient. The UPN is the logon name for the user, and consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides.	• User logon name • User principal name • Wildcard character accepted	Get-CalendarDiagnosticLog Get-DistributionGroupMember Get-LinkedUser Get-Mailbox Get-MailboxPlan Get-MailUser Get-Recipient Get-RemoteMailbox

				Get-RoleGroupMember Get-UMMailboxPin Get-User
WhenChanged	*WhenChanged*	This property contains the date and time stamp of when the object was last changed.	Date-time stamp	Get-AcceptedDomain Get-ActivesyncDevice Get-ActiveSyncDeviceAccessRule Get-ActivesyncDeviceClass Get-ActivesyncMailboxPolicy Get-ActiveSyncOrganizationSettings Get-ActivesyncVirtualDirectory Get-AdminAuditLogConfig Get-AddressList Get-AddressRewriteEntry Get-ADSite Get-ADSiteLink Get-AttachmentFilterEntry Get-AttachmentFilt

				erListConfig Get-AutodiscoverVirtualDirectory Get-AvailabilityAddressSpace Get-AvailabilityConfig Get-CalendarDiagnosticLog Get-CASMailbox Get-CASMailboxPlan Get-ClientAccessArray Get-ClientAccessServer Get-CmdletExtensionAgent Get-Contact Get-ContentFilterConfig Get-DatabaseAvailabilityGroup Get-DeliveryAgentConnector Get-DetailsTemplate Get-DistributionGroup

				Get-DistributionGroupMember Get-DomainController Get-DynamicDistributionGroup Get-ECPVirtualDirectory Get-EdgeSubscription Get-EdgeSyncServiceConfig Get-ExchangeAssistanceConfig Get-EmailAddressPolicy Get-ExchangeServer Get-FederatedOrganizationIdentifier Get-FederationTrust Get-ForeignConnector Get-GlobalAddressList Get-Group Get-IMAPSettings

				Get-IPAllowListConfig Get-IPAllowListProvider Get-IPAllowListProvidersConfig Get-IPBlockListConfig Get-IPBlockListProvider Get-IPBlockListProvidersConfig Get-IRMConfiguration Get-LinkedUser Get-ManagedContentSettings Get-ManagedFolder Get-ManagedFolderMailboxPolicy Get-ManagementRole Get-ManagementRoleAssignment Get-ManagementRoleEntry Get-ManagementScope

				Get-Mailbox Get-MailboxAuditBypassAssociation Get-MailboxDatabase Get-MailboxServer Get-MailContact Get-MailPublicFolder Get-MailUser Get-MessageClassification Get-MoveRequest Get-OABVirtualDirectory Get-OfflineAddressBook Get-OrganizationConfig Get-OrganizationRelationship Get-OrganizationalUnit Get-OutlookAnywhere Get-OutlookProvider

				Get-OWAMailboxPolicy Get-OWAVirtualDirectory Get-PerimeterConfig Get-POPSettings Get-PowershellVirtualDirectory Get-PublicFolderDatabase Get-ReceiveConnector Get-RecipientFilterConfig Get-RemoteDomain Get-RemoteMailbox Get-RetentionPolicy Get-RetentionPolicyTag Get-RoleGroup Get-RoleGroupMember Get-RoutingGroupConnector Get-RPCClientAccess

				Get-Recipient Get-RecipientEnforcementProvisioningPolicy Get-ResourceConfig Get-RetentionPolicy Get-RoleAssignmentPolicy Get-RMSTrustedPublishingDomain Get-SecurityPrincipal Get-SendConnector Get-SenderFilterConfig Get-SenderIDConfig Get-SenderReputationConfig Get-SharingPolicy Get-SystemMessage Get-ThrottlingPolicy Get-ThrottlingPolicyAssociation Get-

				TransportConfig Get-TransportServer Get-Trust Get-UMAutoattendant Get-UMDialPlan Get-UMHuntgroup Get-UMIPGateway Get-UMMailbox Get-UMMailboxPin Get-UMMailboxPlan Get-UMMailboxPolicy Get-UMServer Get-User Get-WebServicesVirtualDirectory Get-x400AuthoritativeDomain
WindowsEmailAddress	*mail*	This property contains the Windows e-mail address for this mailbox. This address is not used by Exchange.	• E-mail address • Wildcard character accepted	Get-CalendarDiagnosticLog Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup

				Get-Group Get-LinkedUser Get-Mailbox Get-Mailboxplan Get-MailContact Get-MailPublicFolder Get-MailUser Get-MoveRequest Get-PublicFolderDatabase Get-RemoteMailbox Get-UMMailboxPin Get-User

Advanced Filterable Properties

The following table contains filterable properties that are not commonly used. These properties are listed here for reference.

Property name	LDAP name	Cmdlets that accept this property
DeletedItemFlags	*deletedItemFlags*	Get-Mailbox
DeliverToMailboxAndForward	*deliverAndRedirect*	Get-Mailbox Get-MailPublicFolder
DirectReports	*directReports*	Get-Contact Get-User
ExchangeSecurityDescriptor	*msExchMailboxSecurityDescriptor*	Get-Mailbox
ExchangeUserAccountControl	*msExchUserAccountControl*	Get-Mailbox Get-MailUser

HasActiveSyncDevicePartnership	Not applicable	Get-CASMailbox Get-Recipient
Id	*distinguishedName*	Get-CASMailbox Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient Get-UMMailbox Get-User
ImapEnabled	Not applicable	Get-CASMailbox
IsSecurityPrincipal	Not applicable	Get-User
LdapRecipientFilter	*msExchDynamicDLFilter*	Get-DynamicDistributionGroup
LegacyExchangeDN	*legacyExchangeDN*	Get-CASMailbox Get-DistributionGroup Get-DynamicDistributionGroup Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-UMMailbox
MAPIEnabled	Not applicable	Get-CASMailbox
MasterAccountSid	*msExchMasterAccountSid*	Get-Mailbox
Members	*member*	Get-Group
NTSecurityDescriptor	*ntSecurityDescriptor*	Get-CASMailbox

		Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient Get-UMMailbox Get-User
ObjectCategory	*objectCategory*	Get-CASMailbox Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient Get-UMMailbox Get-User
ObjectClass	*objectClass*	Get-CASMailbox Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group

		Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient Get-UMMailbox Get-User
ObjectState	Not applicable	Get-CASMailbox Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient Get-UMMailbox Get-User
OriginalId	Not applicable	Get-CASMailbox Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient

		Get-UMMailbox Get-User
OriginalPrimarySmtpAddress	Not applicable	Get-CASMailbox Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient Get-UMMailbox Get-User
OriginalWindowsEmailAddress	Not applicable	Get-CASMailbox Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient Get-UMMailbox Get-User
OWAEnabled	Not applicable	Get-CASMailbox
OWACalendarEnabled	Not applicable	Get-CASMailbox
OWAContactsEnabled	Not applicable	Get-CASMailbox

OWATasksEnabled	Not applicable	Get-CASMailbox
OWAJournalEnabled	Not applicable	Get-CASMailbox
OWANotesEnabled	Not applicable	Get-CASMailbox
OWARemindersAndNotificationsEnabled	Not applicable	Get-CASMailbox
OWAPremiumClientEnabled	Not applicable	Get-CASMailbox
OWASpellCheckerEnabled	Not applicable	Get-CASMailbox
OWASearchFoldersEnabled	Not applicable	Get-CASMailbox
OWASignaturesEnabled	Not applicable	Get-CASMailbox
OWAThemeSelectionEnabled	Not applicable	Get-CASMailbox
OWAJunkEmailEnabled	Not applicable	Get-CASMailbox
OWAUMIntegrationEnabled	Not applicable	Get-CASMailbox
OWAWSSAccessOnPublicComputersEnabled	Not applicable	Get-CASMailbox
OWAWSSAccessOnPrivateComputersEnabled	Not applicable	Get-CASMailbox
OWAUNCAccessOnPublicComputersEnabled	Not applicable	Get-CASMailbox
OWAUNCAccessOnPrivateComputersEnabled	Not applicable	Get-CASMailbox
OWAActiveSyncIntegrationEnabled	Not applicable	Get-CASMailbox
OWAChangePasswordEnabled	Not applicable	Get-CASMailbox
OWAAllAddressListsEnabled	Not applicable	Get-CASMailbox
OWARulesEnabled	Not applicable	Get-CASMailbox
OWAPublicFoldersEnabled	Not applicable	Get-CASMailbox
OWASMimeEnabled	Not applicable	Get-CASMailbox
OWARecoverDeletedItemsEnabled	Not applicable	Get-CASMailbox
PoliciesIncluded	*msExchPoliciesIncluded*	Get-Recipient
PopEnabled	Not applicable	Get-CASMailbox
ProtocolSettings	*protocolSettings*	Get-CASMailbox
PublicFolderRootUrl	*msExchPfRootUrl*	Get-MailPublicFolder
RawCanonicalName	*canonicalName*	Get-CASMailbox Get-Contact Get-DistributionGroup

		Get-DynamicDistributionGroup Get-Group Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient Get-UMMailbox Get-User
RawName	*name*	Get-CASMailbox Get-Contact Get-DistributionGroup Get-DynamicDistributionGroup Get-Group Get-Mailbox Get-MailContact Get-MailPublicFolder Get-MailUser Get-Recipient Get-UMMailbox Get-User
RecipientContainer	*msExchDynamicDLBaseDN*	Get-DynamicDistributionGroup
ReportToManagerEnabled	*reportToOwner*	Get-DistributionGroup Get-DynamicDistributionGroup
ReportToOriginatorEnabled	*reportToOriginator*	Get-DistributionGroup Get-DynamicDistributionGroup
RequireAllSendersAreAuthenticated	*msExchRequireAuthToSendTo*	Get-DistributionGroup Get-

		DynamicDistributionGroup Get-MailContact Get-MailPublicFolder Get-MailUser
ResourceType	Not applicable	Get-Mailbox Get-Recipient
ServerLegacyDN	*msExchHomeServerName*	Get-CASMailbox Get-Mailbox Get-Recipient Get-UMMailbox
Sid	*objectSid*	Get-Group Get-User
SidHistory	*SIDHistory*	Get-Group Get-User
SIPResourceIdentifier	Not applicable	Get-UMMailbox
UserAccountControl	*userAccountControl*	Get-Mailbox
WebPage	*wWWHomePage*	Get-Contact Get-User

1.8.3.3.2 Filterable Properties for the -RecipientFilter Parameter

Filterable Properties for the -RecipientFilter Parameter

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The content for this topic will be similar to a previously published Exchange Server 2007 topic. For more information, see Filterable Properties for the -RecipientFilter Parameter in Exchange 2007 SP1 and SP2.

Filterable Properties for the -ContentFilter Parameter

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-30*

This topic lists the filterable properties for the *ContentFilter* parameter. The *ContentFilter* parameter is used to export messages to a .pst file that match the filter. The *ContentFilter* parameter is used in the New-MailboxExportRequest cmdlet.

Filterable Properties

Many of the properties for the *ContentFilter* parameter accept wildcard characters. If you use a wildcard character, use the **-like** operator instead of the **-eq** operator. The **-like** operator is used to find pattern matches in rich types, such as strings, whereas the **-eq** operator is used to find an exact match.

The following table contains a list of the filterable properties for the *ContentFilter* parameter. This table lists the name of the property, a description, the acceptable values, and a syntax example. For more information about OPATH filters, see Creating Filters in Recipient Commands.

Property	Description	Values	Example syntax
All	This property returns all messages that have a particular string in any of the indexed properties. For example, use this property if you want to export all messages that have "Ayla" as the recipient, the sender, or have the name mentioned in the message body.	String Wildcard	`-ContentFilter {All`
Attachment	This property returns messages that have the specified string in the content of an attachment or in the attachment's file name.	String Wildcard	`-ContentFilter {Atta`
BCC	This property returns sent messages that have the specified recipient in the Bcc field.	Display name Alias SMTP address LegacyDN Wildcard	`-ContentFilter {(BCC`

Body	This property returns messages that have the specified string within the message body.	String Wildcard	-ContentFilter {Body
Category	This property returns messages that have a matching category. Categories are set by users or Inbox rules.	String Wildcard	-ContentFilter {Cate
CC	This property returns sent messages that have the specified recipient in the Cc field.	Display name Alias SMTP address LegacyDN Wildcard	-ContentFilter {(CC
Expires	This property returns messages that have a specified expiration time stamp.	Date-Time stamp	-ContentFilter {Expi
HasAttachment	This property returns messages with or without attachments.	Boolean $true or $false	-ContentFilter {HasA
Importance	This property returns messages that have a specified importance level.	0 or "Low" 1 or "Normal" 2 or "High"	-ContentFilter {Impo -ContentFilter {Impo
IsFlagged	This property returns messages that have been flagged by the user or Inbox rule.	Boolean $true or $false	-ContentFilter {IsFl
IsRead	This property returns messages that have been read or not read by the user.	Boolean $true or $false	-ContentFilter {IsRe
MessageKind	This property returns messages that are of the specified type.	Email Meetings Tasks Notes Docs Journal Contacts	-ContentFilter {Mess -ContentFilter {Mess

		IM Voicemail Fax Posts RSSFeeds	
MessageLocale	This property returns messages that are of the specified locale.	CultureInfo	-ContentFilter {Mess -ContentFilter {Mess
Participants	This property returns messages that have the specified recipient in the To, Bcc, or Cc fields.	Display name Alias SMTP address LegacyDN Wildcard	-ContentFilter {(Par
PolicyTag	This property returns messages that have a policy tag. The Exchange store persists policy tags as GUIDs. Therefore, the string can contain either an explicit GUID value, which is then searched by the PR_POLICY_TAG, or a wildcard string. If the supplied value isn't a GUID, the command uses Active Directory information to resolve names to GUIDs.	String Wildcard	-ContentFilter {Poli
Received	This property returns messages that were received by the recipient with the specified Received time stamp.	Date-Time stamp	-ContentFilter {Rece {(Received -lt '01/0
Sender	This property returns messages that were received from the specified sender.	Display name Alias SMTP address LegacyDN	ContentFilter {Sende

		Wildcard	
Sent	This property returns messages that were sent by the recipient with the specified Sent time stamp.	Date-Time stamp	-ContentFilter {Sent -ContentFilter {(Sen
Size	This property returns messages that are of a specific size.	B (bytes) KB (kilobytes) MB (megabytes)	-ContentFilter {Size
Subject	This property returns messages that have the specified string within the subject of the message.	String Wildcard	-ContentFilter {Subj
To	This property returns sent messages that have the specified recipient in the To field.	Display name Alias SMTP address LegacyDN Wildcard	-ContentFilter {To -

1.8.3.4 Configure Message Delivery Restrictions

Configure Message Delivery Restrictions

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can place restrictions on how messages are delivered to individual recipients. Message delivery restrictions can be useful for controlling access to specific recipients. To learn more about message delivery restrictions, see Understanding Recipient Restrictions.

The message delivery restrictions covered in this topic apply to all recipient types. To learn more about the recipient types, see Understanding Recipients.

Looking for other management tasks related to Mailbox servers? Check out Managing Mailbox Servers.

Use the EMC to configure message delivery restrictions for all recipients, except mail-enabled public folders

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the recipient for which you want to configure message delivery restrictions.
3. In the action pane, under the recipient name, click **Properties**.
4. In **<Recipient> Properties**, click the **Mail Flow Settings** tab.
5. Select **Message Delivery Restrictions** from the list of mail flow settings, and then click **Properties**.
6. **Message Delivery Restrictions** Select this setting and then click **Properties** to open the **Message Delivery Restrictions** dialog box. Use this dialog box to configure the following settings:
   All senders Click this button to specify that the recipient can accept messages from all senders. This includes senders in both your Exchange organization and external senders. This button is selected by default. This option includes external users only if you clear the **Require that all senders are authenticated** check box. If you select this check box, messages from external users will be rejected.
   Only senders in the following list Click this button to specify that the recipient can accept messages only from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.
   Require that all senders are authenticated Select this check box to prevent anonymous users from sending messages to the recipient.
   No senders Click this button to specify that the recipient will not reject messages from any senders in the Exchange organization. This button is selected by default.
   Senders in the following list Click this button to specify that the recipient will reject messages from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now.**
7. Click **OK** to return to the **Mail Flow Settings** tab.

Use the EMC to configure message delivery restrictions for mail-enabled public folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail-enabled public folders" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Public Folder Management Console**, and then in the action pane, click **Open Tool**. The Public Folder Management Console appears in a separate Microsoft Management Console (MMC).
3. In the console tree, expand **Default Public Folders**, and then click the public folder that you want to configure. If the public folder you want to configure is a top-level public folder, click **Default Public Folders**.
4. In the result pane, click the public folder for which you want to configure message delivery restrictions.
5. In **<Recipient> Properties**, click the **Mail Flow Settings** tab.
6. Select **Message Delivery Restrictions** from the list of mail flow settings, and then click **Properties**.
7. **Message Delivery Restrictions** Select this setting and then click **Properties**

to open the **Message Delivery Restrictions** dialog box. Use this dialog box to configure the following settings:

All senders Click this button to specify that the recipient can accept messages from all senders. This includes senders in both your Exchange organization and external senders. This button is selected by default. This option includes external users only if you clear the **Require that all senders are authenticated** check box. If you select this check box, messages from external users will be rejected.

Only senders in the following list Click this button to specify that the recipient can accept messages only from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.

Require that all senders are authenticated Select this check box to prevent anonymous users from sending messages to the recipient.

No senders Click this button to specify that the recipient will not reject messages from any senders in the Exchange organization. This button is selected by default.

Senders in the following list Click this button to specify that the recipient will reject messages from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now.**

8. Click **OK** to save your changes and return to the **Mail Flow Settings** tab.

Use the Shell to configure message delivery restrictions

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section and the "Mail-enabled public folders" entry in the Mailbox Permissions topic.

The following procedure shows you how to use the Shell to configure message delivery restrictions for a mailbox. For other recipient types, use the corresponding **Set-** cmdlet with the same parameters.

This example configures the mailbox John Smith to accept messages only from the users Lori Penor, Jeff Phillips, and members of the distribution group Sales Department.

```
Set-Mailbox -Identity "John Smith" -AcceptMessagesOnlyFrom "Lori Penor","Jeff Phi
```

Note:

If you're configuring a mailbox to accept messages only from individual senders, you must use the *AcceptMessagesOnlyFrom* parameter. If you're configuring a mailbox to accept messages only from senders that are members of a specific distribution group, you must use the *AcceptMessagesOnlyFromDLMembers* parameter.

This example configures the mailbox John Smith to require all senders to be authenticated.

```
Set-Mailbox -Identity "John Smith" -RequireSenderAuthenticationEnabled $true
```

This example configures the mailbox John Smith to reject messages from the users Joe Healy, Terry Adams, and members of the distribution group Sales Department Contractors.

```
Set-Mailbox -Identity "John Smith" -RejectMessagesFrom "Joe Healy","Terry Adams"
```

Note:
If you're configuring a mailbox to reject messages from individual senders, you must use the *RejectMessagesFrom* parameter. If you're configuring a mailbox to reject messages from senders that are members of a specific distribution group, you must use the *RejectMessagesFromDLMembers* parameter.

For detailed syntax and parameter information, see the following topics:

- Set-DistributionGroup
- Set-DynamicDistributionGroup
- Set-Mailbox
- Set-MailContact
- Set-MailPublicFolder
- Set-MailUser

1.8.3.5 Managing Address Lists

Managing Address Lists

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-20*

Apply an Address List

Create an Address List

Create an Address List By Using Recipient Filters

Create a Global Address List

Configure Address List Properties

Configure Global Address List Properties

Move an Address List

Remove an Address List

Remove a Global Address List

Set the Default Address List View for an Outlook User

Update a Global Address List

View the Members of an Address List by Using the Exchange Management Shell

1.8.3.5.1 Apply an Address List

Apply an Address List

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Address lists are a collection of recipient and other Active Directory objects. You apply an address list when the address list filter rule has been edited. To update the membership of the address list to include new recipients and remove those who no longer meet the filtering criteria, you must apply the address list.

Changes that you make to an address list aren't applied to recipients until you apply the list. You can apply changes to address lists immediately or at a scheduled time by using the New Address List wizard or the Edit Address List wizard.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

What Do You Want to Do?

- Use the EMC to apply an address list
- Use the Shell to apply an address list

Use the EMC to apply an address list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address Lists" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Address Lists** tab, and then click the address list that you want to apply.
3. In the action pane, click **Apply**.
4. On the **Introduction** page, complete the following fields:
   - **Apply the address list** Select one of the following options to specify when the address list should be applied:
     Immediately Click this button to apply the changes immediately.
     At the following time Click this button and use the corresponding list to specify a date and time to apply the changes.
   - **Cancel tasks that are still running after (hours)** Select this check box and use the corresponding text box to specify the length of time that the task is permitted to run. The default is 8 hours.
5. On the **Apply Address List** page, review your configuration settings. Click **Apply** to apply the address list. Click **Back** to make configuration changes.
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. Click **Finish** to close the wizard.

Use the Shell to apply an address list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

This example applies the address list Washington State.

```
Update-AddressList "Washington State"
```

If you have more than one address list with the same name, you must specify the full path to the address list you want to update. For example, if you want to update the address list Sales under North America but there is also a Sales address list under Europe, use the following command:

```
Update-AddressList "North America\Sales"
```

For detailed syntax and parameter information, see Update-AddressList.

1.8.3.5.2 Create an Address List

Create an Address List

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Address lists are a collection of recipient and other Active Directory objects. Each address list can contain one or more types of objects (for example, users, contacts, groups, public folders, conferencing, and other resources). Address lists also provide a mechanism to partition mail-enabled objects in Active Directory for the benefit of specific groups of users.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

What Do You Want to Do?

- Use the EMC to create an address list
- Use the Shell to create an address list

Use the EMC to create an address list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Address List**.
3. On the **Introduction** page, complete the following fields:
   - **Name** Use this box to type the name for the new address list. The name can contain as many as 64 characters, including wildcard characters, but can't contain the backslash character (****).
   - **Display Name** Use this box to type the for the new address list. This is the name that's displayed to users when they view the address list from a client such as Outlook. Although this field is automatically populated with the same name you type in the **Name** box, you can modify it.

- **Container** Click **Browse** to select the path to the container for the address list. To add the address list as a child to an existing address list, click the existing address list you want, and then click **OK**. To create a new parent address list, click **All Address Lists**, and then click **OK**.

4. On the **Filter Settings** page, complete the following fields:
   - **Select the recipient container where you want to apply the filter** The recipient container defines the organizational unit (OU) filter for an address list. Click **Browse** to open the **Select Organizational Unit** dialog box. Use this dialog box to specify the OU from which to select the recipients.
   - Select the recipient types you want to include. You can select **All recipient types** or **The following specific types**. If you select **The following specific types**, you can select one or more of the following recipient types:

     Users with Exchange mailboxes Select this check box if you want the address list to apply to users that have Exchange mailboxes. Users that have Exchange mailboxes are those that have a user domain account and a mailbox in the Exchange organization.

     Users with external e-mail addresses Select this check box if you want the address list to apply to users that have external e-mail addresses. Users that have external e-mail accounts have user domain accounts in Active Directory, but use e-mail accounts that are external to the organization. This enables them to be included in the GAL and added to distribution lists.

     Resource mailboxes Select this check box if you want the address list to apply to Exchange resource mailboxes. Resource mailboxes allow you to administer company resources through a mailbox, such as a conference room or company vehicle.

     Contacts with external e-mail addresses Select this check box if you want the address list to apply to contacts that have external e-mail addresses. Contacts that have external e-mail accounts don't have user domain accounts in Active Directory, but the external e-mail address is available in the GAL.

     Mail-enabled groups Select this check box if you want the address list to apply to security groups or distribution groups that have been mail-enabled. Mail-enabled groups are similar to distribution groups. E-mail messages that are sent to a mail-enabled group account will be delivered to several recipients.

     Note:

     If your address list contains distribution groups that aren't universal, these distribution groups aren't displayed when you preview the address list in the EMC. To make sure that all distribution groups are displayed when you click the **Preview** button (as described in Step 5), you must convert the non-universal distribution groups to universal distribution groups. For more information about converting a distribution group to a universal distribution group, see the example in Set-Group.

5. On the **Conditions** page, complete the following fields:

   Step 1: Select conditions Use this section to select one or more conditions for your address list. If you don't want to set any conditions for the list, don't select any of the check boxes.
   - **Recipient is in a State or Province** Select this check box if you want the address list to include only recipients from specific states or provinces. This information is contained on the **Address and Phone** tab in the recipient's properties.
   - **Recipient is in a Department** Select this check box if you want the address list to include only recipients in specific departments. This information is contained on the **Organization** tab in the recipient's

properties.

- **Recipient is in a Company** Select this check box if you want the address list to include only recipients in specific companies. This information is contained on the **Organization** tab in the recipient's properties.
- **Custom Attribute equals Value** There are 15 custom attributes for each recipient. There is a separate condition for each custom attribute. If you want the address list to include only recipients that have a specific value set for a specific custom attribute, select the check box that corresponds to that custom attribute.

Note:

The **State or Province**, **Department**, and **Company** conditions are based on attributes that are applicable only to mailboxes, mail users, and mail contacts. These conditions do not apply to mail-enabled distribution groups. If you configure any of these conditions for an address list, you will in effect be excluding all mail-enabled distribution groups.

Step 2: Edit the conditions by selecting an underlined value: If you select any conditions in Step 1, each condition you select will append to the definition of the address list. For example, if you selected the **Recipient is in a State or Province** check box in Step 1, you will see the **in the specified State or Province(s)** condition in Step 2.
For each condition, click the underlined term to create your condition. By default, the underlined term for new conditions will read **specified**. After you edit the condition, the underlined term will change to the value that you specified.
If you click an underlined value for the **State or Province**, **Department**, or **Company** conditions, a dialog box appears in which you can specify the values for the condition. To create values for the condition, use the following buttons in the dialog box:

- **Add** Enter a value in the text box and click **Add**. You can add more than one value, but you cannot enter duplicate values.
- **Edit** To modify an existing value, select it from the list, and then click **Edit**.
-  To remove an existing value, select it from the list, and then click  .

If you click an underlined value for a custom attribute condition, a dialog box appears in which you can specify the value for the condition. You can specify a single value for each custom attribute. Type the value in the text box and click **OK**.

Important:

The values that you enter in these dialog boxes must exactly match those that appear in the recipient's properties. For example, if you enter **Washington** in the **Specify State or Province** dialog box, but the **Address and Phone** tab in the recipient's properties lists the state as **WA**, the condition will not be met.

Preview Click this button to view the recipients that will be contained in the address list, based on the conditions that you specified.

6. On the **Schedule** page, complete the following fields:
Apply the address list Select one of the following options to specify when the address list should be applied:
   - **Do not apply** Click this button to create the address list without applying it to recipients. To apply this address list to the selected recipients, use the **Update-AddressList** cmdlet or the Apply Address List wizard. For more information, see Apply an Address List.
   - **Immediately** Click this button to apply the address list as soon as it is created.
   - **At the following time** Click this button and use the corresponding lists to specify a time to apply the new address list.

   Cancel tasks that are still running after (hours) Select this check box and use the corresponding text box to specify how long the new address list task

will run. The default is 8 hours.

7. On the **New Address List** page, review your configuration settings. Click **New** to create the address list. Click **Back** to make configuration changes.

8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
9. Click **Finish** to close the wizard.

Use the Shell to create an address list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

This example creates the address list MyAddressList by using the *RecipientFilter* parameter and includes recipients that are mailbox users and have `StateOrProvince` set to `Washington` or `Oregon`:

```
New-AddressList -Name MyAddressList -RecipientFilter {((RecipientType -eq 'UserMa
```

This example creates the child address list Building 34 Meeting Rooms in the All Rooms parent container, using built-in conditions.

```
New-AddressList -Name "Building 34 Meeting Rooms" -Container "\All Rooms" -Includ
```

Other Tasks

After you create an address list in the Shell, you must apply it. Use the **Update-AddressList** cmdlet or the Apply Address List wizard to apply the address list. For more information, see Apply an Address List.

For More Information

Configure Address List Properties

Understanding Address Lists

1.8.3.5.3 Create an Address List By Using Recipient Filters

Create an Address List By Using Recipient Filters

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-09*

This topic explains how to use the Exchange Management Shell to create an address list by using recipient filters. To learn more about address lists, see Managing Address Lists.

To use the *RecipientFilter* parameter to create a custom filter, you must specify a string for the filter. The Shell uses OPATH for the filtering syntax. OPATH is a querying language

designed to query object data sources. For more information about the OPATH filtering syntax, see Creating Filters in Recipient Commands.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Use the Shell to create an address list by using recipient filters

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:
You can't use the EMC to create an address list by using recipient filters.

To create an address list by using the *RecipientFilter* parameter, use the following syntax.

```
New-AddressList -Name <String> -RecipientFilter <String>
```

This example creates an address list for all users with Exchange mailboxes who reside in Washington or Oregon.

```
New-AddressList -Name "Pacific Northwest Mailboxes" -RecipientFilter {((Recipient
```

This example creates an address list for all users with Exchange mailboxes who have AgencyB as the value for the *CustomAttribute15* parameter.

```
New-AddressList -Name "AgencyB" -RecipientFilter {(RecipientType -eq 'UserMailbox
```

For detailed syntax and parameter information, see New-AddressList.

1.8.3.5.4 Configure Address List Properties

Configure Address List Properties

Mailbox > Managing Mailbox Servers > Managing Address Lists >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Address lists are a collection of recipient and other Active Directory objects. Each address list can contain one or more types of objects (for example, users, contacts, groups, public folders, conferencing, and other resources). Address lists also provide a mechanism to partition mail-enabled objects in Active Directory for the benefit of specific groups of users.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Prerequisites

- You can't use the Exchange Management Console (EMC) to edit global address lists (GALs). You can only edit GALs by using the **Set-GlobalAddressList** cmdlet in the Shell.
- You can't use the EMC to move the address list from its container. You must

use the **Move-AddressList** cmdlet in the Shell. For more information, see Move an Address List.

- You can't use the EMC to edit the conditions or recipient types of the following default address lists: **All Contacts**, **All Groups**, **All Rooms**, **All Users**, and **Public Folders**. You must use the Shell to edit these default address lists.

What Do You Want to Do?

- Use the EMC to configure address list properties
- Use the Shell to configure address list properties

Use the EMC to configure address list properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Address List** tab, and then select the address list you want to configure.
3. In the action pane, click **Edit**.
4. On the **Introduction** page, complete the following fields:
   - **Name** Use this box to view the existing name or to type a new name for the address list. The name can contain as many as 64 characters, including wildcard characters, but can't contain the backslash (****) character.
   - **Display Name** Use this box to view the existing display name or to type a new display name for the address list. This is the name that's displayed to users when they view the address list from a client such as Outlook.
   - **Container** This read-only box displays the path to the address list's container that you specified when you created the list.
5. On the **Filter Settings** page, complete the following fields:

Note:

If you created this address list by using a recipient filter in the Shell, you can't edit the recipient types. You must use the Shell to modify the filter. For more information, see Create an Address List By Using Recipient Filters.

- **Select the Recipient container where you want to apply the filter** The recipient container defines the organizational unit (OU) filter for an address list. Click **Browse** to open the **Select Organizational Unit** dialog box. Use this dialog box to specify the OU from which to select the recipients.
- Select the recipient types you want to include. You can select **All recipient types** or **The following specific types**. If you select **The following specific types**, you can select one or more of the following recipient types:

  Users with Exchange mailboxes Select this check box if you want the address list to apply to users that have Exchange 2010 mailboxes. Users that have Exchange mailboxes are those that have a user domain account and a mailbox in the Exchange organization.

  Users with external e-mail addresses Select this check box if you want the address list to apply to users that have external e-mail addresses. Users that have external e-mail accounts have user domain accounts in Active Directory, but use e-mail accounts that are external to the organization. This enables them to be included in the GAL and added to distribution lists.

  Resource mailboxes Select this check box if you want the address list to apply to Exchange resource mailboxes. Resource mailboxes allow you to administer company resources through a

mailbox, such as a conference room or company vehicle.
Contacts with external e-mail addresses Select this check box if you want the address list to apply to contacts that have external e-mail addresses. Contacts that have external e-mail accounts don't have user domain accounts in Active Directory, but the external e-mail address is available in the GAL.
Mail-enabled groups Select this check box if you want the address list to apply to security groups or distribution groups that have been mail-enabled. Mail-enabled groups are similar to distribution groups. E-mail messages that are sent to a mail-enabled group account will be delivered to several recipients.

Note:
If your address list contains distribution groups that aren't universal, these distribution groups aren't displayed when you preview the address list in the EMC. To make sure that all distribution groups are displayed when you click the **Preview** button (as described in Step 6), you must convert the non-universal distribution groups to universal distribution groups. For more information about converting a distribution group to a universal distribution group, see the example in Set-Group.

6. On the **Conditions** page, complete the following fields:
Step 1: Select conditions Use this section to edit or set conditions for your address list. If you don't want to set any conditions for the list, don't select any of the check boxes.
- **Recipient is in a State or Province** Select this check box if you want the address list to include only recipients from specific states or provinces. This information is contained on the **Address and Phone** tab in the recipient's properties.
- **Recipient is in a Department** Select this check box if you want the address list to include only recipients in specific departments. This information is contained on the **Organization** tab in the recipient's properties.
- **Recipient is in a Company** Select this check box if you want the address list to include only recipients in specific companies. This information is contained on the **Organization** tab in the recipient's properties.
- **Custom Attribute equals Value** There are 15 custom attributes for each recipient. There is a separate condition for each custom attribute. If you want the address list to include only recipients that have a specific value set for a specific custom attribute, select the check box that corresponds to that custom attribute.

Note:
The **State or Province**, **Department**, and **Company** conditions are based on attributes that are applicable only to mailboxes, mail users, and mail contacts. These conditions do not apply to mail-enabled distribution groups. If you configure any of these conditions for an address list, you will in effect be excluding all mail-enabled distribution groups.

Step 2: Edit the conditions by selecting an underlined value If you select any conditions in Step 1, each condition you select will append to the definition of the address list. For example, if you selected the **Recipient is in a State or Province** check box in Step 1, you will see **in the specified State or Province(s)** condition in Step 2.
For each condition, click the underlined term to create your condition. By default, the underlined term for new conditions will read **specified**. After you edit the condition, the underlined term will change to the value that you specified.
If you click an underlined value for the **State or Province**, **Department**, or **Company** conditions, a dialog box appears in which you can specify the

values for the condition. To create values for the condition, use the following buttons in the dialog box:

- **Add** Enter a value in the text box and click **Add**. You can add more than one value, but you cannot enter duplicate values.
- **Edit** To modify an existing value, select it from the list, and then click **Edit**.
-  To remove an existing value, select it from the list, and then click  .

If you click an underlined value for a custom attribute condition, a dialog box appears in which you can specify the value for the condition. You can specify a single value for each custom attribute. Type the value in the text box, and then click **OK**.

Important:

The values that you enter in these dialog boxes must exactly match those that appear in the recipient's properties. For example, if you enter **Washington** in the **Specify State or Province** dialog box, but the **Address and Phone** tab in the recipient's properties lists the state as **WA**, the condition will not be met.

7. On the **Schedule** page, complete the following fields:
   Apply the address list Select one of the following options to specify when the address list changes are applied:
   - **Do not apply** Click this button if you don't want to apply the changes. To apply this address list to the selected recipients, use the **Update-AddressList** cmdlet or the Apply Address List wizard. For more information, see Apply an Address List.
   - **Immediately** Click this button to apply the changes immediately.
   - **At the following time** Click this button and use the corresponding lists to specify a time to apply the changes.

   Cancel tasks that are still running after (hours) Select this check box and use the corresponding text box to specify the length of time that the task is permitted run. The default is 8 hours.

8. On the **Edit Address List** page, review your configuration settings. Click **Edit** to apply your changes to the address list. Click **Back** to make configuration changes.

9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
10. Click **Finish** to close the wizard.

Use the Shell to configure address list properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

This example configures the address list Contoso California Branch to include recipients that work in the branch office of the company Contoso in California:

```
Set-AddressList -Identity "Contoso California Branch" -ConditionalCompany Contoso
```

1.8.3.5.5 Move an Address List

Move an Address List

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Exchange Management Shell to move an existing address list to a new container under the root address list.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Use the Shell to move an address list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to move an address list.

This example uses the address list's GUID to move the address list to the Building 4 container, which is located in the All Users\Sales container.

```
Move-AddressList -Identity c3fffd8e-026b-41b9-88c4-8c21697ac8ac -Target "\All Use
```

Type **Y** to confirm that you want to move this address list, and then press ENTER.

For detailed syntax and parameter information, see Move-AddressList.

1.8.3.5.6 Remove an Address List

Remove an Address List

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) or the Exchange Management Shell to remove an address list. You can't remove the default global address list (GAL).

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Use the EMC to remove an address list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Address Lists** tab, click the address list that you want to remove.
3. In the action pane, click **Remove**. A warning appears, asking if you are sure

that you want to remove the address list. Click **Yes** to remove the address list.

4. You can track the progress in the status bar on the bottom of the EMC. When the process is complete, the address list will be removed from the result pane.

Note:

You can't remove a parent address list that contains child address lists. However, you can remove both the child and parent address lists by pressing the CTRL key on the keyboard, and then selecting the parent and child address lists. If you attempt to remove a parent address list without removing the child address lists, you'll receive an error.

Use the Shell to remove an address list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

To remove an address list, use the following syntax.

```
Remove-AddressList -Identity <AddressListIDParameter>
```

This example removes the address list Sales Department, which doesn't contain child address lists.

```
Remove-AddressList -Identity "Sales Department"
```

Type **Y** to confirm that you want to remove this address list, and then press ENTER.

For detailed syntax and parameter information, see Remove-AddressList.

Use the Shell to remove an address list that contains child address lists

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to remove an address list that contains child address lists.

To remove an address list that contains child address lists, use the following syntax.

```
Remove-AddressList -Identity <AddressListIDParameter> -Recursive
```

This example removes the parent address list Departments and all of its child address lists.

```
Remove-AddressList -Identity Departments -Recursive
```

Type **Y** to confirm that you want to remove the parent address list and its child address lists, and then press ENTER.

For detailed syntax and parameter information, see Remove-AddressList.

1.8.3.5.7 View the Members of an Address List by Using the Exchange Management Shell

View the Members of an Address List by Using the Exchange Management Shell

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Exchange Management Shell to view the members of an address list.

You can view the members of an address list by using the Edit Address List wizard or the New Address List wizard in the Exchange Management Console (EMC). However, if you used the Shell to create the address list, you can't use the EMC to view the members of the list. Instead, you must use the **Get-Recipient** cmdlet in the Shell. For more information about how to view the members of an address list by using the EMC, see Configure Address List Properties.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Use the Shell to view the members of an address list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to view the members of an address list that was created using the Shell.

This example finds the distinguished name (DN) of an address list named Humongous Insurance.

```
Get-AddressList -Identity "Humongous Insurance" | fl DistinguishedName
```

This example lists the members of the Humongous Insurance address list by using the DN.

```
Get-Recipient -Filter {AddressListMembership -eq 'CN=Humongous Insurance,CN=All A
```

For detailed syntax and parameter information, see Get-AddressList and Get-Recipient.

1.8.3.5.8 Set the Default Address List View for an Outlook User

Set the Default Address List View for an Outlook User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Microsoft Exchange Server 2010 Service Pack 1 (SP1), you can determine whether the global address list (GAL) should be the default address list displayed to Microsoft Outlook

users. If users aren't intended to use the GAL as their default view, you can configure it so that Outlook automatically displays the user's Contacts list instead. However, Outlook users can still view the GAL by using the Address Book list. By default, the GAL is displayed to all users.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Use the Shell to set the default address list view for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access user settings" entry in the Client Access Permissions topic.

Note:
You can't use the EMC to set the default address list view for a user.

This example sets Tony's Contacts list as his default view in Outlook.

```
Set-CASMailbox -Identity Tony -ShowGalAsDefaultView $false
```

This example sets Ayla's GAL as her default view in Outlook.

```
Set-CASMailbox -Identity Ayla -ShowGalAsDefaultView $true
```

For detailed syntax and parameter information, see Set-CASMailbox.

1.8.3.5.9 Create a Global Address List

Create a Global Address List

Mailbox > Managing Mailbox Servers > Managing Address Lists >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-18*

The global address list (GAL) is a directory that contains entries for every group, user, and contact within an organization's implementation of Microsoft Exchange. If your organization uses address book policies, you may want to create additional GALs. To learn more, see Understanding Address Book Policies.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Use the Shell to create a GAL using conditional filter properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Global address lists" entry in the Mailbox Permissions topic.

Note:
You can't use the Exchange Management Console to create a GAL.

This example creates a GAL named GAL_Contoso that includes recipients who are mailbox users and have their company listed as Contoso.

```
New-GlobalAddressList -Name "GAL_Contoso" -IncludedRecipients MailboxUsers -Condi
```

Note:
If you are using precanned conditional filter properties, the *IncludedRecipients* parameter can't be blank.

For detailed syntax and parameter information, see New-GlobalAddressList.

Use the Shell create a GAL using a recipient filter

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Global address lists" entry in the Mailbox Permissions topic.

Note:
You can't use the Exchange Management Console to create a GAL.

This example creates a GAL named GAL_AgencyA that includes recipients for which the *CustomAttribute15* parameter has a value of AgencyA.

```
New-GlobalAddressList -Name "GAL_AgencyA" -RecipientFilter {CustomAttribute15 -li
```

For more information about recipient filters, see Creating Filters in Recipient Commands.

For detailed syntax and parameter information, see New-GlobalAddressList.

1.8.3.5.10 Configure Global Address List Properties

Configure Global Address List Properties

Mailbox > Managing Mailbox Servers > Managing Address Lists >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to modify a global address list's (GAL) settings by using the Exchange Management Shell.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Important:
You can't edit the settings of the default GAL.

Use the Shell to configure GAL properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to modify a GAL.

This example assigns a new name, FourthCoffee, to the GAL that has the GUID 96d0c505-eba8-4103-ad4f-577a1bf4ad7b.

```
Set-GlobalAddressList -Identity 96d0c505-eba8-4103-ad4f-577a1bf4ad7b -Name Fourth
```

Note:

If you're using precanned conditional filter properties, the value for the *IncludedRecipients* parameter can't be blank.

This example changes the recipients who will be included in the Fourth Coffee global GAL to those whose company is set to Fourth Coffee.

```
Set-GlobalAddressList -Identity Fourth Coffee -RecipientFilter {Company -eq "Four
```

For detailed syntax and parameter information, see Set-GlobalAddressList.

Other Tasks

After you make changes to a GAL, you may also want to update the GAL. For detailed steps, see Update a Global Address List.

1.8.3.5.11 Remove a Global Address List

Remove a Global Address List

Mailbox > Managing Mailbox Servers > Managing Address Lists >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The global address list (GAL) is a directory that contains entries for every group, user, and contact within an Exchange organization.

Important:

You can't remove the default GAL.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Use the Shell to remove a GAL

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Global address lists" entry in the Mailbox Permissions topic.

Note:

You can't use the Exchange Management Console (EMC) to remove a GAL.

This example removes the GAL Fourth Coffee from the domain controller ad-server.fourthcoffee.com.

```
Remove-GlobalAddressList -Identity "Fourth Coffee" -DomainController ad-server.fo
```

To confirm that you want to remove the GAL, type **Y**, and then press ENTER.

For detailed syntax and parameter information, see Remove-GlobalAddressList.

1.8.3.5.12 Update a Global Address List

Update a Global Address List

Mailbox > Managing Mailbox Servers > Managing Address Lists >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can use the Shell to update a global address list (GAL). A GAL is a directory that contains entries for every group, user, and contact within an organization's implementation of Microsoft Exchange.

Looking for other management tasks related to address lists? Check out Managing Address Lists.

Use the Shell to update a GAL

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Global address lists" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to update a GAL.

To update a GAL, use the following syntax.

```
Update-GlobalAddressList -Identity <GlobalAddressListIdParameter> -DomainControll
```

Note:
Running this command only starts the update process. It may take several hours for the GAL to be updated.

This example updates a GAL for the Fourth Coffee company.

```
Update-GlobalAddressList -Identity "Fourth Coffee"
```

For detailed syntax and parameter information, see Update-GlobalAddressList.

1.8.3.6 Managing Address Book Policies

Managing Address Book Policies

Exchange Server 2010 > Mailbox > Managing Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-18*

- Create an Address Book Policy
- Configure Address Book Policy Properties
- Assign an Address Book Policy to a Mail User
- Remove an Address Book Policy

- Understanding Address Book Policies
- Migrate to Exchange 2010 Address Book Policies from Exchange 2007 Address List Segregation

1.8.3.6.1 Create an Address Book Policy

Create an Address Book Policy

Mailbox > Managing Mailbox Servers > Managing Address Book Policies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-29*

Address book policies (ABPs) allow you to segment users into specific groups to provide customized views of your organization's global address list (GAL). When creating an ABP, you assign a GAL, an offline address book (OAB), a room list, and one or more address lists to the policy. You can then assign the ABP to mailbox users, providing them with access to a customized GAL in Outlook and Outlook Web App. The goal is to provide a simpler mechanism to accomplish GAL segmentation for on-premises organizations that require multiple GALs. To learn more about ABPs, see Understanding Address Book Policies.

Looking for other management tasks related to ABPs? Check out Managing Address Book Policies.

What Do You Want to Do?

- Use the EMC to create an address book policy
- Use the Shell to create an address book policy

Use the EMC to create an address book policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address book policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Address Book Policy**.
3. On the **Introduction** page, complete the following fields:
   - **Name** Use this field to type the name of the ABP. This field accepts a maximum of 64 characters.
   - **Global address list** Click **Browse** to select a GAL to assign to this policy. Each ABP must contain one GAL.
   - **Offline address book** Click **Browse** to select an OAB to assign to this policy. Users who are assigned to this ABP will download the OAB you specify. Each ABP must contain one OAB.
   - **Room list** Click **Browse** to select a room list. The room list is used for room booking purposes. Each ABP must contain one room list. If your organization doesn't use room lists, we recommend that you create one that doesn't contain rooms, and then assign it to the ABP.
   - **Address Lists** Click **Add** to add one or more address lists to the ABP.
4. Click **New** to create the ABP.

5. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to close the wizard.

Use the Shell to create an address book policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address book policies" entry in the Mailbox Permissions topic.

This example creates an ABP with the following settings:

- **Name:** All Fabrikam ABP
- **GAL:** All Fabrikam
- **OAB:** Fabrikam-All-OAB
- **Room list:** All Fabrikam Rooms
- **Address lists:** All Fabrikam, All Fabrikam Mailboxes, All Fabrikam DLs, and All Fabrikam Contacts.

```
New-AddressBookPolicy -Name "All Fabrikam ABP" -AddressLists "\All Fabrikam","\Al
```

For detailed syntax and parameter information, see New-AddressBookPolicy.

Other Tasks

After you create the ABP, you may want to assign it to a user. For details, see Assign an Address Book Policy to a Mail User.

1.8.3.6.2 Configure Address Book Policy Properties

Configure Address Book Policy Properties

Mailbox > Managing Mailbox Servers > Managing Address Book Policies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-29*

After you create an address book policy (ABP), you can view or modify the name and the assigned global address list (GAL), offline address book (OAB), room list, and address lists

Looking for other management tasks related to ABPs? Check out Managing Address Book Policies.

What Do You Want to Do?

- Use the EMC to configure ABP properties
- Use the Shell to configure ABP properties

Use the EMC to configure ABP properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address book policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Address Book Policies** tab, click the ABP you want to configure.
3. In the action pane, click **Properties**.
4. Use the **General** tab to view or modify the name of the ABP.
5. Use the **Address Book Policy Detail** tab to view or modify the following settings:
   - **Global Address List** Click **Browse** to change the GAL that's assigned to this policy. Each ABP must contain one GAL.
   - **Offline Address Book** Click **Browse** tochange the OAB that's assigned to this policy. Users who are assigned to this ABP will download the OAB you specify. Each ABP must contain one OAB.
   - **Room list** Click **Browse** to change the room list that's assigned to this policy. The room list is used for room booking purposes. Each ABP must contain one room list. If your organization doesn't use room lists, we recommend that you create one that doesn't contain rooms, and then assign it to the ABP.
   - **Address Lists** Click **Add** to add address lists to the ABP. Click  to remove an address list from the ABP.

Use the Shell to configure ABP properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address book policies" entry in the Mailbox Permissions topic.

This example changes the OAB, room list, and GAL that will be used by mailbox users who are assigned the ABP named All Fabrikam ABP.

```
Set-AddressBookPolicy -Identity "All Fabrikam ABP" -OfflineAddressBook \Fabrikam-
```

This example adds the address lists Contoso-Chicago and Contoso-Seattle to the ABP named ABPContoso

```
Set-AddressBookPolicy -Identity "ABPContoso" -AddressLists @{Add="Contoso-Chicago
```

This example removes the address lists Fabrikam-HR and Fabrikam-Finance from the ABP named ABPFabrikam

```
Set-AddressBookPolicy -Identity "ABPFabrikam" -AddressLists @{Remove="Fabrikam-HR
```

This example replaces the address lists GovernmentAgencyA-ALL and GovernmentAgenceB-ALL with address lists GovernmentAgencyA-Atlanta and GovernmentAgencyA-Moscow for the ABP named GovernmentAgencyA.

```
Set-AddressBookPolicy -Identity GovernmentAgencyA -AddressLists @{Remove="Governm
```

For detailed syntax and parameter information, see Set-AddressBookPolicy.

Assign an Address Book Policy to a Mail User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

After you create an address book policy (ABP), you must assign it to mailbox users. Users aren't assigned a default ABP when their user account is created. If you don't assign an ABP to a user, the global address list (GAL) for your entire organization will be accessible to the user through Outlook and Outlook Web App. To learn more, see Understanding Address Book Policies.

Looking for other management tasks related to ABPs? Check out Managing Address Book Policies.

Prerequisites

You have an existing ABP. If you haven't created one, see Create an Address Book Policy.

Use the EMC to assign an ABP to mailbox users

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address book policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox user or users to which you want to assign the ABP. You can select multiple users by holding down the Ctrl key.
3. In the action pane, click **Properties**.
4. In **<User Mailbox> Properties**, on the **Mailbox Settings** tab, click **Address Book Policy**, and then click **Properties**.
5. In **Address Book Policy**, select the **Address Book Policy** check box, and then click **Browse**.
6. In **Select Address Book Policy**, select the ABP you want to assign to the user or users, and then click **OK**.
7. In **Address Book Policy**, click **OK** .
8. In **<User Mailbox> Properties**, click **OK** to apply the ABP and close the property page.

Note:

If you apply the ABP to more than one mailbox user, the **Bulk Edit Summary** dialog box will appear. Confirm the changes, and then click **OK**.

Use the Shell to assign an ABP to mailbox users

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address book policies" entry in the Mailbox Permissions topic.

This example assigns the ABP named All Fabrikam to the existing mailbox user joe@fabrikam.com.

```
Set-Mailbox -Identity joe@fabrikam.com -AddressBookPolicy "All Fabrikam"
```

This example assigns the ABP named ABP_EngineeringDepartment to all mailbox users whose CustomAttribute11 value contains "Engineering Department".

```
Get-Mailbox -Filter {(CustomAttribute11 -like "Engineering Department")} | Set-Ma
```

For detailed syntax and parameter information, see Set-Mailbox and Get-Mailbox.

1.8.3.6.4 Remove an Address Book Policy

Remove an Address Book Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Use this procedure to remove an address book policy (ABP).

Looking for other management tasks related to ABPs? Check out Managing Address Book Policies.

Prerequisites

You can't remove an ABP if it is assigned to a user's mailbox. To determine if an ABP is assigned to a user, run the following command in the Shell:

```
Get-Mailbox | Where $._AddressBookPolicy -eq <AddressBookPolicyName>
```

To remove an ABP from a user's mailbox, you can use the **Mailbox Settings** tab of the mailbox's property page or the **Set-Mailbox** cmdlet. For details, see Configure User and Resource Mailbox Properties.

Use the EMC to remove an ABP

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address book policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Address Book Policies** tab, select the ABP you want to remove.
3. In the action pane, click **Remove**.
4. In the warning dialog box that appears, click **Yes** to remove the ABP.

Use the Shell to remove an ABP

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address book policies" entry in the Mailbox Permissions topic.

This example removes the ABP named ABP_TailspinToys

```
Remove-AddressBookPolicy -Identity "ABP_TailspinToys"
```

For detailed syntax and parameter reference, see Remove-AddressBookPolicy.

1.8.3.7 Managing Automatic Replies

Managing Automatic Replies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-21*

Enable External Automatic Replies on a Per-User Basis

1.8.3.7.1 Enable External Automatic Replies on a Per-User Basis

Enable External Automatic Replies on a Per-User Basis

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to configure the *Automatic Replies* feature on a per-user basis. For example, you can configure Automatic Replies so that users in the Sales and Marketing divisions can send automatic reply messages to external contacts, but users in the Research division can't. By default, the Automatic Replies feature allows all users to send external automatic reply messages.

Use the Shell to enable external automatic replies

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

You can't use the EMC to enable external automatic replies.

This example enables the external automatic reply messages for Ellen Adams' mailbox.

```
Set-Mailbox "Ellen Adams" -ExternalOofOptions External
```

For detailed syntax and parameter information, see Set-Mailbox.

1.8.3.8 Managing Calendars

Managing Calendars

Exchange Server 2010 > Mailbox > Managing Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-16*

Configure Calendar Repair Log Settings

Configure Calendar Repair Assistant Settings

Enable or Disable Calendar Repair for a Mailbox

Enable Internet Calendar Publishing

Disable Internet Calendar Publishing

1.8.3.8.1 Configure Calendar Repair Log Settings

Configure Calendar Repair Log Settings

Mailbox > Managing Mailbox Servers > Managing Calendars >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Every time the Calendar Repair Assistant (CRA) changes a calendar item on a user's mailbox, it writes to a log file. The log file contains information that identifies the calendar item that was repaired and what repair actions occurred. By default, calendar repair logging is enabled.

You can use the following **Set-MailboxServer** cmdlet parameters to configure calendar repair log settings:

- *CalendarRepairLogEnabled*
- *CalendarRepairLogPath*
- *CalendarRepairLogFileAgeLimit*
- *CalendarRepairLogDirectorySizeLimit*
- *CalendarRepairLogSubjectLoggingEnabled*

Looking for other tasks related to calendar repair? Check out Managing Calendars.

Use the Shell to enable or disable calendar repair logging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to configure calendar repair log settings.

This example disables calendar repair logging for the server MBX01.

```
Set-MailboxServer -Identity MBX01 -CalendarRepairLogEnabled $false
```

This example enables calendar repair logging for the server MBX01.

```
Set-MailboxServer -Identity MBX01 -CalendarRepairLogEnabled $true
```

For detailed syntax and parameter reference, see Set-MailboxServer.

Use the Shell to change the calendar repair log path

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure calendar repair log settings.

The default installation path for the calendar repair log is *<Exchange installation path>*\v14\Logging\Calendar Repair Assistant.

This example changes the log file path to C:\Log Files\Calendar Repair Assistant for the server MBX01.

```
Set-MailboxServer -Identity MBX01 -CalendarRepairLogPath "C:\Log Files\Calendar R
```

For detailed syntax and parameter reference, see Set-MailboxServer.

Use the Shell to change the calendar repair log file age limit

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure calendar repair log settings.

The log file age limit specifies how long to retain calendar repair logs. Log files that exceed the maximum retention period are deleted. The default value for the age limit is 00.00:00:00, which means that there is no limit and all log files are retained.

This example changes the calendar repair log age limit to 90 days for the server MBX01.

```
Set-MailboxServer -Identity MBX01 -CalendarRepairLogFileAgeLimit 90
```

For detailed syntax and parameter reference, see Set-MailboxServer.

Use the Shell to change the calendar repair log directory size limit

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure calendar repair log settings.

The directory size limit determines the size limit for all Calendar Repair Assistant log files on a Mailbox server. After the limit is reached, the oldest files are deleted. The default size value is unlimited.

This example changes the calendar repair log directory size limit to 1 gigabyte (GB) for the server MBX01.

```
Set-MailboxServer -Identity MBX01 -CalendarRepairLogDirectorySizeLimit 1GB
```

For detailed syntax and parameter reference, see Set-MailboxServer.

Use the Shell to enable or disable logging the subject of meetings in the log files

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox server configuration" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure calendar repair log settings.

You can include the subject of repaired calendar items in the calendar repair logs. By default, subject logging is enabled.

This example disables subject logging for the Mailbox server MBX01.

```
Set-MailboxServer MBX01 -CalendarRepairLogSubjectLoggingEnabled $false
```

For detailed syntax and parameter reference, see Set-MailboxServer.

1.8.3.8.2 Configure Calendar Repair Assistant Settings

Configure Calendar Repair Assistant Settings

See Also

Mailbox > Managing Mailbox Servers > Managing Calendars >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-28*

The *Calendar Repair Assistant* (CRA) is a configurable mailbox assistant that runs within the Microsoft Exchange Mailbox Assistants service on Microsoft Exchange Server 2010 Mailbox servers. The CRA detects and corrects inconsistencies that occur in single and recurring calendar items for mailboxes that are homed on the Mailbox server that is running the CRA. The purpose of this process is to make sure that recipients won't miss meetings or have unreliable meeting information.

In Exchange 2010 Service Pack 1 (SP1), the CRA was changed from a time-based assistant to a throttle-based assistant.

By default, the CRA is not set to run automatically. To configure the CRA to run and repair calendar inconsistencies, use the **set-mailboxserver** cmdlet in the Exchange Management Shell to set the work cycle and work cycle checkpoint. The Exchange Management Console cannot be used to configure calendar repair log settings.

You must use the following **Set-MailboxServer** cmdlet parameters to configure the CRA settings:

- *CalendarRepairIntervalEndWindow* This parameter specifies the number of days into the future to repair calendars. For example, if this parameter is set to 90, the CRA repairs calendars on the Mailbox server 90 days from the date it was set. The default value is 30 days.
- *CalendarRepairMissingItemFixDisabled* This parameter specifies that the CRA won't fix missing attendee calendar items for mailboxes homed on this Mailbox server. If an attendee is missing a calendar item, the item will be re-created. The default value is `$false`.
- *CalendarRepairWorkCycle* and *CalendarRepairWorkCycleCheckpoint* These parameters work together. The *CalendarRepairWorkCycle* parameter specifies the time span in which all mailboxes on the specified server will be scanned by the CRA. For example, if you specify seven days for this parameter, the CRA will process all mailboxes on this server every seven days. Calendars that have inconsistencies will be flagged and repaired according to the interval specified by the *CalendarRepairWorkCycleCheckpoint* parameter. For example, if you specify one day for this parameter, the CRA will query every day for new mailboxes that require processing.

Looking for other management tasks related to calendar repair? Check out Managing Calendars.

Use the Shell to change the calendar repair interval window

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar repair" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to change the calendar repair interval window.

This example changes the number of days into the future that the CRA validates calendars to 90 days on Mailbox server MBX02.

```
Set-MailboxServer -Identity MBX02 -CalendarRepairIntervalEndWindow 90
```

For detailed syntax and parameter information, see Set-MailboxServer.

Use the Shell to set the calendar repair work cycle

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar repair" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to set the calendar repair work cycle.

This example sets the CRA to check all mailboxes on the server MBX02 every seven days and to process all calendars that require repairs every day in that seven day cycle.

```
Set-MailboxServer -Identity MBX02 -CalendarRepairWorkCycle 7.00:00:00 -CalendarRe
```

For detailed syntax and parameter information, see Set-MailboxServer.

Use the Shell to enable or disable the fixing of missing items

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar repair" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to enable or disable the fixing of missing items.

This example disables the automatic fixing of missing calendar items for Mailbox server MBX02.

```
Set-MailboxServer -Identity MBX02 -CalendarRepairMissingItemFixDisabled $true
```

For detailed syntax and parameter information, see Set-MailboxServer.

See Also

Concepts

Understanding Calendar Repair
Managing Calendars

1.8.3.8.3 Enable or Disable Calendar Repair for a Mailbox

Enable or Disable Calendar Repair for a Mailbox

See Also

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-28*

The *Calendar Repair Assistant* (CRA) is a configurable, throttle-based Mailbox Assistant that runs within the Microsoft Exchange Mailbox Assistants service on Mailbox servers that run Microsoft Exchange Server 2010. CRA detects and corrects inconsistencies that occur for single and recurring calendar items for mailboxes that are homed on the Mailbox server that is running CRA. The purpose of this process is to make sure that recipients won't miss meetings or have unreliable meeting information.

By default, the CRA is not set to run automatically. To configure the CRA to run and repair calendar inconsistencies, use the **set-mailboxserver** cmdlet in the Exchange Management Shell to set the work cycle and work cycle checkpoint. The Exchange Management Console cannot be used to configure calendar repair log settings.

You can turn on or turn off calendar repair for a mailbox by using the **Set-Mailbox** cmdlet in the Shell.

Looking for other management topics related to calendar repair? Check out Managing Calendars.

Use the Shell to disable calendar repair for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar repair" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to disable calendar repair for a mailbox.

Mailboxes for which calendar repair is disabled won't have their calendar items repaired by the CRA.

This example disables the CRA for the user mailbox tony@contoso.com.

```
Set-Mailbox -Identity tony@contoso.com -CalendarRepairDisabled $true
```

For detailed syntax and parameter reference, see Set-Mailbox.

Use the Shell to enable calendar repair for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar repair" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to enable calendar repair for a mailbox.

This example enables the CRA for the user mailbox ayla@contoso.com.

```
Set-Mailbox -Identity ayla@contoso.com -CalendarRepairDisabled $false
```

For detailed syntax and parameter reference, see Set-Mailbox.

See Also

Concepts

Understanding Calendar Repair
Managing Calendars

1.8.3.8.4 Enable Internet Calendar Publishing

Enable Internet Calendar Publishing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Users in Microsoft Exchange Server 2010 organizations can share calendar availability (free/busy) information with users in non-Exchange organizations and other individuals with Internet access. In versions of Exchange earlier than Exchange 2010 Service Pack 1 (SP1), sharing calendar availability information required you to either:

- Set up Active Directory trusts, manage credentials, and manage replication with multiple external Exchange organizations.
- Establish a federation trust with the Microsoft Federation Gateway and configure organization relationships or sharing policies with other external Exchange organizations.

These methods often resulted in limited sharing capabilities, required complex setup and ongoing maintenance, and were limited solely to sharing calendar availability information between Exchange organizations.

In Exchange 2010, Internet calendar publishing provides increased flexibility and increases the number of users who can share calendar availability information. Enabling Internet calendar publishing consists of three general steps:

1. Configure the Web proxy URL for the Mailbox server.
2. Enable the publishing virtual directory for the Client Access server.
3. Create a sharing policy specifically for Internet calendar publishing. This policy allows users in your Exchange organization to invite other users who have Internet access to view limited calendar availability information by accessing a published URL.

To learn more about Internet calendar publishing and sharing policies, see Understanding Federated Delegation. Looking for other management tasks related to calendars? Check out Managing Calendars.

Prerequisites

- An Exchange 2010 Client Access server exists in the Exchange organization that's sharing user's calendar information.
- User mailboxes are on Exchange 2010 Mailbox servers in the Exchange organization that's sharing user's calendar information.

Step 1: Use the Shell to configure the Web proxy URL

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

Note:
You can't use the Exchange Management Console (EMC) to configure the Web proxy URL.

This example configures a Web proxy URL on Mailbox server MAIL01.

```
Set-ExchangeServer -Identity "MAIL01" -InternetWebProxy "<Webproxy URL>"
```

For detailed syntax and parameter information, see Set-ExchangeServer.

Step 2: Use the Shell to enable the publishing virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to enable the publishing virtual directory.

This example enables the publishing virtual directory on Client Access server CAS01.

```
Set-OwaVirtualDirectory -Identity "CAS01" -ExternalUrl "<URL for the CAS01>" -Cal
```

For detailed syntax and parameter information, see Set-OwaVirtualDirectory.

Step 3: Use the EMC or the Shell to create a sharing policy for Internet calendar publishing

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

Use the EMC

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Sharing Policy** to start the New Sharing Policy wizard.

   Note:
   Although you can add the Anonymous domain used for Internet calendar publishing to the default or existing sharing policies, we recommend that you create a separate sharing policy for Internet calendar publishing.

3. On the **Introduction** page, complete the following fields:
   - **Name** In this box, type **Internet** for the sharing policy name.
   - **Add** Click this button to open the **Add Action to Sharing Policy Domain** dialog box. Complete the following fields, and then click **OK**:
     Specify a domain of an external Exchange organization, or "*" for any domain Type **Anonymous** as the domain for the Internet calendar publishing sharing policy.

Specify the actions that apply to the federated domain Use this list to select the level of sharing you want to enforce for this policy. For this example, select **Calendar sharing with free/busy information, plus subject and location**.

- **Enable sharing policy** Select this check box to enable the Anonymous domain.

4. On the **Mailboxes** page, click **Add** to select the mailboxes to which you want to apply this sharing policy.

Note:
After creating the sharing policy, you can apply it to more mailboxes by using the **Mailboxes** tab in the sharing policy's property page or by using the **Mailbox Settings** tab in the mailbox's property page.

5. On the **New Sharing Policy** page, review your configuration settings. Click **New** to create the sharing policy. Click **Back** to make configuration changes.

Note:
A warning will be displayed by the New Sharing Policy wizard upon completion as a reminder that you've allowed users to share their calendars, and to make sure that the Client Access server publishing the virtual directory is enabled so that published calendars will be accessible.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell

This example creates the Internet calendar publishing sharing policy Internet and configures the policy to share only availability information. The policy is enabled.

```
New-SharingPolicy -Name "Internet" -Domains 'Anonymous: CalendarSharingFreeBusySi
```

This example adds the sharing policy Internet to a user mailbox.

```
Set-Mailbox -Identity <user name> -SharingPolicy "Internet"
```

This example adds the sharing policy Internet to an organizational unit (OU).

```
Set-Mailbox -OrganizationalUnit <OU name> -SharingPolicy "Internet"
```

For detailed syntax and parameter information, see New-SharingPolicy and Set-Mailbox.

Other Tasks

After you enable Internet calendar publishing, you may also want to configure publishing or sharing settings on a calendar folder of a specified mailbox. For detailed steps, see Set-MailboxCalendarFolder.

1.8.3.8.5 Disable Internet Calendar Publishing

Disable Internet Calendar Publishing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you disable a sharing policy used for defining Internet calendar publishing, users who are provisioned to use the policy won't be able to share calendar information with the Anonymous Internet domain specified in the policy. However, you can't delete the sharing policy until all the users who are provisioned to use the policy have the sharing policy setting removed from their mailboxes.

Note:

When the sharing policy is disabled, users provisioned to use the policy will continue to share information until the Sharing Policy Assistant runs. To specify how often the Sharing Policy Assistant runs, use the Set-MailboxServer cmdlet with the *SharingPolicySchedule* parameter.

To fully disable Internet calendar publishing, you should also disable the Microsoft Office Outlook Web App virtual directory used for calendar publishing. Doing this prohibits access to the published calendar links previously shared by your Exchange organization users with external Internet users.

To learn more about Internet calendar publishing and sharing policies, see Understanding Federated Delegation.

Looking for other management tasks related to calendars? Check out Managing Calendars.

Step 1: Use the EMC or the Shell to disable the sharing policy for Internet calendar publishing

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

Use the EMC

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Sharing Policies** tab.
3. In the result pane, click the sharing policy you set up for Internet calendar publishing.
4. In the action pane, under the sharing policy name, click **Properties**.
5. In **Properties**, clear the **Enable sharing policy** check box, and then click **OK** to disable the policy.
6. On the **Sharing Policies** tab, verify that the **Enabled** column for the sharing policy is set to **False**.

Use the Shell

This example disables the Internet calendar publishing sharing policy Internet.

```
Set-SharingPolicy -Identity "Internet" -Enabled $false
```

For detailed syntax and parameter information, see Set-SharingPolicy.

Step 2: Use the Shell to disable the Outlook Web App virtual directory used for calendar publishing

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to disable the Outlook Web App virtual directory used for calendar publishing.

This example disables calendar publishing for the Outlook Web App virtual directory on Client Access server CAS01.

```
Set-OwaVirtualDirectory -Identity "CAS01" -CalendarPublishingEnabled -$false
```

For detailed syntax and parameter information, see Set-OwaVirtualDirectory.

1.8.3.9 Managing Details Templates

Managing Details Templates

Exchange Server 2010 > Mailbox > Managing Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-22*

Customize Details Templates

Restore a Details Template to the Default Configuration

1.8.3.9.1 Customize Details Templates

Customize Details Templates

Mailbox > Managing Mailbox Servers > Managing Details Templates >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Use the Details Templates Editor to customize the client-side graphical user interface (GUI) presentation of object properties that are accessed by using address lists in the Microsoft Outlook client application. For example, when a user opens an address list in Outlook, the properties of a particular object are presented as defined by the details template in the Exchange organization. The objects can be customized by changing field sizes, adding or removing fields, adding or removing tabs, and rearranging fields. The layout of these templates may vary by language.

You can use the default details template or you can customize the template to better suit the needs of your users. Use the Details Templates Editor to customize the following Outlook objects:

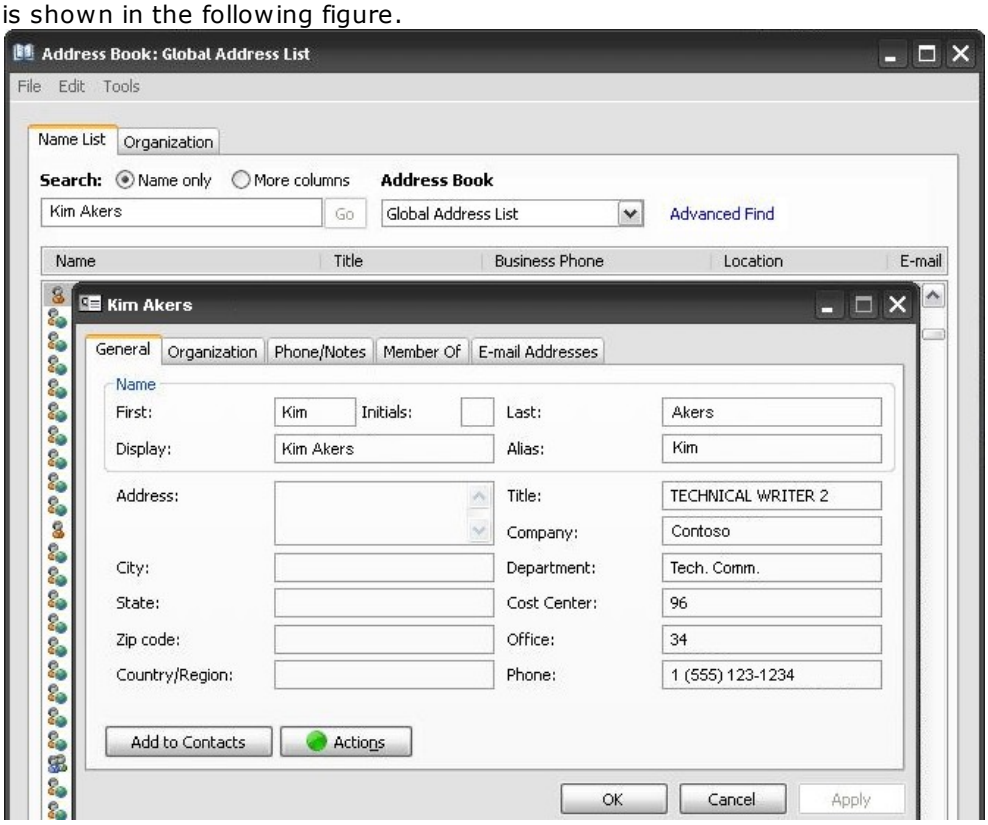
- Contacts
- Users
- Groups
- Mailbox agents
- Public folders
- Search dialog boxes

Not what you're looking for? Try Managing Details Templates.

Customize the details template

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Details templates" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Details Templates Editor**, and then in the action pane, click **Open Tool**.
3. In the console tree of the Details Templates Editor, click **Details Template**. In the details pane, the following columns are displayed:
   - **Language** This column lists the language in which the template was created.
   - **Template Type** This column lists the type of template that you can customize.
   - **Identity** This column lists the unique identity of the template.
   - **Created** This column lists the date and time that the template was created.
   - **Modified** This column lists the date and time that the template was last modified.
4. To edit a template, click the template you want, and then, in the action pane, click **Edit**. For example, the **English (United States)** contacts details template is shown in the following figure.



5. After you click **Edit**, there are several tasks you can perform to customize a details template:
   - To move an object in the designer pane, select the object, and then drag it to its new location on the template. As you move the object, you are provided with alignment lines.
   - To change a label's text, select the label in the design pane. In the properties pane, type the new text in the **Text** box. To create keyboard

shortcuts, you can use the ampersand (&) symbol. Place the ampersand (&) before the letter that you want to use as the shortcut.

- To change the size of an object, select the object, and then drag the sizing handles until the object is the shape and size you want.
- To delete an object, select the object, and then press the DELETE key.

> **Note:**
> The Details Templates Editor doesn't contain an **Undo** button, nor can you use a keyboard shortcut to undo an action. To undo an addition you made to the template, you must use the DELETE key. To undo a deletion, you must reapply the setting. You can also revert to the original settings by exiting the Details Templates Editor without saving your changes. If you want to undo changes after you have saved, you can restore the template. When you restore a template, all customization is lost, and the template is restored to its original configuration. For more information about how to restore the details template, see Restore a Details Template to the Default Configuration.

- To add an "Edit" text boxes, list boxes, multi-valued drop-down boxes, or multi-valued list boxes, in the toolbox pane, drag the object to the design pane. Set the attribute of the object by clicking the attribute drop-down box in the properties pane and then selecting the attribute that will be used by Exchange.

> **Note:**
> You must link the object to an attribute for it to be used by Exchange. In addition, the attribute determines the content that is displayed to the end user in Outlook. If you don't select an attribute, a random attribute is selected automatically.

- To add a group box, drag the object to the design pane. Then, in the properties pane, type a name in the **Text** box. Use group boxes to group similar objects.
- To add a tab to the template, right-click an existing tab, and then click **Add Tab**. A blank tab appears. To name the tab, type the name in the **Text** box in the properties pane.
- To remove a tab from the template, right-click the tab, and then click **Remove Tab**. A warning appears. Click **OK** to confirm that you want to remove the tab.
- To change the tabbing order of the objects on a tab so that users can use the TAB key to navigate the objects in the order you want, select the object in the design pane. Then, in the properties pane, use the **TabIndex** box to change the order.

> **Note:**
> To make sure that users cannot use the TAB key to access the labels of an object (for example **Name** or **Alias**), change the order of the labels so that they are last in the tabbing order.

6. To save changes to the details template, on the **File** menu, click **Save**.
7. To close the template, on the **File** menu, click **Exit**.

Restore a Details Template to the Default Configuration

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Details Templates Editor doesn't contain an **Undo** button, nor can you use a keyboard shortcut to undo an action. To undo an addition you made to the template, you must use the DELETE key. To undo a deletion, you must reapply the setting. You can also revert to the original settings by exiting the Details Templates Editor without saving your changes. If you want to undo changes after you have saved, you can restore the template. When you restore a template, all customization is lost, and the template is restored to its original configuration.

This topic explains how to use the Exchange Management Console (EMC) or the Exchange Management Shell to restore a details template to its default configuration.

Looking for other tasks related to details templates? Check out Managing Details Templates.

Use the EMC to restore a details template to the default configuration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Details templates" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Details Templates Editor**, and then, in the action pane, click **Open Tool**. The Details Templates Editor appears.
3. In the details pane, select the template you want to restore, and then in the action pane, click **Restore**.
4. Click **Yes** to confirm that you want to restore the template to its original state. All customization will be lost.

Use the Shell to restore a details template to the default configuration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Details templates" entry in the Mailbox Permissions topic.

This example restores the United States English contacts details template:

```
Restore-DetailsTemplate -Identity "en-US\Contact"
```

For detailed syntax and parameter information, see Restore-DetailsTemplate.

For More Information

Managing Tools in the Toolbox

1.8.3.10 Managing Distribution Groups

Managing Distribution Groups

Exchange Server 2010 > Mailbox > Managing Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-31*

1.8.3.10.1 Add a Member to a Distribution Group

Add a Member to a Distribution Group

Mailbox > Managing Mailbox Servers > Managing Distribution Groups >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

After you create a distribution group, you can manually add or remove members. Members who belong to a distribution group will receive e-mail messages sent to that group.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Use the EMC to add a member to a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.
2. In the result pane, select the distribution group to which you want to add a member.
3. In the action pane, under the distribution group name, click **Properties**.
4. In **<Distribution Group> Properties**, on the **Members** tab, click **Add** to open the **Select Recipient** dialog box.
5. In **Select Recipient**, click the recipient you want to add to the distribution group, and then click **OK**.

   Note:
   To add multiple recipients, hold down the CTRL key while selecting recipients.
6. Click **OK** to save your changes.

Use the Shell to add a member to a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

This example adds the user adam@contoso.com to the distribution group Marketing Managers.

```
Add-DistributionGroupMember -Identity "Marketing Managers" -Member adam@contoso.c
```

For detailed syntax and parameter information, see Add-DistributionGroupMember.

1.8.3.10.2 Change the Ownership of a Distribution Group

Change the Ownership of a Distribution Group

Mailbox > Managing Mailbox Servers > Managing Distribution Groups >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-06*

In Microsoft Exchange Server 2010, users can create and manage distribution groups and distribution group membership. These users are delegated ownership of the group by the **ManagedBy** property. The default owner of a distribution group is the user or administrator who creates the group. However, you can use the EMC or the Shell to change the ownership of a distribution group.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Note:
In addition to being one of the group owners, users must be assigned a management role assignment policy that contains the My Distribution Groups and My Distribution Group Membership roles.

Use the EMC to change the ownership of a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.
2. In the result pane, select the distribution group that you want to modify.
3. In the action pane, click **Properties**.
4. On the **Group Information** tab, under **Managed by**, you can perform the following tasks:
   - To add an owner to the distribution group, click **Add**, and then select the user from the **Select Mailbox or Mail-Enabled User** dialog box.
   - To remove an owner from the distribution group, select the user, and then click  .

     Note:
     You can't remove the last owner from a distribution group. You must add a new owner before removing the last one.
5. Click **OK**.

Use the Shell to change the ownership of a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

This example replaces the current owner of the distribution group Volunteers with the new owner john@contoso.com.

```
Set-DistributionGroup -Identity Volunteers -ManagedBy john@contoso.com
```

Note:
If you want to add more than one owner to the distribution group, separate users by using a comma. If you don’t include the current owners in the command, the current owners will be replaced by the new list.

This example adds John and Ayla to the list of owners and bypasses getting permission from the group's current manager Administrator.

```
Set-DistributionGroup -Identity 'contoso.com/Users/Summer Interns'-BypassSecurity
```

For detailed syntax and parameter information, see Set-DistributionGroup.

Create a Distribution Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Use the New Distribution Group wizard to create a new distribution group in your Exchange organization or to mail-enable an existing group in Active Directory.

There are two types of distribution groups:

- *Mail-enabled universal distribution groups* can be used only to distribute messages.
- *Mail-enabled universal security groups* can be used to distribute messages as well as to grant access permissions to resources in Active Directory.

It's important to note the terminology differences between Active Directory and Exchange 2010. In Active Directory, a distribution group refers to any group that doesn't have a security context, whether it's mail-enabled or not. In contrast, in Exchange 2010, all mail-enabled groups are referred to as distribution groups, whether they have a security context or not.

Caution:

You can create or mail-enable only universal distribution groups. To convert a domain-local or a global group to a universal group, you can use the Set-Group cmdlet in the Exchange Management Shell. You may have mail-enabled groups that were migrated from previous versions of Exchange that are not universal groups. You can use the Exchange Management Console (EMC) or the Shell to manage these groups

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

What Do You Want to Do?

- Use the EMC to create a distribution group
- Use the Shell to create a distribution group

Use the EMC to create a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Distribution Group**.
3. On the **Introduction** page, select whether to create a new group or to mail-enable an existing group.
   - **New group** Click this button to create a new distribution group.
   - **Existing group** Click this button to mail-enable an existing group in Active Directory, and then click **Browse** to select the existing group.
4. On the **Group Information** page, complete the following fields.
   - **Group type** Click **Distribution** to create a mail-enabled universal distribution group, or click **Security** to create a mail-enabled universal security group.
   - **Specify the organizational unit rather than using a default one** Select this

check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.

- **Name** Use this box to type the name of the group, which can't exceed 64 characters.

  Note:
  If a group naming policy is applied, you must follow the naming constraints enforced for your organization. For more information see, Create a Distribution Group Naming Policy. If you want to override your organization's group naming policy, see Override a Distribution Group Naming Policy.

- **Name (pre-Windows 2000)** Use this box to type the name for the group that is compatible with the legacy versions of Windows (prior to the release of Windows 2000 Server). This required field is automatically populated based on the **Name** field.

  The name of the group that is compatible with earlier versions of Windows can't exceed 64 characters. It can contain letters, numbers, and the following characters: **! # $ % ^ & - . _ { } | ~**.

- **Alias** Use this box to type the name of the alias for the group. The alias cannot exceed 64 characters and must be unique in the forest.

5. On the **New Distribution Group** page, review your configuration settings. To make any configuration changes, click **Back**. To create the new distribution group, click **New**.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. Click **Finish**.

Use the Shell to create a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

This example creates the distribution group Managers with the SAM account name Managers in the organizational unit Contoso.com/users.

Note:
If a group naming policy is applied, you must follow the naming constraints enforced for your organization. For more information see, Create a Distribution Group Naming Policy. If you want to override your organization's group naming policy, see Override a Distribution Group Naming Policy.

```
New-DistributionGroup -Name "Managers" -OrganizationalUnit "Contoso.com/users" -S
```

For More Information

Understanding Recipients

Managing Distribution Groups

1.8.3.10.4 Create a Dynamic Distribution Group

Create a Dynamic Distribution Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Dynamic distribution groups are mail-enabled Active Directory group objects that are created to expedite the mass sending of e-mail messages and other information within an Exchange organization. Use the New Dynamic Distribution Group wizard to create a dynamic distribution group in your Exchange organization.

Unlike regular distribution groups that contain a defined set of members, the membership list for dynamic distribution groups is calculated each time a message is sent to the group, based on the filters and conditions that you define. When an e-mail message is sent to a dynamic distribution group, it is delivered to all recipients in the organization that match the criteria defined for that group.

Caution:

A dynamic distribution group includes any recipient in Active Directory with attributes that match its filter. If a recipient's properties are modified to match the filter, the recipient could inadvertently become a group member and start receiving messages that are sent to the group. Well-defined, consistent account provisioning processes will reduce the chances of this issue occurring.

Looking for other management tasks related to dynamic distribution groups? Check out Managing Distribution Groups.

What Do You Want to Do?

- Use the EMC to create a dynamic distribution group
- Use the Shell to create a dynamic distribution group

Use the EMC to create a dynamic distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Dynamic distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Dynamic Distribution Group**.
3. On the **Introduction** page, complete the following fields. All fields on this page are required:

- **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.
- **Name** Use this box to type the name for the dynamic distribution group. The name cannot exceed 64 characters.
- **Alias** Use this box to type the alias of the dynamic distribution group. The alias cannot exceed 64 characters and must be unique in the forest.

4. On the **Filter Settings** page, define the recipient filter for the new dynamic distribution group:
   - **Browse** Click this button to open the **Select Organizational Unit** dialog box. Use this dialog box to specify the OU from which to select the recipients. A dynamic distribution group contains all recipients that are in the specified OU and any other OUs under it.
   - Select the recipient types you want to include. You can select **All recipient types** or **The following specific types**. If you select **The following specific types**, you can select one or more of the following recipient types:
     Users with Exchange mailboxes Select this check box if you want to include users that have mailboxes. Users that have Exchange mailboxes are those that have a user domain account and a mailbox in the Exchange organization.
     Users with external e-mail addresses Select this check box if you want to include users that have external e-mail addresses. Users that have external e-mail accounts have user domain accounts in Active Directory, but use e-mail accounts that are external to the organization. This enables them to be included in the global address list (GAL) and added to distribution lists.
     Resource mailboxes Select this check box if you want to include Exchange resource mailboxes. Resource mailboxes allow you to administer company resources through a mailbox, such as a conference room or company vehicle.
     Contacts with external e-mail addresses Select this check box if you want to include contacts that have external e-mail addresses. Contacts that have external e-mail accounts do not have user domain accounts in Active Directory, but the external e-mail address is available in the GAL.
     Mail-enabled groups Select this check box if you want to include security groups or distribution groups that have been mail-enabled. Mail-enabled groups are similar to distribution groups. E-mail messages that are sent to a mail-enabled group account will be delivered to several recipients.

5. On the **Conditions** page, define any additional optional conditions to further restrict the recipients that are included in this dynamic distribution group
   - **Step 1: Select conditions** Use this section to select one or more conditions. If you don't want to set any conditions for the list, don't select any of the check boxes.
   - **Step 2: Edit the conditions by selecting an underlined value** If you select any conditions in Step 1, each condition you select will append to the definition. For example, if you selected the **Recipient is in a State or Province** check box in Step 1, you will see the **in the specified State or**

Province(s) condition in Step 2.

For each condition, click the underlined term to create your condition. By default, the underlined term for new conditions will read **specified**. After you edit the condition, the underlined term will change to the value that you specified.

Important:

The values that you enter in these dialog boxes must exactly match those that appear in the recipient's properties. For example, if you enter **Washington** in the **Specify State or Province** dialog box, but the **Address and Phone** tab in the recipient's properties lists the state as **WA**, the condition will not be met.

- **Preview** Click this button to view the recipients that will be included, based on the conditions that you specified.

Note:

If you want to specify conditions other than the ones available on this page, you must use the Exchange Management Shell to create a custom query for the dynamic distribution group. Keep in mind that the filter and condition settings for dynamic distribution groups that have custom recipient filters can be managed only by using the Shell. For an example of how to create a dynamic distribution group with a custom query, see Use the Shell to create a new dynamic distribution group later in this topic. For more information about recipient filters, see Creating Filters in Recipient Commands.

6. On the **New Dynamic Distribution Group** page, review your configuration settings. To make any changes, click **Back**. To create the new dynamic distribution group, click **New**.

7. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
8. Click **Finish** to close the wizard.

Use the Shell to create a dynamic distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Dynamic distribution groups" entry in the Mailbox Permissions topic.

This example creates the dynamic distribution group Mailbox Users DDG that contains only mailbox users.

```
New-DynamicDistributionGroup -IncludedRecipients MailboxUsers -Name "Mailbox User
```

This example creates a dynamic distribution group with a custom recipient filter. The dynamic distribution group contains all mailbox users on a server called Server1:

```
New-DynamicDistributionGroup -Name "Mailbox Users on Server1" -OrganizationalUnit
```

For More Information

Configure Dynamic Distribution Group Properties

Managing Distribution Groups

Understanding Recipients

1.8.3.10.5 Create a Distribution Group Naming Policy

Create a Distribution Group Naming Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

A *group naming policy* is a template applied to the distribution group names in your Microsoft Exchange organization. Specifically, you can specify that a prefix, a suffix, or both be applied to all distribution group names. You can also block certain words from being used in the names.

Prefixes and suffixes can be a string, an attribute, or a combination of both. A prefix or suffix can contain sequences of multiple attributes or strings. You can use the following attributes, which will be gathered from the user who creates the distribution group settings:

- Department
- Company
- Office
- StateOrProvince
- CountryorRegion
- CountryCode
- Title
- CustomAttribute1 to CustomAttribute15

Important:

The maximum length for a distribution group name is 64 characters. This includes the combined number of characters in the prefix, the group name provided by the user, and the suffix.

To use an attribute to create a naming policy, use the following syntax: "<PrefixAttribute><GroupName><SuffixAttribute>". For example, to create a naming policy using Department as a prefix and CustomAttribute1 as the suffix, you would use the following:"<Department><GroupName><CustomAttribute1>".

To use strings to create a naming policy, use the following syntax: "string<GroupName>string". For example, to create a naming policy using the string DL_ as the prefix, you would use the following: "DL_<GroupName>".

Note:

Don't set the <*GroupName*> value; it's used as a placeholder. When a user or administrator creates a distribution group, <*GroupName*> is replaced by the name they provide.

Looking for other management tasks related to distribution groups? Check out Managing

Distribution Groups.

Use the Shell to create a naming policy for a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange server configuration settings" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:

You can't use the Exchange Management Console (EMC) to create a naming policy for a distribution group.

This example creates a distribution group naming policy with the following settings:

- Distribution groups will be created in the Users\Groups container.
- The words "bad", "curse", and "offensive" will be blocked from use in distribution group names.
- All distribution groups will have the prefix "DL_"
- All distribution groups will have the suffix of an underscore (_) followed by the user's department and country code.

```
Set-OrganizationConfig -DistributionGroupDefaultOU Users\Groups -DistributionGrou
```

For detailed syntax and parameter information, see Set-OrganizationConfig.

Other Tasks

After you create the distribution group naming policy, you may also want to override the policy when creating distribution groups. For detailed steps, see Override a Distribution Group Naming Policy.

1.8.3.10.6 Override a Distribution Group Naming Policy

Override a Distribution Group Naming Policy

Mailbox > Managing Mailbox Servers > Managing Distribution Groups >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

A *group naming policy* is a template applied to the distribution group names in your Microsoft Exchange organization. As an administrator, there may be times when you need to override the naming policy.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Use the Shell to override the distribution group naming policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions

topic.

Note:
You can't use the Exchange Management Console (EMC) to override the distribution group naming policy.

This example creates the distribution group ITDepartment and overrides the naming policy.

```
New-DistributionGroup -Name "ITDepartment" -IgnoreNamingPolicy
```

This example changes the name of an existing distribution group and overrides the naming policy.

```
Set-DistributionGroup -Identity "DL_HRDept" -Name "Department_HR_AllStaff" -Ignor
```

For detailed syntax and parameter information, see New-DistributionGroup and Set-DistributionGroup.

1.8.3.10.7 Create a Room List Distribution Group

Create a Room List Distribution Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Microsoft Office Outlook 2007 or earlier, if you wanted to search for a conference room's availability while setting up a meeting, you needed to add all possible conference rooms to the meeting request, and then use the Scheduling Assistant to view available conference rooms.

In Microsoft Exchange Server 2010, you can create *room list* distribution groups to generate a list of building locations so that Outlook 2010 users can select a building and get information about room availability without having to manually add all the rooms in the building.

You can only add room mailboxes to a room list distribution group.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Use the Shell to create a room list distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to create a room list distribution group.

This example creates a room list for all of the conference rooms in Building 31 by using the *Filter* parameter. In this example, `CustomAttribute1` is used to specify that the conference rooms are in Building 31.

1. Save the list of members in a $Members variable.

```
$Members=Get-Mailbox -Filter {(RecipientTypeDetails -eq "RoomMailbox")
```

2. Create the distribution group by using the $Members variable as the value for the *Members* parameter.

```
New-DistributionGroup -Name "Building 31 Conference Rooms" -Organizait
```

For detailed syntax and parameter reference, see Get-Mailbox and New-DistributionGroup.

1.8.3.10.8 Create a Security Group

Create a Security Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A mail-enabled security group can be used to distribute messages as well as to grant access permissions to resources in Active Directory.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Note:

By default, all new distribution groups require that all senders be authenticated. This prevents external senders from sending messages to distribution groups. This setting is different from previous versions of Exchange where, by default, new distribution groups accepted messages from all senders. To configure a distribution group to accept messages from all senders, you must modify the message delivery restriction settings for that distribution group. For more information about configuring message delivery restrictions, see Configure Message Delivery Restrictions.

Use the EMC to create a security group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Distribution Group**.
3. On the **Introduction** page, click **New Group**, and then click **Next**.
4. On the **Group Information** page, complete the following fields:
   - **Group type** Click **Security** to create a mail-enabled universal security group.
   - **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes,

see Understanding Recipient Scope.

- **Name** Use this box to type the name of the group, which can't exceed 64 characters.
- **Name (pre-Windows 2000)** Use this box to type the name for the group that's compatible with the legacy versions of Windows (prior to the release of Windows 2000 Server). This required field is automatically populated based on the **Name** field.

  The name of the group that's compatible with earlier versions of Windows can't exceed 64 characters. It can contain letters, numbers, and the following characters: **! # $ % ^ & - . _ { } | ~**.
- **Alias** Use this box to type the name of the alias for the group. The alias can't exceed 64 characters and must be unique in the forest.

5. On the **New Distribution Group** page, review your configuration settings. To make any configuration changes, click **Back**. To create the security group, click **New**.
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a security group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

This example creates a security group named Managers.

```
New-DistributionGroup -Name "Managers" -OrganizationalUnit "contoso.com/Users" -S
```

For detailed syntax and parameter information, see New-DistributionGroup.

1.8.3.10.9 Convert a Distribution Group into a Room List

Convert a Distribution Group into a Room List

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Microsoft Office Outlook 2007 or earlier, if you wanted to search for a conference room's availability while setting up a meeting, you needed to add all possible conference rooms to the meeting request, and then use Scheduling Assistant to view available conference rooms.

In Microsoft Exchange Server 2010, you can create *room list* distribution groups to generate a list of building locations so that in Outlook 2010, users can select a building and get information about room availability in that building without having to manually add all the rooms in the building.

Note:

In Exchange, you can convert a distribution group to a room list only if all the members of

the distribution group are room mailboxes. In addition, after the distribution group is converted to a room list, or after you create a room list, you can only add room mailboxes to the group.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Prerequisite

You have a distribution group that contains only room mailboxes. For details about how to create a room list, see Create a Distribution Group.

Use the Shell to convert a distribution group into a room list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to convert a distribution group into a room list.

This example converts the Bldg34 Conf Rooms distribution group to a room list.

```
Set-DistributionGroup -Identity "Bldg34 Conf Rooms" -RoomList
```

For detailed syntax and parameter information, see Set-DistributionGroup.

1.8.3.10.10 Configure Distribution Group Properties

Configure Distribution Group Properties

Mailbox > Managing Mailbox Servers > Managing Distribution Groups >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Distribution groups are mail-enabled Active Directory group objects that are created to expedite the mass sending of e-mail messages and other information within an Exchange organization.

There are two types of distribution groups:

- *Mail-enabled universal distribution groups* can be used only to distribute messages.
- *Mail-enabled universal security groups* can be used to distribute messages as well as to grant access permissions to resources in Active Directory.

It's important to note the terminology differences between Active Directory and Exchange 2010. In Active Directory, a distribution group refers to any group that doesn't have a security context, whether it's mail-enabled or not. In contrast, in Exchange 2010, all mail-enabled groups are referred to as distribution groups, whether they have a security context or not.

Looking for other management tasks related to distribution groups? Check out Managing

Distribution Groups.

What Do You Want to Do?

- Use the EMC to configure distribution group properties
- Use the Shell to configure distribution group properties

Use the EMC to configure distribution group properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.
2. In the result pane, click the distribution group that you want to configure.
3. In the action pane, click **Properties**.

4. Use the **General** tab to view or modify the display name, alias, and custom attributes for the distribution group.
   - **Display name** Use this unlabeled box at the top of the page to view or change the display name for the distribution group.
   - **Organizational unit** This read-only field displays the organizational unit (OU) that contains the distribution group.
   - **Modified** This read-only field displays the last date and time a configuration change was made.

     Note:
     Configuration changes made through any other method, such as the Exchange Management Shell or Active Directory Service Interfaces (ADSI) Edit, will also update this field.

   - **Alias** Use this box to view or change the alias of the distribution group. The alias cannot exceed 64 characters and must be unique in the forest.
   - **Custom Attributes** Click this button to open the **Custom Attributes** dialog box. You can specify up to 15 custom attributes for the recipient. To specify the custom attribute values, use the corresponding boxes, and then click **OK**. To learn more, see Understanding Custom Attributes.

5. Use the **Group Information** tab to view or change the Active Directory information for the distribution group.
   - **Name** Use this text box to view or change the name of the group. The name cannot exceed 64 characters.
   - **Name (pre-Windows 2000)** Use this text box to type the name of the group that is compatible with legacy versions of Windows (prior to the release of Windows 2000 Server).

     The name of the group that is compatible with earlier versions of Windows can't exceed 20 characters. It can contain letters, numbers, and the following characters: **! # $ % ^ & - . _ { } | ~**.
   - **Managed By** The recipient that is designated as the manager for this distribution group will be visible when users view the properties of this group in Outlook or Outlook Web App. If the delivery reports option on the **Advanced** tab is set to **Send delivery reports to group manager**, the manager will also receive delivery reports for the group.

     Click **Add** to open the **Select Mailbox or Mail-enabled User** dialog box. Use this dialog box to select the recipient you want to add as a manager of the distribution group, and then click

OK.

Click to remove the selected manager from the distribution group.

- **Notes** Use this box to view or modify administrative notes about the distribution group. These notes are also visible from Outlook. When a user views the properties of the distribution group in Outlook, the notes will be displayed on the **General** tab.

6. Use the **Members** tab to add members to or remove members from the distribution group.
   - Click **Add** to open the **Select Recipient** dialog box. Use this dialog box to select the recipients you want to add to the distribution group, and then click **OK**.

     Click to remove the selected members from the distribution group.

7. Use the **Membership Approval** tab to configure how membership requests should be handled for this distribution group.

   Choose whether owner approval is required to join the group
   - **Open** Click this button to allow users to join this distribution group without the approval of the distribution group owners.
   - **Closed** Click this button to specify that only distribution group owners can add members to this distribution group. Requests to join this distribution group will be rejected automatically.
   - **Owner approval** Click this button to specify that users can request membership to this distribution group. Requests to join the distribution group must be approved by a distribution group owner before the user can join.

   Choose whether the group is open to leave
   - **Open** Click this button to allow users to leave this distribution group without the approval of the distribution group owners.
   - **Closed** Click this button to specify that only distribution group owners can remove members from this distribution group. Requests to leave this distribution group will be rejected automatically.

8. Use the **Member Of** tab to view a list of the groups to which this recipient belongs. Some of these groups may not be mail-enabled. Mail-enabled groups will have an envelope icon next to them. You can't use this tab to modify membership information. The recipient may match the criteria for one or more dynamic distribution groups in your organization. However, dynamic distribution groups aren't displayed on this tab because their membership is calculated each time they are used. For more information, see Managing Distribution Groups.

9. Use the **E-Mail Addresses** tab to configure the e-mail addresses for the recipient. You can modify the existing addresses or create additional ones. Each recipient must have at least one primary STMP address that is internal to your Exchange organization and one external address.
   - **Add** Click **Add** to add a new e-mail address for this recipient. Use the drop-down box to select from the following address types:

     SMTP Address This is the default address type. Click this button and use the corresponding dialog box to add an SMTP address.

     EUM Address This address type is available only for user mailboxes. It's not available for mail users, mail contacts, distribution groups, or mail-enabled public folders. An EUM (Exchange Unified Messaging) address is used by Unified Messaging servers to locate UM-enabled users within an Exchange 2010 organization. EUM addresses contain the

extension number and the UM dial plan for the UM-enabled user. Click this button and use the corresponding dialog box to add an EUM address.
Custom Address Click this button and use the corresponding dialog box to add a custom address (for example, fax or X.400).

Note:
With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.

- **Edit** Click this button to modify the selected e-mail address.
-  Click this button to remove the selected e-mail address.
- **Set as Reply** Click this button to set your selected address as the "reply to" address. A recipient can have multiple e-mail addresses for a specific address type. This allows the recipient to receive messages that are addressed to any one of these e-mail addresses. However, a single address must be used for any messages that are sent by the recipient. If a recipient has multiple e-mail addresses, the primary address is used for any messages sent by the recipient.
  This button is available only when an address other than the primary address is selected. Primary addresses for each address type are displayed in bold type.
  If an e-mail address policy in your Exchange organization applies to this mailbox, the **Set as Reply** setting will be controlled by that policy. To change the primary address for a specific address type, you must clear the **Automatically update e-mail addresses based on e-mail address policy** check box.
- **Set as External** This button is available only for mail users and mail contacts. It's not available for user mailboxes, distribution groups, or mail-enabled public folders. Click **Set as External** to designate the selected e-mail address as the external e-mail address for the recipient.

  Note:
  This button is enabled when an address other than the external e-mail address is selected.

- **Automatically update e-mail addresses based on e-mail address policy** Select this check box to have the recipient's e-mail addresses automatically updated based on changes made to e-mail address policies in your organization. This box is selected by default.

10. Use the **Advanced** tab to view or change the advanced distribution group settings, such as the expansion server and delivery report options.
    - **Simple display name** Use this box to view or modify the simple display name for the recipient. The **Display Name** field (located on the **General** tab) can contain Unicode characters. However, third-party applications and older clients may not support Unicode characters. If the system that is displaying the recipient properties doesn't support Unicode characters, you can use the simple display name. For more information about Unicode characters, see Unicode. The simple display name field accepts only ASCII characters.
    - **Set expansion server** For each message that is sent to a distribution group, Exchange must access the full membership list to route the message to all recipients. This process is known as *distribution group expansion*. Use this box and corresponding **Browse** button to select a Hub Transport server in your Exchange organization that will be responsible for expanding the membership list for this distribution group.
      Expansion of very large distribution groups is a resource intensive process. If it occurs on a production server, it may impact mail flow. To avoid any production impact, you may want

to specify expansion servers for very large distribution groups.

- **Hide from Exchange address lists** Select this check box to prevent the recipient from appearing in the global address list (GAL) and other address lists that are defined in your Exchange organization.
  After you select this check box, users in your Exchange organization can still send messages to the recipient by using the e-mail address.
- **Send out-of-office message to originator** Select this check box to allow Out of Office messages from group members to be sent to the message sender. If this check box is selected, users who send messages to the distribution group will receive Out of Office replies from any member that has an Out of Office rule turned on.
  Clear this check box to prevent Out of Office replies from distribution group members to be sent to the message sender.
- **Send delivery reports to group manager** Click this button to send non-delivery reports (NDRs) to only the distribution group manager.
- **Send delivery reports to message originator** Click this button to send NDRs to the message sender.
- **Do not send delivery reports** Click this button to prevent the sending of NDRs.

11. Use the **Mail Flow Settings** tab to configure message size or message delivery restrictions for the distribution group. To view or change a mail flow setting, select the setting from the list, and then click **Properties**.
    - **Message Size Restrictions** Select this setting and then click **Properties** to open the **Message Size Restrictions** dialog box. Use this dialog box to configure the maximum message size in kilobytes (KB) that users are allowed to send to this distribution group.
      If a message larger than the specified size is sent to the distribution group, the message will be returned to the sender with a descriptive error message.
      In the **Message Size Restrictions** dialog box, select the **Maximum message size (in KB)** check box to set the maximum size for messages that can be received by this distribution group. Use the corresponding box to specify the maximum message size allowed (in KB). The message size must be between 0 and 2,097,151 KB.
      Clear the **Maximum message size (in KB)** check box to remove the size restrictions for receiving messages.
    - **Message Delivery Restrictions** Select this setting and then click **Properties** to open the **Message Delivery Restrictions** dialog box. Use this dialog box to configure the following settings:
      All senders Click this button to allow the group to accept messages from all senders. This includes senders in both your Exchange organization and external senders. This button is selected by default. This option includes external users only if you clear the **Require that all senders are authenticated** check box. If you select this check box, messages from external users will be rejected.
      Only senders in the following list Click this button to specify that the group can accept messages only from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.
      Require that all senders are authenticated Select this check box to prevent anonymous users from sending messages to the group. By default, this check box is selected for distribution

groups. This prevents external senders from sending messages to distribution groups.
No Senders Click this button to specify that the group will not reject messages from any senders in the Exchange organization. This button is selected by default.
Senders in the following list Click this button to specify that the group will reject messages from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now.**

- **Message Moderation** Select this setting and then click **Properties** to open the **Message Moderation** dialog box. Use this dialog box to configure whether messages sent to this distribution group must be approved by a moderator before they are delivered to the distribution group members.
  In the **Message Moderation** dialog box, select the **Messages sent to this group have to be approved by a moderator** check box to require all messages sent to the group to be approved by a moderator.
  In the **Specify group moderators** field, click **Add** to open the **Select Recipient** dialog box. Use this dialog box to select the recipients you want to add as moderators of the distribution group, and then click **OK**.
  Click  to remove the selected moderator from the distribution group.
  In the **Specify senders who don't require message approval** field, click **Add** to open the **Select Recipient** dialog box. Use this dialog box to select the recipients who don't require message approval to send to the distribution group, and then click **OK**.
  Click  to remove the selected recipients who should no longer be allowed to send messages to the group without approval from the group.

Use the Shell to configure distribution group properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

This example changes the *MaxReceiveSize* parameter to 20 MB for the distribution group Seattle Employees.

```
Set-DistributionGroup "Seattle Employees" -MaxReceiveSize 20MB -ModerationEnabled
```

This example enables moderation for the distribution group Customer Support and sets the moderator to Amy. In addition, this moderated distribution group will notify senders who send mail from within the organization if their messages aren't approved.

```
Set-DistributionGroup -Identity 'Customer Support' -ModeratedBy "Amy" -Moderation
```

This example changes the user-created distribution group Dog Lovers to require the group manager to approve users' requests to join the group. In addition, by using the *BypassSecurityGroupManagerCheck* parameter, the group manager will not be notified that a change was made to the distribution group's settings.

```
Set-DistributionGroup -Identity 'Dog Lovers' -MemberJoinRestriction 'ApprovalRequ
```

For More Information

Understanding Recipients

Managing Distribution Groups

1.8.3.10.11 Configure Dynamic Distribution Group Properties

Configure Dynamic Distribution Group Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-20*

Dynamic distribution groups are mail-enabled Active Directory group objects that are created to expedite the mass sending of e-mail messages and other information within an Exchange organization.

Unlike regular distribution groups that contain a defined set of members, the membership list for dynamic distribution groups is calculated each time a message is sent to the group, based on the filters and conditions that you define. When an e-mail message is sent to a dynamic distribution group, it's delivered to all recipients in the organization that match the criteria defined for that group.

Caution:

- A dynamic distribution group includes any recipient in Active Directory with attributes that match its filter. If a recipient's properties are modified to match the filter, the recipient could inadvertently become a group member and start receiving messages that are sent to the group. Well-defined, consistent account provisioning processes will reduce the chances of this issue occurring.
- Take caution when creating or modifying dynamic distribution groups within search scopes, such as organizational unit (OU).
- Avoid creating multiple levels of dynamic distribution group membership (also known as nested groups) as this may cause increased LDAP requests and initiate slow LDAP responses.

Looking for other management tasks related to dynamic distribution groups? Check out Managing Distribution Groups.

What Do You Want to Do?

- Use the EMC to configure dynamic distribution group properties
- Use the Shell to dynamic distribution group properties

Use the EMC to configure dynamic distribution group properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Dynamic distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.

2. In the result pane, click the dynamic distribution group that you want to configure.
3. In the action pane, click **Properties**.

4. Use the **General** tab to view or modify the display name, alias, and custom attributes for the dynamic distribution group.
   - **Display name** Use this unlabeled text box at the top of the page to view or change the display name for the group.
   - **Organizational unit** This read-only field displays the organizational unit (OU) that contains the group.
   - **Modified** This read-only field displays the last date and time a configuration change was made.

     Note:
     Configuration changes made through any other method, such as the Exchange Management Shell or Active Directory Service Interfaces (ADSI) Edit, will also update this field.

   - **Alias** Use this box to view or change the alias of the group. The alias cannot exceed 64 characters and must be unique in the forest.
   - **Custom Attributes** Click this button to open the **Custom Attributes** dialog box. You can specify up to 15 custom attributes for the recipient. To specify the custom attribute values, use the corresponding boxes, and then click **OK**. To learn more, see Understanding Custom Attributes.

5. Use the **Group Information** tab to change the Active Directory information for the dynamic distribution group.
   - **Name** Use this box to view or change the name of the group. The name can't exceed 64 characters.
   - **Managed By** The recipient that's designated as the manager for this dynamic distribution group will be visible when users view the properties of this group in Outlook or Outlook Web App. If the delivery reports option on the **Advanced** tab is set to **Send delivery reports to group manager**, the manager will also receive delivery reports for the group.

     Click **Add** to open the **Select Mailbox or Mail-enabled User** dialog box. Use this dialog box to select the recipient you want to add as a manager of the group, and then click **OK**.

     Click  to remove the selected manager from the dynamic distribution group.
   - **Notes** Use this box to view or modify administrative notes about the group. These notes are also visible in Outlook. When a user views the properties of the group in Outlook, the notes will be displayed on the **General** tab.

6. Use the **Filter** tab to modify the recipient filter for the group:
   - **Select the recipient container where you want to apply this filter** This box is populated with the OU that you selected when you created the dynamic distribution group. To specify a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. A dynamic distribution group contains all recipients that are in the specified OU and any other OUs under it.
   - Select the recipient types you want to include. You can select **All recipient types** or **The following specific types**. If you select **The following specific types**, you can select one or more of the following recipient types:

     Users with Exchange mailboxes Select this check box if you want to include users that have mailboxes. Users that have Exchange mailboxes are those that have a user domain account and a mailbox in the Exchange organization.

     Users with external e-mail addresses Select this check box if you want to include users that have external e-mail addresses.

Users that have external e-mail accounts have user domain accounts in Active Directory, but use e-mail accounts that are external to the organization. This enables them to be included in the global address list (GAL) and added to distribution lists.
Resource mailboxes Select this check box if you want to include Exchange resource mailboxes. Resource mailboxes allow you to administer company resources through a mailbox, such as a conference room or company vehicle.
Contacts with external e-mail addresses Select this check box if you want to include contacts that have external e-mail addresses. Contacts that have external e-mail accounts do not have user domain accounts in Active Directory, but the external e-mail address is available in the GAL.
Mail-enabled groups Select this check box if you want to include security groups or distribution groups that have been mail-enabled. Mail-enabled groups are similar to distribution groups. E-mail messages that are sent to a mail-enabled group account will be delivered to several recipients.

7. Use the **Conditions** tab to define any optional conditions to further restrict the recipients that are included in this dynamic distribution group.
   - **Step 1: Select conditions** Use this section to select one or more conditions. If you don't want to set any conditions for the list, don't select any of the check boxes.
   - **Step 2: Edit the conditions by selecting an underlined value** If you select any conditions in Step 1, each condition you select will append to the definition. For example, if you selected the **Recipient is in a State or Province** check box, you'll see the **in the specified State or Province(s)** condition in Step 2.

     For each condition, click the underlined term to create your condition. By default, the underlined term for new conditions will read **specified**. After you edit the condition, the underlined term will change to the value that you specified.

     Important:
     The values that you enter in these dialog boxes must exactly match those that appear in the recipient's properties. For example, if you enter **Washington** in the **Specify State or Province** dialog box, but the **Address and Phone** tab in the recipient's properties lists the state as **WA**, the condition will not be met.
   - **Preview** Click this button to view the recipients that will be included, based on the conditions that you specified.

     Note:
     If you want to specify conditions other than the ones available on this tab, you must use the Exchange Management Shell to create a custom query for the dynamic distribution group. Keep in mind that the filter and condition settings for dynamic distribution groups that have custom recipient filters can be managed only by using the Shell. For more information about recipient filters, see Creating Filters in Recipient Commands.

8. Use the **E-Mail Addresses** tab to configure the e-mail addresses for the recipient. You can modify the existing addresses or create additional ones. Each recipient must have at least one primary STMP address that is internal to your Exchange organization and one external address.
   - **Add** Click **Add** to add a new e-mail address for this recipient. Use the drop-down box to select from the following address types:

     SMTP Address This is the default address type. Click this

button and use the corresponding dialog box to add an SMTP address.
EUM Address This address type is available only for user mailboxes. It's not available for mail users, mail contacts, distribution groups, or mail-enabled public folders. An EUM (Exchange Unified Messaging) address is used by Unified Messaging servers to locate UM-enabled users within an Exchange 2010 organization. EUM addresses contain the extension number and the UM dial plan for the UM-enabled user. Click this button and use the corresponding dialog box to add an EUM address.
Custom Address Click this button and use the corresponding dialog box to add a custom address (for example, fax or X.400).

Note:
With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.

- **Edit** Click this button to modify the selected e-mail address.
-  Click this button to remove the selected e-mail address.
- **Set as Reply** Click this button to set your selected address as the "reply to" address. A recipient can have multiple e-mail addresses for a specific address type. This allows the recipient to receive messages that are addressed to any one of these e-mail addresses. However, a single address must be used for any messages that are sent by the recipient. If a recipient has multiple e-mail addresses, the primary address is used for any messages sent by the recipient.
  This button is available only when an address other than the primary address is selected. Primary addresses for each address type are displayed in bold type.
  If an e-mail address policy in your Exchange organization applies to this mailbox, the **Set as Reply** setting will be controlled by that policy. To change the primary address for a specific address type, you must clear the **Automatically update e-mail addresses based on e-mail address policy** check box.
- **Set as External** This button is available only for mail users and mail contacts. It's not available for user mailboxes, distribution groups, or mail-enabled public folders. Click **Set as External** to designate the selected e-mail address as the external e-mail address for the recipient.

  Note:
  This button is enabled when an address other than the external e-mail address is selected.

- **Automatically update e-mail addresses based on e-mail address policy** Select this check box to have the recipient's e-mail addresses automatically updated based on changes made to e-mail address policies in your organization. This box is selected by default.

9. Use the **Advanced** tab to view or change the advanced group settings, such as the expansion server and delivery report options.
   - **Simple display name** Use this box to view or modify the simple display name for the group. The **Display name** field (located on the **General** tab) can contain Unicode characters. However, third-party applications and older clients may not support Unicode characters. If the system that is displaying the recipient properties doesn't support Unicode characters, you can use the simple display name. For more information about Unicode characters, see Unicode. The simple display name field accepts only ASCII characters.
   - **Set expansion server** For each message that is sent to the dynamic distribution group, Exchange must access the full membership list to route

the message to all recipients. This process is known as *distribution group expansion*. Use this box and corresponding **Browse** button to select a Hub Transport server in your Exchange organization that will be responsible for expanding the membership list for this group

Expansion of very large dynamic distribution groups is a resource intensive process. If it occurs on a production server, it may impact mail flow. To avoid any production impact, you may want to specify expansion servers for very large groups.

- **Hide from Exchange address lists** Select this check box to prevent the recipient from appearing in the global address list (GAL) and other address lists that are defined in your Exchange organization.

  After you select this check box, users in your Exchange organization can still send messages to the recipient by using the e-mail address.
- **Send out-of-office message to originator** Select this check box to allow Out of Office messages from group members to be sent to the message sender. If this check box is selected, users who send messages to the group will receive Out of Office replies from any member that has an Out of Office rule turned on.

  Clear this check box to prevent Out of Office replies from group members to be sent to the message sender.
- **Send delivery reports to group manager** Click this button to send non-delivery reports (NDRs) to only the group manager.
- **Send delivery reports to message originator** Click this button to send NDRs to the message sender.
- **Do not send delivery reports** Click this button to prevent the sending of NDRs.

10. Use the **Mail Flow Settings** tab to configure message size or message delivery restrictions for the dynamic distribution group. To view or change a mail flow setting, select the setting from the list, and then click **Properties**.
    - **Message Size Restrictions** Select this setting and then click **Properties** to open the **Message Size Restrictions** dialog box. Use this dialog box to configure the maximum message size in kilobytes (KB) that users are allowed to send to this group.

      If a message larger than the specified size is sent to the group, the message will be returned to the sender with a descriptive error message.

      In the **Message Size Restrictions** dialog box, select the **Maximum message size (in KB)** check box to set the maximum size for messages that can be received by this group. Use the corresponding box to specify the maximum message size allowed (in KB). The message size must be between 0 and 2,097,151 KB.

      Clear the **Maximum message size (in KB)** check box to remove the size restrictions for receiving messages.
    - **Message Delivery Restrictions** Select this setting and then click **Properties** to open the **Message Delivery Restrictions** dialog box. Use this dialog box to configure the following settings:

      All senders Click this button to allow the group to accept messages from all senders. This includes senders in both your Exchange organization and external senders. This button is selected by default. This option includes external users only if you clear the **Require that all senders are authenticated** check box. If you select this check box, messages from external users will be rejected.

      Only senders in the following list Click this button to specify that the group can accept messages only from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all

recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.
Require that all senders are authenticated Select this check box to prevent anonymous users from sending messages to the group. By default, this check box is selected for dynamic distribution groups. This prevents external senders from sending messages to dynamic distribution groups.
No Senders Click this button to specify that the group will not reject messages from any senders in the Exchange organization. This button is selected by default.
Senders in the following list Click this button to specify that the group will reject messages from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.

Use the Shell to configure dynamic distribution group properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Dynamic distribution groups" entry in the Mailbox Permissions topic.

This example changes the *MaxSendSize* property to 20MB and sets the *ModerationEnabled* property to `$True`:

```
Set-DynamicDistributionGroup "Seattle Employees" -MaxSendSize 20MB -ModerationEna
```

This example adds a second SMTP e-mail address and changes the group manager to John.

```
Set-DynamicDistributionGroup -Identity "Seattle Employees" -ManagedBy 'mail.conto
```

For detailed syntax and parameter information, see Set-DynamicDistributionGroup

For More Information

Understanding Recipients

Managing Distribution Groups

1.8.3.10.12 Configure Dynamic Distribution Groups in a Hybrid Deployment

Configure Dynamic Distribution Groups in a Hybrid Deployment

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-23*

In a hybrid deployment environment between Microsoft Exchange Online and on-premises Microsoft Exchange organizations, the Microsoft Online Services Directory Synchronization Tool (DirSync) cannot be used to synchronize dynamic distribution groups to Exchange Online. Therefore, mailboxes that have been moved to Exchange Online cannot send mail to dynamic distribution lists. To work around this issue, create a contact in Exchange Online for the dynamic distribution list, and then grant permissions so that only authenticated senders can submit messages to the new contact.

Looking for other management tasks related to Managing Distribution Groups? Check out Managing Distribution Groups.

Looking for more information about hybrid deployments? Check out Hybrid Deployments.

Prerequisites

- Hybrid deployment between an on-premises Exchange organization and Exchange Online.

Enable Exchange Online users to send mail to a dynamic distribution list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Dynamic distribution groups" entry in the Mailbox Permissions topic.

Consider the scope of the dynamic distribution group before the hybrid deployment and before the mailboxes were moved to Exchange Online. If the scope included only mailboxes, the scope must be expanded to include mail users and mail contacts. To do this, follow these steps:

1. On an on-premises Exchange server, start the Exchange Management Console (EMC).
2. In the console tree, navigate to Recipient Configuration. Beneath that, navigate to Distribution Group.
3. In the results pane, click the dynamic distribution group that you want to configure.
4. In the Action pane, click **Properties**.
5. On the **Filter** tab, select **The following specific types**, and then click to select the **Users with Exchange mailboxes** and the **Users with external e-mail addresses** check boxes.
6. Click **Apply**. Then, click **OK**.

To create a contact in Exchange Online to represent the dynamic distribution group, follow these steps:

1. Sign in to Outlook Web App on the Office 365 tenant by using a service administrator account.
2. Click **Options**, and then click **See all options**.
3. Click **Manage Myself**, and then click **Manage Organization**.
4. Click **Users and Groups**, and then click **External Contacts**.
5. Click **New**, and then type the contact details.
6. In the **External e-mail address** box, type the mail address of the Dynamic Distribution group that was created on the on-premises Exchange server.
7. Click **Save**.

Exchange Online users can now select the dynamic distribution group from the global address list (GAL). When they do, messages will be delivered to the members of the group as defined by the settings for the group.

For More Information

Configure Dynamic Distribution Group Properties

Create a Dynamic Distribution Group

Exchange Hybrid Deployment and Migration with Office 365

1.8.3.10.13 Mail-Enable or Mail-Disable a Distribution Group

Mail-Enable or Mail-Disable a Distribution Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can mail-enable or mail-disable a distribution group. By default, distribution groups are mail-enabled when created.

Looking for additional management tasks related to distribution groups? Check out Managing Distribution Groups.

Use the EMC to mail-enable a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.
2. In the action pane, click **New Distribution Group**. The New Distribution Group wizard appears.
3. On the **Introduction** page, click **Existing Group**, and then click **Browse**.
4. In **Select Group**, select the group that you want to mail-enable, and then click **OK**.
5. On the **Group Information** page, in the **Alias** box, type the name of the alias for the group. The alias can't exceed 64 characters and must be unique in the forest.

   Note:

   The **Name** and **Name (pre-Windows 2000)** boxes are read-only and can't be modified at this time. If you want to modify these names, use the **Group Information** tab in the distribution group's properties.

6. On the **New Distribution Group** page, review the **Configuration Summary**. To make any configuration changes, click **Back**. To mail-enable the group, click **New**.
7. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the EMC to mail-disable a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.
2. In the result pane, select the group that you want to mail-disable.
3. In the action pane, under the group name, click **Disable**.
4. A warning appears confirming that you want to mail-disable the group. Click **Yes**.

Use the Shell to mail-enable a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

This example mail-enables the security group Schema Admins. When you mail-enable a group, you must specify the alias, display name, and primary SMTP address.

```
Enable-DistributionGroup -Identity "Schema Admins" -Alias "SchemaAdmins" -Display
```

For detailed syntax and parameter information, see Enable-DistributionGroup.

Use the Shell to mail-disable a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

After you disable a distribution group, you can remove it from the global address list (GAL), without removing it from Active Directory. The Active Directory group object still exists, but the distribution group will be unable to send or receive mail.

This example disables the distribution group Employee Garage Sales.

```
Disable-DistributionGroup -Identity "Employee Garage Sales"
```

For detailed syntax and parameter information, see Disable-DistributionGroup.

1.8.3.10.14 Mail-Enable or Mail-Disable a Security Group

Mail-Enable or Mail-Disable a Security Group

Mailbox > Managing Mailbox Servers > Managing Distribution Groups >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Security groups are used to grant access permissions to resources in Active Directory. If you mail-enable the security group, you can send e-mail to all members of that group. For example, if you create a security group that gives members access to the computers in a specific server lab, you may want to send mail to that group to notify them of a power outage in the lab.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Use the EMC to mail-enable a security group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.
2. In the action pane, click **New Distribution Group**. The New Distribution Group wizard appears.
3. On the **Introduction** page, click **Existing Group**, and then click **Browse**.
4. In the **Select Group** dialog box, select the security group that you want to mail-enable, and then click **OK**.

   Note:

   If the security group that you want to mail-enable doesn't appear in the list, you may need to change the recipient scope. For more information, see Change the Recipient Scope.

5. Click **Next**.
6. On the **Group Information** page, complete the following fields:
   - **Name** This read-only field shows the security group's display name. If you want to modify this name, use the **General** tab in **<Security group> Properties**.
   - **Name (pre-Windows 2000)** This read only field shows the name for the group that's compatible with legacy versions of Windows (prior to the release of Windows 2000 Server).
   - **Alias** Use this box to type an alias for the security group. The alias can't exceed 64 characters and must be unique in the forest.
7. Click **Next**.
8. On the **New Distribution Group** page, review the **Configuration Summary**. To make any configuration changes, click **Back**. To mail-enable the security group, click **New**.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the EMC to mail-disable a security group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution**

Group.
2. In the result pane, select the security group that you want to mail-disable.
3. In the action pane, under the group name, click **Disable**.
4. A warning appears confirming that you want to mail-disable the group. Click **Yes**.

Use the Shell to mail-enable a security group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

This example mail-enables the Server Lab 222 security group.

```
Enable-DistributionGroup -Identity "Server Lab 222"
```

Note:
You may need to change the recipient scope to access security groups. For more information, see Change the Recipient Scope.

For detailed syntax and parameter information, see Enable-DistributionGroup.

Use the Shell to mail-disable a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

After you disable a distribution group, you can remove it from the global address list (GAL), without removing it from Active Directory. The Active Directory group object still exists, but the distribution group will be unable to send or receive mail.

This example disables the distribution group Employee Garage Sales.

```
Disable-DistributionGroup -Identity "Employee Garage Sales"
```

For detailed syntax and parameter information, see Disable-DistributionGroup.

Other Tasks

After you mail-enable the security group, you may also want to:

- Add a Member to a Distribution Group
- Remove a Distribution Group Member

Manage the Members of Distribution Groups

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-03-07*

Microsoft Exchange Server 2010 provides a new feature to manage distribution groups. This feature lets your users join existing groups, manage some of the properties of groups that they own, manage their membership in groups that they own, and even create and remove groups.

Manage Distribution Groups

Microsoft Exchange Server 2010 now offers users the ability to manage distribution groups with more control than that provided by Microsoft Office Outlook 2007. This new feature lets your users join existing groups, manage some of the properties of groups that they own, manage membership in groups that they own, and even create and remove groups.

By default, this feature is turned off. To turn on this feature, use the Exchange Control Panel (ECP) to assign the **MyDistributionGroups RBAC** role to the **Default Role Assignment Policy**.

Although some customers want their users to have the ability to create and remove distribution groups on this role, the control that is offered by this new feature may be more than you want to provide the users on your network.

For example, you may want to modify the functionality of this feature to meet any of the following goals:

- Let users manage distribution groups they own.
- Not let users be able to create distribution groups.
- Not let users be able to remove distribution groups, including those that they own.

To help you change the functionality of the new feature, use the ManageGroupManagementRole.ps1 script. This script is available from the TechNet Script Center. To use this script, follow these steps:

1. Obtain the script by visiting the following TechNet Script Center Web site: Manage-GroupManagementRole.ps1.
2. Copy the contents of the script to a text file on the computer on which you want to run it, and then save the file by using the following filename: **Manage-GroupManagementRole.ps1**.
3. At an Exchange PowerShell command prompt, run the following command: **Manage-Groupmanagmentrole.ps1 -creategroup –removegroup**.

This combination of switches makes the changes that are described in the example mentioned earlier. When the script is finished running, your users will be able to manage distribution groups, but not create or remove them. When you run the script, the script performs the following actions:

1. Creates a new RBAC role that is a child of the MyDistributionGroups Role.
   Removes the **remove-distributiongroup** cmdlet and the **new-distributiongroup** cmdlet from the role that you just created.
   Assigns the new role to the Default Role Assignment Policy.

For more information about how to use this script, examine the contents of the script file.

Or, run the script without switches. Each step that the script takes is documented in the script. You can extract from the script just what you require to change the functionality of the manage distribution groups feature. The script is designed to be flexible. If you run the script by using the default settings, you get a new role and a new role assignment.

How to Use Groups to Manage Groups in Exchange 2010

In Exchange 2010, distribution groups cannot be managed by groups; only individual users can manage groups. This behavior differs from Microsoft Exchange Server 2003, in which you use groups to manage a distribution group. In Exchange 2003, group ownership is handled at a different level. If you move mailboxes from Exchange 2003 to Exchange 2010, members of a group that managed a distribution group in Exchange 2003 can no longer modify the group in Exchange 2010.

The Set-DistributionGroupOwners.ps1 script lets you work around this changed behavior. The script enables you to simulate group ownership of a distribution group in Exchange 2010.

You can run the script in the following modes, depending on the switches that you use together with the script.

- Mode 1: Set Ownership for a particular distribution group. Modifications to the **ManagedBy** attribute are not set at this time. Instead, the script modifies a custom attribute to obtain the information it will require later to set the ManagedBy **attribute**.
- Mode 2: Modify the **ManagedBy** attribute of a specific distribution group so that the members of either a security group or a distribution group can manage the group.
- Mode 3: Automate the process. This mode is designed to be run as a scheduled task and to make sure that individual members of a group have ownership of the distribution group that they are set to own. Use this mode if you prefer to automate the process and, perhaps, run it nightly to find any changes to security group and distribution group membership.

Important:

Windows Server 2008 R2 is required to run the Set-DistributionGroupOwners.ps1 script. The script does not have to be run on a server that's running Exchange Server. However, the Exchange management tools must be installed on the computer on which you run the script.

To run the Set-DistributionGroupOwners.ps1 script, follow these steps:

1. Visit the Script Center, and then download Set-DistributionGroupOwners.txt from the following Web page: Set-DistributionGroupOwners.
2. Change the file name extension from **.txt** to **.ps1**. The filename should now be **Set-DistributionGroupOwners.ps1**.
3. By default, the script populates the **CustomAttribute5** field by using the Distinguished Name (DN) of the group. The DN is specified in the **ManagedBy** attribute of the distribution group that you want to manage. You can change the default behavior to use one of the 15 custom attributes in the default schema. Determine which custom attribute works in your environment. To change the custom attribute, follow these steps:
   3.a. Open the Set-DistributionGroupOwners.ps1 file in Notepad.
   3.b. Locate the following text: **$dn_storage = "CustomAttribute5"**.
   3.c. Change **CustomAttribute5** to the custom attribute that you want to use.
   3.d. Save and then close the Set-DistributionGroupOwners.ps1 file.
4. Determine which of the following modes you want to use to run the script.
   4.a. **Mode 1 - Set Ownership of a Group** In this mode, run the script

together with the *–DistributionGroup* and *–GroupOwner* parameters. Specify the distribution group (-DistributionGroup) and the group that you want to manage it (-GroupOwner). This resets the DN of the owning group (as specified in *–GroupOwner*) to the custom attribute for the Distribution Group (as specified in *–DistributionGroup*).

4.b. **Mode 2 - Modify the ManagedBy attribute for one Group** Mode 2 or Mode 3 don't work until you set the value of the customer attribute to the DN of the owning group. If you have already run the Script in Mode 1, Mode 2 configures the *ManagedBy* attribute for a single group. To run the script in Mode 2, specify only the *–DistributionGroup* parameter, and list the DL that you want to have processed.

4.c. **Mode 3 – Run the Script as a Scheduled Task to look all new modifications to Group Ownership** When you run the script without switches, the script searches the directory in Active Directory Domain Services for all groups that have the defined custom attribute set to a DN. Then, it processes all the groups as in Mode 2. The script is designed to be run in this mode as either a one-off kind of operation for which you know updates are needed or as a scheduled task to keep everything in sync. A key point is that when the script populates the **ManagedBy** attribute, it overwrites the existing values by using the current members of the owning group.

For more information about custom attributes, see Understanding Custom Attributes.

For more information about managing distribution groups, see Managing Distribution Groups.

1.8.3.10.16 Remove a Distribution Group

Remove a Distribution Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove a distribution group from Microsoft Exchange and Active Directory. To disable a distribution group without removing the Active Directory object, see Mail-Enable or Mail-Disable a Distribution Group.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Use the EMC to remove a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.
2. In the result pane, select the distribution group that you want to remove.
3. In the action pane, under the name of the distribution group, click **Remove**.
4. A warning appears confirming that you want to remove the distribution group. Click **Yes**.

Use the Shell to remove a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

This example removes the distribution group Temporary Staff.

```
Remove-DistributionGroup -Identity "Temporary Staff"
```

When prompted, type **Y** to confirm the removal of the distribution group.

For detailed syntax and parameter information, see Remove-DistributionGroup.

1.8.3.10.17 Remove a Distribution Group Member

Remove a Distribution Group Member

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove members from a distribution group by using the EMC or the Shell.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Use the EMC to remove a member from a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.
2. In the result pane, select the distribution group from which you want to remove a recipient.
3. In the action pane, under the distribution group name, click **Properties**.
4. In **<Distribution Group> Properties**, on the **Members** tab, click the recipient you want to remove, and then click  .
5. Click **OK**.

Use the Shell to remove a member from a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

This example removes the user adam@contoso.com from the distribution group Marketing

Managers.

```
Remove-DistributionGroupMember -Identity "Marketing Managers" -Member adam@contos
```

When prompted, type **Y** to confirm the removal.

For detailed syntax and parameter information, see Remove-DistributionGroupMember.

1.8.3.10.18 Stop Automatic Conversion of Universal Distribution Groups to Universal Security Groups

Stop Automatic Conversion of Universal Distribution Groups to Universal Security Groups

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Universal distribution groups and universal security groups are groups of recipients created to expedite the mass sending of e-mail messages and other information. However, unlike universal distribution groups, universal security groups can also be used to assign permissions.

In Microsoft Exchange, only Active Directory objects that have security principals can be used to grant permission to a public folder or to a mailbox folder. However, it's possible for a Microsoft Outlook user to use a universal distribution group to grant permission to a public folder or to a mailbox folder. In this case, the universal distribution group is automatically converted to a universal security group by the Microsoft Exchange Information Store service. This is the default behavior in Exchange Server 2010 and Exchange Server 2007.

You can modify this behavior to prevent the automatic conversion of universal distribution groups to universal security groups. The **msExchDisableUDGConversion** attribute of your Exchange organization object in Active Directory is used to control how the Microsoft Exchange Information Store service responds to requests for conversion of universal distribution groups to universal security groups. The following are the acceptable values for the **msExchDisableUDGConversion** attribute:

- **0** If the attribute is set to 0, or if it isn't configured, universal distribution groups are automatically converted to universal security groups when they're used to grant permissions to public folders or mailbox folders.
- **1** If the attribute is set to 1, Outlook can't request the conversion. However, Exchange system processes can still convert a universal distribution group to a universal security group.
- **2** If the attribute is set to 2, automatic conversions can't occur.

This topic explains how to use Active Directory Service Interfaces (ADSI) Edit to modify the **msExchDisableUDGConversion** attribute to prevent the automatic conversion of universal distribution groups to universal security groups.

Use ADSI Edit to stop the automatic conversion of universal distribution groups to universal security groups

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

1. Start ADSI Edit.
2. In the console tree, expand **Configuration Container**.

   Note:
   If you don't see **Configuration Container**, you'll need to connect to it. From the **Action** menu, click **Connect to**. In **Connection Settings**, select **Configuration** from the **Select a well known Naming Context** list, and then click **OK**.

3. Expand **CN=Configuration,DC=<domain>,DC=<domain extension>**. For example, if your Exchange organization is in the contoso.com forest, this folder name would be **CN=Configuration,DC=contoso,DC=com**.
4. Expand **CN=Services**.
5. Expand **CN=Microsoft Exchange**.
6. Right-click **CN=<Exchange organization name>**, and then click **Properties**.
7. In the **Attributes** list, select **msExchDisableUDGConversion**, and then click **Edit**.

   Note:
   If you can't find this property in the list, you'll need to turn on the ability to view optional settings. On the **Attribute Editor** tab, click **Filter**, and then, under **Show attributes**, select **Optional**.

8. In **Integer Attribute Editor**, in the **Value** box, type **2**, and then click **OK**.
9. Click **Apply**.
10. Click **OK**.

For More Information

For detailed steps about disabling automatic conversion of universal distribution groups to universal security groups in Exchange Server 2003 and Exchange 2000 Server, see Microsoft Knowledge Base article 843587, How to stop automatic conversion of universal distribution groups to universal security groups in Exchange 2000 and in Exchange 2003.

1.8.3.10.19 Turn Off User's Ability to Create Distribution Groups

Turn Off User's Ability to Create Distribution Groups

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

By default, all users in your Microsoft Exchange Server 2010 organization can create and manage distribution groups from their e-mail client. There are several ways to turn off a user's ability to create or manage distribution groups:

- Create an assignment policy and assign it to the users who shouldn't be allowed to create or manage distribution groups.
- Remove the My Distribution Groups and the My Distribution Group Membership roles from the default management role assignment policy.

The procedures in this topic assume that you haven't changed the name of the My Distribution Groups and My Distribution Group Membership management roles.

Looking for other management tasks related to distribution groups? Check out Managing Distribution Groups.

Prerequisites

Read Understanding Management Role Assignment Policies.

Use the Shell to create a role assignment policy to apply to specific users

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to create a role assignment policy to apply to specific users.

You can create a policy that doesn't contain the My Distribution Group and My Distribution Group Membership roles and apply that role to specific users in your organization. Those users won't be able to create or manage distribution groups.

1. Create a role assignment policy. This example creates the policy No Distribution Group Management.

```
New-RoleAssignmentPolicy "No Distribution Group Management"
```

2. Use a variable to get all of the roles assigned to the default role assignment policy.

```
$Roles = Get-ManagementRoleAssignment -RoleAssignee "Default Role Assi
```

Note:
The default role assignment policy that's installed with Exchange 2010 is named Default Role Assignment Policy. If you change the name of that policy or if you have a different default policy, you can locate the default policy by running the following command.

```
Get-RoleAssignmentPolicy | Where { $_.IsDefault -eq $True }
```

3. Add all of the roles assigned to the default assignment policy to the new role assignment policy, excluding the ones that contain the word distribution.

```
$Roles | Where {$_.Role -NotLike "*Distribution*" } | New-ManagementRo
```

4. Apply the No Distribution Group Management assignment policy to the appropriate users. This example applies the No Distribution Group Management role assignment policy to all mailboxes that have the *CustomAttribute1* value set to Contract Employee.

```
Get-Mailbox -Filter {CustomAttribute1 -eq "Contract Employee"} | Set-M
```

For detailed syntax and parameter information, see the following topics:

- Get-Mailbox
- Set-Mailbox
- Get-RoleAssignmentPolicy
- New-RoleAssignmentPolicy

Use the Shell to remove the My Distribution Groups and the My Distribution Groups Membership roles from the default management role

assignment policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:
You can't use the EMC to remove the My Distribution Groups and the My Distribution Group Membership roles from the default management role assignment policy.

Removing the My Distribution Groups and My Distribution Group Membership roles from the default role assignment policy is the easiest way to remove this permission from most users in your organization. However, this doesn't affect recipients who have been assigned a different role assignment policy.

Note:
By creating a default role assignment policy, you can save the master settings and create additional policies from it.

1. Create a role assignment policy. This example creates the policy No Distribution Group Management.

```
New-RoleAssignmentPolicy "No Distribution Group Management"
```

2. Use a variable to get all of the roles assigned to the Default Role Assignment Policy.

```
$Roles = Get-ManagementRoleAssignment -RoleAssignee "Default Role Assi
```

Note:
The default role assignment policy that's installed with Exchange 2010 is named Default Role Assignment Policy. If you change the name of that policy or if you have a different default policy, you can locate the default policy by running the following command.

```
Get-RoleAssignmentPolicy | Where { $_.IsDefault -eq $True }
```

3. Add all of the roles assigned to the default assignment policy to the new role assignment policy, excluding the ones that contain the word distribution.

```
$Roles | Where {$_.Role -NotLike "*Distribution*" } | New-ManagementRo
```

4. Make the new role assignment policy the default policy so that it will apply to all users in the organization.

```
Set-RoleAssignmentPolicy "No Distribution Group Management" -IsDefault
```

5. Rename the old default role assignment policy something more appropriate. This example renames it Old_Default Role Assignment Policy.

```
Set-RoleAssignmentPolicy "Default Role Assignment Policy" -Name "Old_D
```

For detailed syntax and parameter information, see the following topics:

- Get-RoleAssignmentPolicy
- Set-RoleAssignmentPolicy
- New-RoleAssignmentPolicy

1.8.3.10.20 View Members of a Dynamic Distribution Group

View Members of a Dynamic Distribution Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Dynamic distribution groups are distribution groups whose membership is based on specific recipient filters rather than a defined set of recipients. Microsoft Exchange Server 2010 provides precanned filters to make it easier to create recipient filters for dynamic distribution groups. A *precanned filter* is a commonly used filter that you can use to meet a variety of recipient-filtering criteria. You can specify the recipient types you want to include in a dynamic distribution group. Additionally, you can also specify a list of conditions that the recipients must meet. You can use both the EMC and the Shell to preview the list of recipients for a dynamic distribution group that uses precanned filters.

You can also specify conditions based on recipient fields other than what the precanned filters provide. To do this, you must use the Shell to create a custom query for the dynamic distribution group. Filter and condition settings for dynamic distribution groups that have custom recipient filters can be managed only by using the Shell.

Looking for other management tasks related to dynamic distribution groups? Check out Managing Distribution Groups.

Use the EMC to preview the list of members for a dynamic distribution group that uses precanned filters

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Dynamic distribution groups" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Distribution Group**.
2. In the result pane, select the dynamic distribution group for which you want to preview the list of members.
3. In the action pane, under the dynamic distribution group name, click **Properties**.
4. In **<Dynamic distribution group> Properties**, click the **Conditions** tab.
5. Click **Preview**.

Use the Shell to preview the list of members of a dynamic distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Dynamic distribution groups" entry in the Mailbox Permissions topic.

This example returns the list of members for the dynamic distribution group Marketing Department. The first command stores the dynamic distribution group object in the variable `$MarketingDepartment`. The second command uses the **Get-Recipient** cmdlet to list the recipients that match the criteria defined for the dynamic distribution group.

```
$MarketingGroup = Get-DynamicDistributionGroup "Marketing Group"
Get-Recipient -RecipientPreviewFilter $MarketingGroup.RecipientFilter -Organizati
```

For detailed syntax and parameter information, see Get-DynamicDistributionGroup and Get-Recipient.

1.8.3.11 Managing E-Mail Address Policies

Managing E-Mail Address Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-16*

Apply an E-Mail Address Policy

Create an E-Mail Address Policy

Create an E-Mail Address Policy By Using Recipient Filters

Change E-Mail Address Policy Priorities

Edit an E-Mail Address Policy

Remove an E-Mail Address Policy

View the Members of an E-Mail Address Policy by Using the Exchange Management Shell

1.8.3.11.1 Apply an E-Mail Address Policy

Apply an E-Mail Address Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

E-mail address policies generate the primary and secondary e-mail addresses for your recipients (which include users, contacts, and groups) so they can receive and send e-mail. After you create an e-mail address policy, you need to apply it to the intended recipients for the policy to take effect.

Note:

Although this topic shows you how to use the Apply E-Mail Address Policy wizard to apply an e-mail address policy, the New E-Mail Address Policy and the Edit E-Mail Address Policy wizards also allow you to apply the policy as you create or edit it.

Looking for other management tasks related to e-mail address policies? Check out Managing E-Mail Address Policies.

Prerequisites

You can't edit e-mail address policies that were created in the Shell with a recipient filter. For more information, see Create an E-Mail Address Policy By Using Recipient Filters.

What Do You Want to Do?

- Use the EMC to apply an e-mail address policy
- Use the Shell to apply an e-mail address policy

Use the EMC to apply an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **E-Mail Address Policies** tab, and then select the e-mail address policy that you want to apply.
3. In the action pane, click **Apply**.
4. On the **Introduction** page, complete the following fields:
   - **Apply the e-mail address policy** Select one of the following schedule settings to specify when the e-mail address policy should be applied:
     Immediately Select this option to apply the e-mail address policy immediately.
     At the following time Select this option and use the corresponding lists to specify a time to apply the e-mail address policy.
   - **Cancel tasks that are still running after (hours)** Select this check box and use the corresponding text box to specify how long the e-mail address policy task will run. The default is 8 hours.
5. On the **Apply E-Mail Address Policy** page, review your configuration settings. Click **Apply** to apply the e-mail address policy. Click **Back** to make configuration changes.

   Note:
   Although the process begins when you click **Apply**, you may have to wait several hours for the process to complete and the e-mail address policy to be applied.
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to apply an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

This example applies the e-mail address policy Marketing.

```
Update-EmailAddressPolicy -Identity Marketing
```

Note:
Although running the **Update-EmailAddressPolicy** cmdlet starts the update process, you may have to wait several hours for the process to complete and the e-mail address policy to be applied.

For syntax and parameter information, see Update-EmailAddressPolicy.

For More Information

Understanding E-Mail Address Policies

Edit an E-Mail Address Policy

1.8.3.11.2 Create an E-Mail Address Policy

Create an E-Mail Address Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

For a recipient to receive or send e-mail messages, the recipient must have an e-mail address. E-mail address policies generate the primary and secondary e-mail addresses for your recipients (which include users, contacts, and groups) so they can receive and send e-mail.

Looking for other management tasks related to e-mail address policies? Check out Managing E-Mail Address Policies.

Prerequisite

Before an SMTP address domain can be used in an e-mail address policy, you must configure an accepted domain. For more, see Understanding Accepted Domains.

What Do You Want to Do?

- Use the EMC to create an e-mail address policy
- Use the Shell to create an e-mail address policy

Use the EMC to create an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the action pane, click **New E-mail Address Policy**.
3. On the **Introduction** page, complete the following fields to define the recipient scope:

- **Name** Use this text box to create the display name for the new e-mail address policy. The name can contain as many as 64 characters but cannot include wildcard characters.
- **Select the recipient container where you want to apply this filter** Click **Browse** to open the **Select Organizational Unit** dialog box. Specify an organizational unit (OU), and then click **OK**. The recipient container filters the recipients that the e-mail address policy will affect based upon their location in Active Directory.
- Select the recipient types you want to include in the policy. You can select **All recipient types** or **The following specific types**. If you select **The following specific types**, you can select one or more of the following recipient types:

  Users with Exchange mailboxes Select this check box if you want your e-mail address policy to apply to users with Exchange 2010, Exchange 2007, or Exchange 2003 mailboxes. Users with Exchange mailboxes are those that have a user domain account and a mailbox in the Exchange organization.

  Users with external e-mail addresses Select this check box if you want your e-mail address policy to apply to users with external e-mail addresses. Users with external e-mail accounts have user domain accounts in Active Directory, but use e-mail accounts that are external to the organization. This enables them to be included in the global address list (GAL) and added to distribution lists.

  Resource mailboxes Select this check box if you want your e-mail address policy to apply to Exchange resource mailboxes. Resources mailboxes allow you to administer company resources through a mailbox, such as a conference room or company vehicle.

  Contacts with external e-mail addresses Select this check box if you want your e-mail address policy to apply to contacts with external e-mail addresses. Contacts with external e-mail accounts do not have user domain accounts in Active Directory, but the external e-mail address is available in the GAL.

  Mail-enabled groups Select this check box if you want your e-mail address policy to apply to security groups or distribution groups that have been mail-enabled. Mail-enabled groups are similar to distribution groups. E-mail messages that are sent to a mail-enabled group account will be delivered to several recipients.

4. On the **Conditions** page, compete the following fields to further filter the recipients who will be affected by this e-mail address policy:

   Step 1: Select condition(s) Use this section to select one or more conditions for your e-mail address policy. If you don't want to set any conditions for the policy, don't select any of the check boxes. Select from the following conditions:

   - **Recipient is in a State or Province** Select this check box if you want the e-mail address policy to include only recipients from specific states or provinces. This information is contained on the **Address and Phone** tab in the recipient's properties.
   - **Recipient is in a Department** Select this check box if you want the e-mail address policy to include only recipients in specific departments. This information is contained on the **Organization** tab in the recipient's properties.
   - **Recipient is in a Company** Select this check box if you want the e-mail address policy to include only recipients in specific companies. This information is contained on the **Organization** tab in the recipient's properties.

Note:
The **State or Province**, **Department**, and **Company** conditions are based on attributes that are applicable only to mailboxes, mail users, and mail contacts. These conditions do not apply to mail-enabled distribution groups. If you configure any of these conditions for an e-mail address policy, you will in effect be excluding all mail-enabled distribution groups.

- **Custom Attribute equals Value** There are 15 custom attributes for each recipient. There is a separate condition for each custom attribute. If you want the e-mail address policy to include only recipients that have a specific value set for a specific custom attribute, select the check box that corresponds to that custom attribute.

Step 2: Edit the conditions by selecting an underlined value If you select any conditions in Step 1, each condition you select will append to the definition of the e-mail address policy. For example, if you selected the **Recipient is in a State or Province** check box in Step 1, you will see **in the specified State or Province(s)** condition in Step 2.
For each condition, click the underlined term to create your condition. By default, the underlined term for new conditions will read **specified**. After you edit the condition, the underlined term will change to the value that you specified.
If you click an underlined value for the **State or Province**, **Department**, or **Company** conditions, a dialog box appears in which you can specify the values for the condition. To create values for the condition, use the following buttons in the dialog box:

- **Add** Enter a value in the text box and click **Add**. You can add more than one value, but you cannot enter duplicate values.
- **Edit** To modify an existing value, select it from the list, and then click **Edit**.
- To remove an existing value, select it from the list, and then click .

If you click an underlined value for a custom attribute condition, a dialog box appears in which you can specify the value for the condition. You can specify a single value for each custom attribute. Type the value in the text box and click **OK**.

Important:
The values that you enter in these dialog boxes must exactly match those that appear in the recipient's properties. For example, if you enter **Washington** in the **Specify State or Province** dialog box, but the **Address and Phone** tab in the recipient's properties lists the state as **WA**, the condition will not be met.

Preview Click this button to view the recipients that will be contained in the e-mail address policy, based on the conditions that you specified.

5. On the **E-Mail Addresses** page, specify an e-mail address for your e-mail address policy.
   - **Add** Click **Add** to add a new e-mail address for the policy. Use the drop-down box to select from the following address types:

     SMTP Address This is the default address type. Click this button and use the corresponding dialog box to add an SMTP address. The following settings are available:
     ?Select the **E-mail address local part** check box and use the corresponding options to configure how the local part of the SMTP e-mail address will appear. The local part of an e-mail address is the name that appears before the at sign (@). If you clear the check box, the local part uses the recipient's alias.
     ?Click **Select the accepted domain for the e-mail address** and then click **Browse** to select the e-mail address domain to which this e-mail address policy applies. You can also create additional e-mail address policies if your organization receives mail for multiple domains, or if your default domain is used strictly for

internal purposes and you use a different external mail domain.
?Click **Specify the custom fully qualified domain name (FQDN) for the e-mail address**, and then type the FQDN for the domain part of the e-mail address that appears after the at sign (@). This FQDN must match an accepted domain.
Custom Address Click this button and use the corresponding dialog box to add a custom address (for example, fax or X.400).

Note:
With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.

- **Edit** Click this button to modify the selected e-mail address.
- **Set as Reply** Click this button to set your selected address as the "reply to" address. A recipient can have multiple e-mail addresses for a specific address type. This allows the recipient to receive messages that are addressed to any one of these e-mail addresses. However, a single address must be used for any messages that are sent by the recipient. If a recipient has multiple e-mail addresses, the primary address is used for any messages sent by the recipient.
  This button is available only when an address other than the primary address is selected. Primary addresses for each address type are displayed in bold type.
  If an e-mail address policy in your Exchange organization applies to a mailbox, the **Set as Reply** setting will be controlled by that policy. To change the primary address for a specific address type, you must clear the **Automatically update e-mail addresses based on e-mail address policy** check box.

6. On the **Schedule** page, complete the following fields:
   - **Apply the e-mail address policy** Select one of the following options to specify when the e-mail address policy should be applied.
     Do not apply Click this button to create the e-mail address policy without applying it to the mailboxes. For more information, see Apply an E-Mail Address Policy.
     Immediately Click this button to apply the e-mail address policy as soon as the e-mail address policy is created.
     At the following time Click this button and use the corresponding lists to specify a time to apply the new e-mail address policy.
   - **Cancel tasks that are still running after (hours)** Select this check box and use the corresponding text box to specify how long the new e-mail address policy task will run. The default is 8 hours.

7. On the **New E-Mail Address Policy** page, review your configuration settings. Click **New** to create the e-mail address policy. Click **Back** to make configuration changes.

8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
9. Click **Finish** to close the wizard.

Use the Shell to create an e-mail address

policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

This example creates a e-mail address policy that includes mailbox users in the Southeast offices who will have e-mail addresses that include their last name combined with the first two letters of their first name.

```
New-EmailAddressPolicy -Name "southeast offices" -IncludedRecipients MailboxUsers
```

For More Information

Understanding E-Mail Address Policies

Apply an E-Mail Address Policy

Edit an E-Mail Address Policy

1.8.3.11.3 Create an E-Mail Address Policy By Using Recipient Filters

Create an E-Mail Address Policy By Using Recipient Filters

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to create an e-mail address policy by using recipient filters. To learn more about e-mail address policies, see Understanding E-Mail Address Policies.

Looking for other management tasks related to e-mail address policies? Check out Managing E-Mail Address Policies.

Prerequisites

- Before an SMTP address domain can be used in an e-mail address policy, you must configure an accepted domain. For information about configuring accepted domains, see Understanding Accepted Domains.
- To use the *RecipientFilter* parameter to create a custom filter, you must specify a string for the filter. The Shell uses OPath for the filtering syntax. OPath is a querying language designed to query object data sources. For more information about the OPath filtering syntax, see Creating Filters in Recipient Commands.

Important:

If you use a recipient filter to create or edit an e-mail address policy, you can't use the EMC to edit the e-mail address policy. You must use the **Set-EmailAddressPolicy** cmdlet in the Shell. For detailed syntax and parameter information, see Set-EmailAddressPolicy.

Use the Shell to create an e-mail address

policy by using recipient filters

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to create an e-mail address policy by using recipient filters.

To create an e-mail address policy by using recipient filters, use the following syntax.

```
New-EmailAddressPolicy -Name <String> -RecipientFilter <String>
```

This example creates an e-mail address policy that applies to all executives and for which the local part of the e-mail address consists of the first two letters of their first name and their entire last name.

```
New-EmailAddressPolicy -Name 'Execs' -EnabledEmailAddressTemplates 'SMTP:%2g%s@co
```

For detailed syntax and parameter information, see New-EmailAddressPolicy.

1.8.3.11.4 Change E-Mail Address Policy Priorities

Change E-Mail Address Policy Priorities

Mailbox > Managing Mailbox Servers > Managing E-Mail Address Policies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the **Change Priority** dialog box to change the priority of your e-mail address policies.

When you create an e-mail address policy in the Exchange Management Console (EMC), or when you create a policy in the Exchange Management Shell and don't define the priority, by default, the new e-mail address policy will be assigned a priority of 1. However, if you already specified a priority for the policy, subsequent policies that you create will be assigned a lower priority.

For example, let's say you already have two e-mail address policies, and you used the EMC or the Shell to assign them priorities of 1 and 2**.** If you create another policy, it will automatically be assigned a priority of 3. However, let's say you have two policies, and you used the EMC or the Shell to specify that one of them is priority 1, but the other policy was assigned a default priority of 2 when it was created. In this case, the next policy you create will, by default, become the priority 2 policy. The previous priority 2 policy will be assigned a priority of 3.

Note:
You can't change the priority of the Default Policy. The Default Policy's priority will always be "Lowest".

Looking for other management tasks related to e-mail address policies? Check out Managing E-Mail Address Policies.

What Do You Want to Do?

- Use the EMC to change the priority of an e-mail address policy

- Use the Shell to change the priority of an e-mail address policy

Use the EMC to change the priority of an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **E-Mail Address Policies** tab, and then select the e-mail address policy for which you want to change the priority.
3. In the action pane, click **Change Priority**.

   Note:
   This action is available only when you have more than one e-mail address policy (not including the default policy).

4. In **Change E-mail Address Policy Priority**, type the priority number for the e-mail address policy.

   Note:
   You can't change the priority to a level higher than the number of e-mail address policies you currently have in your organization.

5. Click **OK**.

Use the Shell to change the priority of an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

This example changes the priority of the e-mail address policy Conference Rooms to priority 5.

Note:
You can't change the priority to a level higher than the number of e-mail address policies you currently have in your organization.

```
Set-EmailAddressPolicy -Identity "Conference Rooms" -Priority 5
```

For More Information

Understanding E-Mail Address Policies

Edit an E-Mail Address Policy

1.8.3.11.5 Edit an E-Mail Address Policy

Edit an E-Mail Address Policy

Mailbox > Managing Mailbox Servers > Managing E-Mail Address Policies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

E-mail address policies generate the primary and secondary e-mail addresses for your recipients (which include users, contacts, and groups) so they can receive and send e-mail. You can use the Edit E-mail Address Policy wizard to modify the settings of a policy.

Looking for other management tasks related to e-mail address policies? Check out Managing E-Mail Address Policies.

Caution

You can't use the EMC to edit an e-mail address policy if the policy was created by using one of the following methods:

- **Exchange Server 2003** If this is an Exchange Server 2003 e-mail address policy, you must use Exchange System Manager in Exchange 2003 to edit this object or upgrade the object to an Exchange 2010 object. For more information, see Upgrade Custom LDAP Filters to OPATH Filters.
- **Exchange Management Shell** Some e-mail address policy settings that you can set in the Shell cannot be managed in the EMC. If this is an e-mail address policy that was created or edited by using the Shell, use the Shell to edit this policy.

What Do You Want to Do?

- Use the EMC to edit an e-mail address policy
- Use the Shell to edit an e-mail address policy

Use the EMC to edit an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **E-mail Address Policies** tab, and then select the policy you want to edit.
3. In the action pane, click **Edit**.
4. On the **Introduction** page, edit the following fields to define the recipient scope:
   - **Name** This box contains the display name of the e-mail address policy that you specified when it was created. You can modify the name. The name can contain as many as 64 characters but cannot include wildcard characters.
   - **Select the recipient container where you want to apply the filter** If you want to specify a different recipient container, click **Browse** to open the **Select Organizational Unit** dialog box. Specify an organizational unit (OU), and then click **OK**. The recipient container filters the recipients that the e-mail address policy will affect based upon their location in Active Directory.
   - Select the recipient types you want to include in the policy. You can select **All recipient types** or **The following specific types**. If you select **The following specific types**, you can select one or more of the following recipient types:

     Users with Exchange mailboxes Select this check box if you want your e-mail address policy to apply to users who have Exchange 2010, Exchange Server 2007, or Exchange Server

2003 mailboxes. Users with Exchange mailboxes are those that have a user domain account and a mailbox in the Exchange organization.
Users with external e-mail addresses Select this check box if you want your e-mail address policy to apply to users who have external e-mail addresses. Users with external e-mail accounts have user domain accounts in the Active Directory directory service, but use e-mail accounts that are external to the organization. This enables them to be included in the global address list (GAL) and added to distribution lists.
Resource mailboxes Select this check box if you want your e-mail address policy to apply to Exchange resource mailboxes. Resource mailboxes let you administer company resources through a mailbox, such as a conference room or a company vehicle.
Contacts with external e-mail addresses Select this check box if you want your e-mail address policy to apply to contacts with external e-mail addresses. Contacts with external e-mail accounts do not have user domain accounts in Active Directory, but the external e-mail address is available in the GAL.
Mail-enabled groups Select this check box if you want your e-mail address policy to apply to security groups or distribution groups that have been mail-enabled. Mail-enabled groups are similar to distribution groups. E-mail messages that are sent to a mail-enabled group account will be delivered to several recipients.

5. On the **Conditions** page, edit the following fields to further filter the recipients who will be affected by this e-mail address policy:
Step 1: Select condition(s) Use this section to set one or more conditions for your e-mail address policy. If you don't want to set any conditions for the policy, don't select any of the check boxes.
You can select from the following conditions:
   - **Recipient is in a State or Province** Select this check box if you want the e-mail address policy to include only recipients from specific states or provinces. This information is contained on the **Address and Phone** tab in the recipient's properties.
   - **Recipient is in a Department** Select this check box if you want the e-mail address policy to include only recipients in specific departments. This information is contained on the **Organization** tab in the recipient's properties.
   - **Recipient is in a Company** Select this check box if you want the e-mail address policy to include only recipients in specific companies. This information is contained on the **Organization** tab in the recipient's properties.

Note:
The **State or Province**, **Department**, and **Company** conditions are based on attributes that are applicable only to mailboxes, mail users, and mail contacts. These conditions do not apply to mail-enabled distribution groups. If you configure any of these conditions for an e-mail address policy, you will in effect be excluding all mail-enabled distribution groups.

   - **Custom Attribute equals Value** There are 15 custom attributes for each recipient. There is a separate condition for each custom attribute. If you want the e-mail address policy to include only recipients that have a specific value set for a specific custom attribute, select the check box that corresponds to that custom attribute.

Step 2: Edit the conditions by selecting an underlined value If you select any conditions in Step 1, each condition you select will append to the definition of the e-mail address policy. For example, if you selected the

Recipient is in a State or Province check box in Step 1, you will see **in the specified State or Province(s)** condition in Step 2.
For each condition, click the underlined term to create your condition. By default, the underlined term for new conditions will read **specified**. After you edit the condition, the underlined term will change to the value that you specified.
If you click an underlined value for the **State or Province**, **Department**, or **Company** conditions, a dialog box appears in which you can specify the values for the condition. To create values for the condition, use the following buttons in the dialog box:

- **Add** Enter a value in the text box and click **Add**. You can add more than one value, but you cannot enter duplicate values.
- **Edit** To modify an existing value, select it from the list, and then click **Edit**.
- To remove an existing value, select it from the list, and then click .

If you click an underlined value for a custom attribute condition, a dialog box appears in which you can specify the value for the condition. You can specify a single value for each custom attribute. Type the value in the text box and click **OK**.

Important:

The values that you enter in these dialog boxes must exactly match those that appear in the recipient's properties. For example, if you enter **Washington** in the **Specify State or Province** dialog box, but the **Address and Phone** tab in the recipient's properties lists the state as **WA**, the condition will not be met.

Preview Click this button to view the recipients that will be contained in the e-mail address policy, based on the conditions that you specified.

6. On the **E-Mail Addresses** page, specify an e-mail address for your e-mail address policy.
   - **Add** Click **Add** to add a new e-mail address for the policy. Use the drop-down box to select from the following address types:
     SMTP Address This is the default address type. Click this button and use the corresponding dialog box to add an SMTP address. The following settings are available:
     ?Select the **E-mail address local part** check box and use the corresponding options to configure how the local part of the SMTP e-mail address will appear. The local part of an e-mail address is the name that appears before the at sign (@). If you clear the check box, the local part uses the recipient's alias.
     ?Click **Select the accepted domain for the e-mail address** and then click **Browse** to select the e-mail address domain to which this e-mail address policy applies. You can also create additional e-mail address policies if your organization receives mail for multiple domains, or if your default domain is used strictly for internal purposes and you use a different external mail domain.
     ?Click **Specify the custom fully qualified domain name (FQDN) for the e-mail address**, and then type the FQDN for the domain part of the e-mail address that appears after the at sign (@). This FQDN must match an accepted domain.
     Custom Address Click this button and use the corresponding dialog box to add a custom address (for example, fax or X.400).

     Note:

     With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.
   - **Edit** Click this button to modify the selected e-mail address.
   - **Set as Reply** Click this button to set your selected address as the "reply

to" address. A recipient can have multiple e-mail addresses for a specific address type. This allows the recipient to receive messages that are addressed to any one of these e-mail addresses. However, a single address must be used for any messages that are sent by the recipient. If a recipient has multiple e-mail addresses, the primary address is used for any messages sent by the recipient.

This button is available only when an address other than the primary address is selected. Primary addresses for each address type are displayed in bold type.

If an e-mail address policy in your Exchange organization applies to a mailbox, the **Set as Reply** setting will be controlled by that policy. To change the primary address for a specific address type, you must clear the **Automatically update e-mail addresses based on e-mail address policy** check box.

7. On the **Schedule** page, complete the following fields:
   - **Apply the e-mail address policy** Select one of the following schedule settings to specify when the e-mail address policy should be applied:
     Do not apply Click this button to update the e-mail address policy without applying it to the intended recipients.
     Immediately Select this option to apply the e-mail address policy as soon as the e-mail address policy is edited.
     At the following time Select this option and use the corresponding lists to specify a time to apply the e-mail address policy.
   - **Cancel tasks that are still running after (hours)** Select this check box and use the corresponding text box to specify how long the e-mail address policy task will run. The default is 8 hours.

8. On the **Edit E-Mail Address Policy** page, review your configuration settings. Click **Edit** to apply your changes to the e-mail address policy. Click **Back** to make any configuration changes.

   Note:
   Although the process begins when you click **Edit**, you may have to wait several hours for the process to complete and the e-mail address policy to be applied.

9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
10. Click **Finish** to close the wizard.

Use the Shell to edit an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

This example edits the e-mail address policy South East Offices that currently includes recipients in Georgia, Alabama, and Louisiana to also include recipients in Texas.

```
Set-EmailAddressPolicy -Identity "South East Offices" -ConditionalStateorProvince
```

Note:
Although the e-mail address policy is already applied to recipients in Georgia, Alabama, and Louisiana, you must include them in the parameter because the parameter overwrites values; it doesn't append values to existing ones.

For More Information

Understanding E-Mail Address Policies

Managing E-Mail Address Policies

1.8.3.11.6 Remove an E-Mail Address Policy

Remove an E-Mail Address Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to remove an e-mail address policy. By default, Exchange contains an e-mail address policy that specifies the recipient's alias as the local part of the e-mail address and uses the default accepted domain. The local part of an e-mail address is the name that appears before the "at" sign (@).This e-mail address policy applies to all users in the organization. You can't remove this e-mail address policy.

Looking for other management tasks related to e-mail address policies? Check out Managing E-Mail Address Policies.

Note:
If you remove an e-mail address policy that's used by recipients as the primary e-mail address policy, and no other e-mail address policies have been configured for recipients, the default e-mail address policy will be used.

Use the EMC to remove an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **E-mail Address Policies** tab, and then select the e-mail address policy that you want to remove.
3. In the action pane, click **Remove**.
4. A warning appears. Click **Yes** to confirm that you want to remove the e-mail address policy.

Use the Shell to remove an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry in the Mailbox Permissions

topic.

To remove an e-mail address policy, use the following syntax.

```
Remove-EmailAddressPolicy -Identity <EmailAddressPolicyIdParameter>
```

This example removes the e-mail address policy South East Offices.

```
Remove-EmailAddressPolicy -Identity "South East Offices"
```

Type **Y** to confirm that you want to remove the e-mail address policy, and then press ENTER.

For detailed syntax and parameter information, see Remove-EmailAddressPolicy.

1.8.3.11.7 View the Members of an E-Mail Address Policy by Using the Exchange Management Shell

View the Members of an E-Mail Address Policy by Using the Exchange Management Shell

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Exchange, you can view the members of an e-mail address policy by using the Edit E-Mail Address Policy wizard or New E-Mail Address Policy wizard in the EMC. However, if you used the Shell to create the policy, you can't use the EMC to view the members. Instead, you must use the **Get-Recipient** cmdlet in the Shell. For more information about how to use the EMC to view the members of an e-mail address policy, see Edit an E-Mail Address Policy.

Looking for other management tasks related to e-mail address policies? Check out Managing E-Mail Address Policies.

Use the Shell to view members of an e-mail address policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "E-mail address policies" entry and the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. This example finds the GUID of an e-mail address policy Tokyo Division.

```
Get-EmailAddressPolicy -Identity "Tokyo Division" | fl GUID
```

2. This example lists the members of an e-mail address policy by using the GUID of the e-mail address policy Tokyo Division.

```
Get-Recipient -Filter {PoliciesIncluded -like '{82025f12-8000-4d5e-805
```

For detailed syntax and parameter information, see Get-Recipient.

1.8.3.12 Managing Exchange Search

Managing Exchange Search

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-16*

Default Filters for Exchange Search

Disable or Enable Exchange Search

Diagnose Exchange Search Issues

Reseed the Search Catalog

1.8.3.12.1 Default Filters for Exchange Search

Default Filters for Exchange Search

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2010, Exchange Search includes a number of default filters to index different types of message attachments. You can also install filters to index additional file types.

When managing or using Exchange Search and the features that depend on it (such as Multi-Mailbox Search), consider the following factors:

- **Unsearchable items** When Exchange Search can't index a particular file type for any reason (for example, if a filter isn't installed), the search for the file type fails.
- **Safe lists** Certain file types don't contain any indexable data and therefore aren't indexed. These file types are indicated by a null filter entry in the registry. Items with an attachment type for which a null filter exists aren't searched and aren't returned as unsearchable items.

This topic includes the default filters and safe list filters that are installed on an Exchange 2010 Mailbox server. It also shows you how to use the Shell to retrieve.

Looking for other management tasks related to Exchange Search? Check out Managing Exchange Search.

Default Filters

The following table lists the default search filters installed on an Exchange 2010 Mailbox server. You can retrieve the list of default filters on a Mailbox server from the following registry location:

HKLM\SOFTWARE\Microsoft\ExchangeServer\v14\MSSearch\Filters

File extension

.ascx
.asm
.asp
.aspx
.bat
.c
.cmd
.cpp
.cxx
.def
.dic
.doc
.docx
.dot
.h
.hhc
.hpp
.htm
.html
.htw
.htx
.hxx
.ibq
.idl
.inc
.inf
.ini
.inx
.js
.log
.m3u
.mht
.odc

.one
.pl
.pot
.ppt
.pptx
.rc
.reg
.rtf
.stm
.txt
.url
.vbs
.wtx
.xlc
.xls
.xlsb
.xlsx
.xlt
.xml
.zip

Default Safe List Filters

The following table lists the default safe list filters that are installed on an Exchange 2010 Mailbox server. Exchange Search doesn't index file types for which a safe list filter exists. You can retrieve the safe list filters from the following registry location:

HKLM\SOFTWARE\Microsoft\ExchangeServer\v14\MSSearch\NullFilters

File extension
.aif
.aifc
.aiff
.asx
.au
.bmp
.dib

.emf
.gif
.ico
.IVF
.jfif
.jpe
.jpeg
.jpg
.mlv
.mid
.midi
.mp2
.mp2v
.mp3
.mpa
.mpe
.mpeg
.mpg
.mpv2
.png
.rle
.rmi
.snd
.wav
.wax
.wdp
.wm
.wma
.wmf
.wmx
.wvx

Use the Shell to retrieve default and safe

list filters

You can use the **Get-ChildItem** cmdlet to retrieve registry keys. This is particularly useful when you need to retrieve a large number of registry keys, such as the list of default and safe list search filters.

This example retrieves the list of default search filters used by Exchange Search on an Exchange 2010 Mailbox server.

```
Get-ChildItem HKLM:SOFTWARE\Microsoft\ExchangeServer\v14\MSSearch\Filters | Forma
```

This example retrieves the list of safe list filters for file types that aren't indexed by Exchange Search on an Exchange 2010 Mailbox server.

```
Get-ChildItem HKLM:SOFTWARE\Microsoft\ExchangeServer\v14\MSSearch\NullFilters | F
```

For detailed syntax and parameter information, see Get-ChildItem.

1.8.3.12.2 Disable or Enable Exchange Search

Disable or Enable Exchange Search

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-15*

By default, Exchange Search is enabled for all new mailbox databases and does not require additional configuration. However, if you want to stop Exchange Search from indexing mailbox content, you can disable it for individual mailbox databases or for an entire Mailbox server.

Caution:

Disabling Exchange Search impacts the functionality and performance of the full-text searches that are performed by your users using Outlook in online mode, Outlook Live, or on Windows Mobile devices.
The Discovery feature in Exchange 2010 also relies on Exchange Search. If you disable Exchange Search for a mailbox database or for a Mailbox server, Discovery won't return any messages from the database or server. For more information, see Understanding Multi-Mailbox Search.

Note:

You can enable or disable Exchange Search for servers or mailbox databases, but not for individual mailbox users.

What Do You Want to Do?

- Disable or enable Exchange Search for a mailbox database
- Disable or enable Exchange Search for a Mailbox server

Disable or enable Exchange Search for a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Exchange Search" entry in the Mailbox Permissions topic.

This command disables Exchange Search for a mailbox database named EXCH01:

```
Set-MailboxDatabase "Mailbox Database (EXCH01)" -IndexEnabled $false
```

This command enables Exchange Search for a mailbox database named EXCH01:

```
Set-MailboxDatabase "Mailbox Database (EXCH01)" -IndexEnabled $true
```

For detailed syntax and parameter information, see Set-MailboxDatabase.

Disable or enable Exchange Search for a Mailbox server

To disable or enable Exchange Search for a Mailbox server, you must disable and stop or enable and start the Microsoft Exchange Search Indexer service. You can use either the Services console or the Shell to do this.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Manage Exchange Search Indexer service on a Mailbox server" entry in the Mailbox Permissions topic.

Use the Services console

1. Navigate to **Start** > **Administrative Tools** > **Services**.
2. In the **Services** details pane, right-click the **Microsoft Exchange Search Indexer** service, and then select **Properties**.
3. On the **General** tab, in the **Startup type** list, select **Disabled** to disable the service or **Automatic** to start it automatically.

   Note:
   The startup type impacts the service the next time an attempt is made to start it, either automatically after the server is restarted or by manually starting the service. In the next step, the service is stopped or started manually.

4. Click **Stop** to stop the service or **Start** to start the service.

Use the Shell

The following examples stop and disable the Microsoft Exchange Search Indexer service.

```
Stop-Service MSExchangeSearch
Set-Service MSExchangeSearch -StartupType Disabled
```

The following examples configure the Exchange Search Indexer service to start automatically and then start the service.

```
Set-Service MSExchangeSearch -StartupType Automatic
Start-Service MSExchangeSearch
```


1.8.3.12.3 Diagnose Exchange Search Issues

Diagnose Exchange Search Issues

Mailbox > Managing Mailbox Servers > Managing Exchange Search >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Exchange Search indexes mailboxes and supported attachments in Exchange mailboxes. With increasing volumes of e-mail, increasing mailbox sizes and storage quotas, provisioning of personal archive mailboxes for users, and the introduction of Multi-Mailbox Search for performing discovery searches, Exchange Search is a critical component of the Mailbox servers in your Microsoft Exchange Server 2010 organization. Issues with Exchange Search can affect user productivity and impact Multi-Mailbox Search functionality.

To learn more about Exchange Search, see Understanding Exchange Search.

Looking for management tasks related to managing Exchange Search? See Managing Exchange Search.

Using the Test-ExchangeSearch Cmdlet

Step 5 of the procedure in this topic describes running the **Test-ExchangeSearch** cmdlet to help diagnose Exchange Search issues. You can use the **Test-ExchangeSearch** cmdlet to test Exchange Search functionality for a Mailbox server, a mailbox database, or a specific mailbox. The cmdlet delivers a test message to the specified mailbox (or to a database's system mailbox if a mailbox isn't specified), and then performs a search to determine whether the message is indexed, including the time taken to index it. Under normal conditions, Exchange Search indexes a message within about 10 seconds of the message being created or delivered to a mailbox. The test message is automatically deleted after the test.

Exchange 2010 includes the following enhancements to the **Test-ExchangeSearch** cmdlet:

- The *Mailbox* parameter has been added to the standard output.
- When you specify a server name, the cmdlet simultaneously tests all mailbox databases on the Mailbox server. For databases that are replicated to other Mailbox servers in a database availability group (DAG), if you run the command on a Mailbox server that doesn't contain the active database copy, the test is automatically performed against the server that contains the active database copy.
- When you use the cmdlet with the *MonitoringContext* parameter, it provides additional data that can be used by monitoring software such as Microsoft System Center Operations Manager 2007.
- When you use the cmdlet with the *Verbose* switch, the cmdlet returns detailed results and status for every step, and additional diagnostic information to help you troubleshoot issues related to search.

For detailed syntax and parameter information, see Test-ExchangeSearch.

Retrieving Unsearchable Items

You can use the **Get-FailedContentIndexDocuments** cmdlet to retrieve a list of unsearchable mailbox items that couldn't be successfully indexed by Exchange Search. You can run the cmdlet against a Mailbox server, a mailbox database, or a specific mailbox. The cmdlet returns details about each item that couldn't be searched. There are several reasons why a mailbox item can't be searched; for example, an e-mail message includes an attachment file type for which a search filter isn't installed. If a search filter for that file type is available, you can install it on your Exchange servers.

Important:

Search filters provided by Microsoft are tested and supported by Microsoft. We recommend that you test any third-party search filters in a test environment before installing them on Exchange servers in a production environment.

Note:
Messages that contain an attachment file format that's listed on the safe list aren't returned in the list of unsearchable items. For more details, see "Exchange Search and Attachments" in Understanding Exchange Search.

For detailed syntax and parameter information, see Get-FailedContentIndexDocuments.

Diagnose Exchange Search Issues

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Search" entry in the Mailbox Permissions topic.

1. **Check service state** Is the Microsoft Exchange Search Indexer (MSExchangeSearch) service started on the Mailbox server? If yes, go to Step 2. If no, use the Services MMC snap-in to verify that the MSExchangeSearch service is running as follows:
   1.a.Click **Start**, point to **Administrative Tools**, and then click **Services**.
   1.b.In **Services**, verify that the **Status** for the **Microsoft Exchange Search Indexer** service is listed as **Started**.
2. **Check mailbox database configuration** Is the *IndexEnabled* parameter set to true for the user's mailbox database? If yes, go to Step 3. If no, run the following command in the Shell to verify that the *IndexEnabled* flag is set to true.

   ```
   Get-MailboxDatabase | Format-Table Name,IndexEnabled
   ```

   For detailed syntax and parameter information, see Get-MailboxDatabase.
3. **Check mailbox database crawl state** Has the Exchange database been crawled? If yes, go to Step 4. If no, use Reliability and Performance Monitor to check the **Full Crawl Mode Status** counter of the **MSExchange Search Indices** performance object. Perform the following steps:
   3.a.Open Reliability and Performance Monitor (perfmon.exe).
   3.b.In the console tree, under **Monitoring Tools**, click **Performance Monitor**.
   3.c.In the Performance Monitor pane, click **Add** (green plus sign).
   3.d.In **Add Counters**, in the **Select counters from computer** list, select the server on which the mailbox database you want to monitor is located.
   3.e.In the unlabeled box below the **Select counters from computer** list, select the **MSExchange Search Indices** performance object.
   3.f.In the **Instances of selected object** box, select the instance for the user's mailbox database.
   3.g.Click **Add**, and then click **OK**.
   In the Performance Monitor pane, the **MSExchange Search Indices** performance object is listed in the **Object** column, and its various counters are listed in the **Counter** column. View the **Full Crawl Mode Status** counter. When the database is still being crawled, it has a value of **1**. When the crawl is complete, the value is **0**.
   To view other relevant search counters, use the preceding Steps a though g to add the following performance objects:
   3.h.**MSExchange Search Indexer**
   3.i.**MSFTESQL-Exchange:Catalogs**
   3.j.**MSFTESQL-Exchange:FD**
   3.k.**MSFTESQL-Exchange:Indexer**
   3.l.**MSFTESQL-Exchange:Service**
   For information about using Performance Monitor, see Performance and Reliability Monitoring Step-by-Step Guide for Windows Server 2008
4. **Check the database copy indexing health** Is the content index healthy? Use the **Get-MailboxDatabaseCopyStatus** cmdlet to check the content indexing health for a database copy.

   ```
   Get-MailboxDatabaseCopyStatus | Format-Table Identity,ActiveDatabaseCo
   ```

   For detailed syntax and parameter information, see Get-

MailboxDatabaseCopyStatus.

5. **Run the Test-ExchangeSearch cmdlet** If the mailbox database has already been crawled, you can run the **Test-ExchangeSearch** cmdlet for the mailbox database or for a specific mailbox.

```
Test-ExchangeSearch -Identity AlanBrewer@contoso.com
```

For detailed syntax and parameter information, see Test-ExchangeSearch.

6. **Check the Application event log** Using Event Viewer or the Shell, check the Application event log for search-related error messages. Check the **Source: MSExchangeSearch Indexer** and **msftesql-Exchange** events. For more information, follow the link in the event log entry.
7. **Restart the Microsoft Exchange Search Indexer service** Use the Services MMC snap-in or the Shell to stop and then restart the Microsoft Exchange Search Indexer (MSExchangeSearch) service:
   7.a.Click **Start**, point to **Administrative Tools**, and then click **Services**.
   7.b.In **Services**, right-click **Microsoft Exchange Search Indexer**, and then click **Stop**. After the service is stopped, right-click the service again, and then click **Start**.
8. **Reseed the search catalog** In some cases, such as when the search catalog is corrupted, you may need to reseed the catalog. When a search catalog needs to be reseeded, Exchange Search notifies you by logging entries in the Application event log. For more information about reseeding the Search catalog, see Reseed the Search Catalog.

1.8.3.12.4 Reseed the Search Catalog

Reseed the Search Catalog

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If the content index catalog for a mailbox database copy gets corrupted, you may need to reseed the catalog. Corrupted content indexes are indicated in the Application event log by the following event.

Event ID	Level	Source	Details
123	Error	ExchangeStoreDB	At *<timestamp>* the Microsoft Exchange Information Store Database *<identity>* copy on this server experienced a corrupted search catalog. Consult the event log on the server for other "ExchangeStoreDb" and "MSExchange Search Indexer" events for more specific information about the failure. Reseeding the

			catalog is recommended via the 'Update-MailboxDatabaseCopy' task.

Note:
If the mailbox database copy is the only copy, Exchange Search must create a new content index catalog. You can use the `ResetSearchIndex.ps1` script to do this.

Looking for other management tasks related to Exchange Search? Check out Managing Exchange Search.

Reseed the content index catalog from any source

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Search" entry in the Mailbox Permissions topic.

This example reseeds the content index catalog for the database copy DB1 on Mailbox server MBX1 from any source server that has a copy of the database.

```
Update-MailboxDatabaseCopy -Identity DB1\MBX1 -CatalogOnly
```

For detailed syntax and parameter information, see Update-MailboxDatabaseCopy.

Reseed the content index catalog from a specific source

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Search" entry in the Mailbox Permissions topic.

This example reseeds the content index catalog for the database copy DB1 on Mailbox server MBX1 from Mailbox server MBX2, which also has a copy of the database.

```
Update-MailboxDatabaseCopy -Identity DB1\MBX1 -SourceServer MBX2 -CatalogOnly
```

For detailed syntax and parameter information, see Update-MailboxDatabaseCopy.

1.8.3.12.5 Error Codes for Exchange Search Failed Documents

Error Codes for Exchange Search Failed Documents

Mailbox > Managing Mailbox Servers > Managing Exchange Search >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-30*

When Exchange Search fails to index a document, the document is treated as a *failed document*. When you use the Get-FailedContentIndexDocuments cmdlet to retrieve a list of failed documents, an error code is returned for each failed document.

The following table lists the error codes, error messages, and associated metadata for

errors that occur when Exchange Search fails to index a document.

Error Code	Severity	Symbolic Name	Message
0x0DA5	Warning	GTHR_E_SINGLE_THREADED_EMBEDDING	The system attempted to load a filter marked as apartment from an embedded component in a multi-threaded filter daemon. The document will be retried in a single-threaded filter daemon. Since multithreaded filtering is more efficient, try to obtain the version of the filter that is multi-threaded.
0x0D16	Warning	GTHR_E_FILTER_NOT_FOUND	A filter for the document cannot be created, likely because it isn't installed. Install the corresponding filter for this document format to index this file.
0x120D	Warning	PRTH_E_MIME_EXCLUDED	The URL is excluded because its content type (multipart/x-mixed-replace) is not supported.
0x120E	Warning	PRTH_E_CANT_TRANSFORM_EXTERNAL_ACL	Search was unable to convert the Access Control List of the crawled store into a Windows NT Access Control List. Make sure local information is not used in the store.
0x1217	Warning	PRTH_E_LOAD_FAILED	Loading Protocol handler failed.
0x1218	Warning	PRTH_E_INIT_FAILED	Initializing Protocol handler failed.
0x3600	Warning	FTE_E_CATALOG_ALREADY_MOUNTED	A catalog is already mounted with this name, so another can't be mounted.
0x3601	Warning	FTE_E_CATALOG_NOT_FOUND	The specified catalog was not found in the

			current list of mounted catalogs.
0x3603	Warning	FTE_E_PIPE_NOT_CONNECTED	The named pipe used to communicate with the filter daemon has not been connected.
0x3604	Warning	FTE_E_ADMIN_BLOB_CORRUPT	The configuration data given to the MSFTESQL service is corrupt.
0x3605	Warning	FTE_E_FILTER_SINGLE_THREADED	The system attempted to load an apartment threading model filter marked in a multi-threaded filter daemon. The document will be retried in a single-threaded filter daemon process. Since multithreaded filtering is more efficient, try to obtain the version of the filter that is multi-threaded.
0x3606	Warning	FTE_E_ERROR_WRITING_REGISTRY	The value cannot be set, because the object was already deleted or was not initialized properly. Make sure the object reference is still valid, increase the registry size, or recreate the catalog configuration.
0x3607	Warning	FTE_E_PROJECT_SHUTDOWN	An internal interface is being used after the corresponding catalog has been shutdown. The operation will be aborted.
0x3608	Warning	FTE_E_PROJECT_NOT_INITALIZED	An internal interface is being used prior to being initialized. The operation will be aborted.
0x3609	Warning	FTE_E_PIPE_DATA_CORRUPTED	Data transferred between the MSFTESQL service and a filter daemon process is corrupted.

			This is an internal error.
0x3610	Warning	FTE_E_URB_TOO_BIG	This is an internal error: The URB has exceeded the maximum size.
0x3611	Warning	FTE_E_INVALID_DOCID	This is an internal error: Document IDs should be greater than 0 and less than or equal to 0x7FFFFCCf.
0x3612	Warning	FTE_E_PAUSE_EXTERNAL	An external status change has put the catalog in a paused state.
0x3613	Warning	FTE_E_REJECTED_DUE_TO_PROJECT_STATUS	A status change is occurring or the project is in a force paused state, so MSFTESQL cannot accept input at this time.
0x3614	Warning	FTE_E_FD_DID_NOT_CONNECT	The MSFTEFD process was launched but did not connect with the MSFTESQL service.
0x3616	Warning	FTE_E_PROGID_REQUIRED	This is an internal error: Initialization of the datasink is incorrect. At least one protocol handler PROGID is required.
0x3617	Warning	FTE_E_STATIC_THREAD_INVALID_ARGUMENTS	This is an internal error: A static thread has gotten invalid arguments and will force batches to be aborted and retried.
0x3618	Warning	FTE_E_CATALOG_ALREADY_EXISTS	A catalog already exists with this name, so another can be created or mounted.
0x3619	Success	FTE_S_RESOURCES_STARTING_TO_GET_LOW	The Full Text Engine's input queue is getting full. This batch has been accepted for processing. This success code is intended to help pause input until the queue is less full.

0x361A	Warning	FTE_E_PATH_TOO_LONG	A file path exceeds the maximum limit for paths in Windows, so it can't be used.
0x361B	Warning	FTE_INVALID_ADMIN_CLIENT	Access is denied to the caller of this administration interface.
0x361C	Warning	FTE_E_COM_SIGNATURE_VALIDATION	Signature validation cannot be performed on modules loaded by COM, so the object will not be created. The object is likely a filter, wordbreaker, stemmer, or protocol handler.
0x361D	Warning	FTE_E_AFFINITY_MASK	The processor affinity mask is invalid.
0x3621	Warning	FTE_E_EXCEEDED_MAX_PLUGINS	The maximum number of plug-ins has been exceeded, so a new plug-in can't be loaded.
0x3622	Success	FTE_S_BEYOND_QUOTA	The Full Text Engine's input queue is full. This batch has been accepted for processing; however, the Full Text Engine will soon go into a forced paused state until the queue is less full.
0x3624	Warning	FTE_E_DUPLICATE_OBJECT	An object could not be inserted because it was a duplicate of an existing object. The object may be a catalog or other named entity.
0x3625	Success	FTE_S_REDUNDANT	This transaction was superseded by a subsequent transaction, so it will not be completed.
0x3626	Warning	FTE_E_REDUNDANT_TRAN_FAILURE	The transaction that superseded this one ended in error.
0x3627	Warning	FTE_E_DEPENDENT_TRAN_FAILED_TO_PERSIST	The transaction that superseded this one ended in error.

0x3628	Warning	FTE_E_FD_SHUTDOWN	This is an internal error: This request cannot be completed because the Filter Daemon has been shutdown.
0x3629	Warning	FTE_E_CATALOG_DOES_NOT_EXIST	The catalog does not exist, so the operation can't be performed.
0x362A	Warning	FTE_E_NO_PLUGINS	There are no plug-in components in the indexing pipeline, so the data collected will not be used.
0x362B	Success	FTE_S_STATUS_CHANGE_REQUEST	The project state has changed or is changing due to a status change request.
0x362D	Warning	FTE_E_ANOTHER_STATUS_CHANGE_IS_ALREADY_ACTIVE	A status change is active on another thread. Since only one status change is allowed at a time this request can't be handled.
0x362E	Success	FTE_S_RESUME	This is an internal error: The project will be resumed.
0x362F	Warning	FTE_E_NOT_PROCESSED_DUE_TO_PREVIOUS_ERRORS	A previous error prevented further processing of the batch.
0x3630	Warning	FTE_E_FD_TIMEOUT	The filter daemon process MSFTEFD timed out for an unknown reason. This may indicate a bug in a filter, wordbreaker, or protocol handler.
0x3631	Warning	FTE_E_RESOURCE_SHUTDOWN	This is an internal error: This activity is no longer valid because the resource is shutdown.
0x3632	Warning	FTE_E_INVALID_PROPERTY	The property specified is invalid.
0x3633	Warning	FTE_E_NO_MORE_PROPERTIES	There are no more properties.

0x3634	Warning	FTE_E_UNKNOWN_PLUGIN	The plug-in specified is not known likely because it isn't loaded, so the operation can't succeed. Only specify plug-ins that are loaded.
0x3635	Warning	FTE_E_LIBRARY_NOT_LOADED	The performance monitor library could not be loaded.
0x3636	Warning	FTE_E_PERFMON_FULL	There are no more slots available for this performance monitor instance
0x1600	CoError	QUERY_E_FAILED	Call failed for unknown reason.
0x1601	CoError	QUERY_E_INVALIDQUERY	Invalid parameter.
0x1602	CoError	QUERY_E_INVALIDRESTRICTION	The query restriction could not be parsed.
0x1605	CoError	QUERY_E_ALLNOISE	A clause of the query contained only ignored words.
0x1606	CoError	QUERY_E_TOOCOMPLEX	The query was too complex to be executed.
0x1607	CoError	QUERY_E_TIMEDOUT	The query exceeded its execution time limit.
0x160C	CoError	QUERY_S_NO_QUERY	The catalog is in a state where indexing continues, but queries are not allowed.
0x160D	CoError	QUERY_E_ALLNOISE_AND_NO_RELDOC	A clause of the query contained only ignored words and all the relevant documents specified are not found.
0x160E	CoError	QUERY_E_NO_RELDOC	All the relevant documents specified in the query are not found.
0x160F	CoError	QUERY_E_ALLNOISE_AND_NO_RELPROP	A clause of the query contained only ignored words and no data is found in the

			relevant documents under the specified property(ies).
0x1613	CoError	QUERY_E_INVALID_DOCUMENT_IDENTIFIER	The document identifier specified is not valid.
0x1614	CoError	QUERY_E_INCORRECT_VERSION	The server version is older and cannot handle this query
0x1618	CoError	QUERY_E_UPGRADEINPROGRESS	Queries are disabled due to catalog upgrade. Try your query again in a few minutes.
0x1680	Success	FDAEMON_W_WORDLISTFULL	Wordlist has reached maximum size. Additional documents should not be filtered.
0x1681	CoError	FDAEMON_E_LOWRESOURCE	The system is running out of one of more resources needed for filtering, usually memory.
0x1682	CoError	FDAEMON_E_FATALERROR	A critical error occurred during document filtering. Consult system administrator.
0x1683	CoError	FDAEMON_E_PARTITIONDELETED	Documents not stored in content index because partition has been deleted.
0x1684	CoError	FDAEMON_E_CHANGEUPDATEFAILED	Documents not stored in content index because update of changelist failed.
0x1685	Success	FDAEMON_W_EMPTYWORDLIST	Final wordlist was empty.
0x1686	CoError	FDAEMON_E_WORDLISTCOMMITFAILED	Commit of wordlist failed. Data not available for query.
0x1688	CoError	FDAEMON_E_TOOMANYFILTEREDBLOCKS	During document filtering the limit on buffers has been exceeded.
0x1730	CoError	FILTER_E_TOO_BIG	File is too large to filter.
0x1733	Success	FILTER_S_CONTENTSCAN_DELAYED	A content scan of the disk needs to be

			scheduled for execution later.
0x1734	CoFail	FILTER_E_CONTENTINDEXCORRUPT	The content index is corrupt. A content scan will to be scheduled after chkdsk or autochk is run.
0x1735	Success	FILTER_S_DISK_FULL	The disk is getting full.
0x1736	CoError	FILTER_E_ALREADY_OPEN	A file is already open. Cannot open another one while a file is open.
0x1738	CoError	FILTER_E_IN_USE	The document is in use by another process.
0x173D	CoError	FILTER_E_OFFLINE	The document is offline.
0x173E	CoError	FILTER_E_PARTIALLY_FILTERED	The document was too large to filter in its entirety. Portions of the document were not emitted.
0x1781	Success	LANGUAGE_S_LARGE_WORD	Word larger than maximum length. May be truncated by word sink.
0x1783	CoError	WBREAK_E_BUFFER_TOO_SMALL	Buffer too small to hold composed phrase.
0x1784	CoError	LANGUAGE_E_DATABASE_NOT_FOUND	Language database/ cache file could not be found.
0x1785	CoError	WBREAK_E_INIT_FAILED	Initialization of word breaker failed.
0x1800	CoFail	CI_CORRUPT_DATABASE	The content index is corrupt.
0x1801	CoFail	CI_CORRUPT_CATALOG	The content index meta data is corrupt.
0x1802	CoFail	CI_INVALID_PARTITION	The content index partition is invalid.
0x1805	CoFail	CI_OUT_OF_INDEX_IDS	The content index is out of index ids.
0x1806	CoFail	CI_NO_CATALOG	There is no catalog.
0x1807	CoFail	CI_CORRUPT_FILTER_	The filter buffer is

		BUFFER	corrupt.
0x1808	CoFail	CI_INVALID_INDEX	The index is invalid.
0x1809	CoFail	CI_PROPSTORE_INCONSISTENCY	Inconsistency in property store detected.
0x180B	CoError	CI_E_NOT_INITIALIZED	The object is not initialzed.
0x180F	CoError	CI_E_INVALID_STATE	The object is not in a valid state.
0x1811	CoError	CI_E_DISK_FULL	The disk is full and the specified operation cannot be done.
0x1812	CoError	CI_E_SHUTDOWN	The request could not be completed because the process and/or catalog are being shutdown
0x1818	CoError	CI_E_UPDATES_DISABLED	A document update was rejected because updates were disabled.
0x181B	CoError	CI_E_SHARING_VIOLATION	A sharing or locking violation caused a failure.
0x181C	CoError	CI_E_LOGON_FAILURE	A logon permission violation caused a failure.
0x181E	CoError	CI_E_STRANGE_PAGEORSECTOR_SIZE	Page size is not an integral multiple of the sector size of the volume where index is located.
0x181F	CoError	CI_E_TIMEOUT	Service is too busy.
0x1820	CoError	CI_E_NOT_RUNNING	Service is not running.
0x1828	CoError	CI_E_CONFIG_DISK_FULL	The disk has reached its configured space limit.
0x182D	CoFail	CI_E_CORRUPT_FWIDX	The forward index is corrupt.
0x182E	CoFail	CI_E_DIACRITIC_SETTINGS_DIFFER	Catalog was created with different diacritic settings.
0x182F	CoFail	CI_E_INVALID_THESAURUS_FILE	The thesaurus file is invalid.

0x1830	CoFail	CI_E_THESAURUS_FILE_BOM_MISSING	Unicode byte order mark (0xFEFF) missing at the beginning of thesaurus file.
0x170b	CoError	FILTER_E_PASSWORD	File was not filtered due to password protection.
0x170C	CoError	FILTER_E_UNKNOWNFORMAT	The document format is not recognized by the filter.

1.8.3.13 Managing Hierarchical Address Books

Managing Hierarchical Address Books

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-06-22*

Configure Hierarchical Address Books

1.8.3.13.1 Configure Hierarchical Address Books

Configure Hierarchical Address Books

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure a hierarchical address book (HAB), which is a feature in Microsoft Exchange Server 2010 and the Microsoft Outlook 2010 Address Book. With a HAB, users can browse recipients in their Exchange organization by using an organizational hierarchy. To learn more about HABs, see Understanding Hierarchical Address Books.

Prerequisites

- Read Understanding Hierarchical Address Books. You should understand if a HAB is appropriate for your Exchange organization.
- Understand how organizational units (OUs), groups, users, and contacts are currently configured in your Exchange organization.
- Understand the cmdlets and associated parameters in the following table, which are required to configure a HAB.

Cmdlet	Parameter
Set-OrganizationConfig	*HierarchicalAddressBookRoot*
Set-Group	*IsHierarchicalGroup* *SeniorityIndex* *PhoneticDisplayName*

Set-User	*SeniorityIndex* *PhoneticDisplayName*
Set-Contact	*SeniorityIndex* *PhoneticDisplayName*

Use the Shell to enable a hierarchical address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to enable a HAB. However, after you enable a HAB, you can use the EMC to manage the membership of the groups in the organizational hierarchy.

For this example, an OU called HAB will be created for the HAB. The name of the domain for the Exchange 2010 organization is Contoso-dom, and Contoso,Ltd will be the name of the top-level organization in the hierarchy (the *root organization*). Subordinate groups named Corporate Office, Product Support Organization, and Sales & Marketing Organization will be created as child organizations under Contoso,Ltd. Additionally, the groups Human Resources, Accounting Group, and Administration Group will be created as child organizations under Corporate Office.

For detailed information about creating distribution groups, see Create a Distribution Group.

1. Create an OU named HAB in the Contoso organization. You can use Active Directory Users and Computers or type the following at a command prompt.

   Note:
   Alternatively, you can use an existing OU in your Exchange forest.

   ```
   dsadd ou "OU=HAB,DC=Contoso-dom,DC=Contoso,DC=com"
   ```

   Note:
   For details, see Create a New Organizational Unit.

2. Create the root distribution group Contoso,Ltd for the HAB.

   Note:
   For the purposes of this topic, the Shell example is provided. However, you can also use the EMC to create a distribution group. For details, see Create a Distribution Group.

   ```
   New-DistributionGroup -Name "Contoso,Ltd" -DisplayName "Contoso,Ltd" -
   ```

3. Designate Contoso,Ltd as the root organization for the HAB.

   ```
   Set-OrganizationConfig -HierarchicalAddressBookRoot "Contoso,Ltd"
   ```

4. Create distribution groups for the other tiers in the HAB. For this example, you would create the following groups: Corporate Office, Product Support Organization, Sales & Marketing Organization, Human Resources, Accounting Group, and Administration Group. This example creates the distribution group Corporate Office.

   Note:
   For the purposes of this topic, the Shell example is provided. However, you can also use the EMC to create distribution groups. For details, see Create a Distribution Group.

```
New-DistributionGroup -Name "Corporate Office" -DisplayName "Corporate
```

5. Designate each of the groups as members of the HAB. For this example, you would designate the following groups as being hierarchical groups: Contoso,Ltd, Corporate Office, Product Support Organization, Sales & Marketing Organization, Human Resources, Accounting Group, and Administration Group. This example designates the distribution group Contoso,Ltd as a member of the HAB.

```
Set-Group -Identity "Contoso,Ltd" -IsHierarchicalGroup $true
```

6. Add each of the subordinate groups as members of the root organization. For this example, distribution groups Corporate Office, Product Support Organization, and Sales & Marketing Organization, are added as members of the root organization Contoso,Ltd in the HAB. This example adds the Corporate Office distribution group as a member of the Contoso,Ltd root distribution group.

Note:
This example uses the alias of the distribution groups.

```
Add-DistributionGroupMember -Identity "ContosoRoot" -Member "Corporate
```

7. Add each of the groups that are subordinate to the distribution group Corporate Office as members of the group. For this example, distribution groups Human Resources, Accounting Group, and Administration Group, are added as members of the distribution group Corporate Office. This example adds the Human Resources distribution group as a member of the Corporate Office distribution group.

Note:
This example uses the alias of the distribution groups and assumes the Human Resources distribution group alias is HumanResources.

```
Add-DistributionGroupMember -Identity "CorporateOffice" -Member "Human
```

8. Add users to the groups in the HAB. For this example, David Hamilton (SMTP address DHamilton@contoso.com) is an existing user in the OU Contoso-dom.Contoso.com/Users and will be added to the group Corporate Office. Repeat this step to add other users to groups in the HAB.

```
Add-DistributionGroupMember -Identity "CorporateOffice" -Member "DHami
```

9. Set the *SeniorityIndex* parameter for groups in the HAB. For this example, the Corporate Office group contains three child groups: Human Resources, Accounting Group, and Administration Group. Instead of having the groups listed in ascending alphabetical order, which is the default, the preferred sorting will be Human Resources (*SeniorityIndex* = 100), Accounting Group (*SeniorityIndex* = 50), and then Administration Group (*SeniorityIndex* = 25). This example sets the *SeniorityIndex* parameter for the Human Resources group to 100.

```
Set-Group -Identity "Human Resources" -SeniorityIndex 100
```

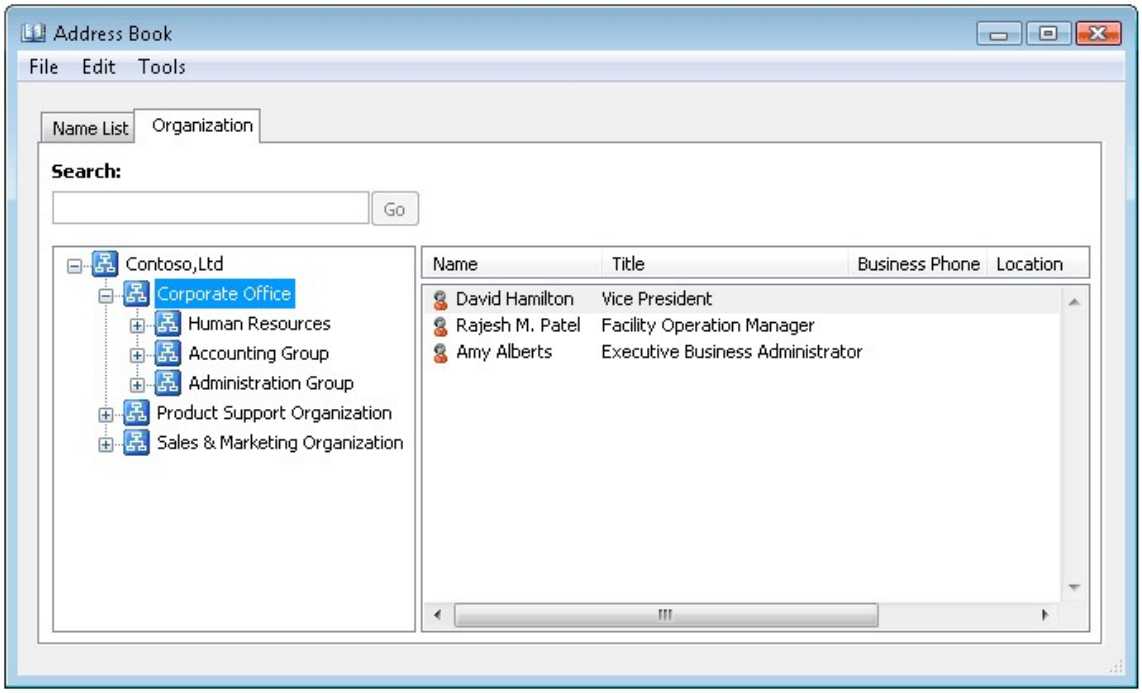
Note:
The *SeniorityIndex* parameter is a numerical value used to sort groups or users in descending numerical order in a HAB. If the *SeniorityIndex* parameter isn't set or is equal for two or more users, the HAB sorting order uses the *PhoneticDisplayName* parameter value to list the users in ascending alphabetical order. If the *PhoneticDisplayName* value isn't set, the HAB sorting order defaults to the *DisplayName* parameter value and lists the users in ascending alphabetical order.

10. Set the *SeniorityIndex* parameter for users in the HAB groups. For this example, the Corporate Office group contains three users: Amy Alberts, David Hamilton, and Rajesh M. Patel. Instead of having the users listed in ascending alphabetical order by default, the preferred sorting will be David

Hamilton (*SeniorityIndex* = 100), Rajesh M. Patel (*SeniorityIndex* = 50), and then Amy Alberts (*SeniorityIndex* = 25). This example sets the *SeniorityIndex* parameter for the user David Hamilton to 100.

```
Set-User -Identity "DHamilton@contoso.com" -SeniorityIndex 100
```

After completing the preceding steps, the HAB will be visible in Outlook 2010. To view the HAB, open Outlook 2010 and click **Address Book**. The HAB is displayed on the **Organization** tab, similar to the following figure.



After the HAB is created, you can use the EMC to manage the membership of the groups in the organizational hierarchy. However, you must use the Shell to modify the *SeniorityIndex* parameter for any new groups or users.

For detailed syntax and parameter information, see the following:

- New-DistributionGroup
- Set-OrganizationConfig
- Set-Group
- Add-DistributionGroupMember
- Set-User

Use the Shell to disable a hierarchical address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to disable a HAB.

This example disables the root organization used for the HAB.

```
Set-OrganizationConfig -HierarchicalAddressBookRoot $null
```

Note:
This command doesn't delete the root organization or child groups used in the HAB structure or reset the *SeniorityIndex* values for groups or users. It only prevents the HAB from being displayed in Outlook 2010. To enable the HAB with the same configuration settings again, you only need to enable the root organization again.

For detailed syntax and parameter information, see Set-OrganizationConfig.

1.8.3.14 Managing Mail Contacts and Mail Users

Managing Mail Contacts and Mail Users

Exchange Server 2010 > Mailbox > Managing Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-18*

1.8.3.14.1 Create a Mail Contact

Create a Mail Contact

Mailbox > Managing Mailbox Servers > Managing Mail Contacts and Mail Users >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Mail contacts are mail-enabled Active Directory objects that contain information about people or organizations that exist outside your Exchange organization. Each mail contact has an external e-mail address.

Looking for other management tasks related to mail contacts? Check out Managing Mail Contacts and Mail Users.

Prerequisite

If you want to create a new mail contact in a domain that is different than the one in which your Exchange servers reside, you must first prepare that domain for Exchange 2010. To learn more about preparing a domain for Exchange 2010, see Prepare Active Directory and Domains.

What Do You Want to Do?

- Use the EMC to create a mail contact
- Use the Shell to create a mail contact

Use the EMC to create a mail contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Mail Contact**.
3. On the **Introduction** page, under **Create a mail contact for**, select one of the following options.
   - **New contact** This button is selected by default. Click this button to create and mail-enable a new contact. If you click this button, you'll need to provide the required account information for the contact on the **Contact Information** page of this wizard.
   - **Existing contact** Click this button to mail-enable an existing contact in Active Directory. Click **Browse** to open the **Select Contact** dialog box. This dialog box displays a list of all contacts in the forest that aren't mail-enabled. Select the contact that you want, and then click **OK** to return to the wizard.
4. If you selected **New Contact** in Step 3, complete the following fields on the **Contact Information** page. Otherwise skip to Step 5:
   - **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.
   - **First name** Use this box to type the contact's first name. This field is optional.
   - **Initials** Use this box to type the contact's initials. This field is optional.
   - **Last name** Use this box to type the contact's last name. This field is optional.
   - **Name** Use this box to type a name for the contact. This is the name that's listed in Active Directory. By default, this box is populated with the names you enter in the **First name**, **Initials**, and **Last name** boxes. If you didn't use those boxes, you must still type a name in this field. The name can't exceed 64 characters.
   - **Alias** Use this box to type a unique alias (64 characters or less) for the contact. This field is required.
   - **External e-mail address** To specify the external e-mail address, perform one of the following tasks:

     To specify a SMTP e-mail address, click **Edit**. In the **SMTP**

address dialog box, type the SMTP e-mail address.

Note:
Exchange validates SMTP addresses for proper formatting. If your entry is inconsistent with the SMTP format, an error message will be displayed when you click **OK**.

To specify a custom e-mail address, click the arrow next to **Edit**, and then click **Custom Address**. In the **Custom Address** dialog box, use the **E-mail address** box to type the e-mail address and the **E-mail type** box to specify the e-mail type. For example, you can specify an X.400, GroupWise, or Lotus Notes address.

5. On the **New Mail Contact** page, review your configuration settings. To make changes, click **Back**. To create the new mail contact, click **New**. Click **Cancel** to close the wizard without creating the new mail contact.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. Click **Finish** to close the wizard.

Use the Shell to create a mail contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

This example creates a mail contact for Ted Bremer.

```
New-MailContact -Name "Ted Bremer" -ExternalEmailAddress ted@tailspintoys.com -Or
```

This example mail-enables an existing contact named David.

```
Enable-MailContact -Identity David -ExternalEmailAddress David@thirdcoffee.com
```

For More Information

Understanding Recipients

Managing Mail Contacts and Mail Users

1.8.3.14.2 Create a Mail User

Create a Mail User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Mail users are similar to mail contacts. Both have external e-mail addresses and both contain information about people outside your Exchange Server 2010 organization that can be displayed in the global address list (GAL) and other address lists. However, unlike

a mail contact, a mail user has Active Directory logon credentials and can access resources.

Looking for other management tasks related to mail users? Check out Managing Mail Contacts and Mail Users.

Prerequisite

If you want to create a mail user in a domain that is different than the one in which your Exchange servers reside, you must first prepare that domain for Exchange 2010. To learn more about preparing a domain for Exchange 2010, see Prepare Active Directory and Domains.

What Do You Want to Do?

- Use the EMC to create a mail user
- Use the Shell to create a mail user

Use the EMC to create a mail user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail users" entry in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Mail User**.
3. On the **Introduction** page, select the type of user that you want to create or mail-enable.
   - **New user** This button is selected by default. Click this button to create a new user account for the mail user. This allows you to provision the user account and mail-enable it simultaneously.
     If you click this button, you'll need to provide the required user account information on the **User Information** page of this wizard.
   - **Existing user** Click this button to mail-enable an existing user account in Active Directory. Click **Browse** to open the **Select User** dialog box. This dialog box displays a list of user accounts in the forest that aren't mail-enabled or don't have Exchange mailboxes. Select the user account you want, and then click **OK** to return to the wizard.
4. If you selected **New User** in Step 3, complete the following fields on the **User Information** page. Otherwise skip to Step 5:
   - **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.
   - **First name** Use this box to type the user's first name. This field is optional.
   - **Initials** Use this box to type the user's middle initials. This field is optional.
   - **Last name** Use this box to type the user's last name. This field is optional.

- **Name** Use this box to type a name for the user. This is the name that's listed in Active Directory. By default, this box is populated with the names you enter in the **First name**, **Initials**, and **Last name** boxes. If you didn't use those boxes, you must still type a name in this field. The name can't exceed 64 characters.

  User logon name (User Principal Name) Use this box to type the name that the user will use to log on to the mailbox. The user logon name consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides. This name can't exceed 1,024 characters and must be unique in the forest.
- **User logon name (pre-Windows 2000)** Use this box to type the name for the user that is compatible with the legacy versions of Microsoft Windows (prior to the release of Windows 2000 Server). This field is automatically populated based on the **User logon name (User Principal Name)** field. This name can't exceed 20 characters and must not contain any of the following characters: **\/ []:|<> + = ; ? , ***.
- **Password** Use this box to type the password for the user.

  Note:
  Make sure that the password you supply complies with the password length, complexity, and history requirements of the domain in which you are creating the user account.
- **Confirm password** Use this box to confirm the password that you typed in the **Password** box.
- **User must change password at next logon** Select this check box if you want the user to reset the password when they first logon to the mailbox.

  If you select this check box, at first logon, the new user will be prompted with a dialog box in which to change the password. The user won't be allowed to perform any tasks until the password is successfully changed.

5. On the **Mail Settings** page, complete the following fields:
   - **Alias** Use this text box to type the alias of the user. The alias can't exceed 64 characters and must be unique in the forest.
   - **External e-mail address** To specify the external e-mail address, perform one of the following tasks:

     To specify a SMTP e-mail address, click **Edit**. In the **SMTP address** dialog box, type the SMTP e-mail address.

     Note:
     Exchange validates SMTP addresses for proper formatting. If your entry is inconsistent with the SMTP format, an error message will be displayed when you click **OK**.

     To specify a custom e-mail address, click the arrow next to **Edit**, and then click **Custom Address**. In the **Custom Address** dialog box, use the **E-mail address** box to type the e-mail address and the **E-mail type** box to specify the e-mail type. For example, you can specify an X.400, GroupWise, or Lotus Notes address.

6. On the **New Mail User** page, review your configuration settings. To make changes, click **Back**. To create the new mail user, click **New**. Click **Cancel** to close the wizard without creating the new mail contact.

7. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task

fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a mail user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail users" entry in the Mailbox Permissions topic.

This example creates the mail user Ted Bremer with the external e-mail address ted@tailspintoys.com.

```
New-MailUser -Name Ted -FirstName Ted -LastName Bremer -ExternalEmailAddress ted@
```

For More Information

Understanding Recipients

Configure Mail User Properties

1.8.3.14.3 Configure Mail Contact Properties

Configure Mail Contact Properties

Mailbox > Managing Mailbox Servers > Managing Mail Contacts and Mail Users >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Mail contacts are mail-enabled Active Directory objects that contain information about people or organizations that exist outside your Exchange organization. Each mail contact has an external e-mail address. You can use the **<Mail Contact> Properties** dialog box to configure settings for a mail-enabled contact.

Looking for other management tasks related to mail contacts? Check out Managing Mail Contacts and Mail Users.

What Do You Want to Do?

- Use the EMC to configure mail contact properties
- Use the Shell to configure mail contact properties

Use the EMC to configure mail contact properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

Properties specific to a mail user are controlled by the **Set-MailContact** cmdlet. The EMC allows you to set additional properties, and the permissions may vary depending on the feature that you're configuring. The permissions listed above grant permission to edit all of the properties of the **<Mail Contact> Properties** dialog box.

1. In the console tree, navigate to **Recipient Configuration** > **Mail Contact**.
2. In the result pane, select the mail contact that you want to configure.
3. In the action pane, click **Properties**.

4. Use the **General** tab to modify the display name, alias, and custom attributes.
   - **Display name** Use this unlabeled box at the top of the page to view or change the display name.
   - **Organizational unit** This field displays the organizational unit (OU) that contains the user account.
   - **Modified** This read-only field displays the last date and time that a configuration change was made to the recipient.
     Configuration changes made through any other method, such as the through the Exchange Management Shell or Active Directory Service Interfaces (ADSI) Edit, will also update this field.
   - **Alias** Use this box to view or change the recipient's alias. The alias can't exceed 64 characters and must be unique in the forest. One of the reasons why the alias field must be unique is because it's used to generate the SMTP address in a default installation.
   - **Use MAPI rich text format** Select one of the following options from the corresponding list:
     Never If you select this option, messages sent to this recipient will be converted to plain text.
     Always If you select this option, messages sent to this recipient will be in the MAPI rich text format (RTF).
     Use Default Settings If you select this option, messages sent to this recipient will be sent in either MAPI RTF or plain text, depending on the settings of the client computer from which the message is sent.
   - **Hide from Exchange address lists** Select this check box to prevent the recipient from appearing in the global address list (GAL) and other address lists that are defined in your Exchange organization.
     After you select this check box, users in your Exchange organization can still send messages to the recipient by using the e-mail address.
   - **Custom Attributes** Click this button to open the **Custom Attributes** dialog box. You can specify up to 15 custom attributes for the recipient. To specify the custom attribute values, use the corresponding boxes, and then click **OK**.

5. Use the **Contact Information** tab to modify the following fields.
   - **First name** Use this box to modify the contact's first name.
   - **Initials** Use this box to modify the contact's middle initials.
   - **Last name** Use this box to modify the contact's last name.
   - **Name** Use this box to modify the contact's directory name. This is the name that is listed in Active Directory.
   - **Simple display name** Use this box to modify the contact's simple display name. This field accepts only ASCII characters.
     The **Display name** field (located on the **General** tab) can contain Unicode characters. However, third-party applications and older clients may not support Unicode characters. If the system that is displaying the recipient properties doesn't support Unicode characters, you can use the simple display name. For more information about Unicode characters, see Unicode.
   - **Web page** Use this box to modify the contact's Web page address.
   - **Notes** Use this box to modify administrative notes about the contact.
     These notes are also visible in Outlook. When a user views the recipient's properties in Outlook, the notes will be displayed on the **Phone/Notes** tab.

6. Use the **Address and Phone** tab to view or modify the following fields:

- **Street address** Use this box to view or change the recipient's street.
- **City** Use this box to view or change the city where the recipient is located.
- **State/Province** Use this box to view or change the state or province where the recipient is located.

  You can use the **State/Province** field as a condition for dynamic distribution groups and e-mail address policies. If you plan to use this field as a condition, you must devise and follow a consistent naming convention to ensure accurate results for dynamic distribution groups and e-mail address policies.
- **ZIP/Postal code** Use this box to view or change the ZIP code or the postal code where the recipient is located.
- **Country/region** Use this list to view or change the country or region where the recipient is located.
- **Business** Use this box to view or change the recipient's business phone number.
- **Pager** Use this box to view or change the recipient's pager number.
- **Fax** Use this box to view or change the recipient's fax number.
- **Home** Use this box to view or change the recipient's home phone number.
- **Mobile** Use this box to view or change the recipient's mobile phone number.

7. Use the **Organization** tab to view or change the information about the recipient's role in your organization.
   - **Title** Use this box to view or change the recipient's title.
   - **Company** Use this box to view or change the company for which the recipient works. You can use this field to create recipient conditions for dynamic distribution groups, e-mail address policies, or address lists.
   - **Department** Use this box to view or change the department in which the recipient works. You can use this field to create recipient conditions for dynamic distribution groups, e-mail address policies, or address lists.
   - **Office** Use this box to view or change the office location for the recipient.
   - **Manager** Select this check box if you want to specify this recipient's manager. By specifying the manager for each recipient in your organization, you can create a virtual organization chart that is accessible from e-mail clients such as Outlook.

     Click **Browse** to open the **Select Recipient User or Contact** dialog box. Select the recipient's manager, and then click **OK** to return to the property page.
   - **Direct Reports** Use this box to view the list of mailbox users and contacts that are managed by this recipient. This field is read-only and is populated automatically when this recipient is designated as a manager for another recipient.

8. Use the **Member Of** tab to view a list of the groups to which this recipient belongs. Some of these groups may not be mail-enabled. Mail-enabled groups will have an envelope icon next to them. You can't use this tab to modify membership information. The recipient may match the criteria for one or more dynamic distribution groups in your organization. However, dynamic distribution groups aren't displayed on this tab because their membership is calculated each time they are used. For more information, see Managing Distribution Groups.

9. Use the **E-Mail Addresses** tab to configure the e-mail addresses for the recipient. You can modify the existing addresses or create additional ones. Each recipient must have at least one primary STMP address that is internal to your Exchange organization and one external address.
   - **Add** Click **Add** to add a new e-mail address for this recipient. Use the drop-down box to select from the following address types:

     SMTP Address This is the default address type. Click this

button and use the corresponding dialog box to add an SMTP address.
EUM Address This address type is available only for user mailboxes. It's not available for mail users, mail contacts, distribution groups, or mail-enabled public folders. An EUM (Exchange Unified Messaging) address is used by Unified Messaging servers to locate UM-enabled users within an Exchange 2010 organization. EUM addresses contain the extension number and the UM dial plan for the UM-enabled user. Click this button and use the corresponding dialog box to add an EUM address.
Custom Address Click this button and use the corresponding dialog box to add a custom address (for example, fax or X.400).

Note:
With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.

- **Edit** Click this button to modify the selected e-mail address.
- Click this button to remove the selected e-mail address.
- **Set as Reply** Click this button to set your selected address as the "reply to" address. A recipient can have multiple e-mail addresses for a specific address type. This allows the recipient to receive messages that are addressed to any one of these e-mail addresses. However, a single address must be used for any messages that are sent by the recipient. If a recipient has multiple e-mail addresses, the primary address is used for any messages sent by the recipient.
  This button is available only when an address other than the primary address is selected. Primary addresses for each address type are displayed in bold type.
  If an e-mail address policy in your Exchange organization applies to this mailbox, the **Set as Reply** setting will be controlled by that policy. To change the primary address for a specific address type, you must clear the **Automatically update e-mail addresses based on e-mail address policy** check box.
- **Set as External** This button is available only for mail users and mail contacts. It's not available for user mailboxes, distribution groups, or mail-enabled public folders. Click **Set as External** to designate the selected e-mail address as the external e-mail address for the recipient.

  Note:
  This button is enabled when an address other than the external e-mail address is selected.

- **Automatically update e-mail addresses based on e-mail address policy** Select this check box to have the recipient's e-mail addresses automatically updated based on changes made to e-mail address policies in your organization. This box is selected by default.

10. Use the **Mail Flow Settings** tab to configure message size or message delivery restrictions for the contact.
    - **Message Size Restrictions** Select this setting and then click **Properties** to open the **Message Size Restrictions** dialog box. In this dialog box, select the **Maximum message size (in KB)** check box to set the maximum size for messages that can be received by this recipient. Use the corresponding text box to specify the maximum message size allowed (in KB). The message size must be between 0 and 2,097,151 KB. If a message larger than the specified size is sent to the recipient, the message will be returned to the sender with a descriptive error message.
    - **Message Delivery Restrictions** Select this setting and then click

Properties to open the **Message Delivery Restrictions** dialog box. Use this dialog box to configure the following settings:

All senders Click this button to specify that the recipient can accept messages from all senders. This includes senders in both your Exchange organization and external senders. This button is selected by default. This option includes external users only if you clear the **Require that all senders are authenticated** check box. If you select this check box, messages from external users will be rejected.

Only senders in the following list Click this button to specify that the recipient can accept messages only from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.

Require that all senders are authenticated Select this check box to prevent anonymous users from sending messages to the recipient.

No senders Click this button to specify that the recipient will not reject messages from any senders in the Exchange organization. This button is selected by default.

Senders in the following list Click this button to specify that the recipient will reject messages from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now.**

Use the Shell to configure mail contact properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

This example sets the contact John Peoples' external e-mail address to john@contoso.com.

```
Set-MailContact -Identity "John Peoples" -ExternalEmailAddress "john@contoso.com"
```

For More Information

Understanding Recipients

Managing Mail Contacts and Mail Users

1.8.3.14.4 Configure Mail User Properties

Configure Mail User Properties

Mailbox > Managing Mailbox Servers > Managing Mail Contacts and Mail Users >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-24*

Mail users are similar to mail contacts. Both have external e-mail addresses and both contain information about people outside your Exchange organization that can be displayed in the global address list (GAL) and other address lists. However, unlike a mail contact, a mail user has Active Directory logon credentials and can access resources.

Properties specific to a mail user are controlled by the **Set-MailUser** cmdlet. You can use the EMC to set additional properties, but the permissions may vary depending upon the feature that you're configuring.

Looking for other management tasks related to mail users? Check out Managing Mail Contacts and Mail Users.

What Do You Want to Do?

- Use the EMC to configure mail user properties
- Use the Shell to configure mail user properties

Use the EMC to configure mail user properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Provisioning Recipient Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mail Contact**.
2. In the result pane, select the mail user that you want to configure.
3. In the action pane, click **Properties**.
4. Use the **General** tab to modify the display name, alias, and custom attributes.
   - **Display name** Use this unlabeled box at the top of the page to view or change the display name.
   - **Organizational unit** This field displays the organizational unit (OU) that contains the user account.
   - **Modified** This read-only field displays the last date and time that a configuration change was made to the recipient.
     Configuration changes made through any other method, such as the through the Exchange Management Shell or Active Directory Service Interfaces (ADSI) Edit, will also update this field.
   - **Alias** Use this box to view or change the recipient's alias. The alias can't exceed 64 characters and must be unique in the forest. One of the reasons why the alias field must be unique is because it's used to generate the SMTP address in a default installation.
   - **Use MAPI rich text format** Select one of the following options from the corresponding list:
     Never If you select this option, messages sent to this recipient will be converted to plain text.
     Always If you select this option, messages sent to this recipient will be in the MAPI rich text format (RTF).
     Use Default Settings If you select this option, messages sent to this recipient will be sent in either MAPI RTF or plain text, depending on the settings of the client computer from which the message is sent.
   - **Hide from Exchange address lists** Select this check box to prevent the recipient from appearing in the global address list (GAL) and other address

lists that are defined in your Exchange organization.

After you select this check box, users in your Exchange organization can still send messages to the recipient by using the e-mail address.

- **Custom Attributes** Click this button to open the **Custom Attributes** dialog box. You can specify up to 15 custom attributes for the recipient. To specify the custom attribute values, use the corresponding boxes, and then click **OK**.

5. Use the **User Information** tab to modify the following fields.
   - **First name** Use this box to modify the recipient's first name.
   - **Initials** Use this box to modify the recipient's middle initials.
   - **Last name** Use this box to modify the recipient's last name.
   - **Name** Use this box to modify the recipient's directory name. This is the name that's listed in Active Directory.
   - **Simple display name** Use this box to modify the recipient's simple display name. The simple display name field accepts only ASCII characters.

     In Exchange 2010, the **Display name** field (located on the **General** tab) can contain Unicode characters. However, third-party applications and older clients may not support Unicode characters. If the system that is displaying the recipient properties doesn't support Unicode characters, you can use the simple display name. For more information about Unicode characters, see Unicode.
   - **Web page** Use this box to modify the recipient's Web page address.
   - **Notes** Use this box to modify administrative notes about the recipient.

     These notes are also visible in Outlook. When a user views the recipient's properties in Outlook, the notes will be displayed on the **Phone/Notes** tab.

6. Use the **Address and Phone** tab to view or modify the following fields:
   - **Street address** Use this box to view or change the recipient's street.
   - **City** Use this box to view or change the city where the recipient is located.
   - **State/Province** Use this box to view or change the state or province where the recipient is located.

     You can use the **State/Province** field as a condition for dynamic distribution groups and e-mail address policies. If you plan to use this field as a condition, you must devise and follow a consistent naming convention to ensure accurate results for dynamic distribution groups and e-mail address policies.
   - **ZIP/Postal code** Use this box to view or change the ZIP code or the postal code where the recipient is located.
   - **Country/region** Use this list to view or change the country or region where the recipient is located.
   - **Business** Use this box to view or change the recipient's business phone number.
   - **Pager** Use this box to view or change the recipient's pager number.
   - **Fax** Use this box to view or change the recipient's fax number.
   - **Home** Use this box to view or change the recipient's home phone number.
   - **Mobile** Use this box to view or change the recipient's mobile phone number.

7. Use the **Organization** tab to view or change the information about the recipient's role in your organization.
   - **Title** Use this box to view or change the recipient's title.
   - **Company** Use this box to view or change the company for which the recipient works. You can use this field to create recipient conditions for dynamic distribution groups, e-mail address policies, or address lists.
   - **Department** Use this box to view or change the department in which the

recipient works. You can use this field to create recipient conditions for dynamic distribution groups, e-mail address policies, or address lists.

- **Office** Use this box to view or change the office location for the recipient.
- **Manager** Select this check box if you want to specify this recipient's manager. By specifying the manager for each recipient in your organization, you can create a virtual organization chart that is accessible from e-mail clients such as Outlook.

  Click **Browse** to open the **Select Recipient User or Contact** dialog box. Select the recipient's manager, and then click **OK** to return to the property page.
- **Direct Reports** Use this box to view the list of mailbox users and contacts that are managed by this recipient. This field is read-only and is populated automatically when this recipient is designated as a manager for another recipient.

8. Use the **Account** tab to modify the logon names for the Active Directory domain service user account that is associated with the recipient:
   - **User logon name (User Principal Name)** The user logon name consists of a user name and a suffix. Use this box to type the user name that the user will use to log on to the Active Directory domain. The user logon name cannot exceed 1,024 characters and must be unique in the forest.

     Use the corresponding drop-down list to select the suffix for this user. Typically, the suffix is the Active Directory domain name in which the user account resides. To view or change the list of available domain suffixes in your forest, use Active Directory Domains and Trusts. In the Active Directory Domains and Trusts console tree, right-click **Active Directory Domains and Trusts**, and then click **Properties**. In the property page, use the **UPN suffixes** tab to view the list of available domain suffixes in the forest.
   - **User logon name (pre-Windows 2000)** Use this box to type a user name that is compatible with legacy versions of Windows (prior to the release of Windows 2000 Server). The user logon name for a version of Windows earlier than Windows 2000 Server can't exceed 20 characters and can't contain any of the following characters: **\/ [] : | <> + = ; ? , ***.

     When the user account is first created, this field is automatically populated based on the **User logon name (User Principal Name)** field.
   - **User must change password at next logon** Select this check box if you want the user to change the password at next logon. The user won't be able to log on until the password is successfully changed.

9. Use the **Member Of** tab to view a list of the groups to which this recipient belongs. Some of these groups may not be mail-enabled. Mail-enabled groups will have an envelope icon next to them. You can't use this tab to modify membership information. The recipient may match the criteria for one or more dynamic distribution groups in your organization. However, dynamic distribution groups aren't displayed on this tab because their membership is calculated each time they are used. For more information, see Managing Distribution Groups.

10. Use the **E-Mail Addresses** tab to configure the e-mail addresses for the recipient. You can modify the existing addresses or create additional ones. Each recipient must have at least one primary STMP address that is internal to your Exchange organization and one external address.
    - **Add** Click **Add** to add a new e-mail address for this recipient. Use the drop-down box to select from the following address types:

      SMTP Address This is the default address type. Click this button and use the corresponding dialog box to add an SMTP address.

EUM Address This address type is available only for user mailboxes. It's not available for mail users, mail contacts, distribution groups, or mail-enabled public folders. An EUM (Exchange Unified Messaging) address is used by Unified Messaging servers to locate UM-enabled users within an Exchange 2010 organization. EUM addresses contain the extension number and the UM dial plan for the UM-enabled user. Click this button and use the corresponding dialog box to add an EUM address.
Custom Address Click this button and use the corresponding dialog box to add a custom address (for example, fax or X.400).

Note:
With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.

- **Edit** Click this button to modify the selected e-mail address.
-  Click this button to remove the selected e-mail address.
- **Set as Reply** Click this button to set your selected address as the "reply to" address. A recipient can have multiple e-mail addresses for a specific address type. This allows the recipient to receive messages that are addressed to any one of these e-mail addresses. However, a single address must be used for any messages that are sent by the recipient. If a recipient has multiple e-mail addresses, the primary address is used for any messages sent by the recipient.
  This button is available only when an address other than the primary address is selected. Primary addresses for each address type are displayed in bold type.
  If an e-mail address policy in your Exchange organization applies to this mailbox, the **Set as Reply** setting will be controlled by that policy. To change the primary address for a specific address type, you must clear the **Automatically update e-mail addresses based on e-mail address policy** check box.
- **Set as External** This button is available only for mail users and mail contacts. It's not available for user mailboxes, distribution groups, or mail-enabled public folders. Click **Set as External** to designate the selected e-mail address as the external e-mail address for the recipient.

  Note:
  This button is enabled when an address other than the external e-mail address is selected.

- **Automatically update e-mail addresses based on e-mail address policy** Select this check box to have the recipient's e-mail addresses automatically updated based on changes made to e-mail address policies in your organization. This box is selected by default.

11. Use the **Mail Flow Settings** tab to configure message size or message delivery restrictions for the mail user.
    - **Message Size Restrictions** Select this setting and then click **Properties** to open the **Message Size Restrictions** dialog box. In this dialog box, select the **Maximum message size (in KB)** check box to set the maximum size for messages that can be received by this recipient. Use the corresponding text box to specify the maximum message size allowed (in KB). The message size must be between 0 and 2,097,151 KB. If a message larger than the specified size is sent to the recipient, the message will be returned to the sender with a descriptive error message.
    - **Message Delivery Restrictions** Select this setting and then click **Properties** to open the **Message Delivery Restrictions** dialog box. Use this dialog box to configure the following settings:

All senders Click this button to specify that the recipient can accept messages from all senders. This includes senders in both your Exchange organization and external senders. This button is selected by default. This option includes external users only if you clear the **Require that all senders are authenticated** check box. If you select this check box, messages from external users will be rejected.
Only senders in the following list Click this button to specify that the recipient can accept messages only from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.
Require that all senders are authenticated Select this check box to prevent anonymous users from sending messages to the recipient.
No senders Click this button to specify that the recipient will not reject messages from any senders in the Exchange organization. This button is selected by default.
Senders in the following list Click this button to specify that the recipient will reject messages from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now.**

Use the Shell to configure mail user properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Provisioning Recipient Permissions" section in the Mailbox Permissions topic.

This example sets the e-mail address outside of the organization to which mail-enabled user John Peoples' e-mail is sent.

```
Set-MailUser john -ExternalEmailAddress john@tailspintoys.com
```

This example sets the maximum size of messages that John Peoples is allowed to receive to 10 MB.

```
Set-MailUser -Identity john -MaxReceiveSize '10 MB'
```

For More Information

Understanding Recipients

Managing Mail Contacts and Mail Users

1.8.3.14.5 Disable E-Mail for a Mail Contact

Disable E-Mail for a Mail Contact

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can disable e-mail for an existing mail contact object in Active Directory by removing its Exchange attributes.

Important:

There are two types of mail contacts in Microsoft Exchange Server 2010: mail contacts and mail forest contacts. Mail forest contacts are read-only recipient objects that are updated only through Microsoft Identity Integration Server (MIIS) or a similar custom synchronization. You can't remove or modify a mail forest contact by using the EMC or the Shell.

Looking for other management tasks related to managing mail contacts and mail users? Check out Managing Mail Contacts and Mail Users.

Use the EMC to disable e-mail for a mail contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mail Contact**.
2. In the result pane, select the mail contact that you want to disable.
3. In the action pane, under the name of the mail contact, click **Disable**.
4. In the warning appears verifying that you want to disable e-mail for the mail contact. Click **Yes**.

Use the Shell to disable e-mail for a mail contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

This example disables e-mail for the mail contact Ellen Adams.

```
Disable-MailContact -Identity "Ellen Adams" -DomainController Domain.Contoso.com
```

For detailed syntax and parameter information, see Disable-MailContact.

1.8.3.14.6 Disable Mail for a Mail-Enabled User

Disable Mail for a Mail-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can disable mail for a mail-enabled user. This task removes all the Exchange attributes from the user object in Active Directory. However, it doesn't remove the user from Active Directory.

Looking for other management tasks related to managing mail contacts and mail users? Check out Managing Mail Contacts and Mail Users.

Use the EMC to disable mail for a mail-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail users" entry in the Mailbox Permissions topic.

1. In the console tree, expand **Recipient Configuration**, and then click **Mail Contact**.
2. In the result pane, select the mail user for which you want to disable mail.
3. In the action pane, under the name of the mail user, click **Disable**.
4. A warning appears verifying that you want to disable mail for the user. Click **Yes**.

Use the Shell to disable mail for a mail-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail users" entry in the Mailbox Permissions topic.

This example disables mail for the mail-enabled user John.

```
Disable-MailUser john@contoso.com
```

When prompted, type **Y** to confirm the disabling of the mail user.

For detailed syntax and parameter information, see Disable-MailUser.

1.8.3.14.7 Mail-Enable an Existing Contact

Mail-Enable an Existing Contact

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can mail-enable an existing contact object in Active Directory by populating its Exchange attributes (such as the contact's alias and external e-mail address).

Note:

This procedure doesn't create a mail contact in Active Directory.

Looking for other management tasks related to managing mail contacts and mail users? Check out Managing Mail Contacts and Mail Users.

Use the EMC to mail-enable an existing

mail contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

1. In the console tree, expand **Recipient Configuration**, and then click **Mail Contact**.
2. In the action pane, click **New Mail Contact**. The New Mail Contact wizard appears.
3. On the **Introduction** page, click **Existing contact**, and then click **Browse**.
4. In **Select Contact**, select the contact that you want to mail-enable, click **OK**, and then click **Next**.
5. On the **Contact Information** page, complete the following fields:
   - **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.
   - **First name** This read-only box displays the first name of the contact.
   - **Initials** This read-only box displays the initials of the contact.
   - **Last name** This read-only box displays the last name of the contact.
   - **Name** This read-only box displays the name of the contact that's listed in Active Directory. This name may be different than the first and last names.
   - **Alias** Use this box to type a unique alias (64 characters or less) for the contact. This field is required.
   - **External e-mail address** To specify the external e-mail address, perform one of the following tasks:

     To specify an SMTP e-mail address, click **Edit**. In the **SMTP address** dialog box, type the SMTP e-mail address.

     Note:

     Exchange validates SMTP addresses for proper formatting. If your entry is inconsistent with the SMTP format, an error message is displayed when you click **OK**.

     To specify a custom e-mail address, click the arrow next to **Edit**, and then click **Custom Address**. In the **Custom Address** dialog box, use the **E-mail address** box to type the e-mail address and the **E-mail type** box to specify the e-mail type. For example, you can specify an X.400, GroupWise, or Lotus Notes address.
6. On the **New Mail Contact** page, review your configuration settings. To make changes, click **Back**. To create the mail-enabled contact, click **New**. Click **Cancel** to close the wizard without mail-enabling the contact.
7. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to mail-enable an existing mail contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

This example mail-enables the existing mail contact Ellen Adams.

```
Enable-MailContact -Identity EllenAdams -ExternalEmailAddress EllenAdams@Contoso.
```

For detailed syntax and parameter information, see Enable-MailContact.

1.8.3.14.8 Mail-Enable Multiple Existing Contacts

Mail-Enable Multiple Existing Contacts

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can mail-enable existing contact objects in Active Directory by populating their Exchange attributes (such as the contact's alias and external e-mail address).

Note:

This procedure doesn't create new contacts in Active Directory.

To mail-enable existing contacts, at a minimum you must provide external e-mail addresses. When mail-enabling several contacts in bulk, it's easier to first export the list of contacts to a .csv file, and then add the external e-mail addresses to the .csv file by using a text editor such as Notepad, or a spreadsheet application such as Microsoft Office Excel. You can then use the updated .csv file in your bulk mail-enabling operation.

Looking for other management tasks related to managing mail contacts and mail users? Check out Managing Mail Contacts and Mail Users.

Use the Shell to mail-enable multiple existing contacts

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to mail-enable multiple existing contacts.

1. This example exports the list of existing contacts in your organization that aren't mail-enabled to the .csv file ContactsList.

   ```
   Get-Contact | Out-File "C:\ContactsList.CSV"
   ```

   The resulting .csv file will be similar to the following:

   ```
   #TYPE System.Management.Automation.PSCustomObject,
   Name
   Kim Abercrombie
   Don Funk
   Sanjay Patel
   ```

```
Amy Strande
...
```

2. For each contact, add a column heading and the external e-mail addresses to the .csv file. The updated .csv file should look similar to the following:

```
#TYPE System.Management.Automation.PSCustomObject,
Name,ExternalAddress
Kim Abercrombie,Kim@contoso.com
Don Funk,Don@fabrikam.com
Sanjay Patel,Sanjay@fabrikam.com
Amy Strande,Amy@contoso.com
...
```

3. This example imports and uses the data in the .csv file so you can mail-enable the contacts in bulk.

```
Import-CSV "C:\ContactsList.CSV" | ForEach-Object {Enable-MailContact
```

For detailed syntax and parameter information, see Get-Contact or Enable-MailContact.

1.8.3.14.9 Remove a Mail Contact

Remove a Mail Contact

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove an existing mail contact from Active Directory.

Important:

There are two types of mail contacts in Microsoft Exchange Server 2010: mail contacts and mail forest contacts. Mail forest contacts are read-only recipient objects that are updated only through Microsoft Identity Integration Server (MIIS) or a similar custom synchronization. You can't remove or modify a mail forest contact by using the EMC or the Shell.

Looking for other management tasks related to managing mail contacts and mail users? Check out Managing Mail Contacts and Mail Users.

Use the EMC to remove a mail contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

1. In the console tree, expand **Recipient Configuration**, and then click **Mail Contact**.
2. In the result pane, click the mail contact that you want to remove.
3. In the action pane, under the name of the mail contact, click **Remove**.
4. In the warning that asks if you're sure you want to remove the mail contact, click **Yes**.

Use the Shell to remove a mail contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mail contacts" entry in the Mailbox Permissions topic.

This example removes the mail contact Ellen Adams.

```
Remove-MailContact -Identity "Ellen Adams" -DomainController Contoso.Domain.Com
```

For detailed syntax and parameter information, see Remove-MailContact.

1.8.3.15 Managing Mailbox Databases

Managing Mailbox Databases

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-30*

Create a Mailbox Database

Mount a Database

Dismount a Database

Remove a Mailbox Database

Maintain Mailbox Databases

Modify a Database Size Limit

Move the Database Path

Configure Mailbox Database Properties

1.8.3.15.1 Create a Mailbox Database

Create a Mailbox Database

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can create a mailbox database, which is a unit of granularity where mailboxes are created and stored. A mailbox database is stored as an Exchange database (.edb) file.

Looking for other management tasks related to mailbox databases? Check out Managing Mailbox Databases.

Prerequisites

Sufficient disk space exists to create the database. For more information, see Mailbox Server Storage Design.

What Do You Want to Do?

- Use the EMC to create a mailbox database

- Use the Shell to create a mailbox database

Use the EMC to create a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Mailbox Database**. The New Mailbox Database wizard appears.
3. On the **Introduction** page, complete the following fields:
   - **Mailbox database name** Use this box to type a name for the new mailbox database. The name can contain up to 64 characters but can't include the following characters: \ / " = , ;.
   - **Browse** Click this button to locate the server on which to create the database. Select the server, and then click **OK**.
4. On the **Set Paths** page, complete the following fields:
   - **Database file path** This box displays the default path to the database file. You can change the location by typing a new path.
   - **Log folder path** This box displays the default path to the log folder. You can change the location by typing a new path.
   - **Mount this database** Select this check box if you want to mount this database. Mounting a database puts it online, making its data available to users.
5. On the **New Mailbox Database** page, click **New** to create the mailbox database.
6. On the **Completion** page, confirm whether the new mailbox database was created successfully. A status of **Completed** indicates that the wizard completed the task successfully. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. Click **Finish** to complete the wizard. The new mailbox database appears on the **Database Management** tab.

Use the Shell to create a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

This example creates the mailbox database MailboxDatabase01 and specifies where to create the .edb database file.

```
New-MailboxDatabase -Name "MailboxDatabase01" -EdbFilePath D:\DatabaseFiles\Mailb
```

This example creates the mailbox database MailboxDatabase01 and specifies where to create the .edb database file and the log folder path.

```
New-MailboxDatabase -Name "MailboxDatabase01" -EdbFilePath D:\DatabaseFiles\Mailb
```

This example mounts the newly created database MailboxDatabase01.

```
Mount-Database -Identity "MailboxDatabase01"
```

For detailed syntax and parameter information, see New-MailboxDatabase and Mount-Database.

1.8.3.15.2 Mount a Database

Mount a Database

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the EMC or the Shell to mount a mailbox database on a computer that has the Microsoft Exchange Server 2010 Mailbox server role installed.

Note:
You can mount a database only if the Microsoft Exchange Information Store service is running.

Looking for other management tasks related to mailbox databases? Check out Managing Mailbox Databases.

What Do You Want to Do?

- Use the EMC to mount a database
- Use the Shell to mount a database

Use the EMC to mount a database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database permissions" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, select the server on which the database is located.
3. In the work pane, select the mailbox database that you want to mount.
4. In the action pane, click **Mount Database**.
5. Verify that the status indicated in the **Status** column has changed from **Dismounted** to **Mounted**.

Use the Shell to mount a database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database permissions" entry in the Mailbox Permissions topic.

This example uses the **Mount-Database** command to mount the database MyDatabase.

```
Mount-Database "MyDatabase"
```

For detailed syntax and parameter information, see Mount-Database.

1.8.3.15.3 Dismount a Database

Dismount a Database

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Exchange Management Console or the Shell to dismount a mailbox database on a computer that has the Microsoft Exchange Server 2010 Mailbox server role installed.

Looking for other management tasks related to mailbox databases? Check out Managing Mailbox Databases.

What Do You Want to Do?

- Use the EMC to dismount a database
- Use the Shell to dismount a database

Use the EMC to dismount a database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database permissions" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, select the server on which the mailbox or public folder database is located.
3. In the work pane, select the database that you want to dismount.
4. In the action pane, click **Dismount Database**.
5. A warning appears asking if you want to dismount the database. Click **Yes**.

Use the Shell to dismount a database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database permissions" entry in the Mailbox Permissions topic.

This example uses the **Dismount-Database** command to dismount the database MyDatabase.

```
Dismount-Database "MyDatabase"
```

Note:

You can dismount a database only if the Microsoft Exchange Information Store service is running.

1.8.3.15.4 Remove a Mailbox Database

Remove a Mailbox Database

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Exchange Management Console or the Shell to remove a mailbox database.

Looking for other management tasks related to mailbox databases? Check out Managing Mailbox Databases.

What Do You Want to Do?

- Use the EMC to remove a mailbox database
- Use the Shell to remove a mailbox database

Use the EMC to remove a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database permissions" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the work pane, expand the mailbox database you want to remove.
3. In the action pane, click **Remove**.
4. A warning appears asking if you're sure you want to remove the mailbox database. Click **Yes**.
5. When the dialog box appears stating that the database was removed successfully, note the location of the Exchange database (.edb) file. If you want to remove this file from the hard drive, you must remove it manually. Click **OK**.

Use the Shell to remove a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database permissions" entry in the Mailbox Permissions topic.

This example uses the **Remove-MailboxDatabase** command to remove the database MyDatabase.

```
Remove-MailboxDatabase -Identity "MyDatabase"
```

1. When you are prompted about whether you're sure that you want to perform the action, type **Y**.
2. When the dialog box appears stating that the database was removed successfully, note the location of the Exchange database (.edb) file. If you want to remove this file from the hard drive, you must remove it manually.

For detailed syntax and parameter information, see Remove-MailboxDatabase.

1.8.3.15.5 Maintain Mailbox Databases

Maintain Mailbox Databases

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use several tools to maintain your mailbox database. The following sections describe how to use these tools to ensure that your mailbox databases continue to operate efficiently. These tools help to reduce the administrative database maintenance tasks that you had to perform in previous versions of Exchange.

Looking for other management tasks related to managing mailbox databases? Check out Managing Mailbox Databases.

Use performance counters to monitor online defragmentation

In Microsoft Exchange Server 2010, the following performance counters for monitoring the behavior of database defragmentation have been added for use with Performance Monitor:

- **MSExchange Database ==> Instances \ Defragmentation tasks** Shows the background database defragmentation tasks currently executing.
- **MSExchange Database ==> Defragmentation Tasks completed/Sec** Shows the number of background database defragmentation tasks completing execution per second.
- **MSExchange Database ==> Defragmentation Tasks Discarded** Shows the background database defragmentation tasks that couldn't be registered.
- **MSExchange Database ==> Defragmentation Tasks Pending** Shows the background database defragmentation tasks currently pending.
- **MSExchange Database ==> Instances \ Defragmentation Tasks Scheduled/Sec** Shows the background database defragmentation tasks scheduled for execution per second.

These are informational performance counters to show the performance of the database and aren't required to be part of the daily maintenance of your database.

You can also enable extended Extensible Storage Engine (ESE) performance counters to further help with monitoring your databases. For more information, see How to Enable Extended ESE Performance Counters.

Use the EMC to set the maintenance schedule for a database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

You can use the EMC to set the maintenance schedule for a database or allow 24x7 database maintenance. Online defragmentation no longer runs only during the maintenance window as it did in Exchange Server 2007. Instead, it's performed continuously as data is read from and written to the database. For more information, see New Exchange Core Store Functionality.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Management** tab, click the mailbox database for which you want to set the maintenance schedule.
3. In the action pane, under the name of the database, click **Properties**. The **<Database Name> Properties** dialog box appears.
4. On the **Maintenance** tab, select the **Enable background database maintenance (24 x 7 ESE scanning)** check box, and then click **Customize** to

select a predefined schedule or to create a customized schedule.
5. Click **OK** to save your changes.

Use the Shell to set the maintenance schedule for a database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

This example sets the database schedule for the mailbox database MailboxDatabase1 on Server01 to run between 02:00 and 03:00 on Sundays and Wednesdays.

```
Set-MailboxDatabase -Identity "Server01\MailboxDatabase1" -MaintenanceSchedule "S
```

This example mounts the database in 24 x 7 background check-summing mode.

```
Set-MailboxDatabase -BackgroundDatabaseMaintenance $true -Identity <dbname>
```

When set to `$false`, the database will be mounted without the 24x7 checksum mode and will perform the ESE checksum maintenance during the online maintenance period that you selected.

For detailed syntax and parameter information, see Set-MailboxDatabase.

For more information about database maintenance, see the "Database Maintenance" section in New Exchange Core Store Functionality.

1.8.3.15.6 Modify a Database Size Limit

Modify a Database Size Limit

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-20*

You can use Registry Editor to modify a database size limit in Microsoft Exchange Server 2010. The default database size limit for Exchange 2010 Standard Edition is 1024 gigabytes (GB). There is no default database size limit for the Exchange 2010 Enterprise Edition. The Exchange store checks any database size limits periodically and dismounts a database when the size limit is reached. You can modify the database size limit by adding or changing a value in the registry.

Note:
When you change this setting, this change is propagated to all servers that host a copy of this database.

Looking for other management tasks related to mailbox databases? Check out Managing Mailbox Databases.

Use Registry Editor to Modify a Database Size Limit

If you change the size limit of your Exchange databases, you may want to evaluate your

Exchange database backup and restore plan. Specifically, if you increase the size limit of the Exchange databases, test your backup and recovery operations using the new database size limits to make sure that you can still meet your service level agreements (SLAs).

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

1. Start Registry Editor (regedit).
2. Locate the following registry subkey:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server Name>\Private-<database GUID>

   Note:

   You can get the GUID of a database by running the following command in the Exchange Management Shell: `Get-MailboxDatabase -Identity "<database name>" | Format-Table Name, GUID`
3. If the **Database Size Limit in GB** DWORD exists for the subkey, change its value to the desired size in gigabytes.
4. If the **Database Size Limit in GB** DWORD doesn't exist for the subkey, create a new DWORD with that name, and then set its value to the desired size in gigabytes.

For more information about managing databases, see Managing Mailbox Databases.

To learn more about Registry Editor, see Registry Editor overview.

1.8.3.15.7 Move the Database Path

Move the Database Path

Mailbox > Managing Mailbox Servers > Managing Mailbox Databases >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-04-24*

You can move the mailbox database path on a server that is running Microsoft Exchange Server 2010. To set a new path to the location of a database, and to move the related files to that location, you can use the EMC or the Exchange Management Shell.

Looking for other management tasks related to mailbox databases? Check out Managing Mailbox Databases.

Prerequisites

To perform the move operation, you must temporarily dismount the database. This makes the database inaccessible to all users. If the database is currently dismounted, it isn't remounted upon completion.

What Do You Want to Do?

- Use the EMC to move the mailbox database path
- Use the Shell to move the mailbox database path

Use the EMC to move the mailbox database path

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Management** tab, select the database you want to configure.
3. In the work pane, click M**ove Database Path**.
4. In the Move Database Path wizard, under **Database paths**, click **Move** to move the database path to the default location. You can change the location for the database file path by editing the **Database file path** field. You can change the location for the log folder path by editing the **Log folder path** text field.
5. View the status of the move operation. The wizard moves the database file path and the log folder path to the new location. Click **Back** to make configuration changes.
6. On the **Completion** page, confirm whether the move process completed successfully. A status of **Completed** indicates that the wizard completed the task successfully. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. Click **Finish** to complete the Move Database Path wizard.

Note:

After the database is moved, the Indexing service maintains a lock on the Catalog files. Before you can delete these files from the old location, you must restart the Microsoft Exchange Search Indexer service.

Use the Shell to move the mailbox database path

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database permissions" entry in the Mailbox Permissions topic.

This example uses the **Move-DatabasePath** command to set a new path for the mailbox database specified by the GUID.

```
Move-DatabasePath -Identity a0ec9f03-12a9-4e40-9310-43f9105fd4d2 -EdbFilePath C:\
```

For detailed syntax and parameter information, see Move-DatabasePath.

Note:

After the database is moved, the Indexing service maintains a lock on the Catalog files. Before you can delete these files from the old location, you must restart the Microsoft Exchange Search Indexer service.

Configure Mailbox Database Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Microsoft Exchange Server 2010, each mailbox database has its own properties that you can configure. These properties include mounting, dismounting, and moving a database path.

Looking for other management tasks related to mailbox databases? Check out Managing Mailbox Databases.

What Do You Want to Do?

- Use the EMC to configure mailbox database properties
- Use the Shell to configure mailbox database properties

Use the EMC to configure mailbox database properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Management** tab, select the database you want to configure.
3. In the action pane, under the database name, click **Properties**.
4. Use the **General** tab to view status about the mailbox database, including the mailbox database path, last backup, and mailbox database status:
   - **Database path** This read-only field displays the full path to the Exchange database (.edb) file for the selected mailbox database. To view the entire path, you may have to click the path and use the Right Arrow key. You can't use this field to change the path. To change the location of the database files, close **Properties**, right-click the database, and then click **Move Database Path**. You can also change the location by using the Move-DatabasePath cmdlet.
   - **Last full backup** This read-only field displays the date and time of the last complete backup of the mailbox database.
   - **Last incremental backup** This read-only field displays the date and time of the last incremental backup of the mailbox database.
   - **Status** This read-only field displays whether the mailbox database is mounted or dismounted.
   - **Mounted on server** This read-only field displays which server the database is mounted on.
   - **Master** This read-only field displays the master server for the mailbox database. The Mailbox server that hosts the active copy of a database is referred to as the mailbox database master. For more information, see Managing Mailbox Database Copies.
   - **Master type** This read-only field displays the type of mailbox database master.
   - **Modified** This read-only field displays the date and time the database was last modified.

- **Servers hosting a copy of this database** This read-only field displays the other servers that have a copy of this database.

5. Use the **Maintenance** tab to configure mailbox database settings, including specifying a journal recipient, setting a maintenance schedule, and mounting the database at startup:
   - **Journal Recipient** Select this check box to enable transport journaling of e-mail. To learn more, see Understanding Journaling.
   - **Maintenance schedule** Use this list to select one of the preset maintenance schedules. You can also configure a custom schedule. To configure a custom schedule, click **Customize**.
   - **Enable background database maintenance (24 x 7 ESE scanning)** Select this check box to enable online database scanning, which runs continuously in the background. Online database scanning performs a checksum calculation of the database and performs operations that allow Exchange to scan for lost space on the database and recover it. If you select this check box, Exchange scans the database no more than one time per day and will issue a warning event if it can't finish scanning the database in a seven day period. For more information, see Maintain Mailbox Databases.
   - **Don't mount this database at startup** Select this check box to prevent Exchange from mounting this mailbox database when it starts.
   - **This database can be overwritten by a restore** Select this check box to allow the mailbox database to be overwritten during a restore process.
   - **Enable circular logging** Select this check box to enable circular logging. For more information about circular logging, see Understanding the Exchange 2010 Store.

6. Use the **Limits** tab to specify the storage limits, the warning message interval, and the deletion settings for a mailbox database:
   - **Issue warning at (MB)** Select this check box to automatically warn mailbox users that their mailbox is approaching its storage limit. To specify the storage limit, select the check box, and then specify in kilobytes (KB) how much content can be stored in the mailbox before a warning e-mail message is sent to the mailbox users. You can enter a value from 0 through 2,097,151 megabytes (MB) (2.0 terabytes).
   - **Prohibit send at (MB)** Select this check box to prevent users from sending new e-mail messages after the size of their mailbox reaches the specified limit. To specify this limit, select the check box, and then type the size of the mailbox in MB at which you want to prohibit the sending of new e-mail messages and notify the user. You can enter a value from 0 through 2,097,151 MB (2.0 terabytes).
   - **Prohibit send and receive at (MB)** Select this check box to prevent users from sending and receiving e-mail messages after their mailbox size reaches the specified limit. To specify this limit, select the check box, and then type the size of the mailbox in MB at which you want to prohibit the sending and receiving of e-mail messages and notify the user. You can enter a value from 0 through 2,097,151 MB (2.0 terabytes).
   - **Warning message interval** Use this list to specify the time at which mailboxes are scanned for compliance with the storage limits that you set. To configure a custom time, click **Customize**.
   - **Keep deleted items for (days)** Use this box to set the number of days that deleted items are retained in a mailbox. You can enter a value from 0 through 24,855 days.
   - **Keep deleted mailboxes for (days)** Use this box to set the number of days that deleted mailboxes are retained. You can enter a value from 0 through 24,855 days.
   - **Don't permanently delete items until the database has been backed up** Select this check box to prevent mailboxes and e-mail messages from

being deleted until after the mailbox database has been backed up.

7. Use the **Client Settings** tab to view and select the default public folder database and the offline address book (OAB) for the mailbox:
   - **Default public folder database** This box shows the location of the default public folder database. The public folder database stores public folder data, OAB information, and free/busy information for Microsoft Exchange Server 2003 and earlier versions. To change the location of the default public folder database, click **Browse** and select a new location.
   - **Offline address book** This box shows the location of the OAB. To change the location of the OAB, click **Browse**, and then select a new location.

Use the Shell to configure mailbox database properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

This example sets the length of time that deleted items are retained. If a particular mailbox has its own item retention set, that value is used instead of this value, which is set on the mailbox database.

```
Set-MailboxDatabase "Mailbox Database01" -DeletedItemRetention 7.00:00:00
```

For detailed syntax and parameter information, see Set-MailboxDatabase.

1.8.3.15.9 Turn Off Exchange Store Time-Out Detection

Turn Off Exchange Store Time-Out Detection

Mailbox > Managing Mailbox Servers > Managing Mailbox Databases >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-29*

An indication of an unhealthy Exchange store is that threads are either deadlocked or are otherwise not making progress. If there are more than five threads on a single mailbox, ten threads on a single database, or twenty threads on a single server that haven't progressed in one minute, a time-out is reported on the server. The performance counters that indicate time-outs are:

- RPC Request Timeout Detected on Mailbox
- RPC Request Timeout Detected on Database
- RPC Request Timeout Detected on Server

The Exchange store also writes the following events to the server under the MSExchangeIS source:

- **Event 10025** Reports a time-out on the Exchange server
- **Event 10026** Reports a time-out on the database
- **Event 10027** Reports a time-out on an individual mailbox

If the time-out is detected on a single mailbox, the mailbox is potentially considered to be poisoned and is handled similarly to a failure by increasing the **CrashCount** property. This action makes the mailbox susceptible to being quarantined. Therefore, you may want to turn off Exchange store time-out detection for Mailbox servers that regularly have a large number of threads operating against them.

Use the Registry to turn off Exchange store time-out detection

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

1. Open Registry Editor (regedit).
2. Navigate to the following subkey:
   \\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server Name>
3. Right-click the *<Server Name>*, point to **New**, and then click **DWORD (32-bit) Value**. The new DWORD value displays in the results pane.
4. Rename the key to **DisableTimeoutDetection**, and then press Enter.
5. Right-click **DisableTimeoutDetection**, and then click **Modify**.
6. Change the **Value data** to **1**.
7. Click **OK**.

Manage Database Log Growth by Using the Troubleshoot-DatabaseSpace.ps1 Script in the Shell

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The **Troubleshoot-DatabaseSpace.ps1** script is used by Microsoft System Center Operations Manager 2007 to detect and correct any excess log growth or Microsoft Exchange database (.edb) file growth that, if unchecked, may cause database downtime. By default, System Center Operations Manager 2007 runs the script every 15 minutes. However, you can use Task Scheduler to configure and run this script to monitor database log and file growth.

Note:

A script must be run from the folder in which it resides. By default, scripts installed with Exchange 2010 are installed at C:\Program Files\Microsoft\Exchange Server\V14\Scripts. The Shell doesn't load scripts automatically. To run a script from the local file, you must precede all scripts with "**.**" For example, to run the SampleScript.ps1 script, type `.\SampleScript.ps1`. To run a script and specify the default installation path, type `"C:\Program Files\Microsoft\Exchange Server\V14\Scripts\SampleScript.ps1"`. For more information, see Scripting with the Exchange Management Shell.

The **Troubleshoot-DatabaseSpace.ps1** script performs the following actions:

1. Keeps track of log generation rate for the highest log generators per database. This helps determine which users are logging too heavily and potentially causing space issues.
2. Keeps track of the available disk space for both the database and the log files. If either of these is within a configurable threshold of being full, further action must be taken.
3. Keeps track of the log generation rate. If it appears that the disk is going to run out of space within the value specified by the *HourThreshold* parameter (based on the log generation rate), further action must be taken.

   Note:

   To avoid critical issues, make sure the value for the *HourThreshold* parameter is large enough to give you time to react during normal business hours while enough free space is available. If drives are filling up faster than the value specified, immediate action must be taken to protect the disk.

4. If all of the preceding conditions are fulfilled, the script determines the list of top 25 users who accessed the database during the last one-hour period. The script then quarantines the top high-usage mailboxes for which the sum of the log generation rate is greater than the difference between the current generation rate and the sustainable generation rate that would allow tiding over the configurable time threshold. These users are quarantined for six hours, during which they won't have access to e-mail.
5. If the troubleshooter is unsuccessful at dropping the log generation rate to below the threshold level, it will write out events that translate into health model alerts. At this point, the script removes the database from provisioning by running the Set-MailboxDatabase cmdlet with the *ExcludeFromProvisioning* parameter set to `$true` against the specified database. You may need to move mailboxes to a new server to rebalance space.
6. If the troubleshooter quarantines more than 10 users, this indicates a systemic issue, which you need to follow up on. The health model will trigger an urgent alert from this condition.

The default settings used in the **Troubleshoot-DatabaseSpace.ps1** script are defined in the **StoreTSConstants.ps1** script.

Looking for other management tasks related to databases? Check out Managing Mailbox Databases.

Use the Troubleshoot-DatabaseSpace.ps1 script

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

The following parameter syntax set and table lists the parameters that you can use to move specific mailboxes.

```
Troubleshoot-DatabaseSpace.ps1 -MailboxDatabaseName <DatabaseID> [-PercentEdbFree
Troubleshoot-DatabaseSpace.ps1 -Server <ServerID> [-PercentEdbFreeSpaceThreshold
```

Parameter	Required	Description
MailboxDatabaseName	Required	The *MailboxDatabaseName* parameter specifies the mailbox database on which you're monitoring the log growth. This parameter accepts the following

		values: • GUID • Distinguished name (DN) • Database name **Note:** You can't use this parameter in conjunction with the *Server* parameter.
Server	Required	The *Server* parameter specifies the Mailbox server on which you're monitoring the log growth for all mailbox databases. **Note:** You can't use this parameter in conjunction with the *MailboxDatabaseName* parameter.
HourThreshold	Optional	The *HourThreshold* parameter specifies the number of hours you can wait until running out of space. The default value is 12 hours.
MonitoringContext	Optional	The *MonitoringContext* parameter specifies whether the results of the command include monitoring events to be written in the regular Application logs in Event Viewer and in the Operations log. If you don't specify this value, the Operations logs will be written to the following location in Event Viewer: **Event Viewer** > **Application and Services Logs** > **Microsoft-Exchange-Troubleshooters/ Operational**. You don't have to specify a value for this parameter.
PercentEdbFreeSpaceThreshold	Optional	The *PercentEdbFreeSpaceThreshold* parameter specifies the percentage of disk space for the .edb file at which Exchange should begin quarantining users. For example, if you specify 10 percent, Exchange will begin quarantining the heaviest users when the command detects that the hard drive will run out of space due to growth of the .edb file within the time specified in the *HourThreshold* parameter. The default value for this parameter is 25 percent.
PercentLogFreeSpaceThre	Optional	The *PercentLogFreeSpaceThreshold* parameter specifies the percentage of

shold		disk space for the log files at which Exchange should begin quarantining users. For example, if you specify 10 percent, Exchange will begin quarantining the heaviest users when the command detects that the hard drive will run out of space due to log growth within the time specified in the *HourThreshold* parameter. The default value for this parameter is 25 percent.
Quarantine	Optional	The *Quarantine* parameter specifies that heavy users will be quarantined. If you don't specify this parameter, users won't be quarantined. You don't need to specify a value for this parameter.

Example

This example shows how to run the **Troubleshoot-DatabaseSpace.ps1** script with the following settings:

- The warnings are set at 10 percent free space in the volume containing the database logs and 10 percent free space in the database file and the volume containing it.
- The hour threshold is set at 5 hours.

With these settings, if the troubleshooter determines that the free space on the hard drive will be at 10 percent or less capacity within 5 hours, it will quarantine the heaviest users.

```
.\Troubleshoot-databasespace.ps1 -server MBX01 -PercentLogFreeSpace 10 -PercentED
```

Note:

This example shows how to run the command manually once. To produce the data that the troubleshooter needs to effectively monitor your server or database, you must run this command several times at regular intervals. We recommend that you use the Task Scheduler in the Microsoft Windows operating system to set up this task. For more information, see Task Scheduler Overview.

View the log growth troubleshooter output

In Event Viewer, the results of the **Troubleshoot-DatabaseSpace.ps1** script will be available in the following location: **Event Viewer** > **Application and Services Logs** > **Microsoft-Exchange-Troubleshooters/Operational**.

For example, the following represents output from event ID 5101. This output would be returned if the script ran successfully without errors.

```
The database space troubleshooter finished on volume D:\ for database MBD01, no problems were detected.

EDB drive free space: 151938752512 B

Log drive free space: 151845265408 B
```

EDB free space threshold: 10%

Log free space threshold: 10%

Hour threshold: 12 Hrs

Current growth rate: 314572800 B/Hr

The following table displays the event ID, the description of the event, and if necessary, the action to take.

Note:
The descriptions in this table are examples of the information that may be included in these events.

Event ID	Description	Action
5100	The database space troubleshooter started on volume D:\ for database MBD01.	Informational only. No action is required.
5101	The database space troubleshooter finished on volume D:\ for database MBD01. No problems were detected.	Informational only. No action is required.
5400	The database space troubleshooter finished on volume D:\ for database MBD01. The database is over the free space threshold. Users were quarantined to avoid running out of space.	Warning event: Continue monitoring. Users will be quarantined for six hours and won't be able to access their mailboxes.
5401	The database space troubleshooter finished on volume D:\ for database MBD01. The database is under the free space threshold, but not growing at an unusual rate. No action was taken.	Warning event: Continue monitoring.
5410	The database space troubleshooter quarantined mailbox f3bb8007-b6d1-45f5-b748-211d66fa43f6 in database MBD01.	Warning event: This event will be created when event 5400 is created. Continue monitoring.
5700	The database space troubleshooter finished on volume D:\ for database MBD01. The database is over the free space threshold and continues to grow. Manual intervention is required.	This error event indicates that the database space is over the free space threshold. Run the Microsoft Exchange Server User Monitor tool (Exmon) to track users or services that are creating excessive log

		growth. For details, see Microsoft Exchange Server User Monitor.
5701	The database space troubleshooter detected a low space condition on volume D:\ for database MBD01. Provisioning for this database has been disabled. Free space for this database is less than 10 percent.	This error event indicates that the database has been removed from provisioning. In this case, the script runs the Set-MailboxDatabase cmdlet with the *ExcludeFromProvisioning* parameter set to `$true` against the specified database. When the database space problem is resolved, you must manually turn provisioning back on for the mailbox database. You may need to move mailboxes to a new server to rebalance space.
5702	The database space troubleshooter has detected a critically low space condition on volume D:\ for database MBD01. Provisioning for this database has been disabled. Free space for this database is less than 10 percent.	This error event indicates that the database has been removed from provisioning because resources are critically low. In this case, the script runs the Set-MailboxDatabase cmdlet with the *ExcludeFromProvisioning* parameter set to `$true` against the specified database. When the database space problem is resolved, you must manually turn provisioning back on for the mailbox database. You may need to move users to a new database to rebalance space.

1.8.3.15.11 Manage Database Latencies by Using the Troubleshoot-DatabaseLatency.ps1 Script in the Shell

Manage Database Latencies by Using the Troubleshoot-DatabaseLatency.ps1 Script in the Shell

Mailbox > Managing Mailbox Servers > Managing Mailbox Databases >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The **Troubleshoot-DatabaseLatency.ps1** script is used by Microsoft System Center Operations Manager 2007 to detect and correct high latencies on a database. You can create a scheduled task by using Task Scheduler to run this script. Database latencies can be caused by a number of issues, including the following problems:

- **Disk latencies due to a bad disk** Disks with very high read or write latencies can be caused by a bad disk if the latencies persist over long periods of time.
- **Domain controller latencies** A domain controller may exhibit long latencies in responding to LDAP search queries.
- **High user workload** A single user (or set of users) conducting heavy operations can result in database latencies.

The **Troubleshoot-DatabaseLatency.ps1** script performs the following actions:

1. Checks whether database latencies are above the latency threshold (as specified by the *LatencyThreshold* parameter). The default is 70 milliseconds (ms).
2. Checks whether the disk's transfers-per-second rate is less than the DiskReadRateThreshold performance counter and whether the disk's seconds-per-transfer rate is greater than the DiskReadLatencyThreshold performance counter. If this is the case, the script determines that the disk must be replaced because it's under low-load conditions but is exhibiting high latencies.
3. Checks whether a single user is using more than one thread over the last 10 minute period for longer than the value specified by the *TimeInServerThreshold* parameter. If this is the case, the user is likely contributing to the high latencies, and, as a result, the user's mailbox is quarantined. The user's mailbox is quarantined for six hours, during which the user won't have access to e-mail.

The default settings used in the **Troubleshoot-DatabaseLatency.ps1** script are defined in the **StoreTSConstants.ps1** script.

Note:

A script must be run from the folder in which it resides. By default, scripts installed with Exchange 2010 are installed at C:\Program Files\Microsoft\Exchange Server\V14\Scripts. The Shell doesn't load scripts automatically. To run a script from the local file, you must precede all scripts with "**.**" For example, to run the SampleScript.ps1 script, type `.\SampleScript.ps1`. To run a script and specify the default installation path, type `"C:\Program Files\Microsoft\Exchange Server\V14\Scripts\SampleScript.ps1"`. For more information, see Scripting with the Exchange Management Shell.

Use the Troubleshoot-DatabaseLatency.ps1 script

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

The following parameter syntax set and table lists the parameters that you can use to detect and troubleshoot database latency issues.

```
Troubleshoot-DatabaseLatency.ps1 -MailboxDatabaseName <DatabaseID> [-LatencyThres
```

Parameter	Required	Description

MailboxDatabaseName	Required	The *MailboxDatabase* parameter specifies the mailbox database on which you're monitoring the database latency. This parameter accepts the following values: • GUID • Distinguished name (DN) • Database name
LatencyThreshold	Optional	The *LatencyThreshold* parameter specifies the amount of time in ms that the database can be idle before it's considered to be latent. The default value is 70 ms.
MonitoringContext	Optional	The *MonitoringContext* parameter specifies whether the results of the command are written in the Application event log. If you don't specify this value, the event logs are written to the following location in Event Viewer: **Event Viewer** > **Application and Services Logs** > **Microsoft** > **Microsoft-Exchange-Troubleshooters/Operational**. You don't have to specify a value with this parameter.
Quarantine	Optional	The *Quarantine* parameter specifies that heavy users who are contributing to the high latencies will be quarantined. If you don't specify this parameter, users won't be quarantined. You don't have to specify a value with this parameter.
TimeInServerThreshold	Optional	The *TimeInServerThreshold* parameter specifies how much time (in seconds) that any user activity for which the Exchange store uses a thread can be spent per minute for a single mailbox before the mailbox is considered hazardous to the health of the database. The number of seconds is measured by aggregating the time that all threads working on behalf of the mailbox (during the period reported by the Get-StoreUsageStatistics cmdlet) spend inside the Exchange store. The number of seconds of work per minute is calculated by dividing this aggregate number by the period

		reported by the **Get-StoreUsageStatistics** cmdlet (by default 10 minutes). For example, if you set this parameter to 80 seconds, and a single user uses more than one thread for longer than 80 seconds in a 10 minute period, an event error is returned. If you specify the *Quarantine* parameter, the event error is returned, and the user's mailbox is also quarantined for six hours. The default value is 200 seconds.

Example

This example shows how to run the **Troubleshoot-DatabaseLatency.ps1** script with the following settings:

- The *LatencyThreshold* parameter is set to 100 ms. If the database is latent for more than 100 ms, an error is returned.
- The *TimeInServerThreshold* parameter is set to 80 seconds. If a single user uses more than one thread for longer than 80 seconds in a 10 minute period, that user is quarantined.

```
.\Troubleshoot-DatabaseLatency.ps1 -MailboxDatabaseName MBD01 -LatencyThreshold 1
```

Note:

This example shows how to run the command manually once. To produce the data that the troubleshooter needs to effectively monitor your databases, you must run this command at regular intervals. We recommend that you use the Task Scheduler in the Microsoft Windows operating system to set up this task. For more information, see Task Scheduler Overview.

View the database latency troubleshooter output

In Event Viewer, the results of the **Troubleshoot-DatabaseLatency.ps1** script are available in the following location: **Event Viewer** > **Application and Services Logs** > **Microsoft** > **Microsoft-Exchange-Troubleshooters/Operational**.

For example, the following represents output from event ID 5111. This output would be returned if the script ran successfully without errors.

```
The database latency troubleshooter has detected that the current latency of 1 ms for database MBD01 is within the threshold of 100 ms.
```

The following table displays the event ID, the description of the event, and, if necessary, the action to take.

Note:

The descriptions in this table are examples of the information that may be included in these events.

Event ID	Description	Action
5110	The database latency troubleshooter started on	Informational only. No action is required.

	database MBD01.	
5111	The database latency troubleshooter has detected that the current latency of 30 ms for database MBD01 is within the threshold of 70 ms.	Informational only. No action is required.
5411	The database latency troubleshooter quarantined user f3bb8007-b6d1-45f5-b748-211d66fa43f6 on database MBD01 due to unusual activity in the mailbox. If the problem persists, manual intervention will be required.	Warning event: Continue monitoring.
5412	The database latency troubleshooter identified a problem with user f3bb8007-b6d1-45f5-b748-211d66fa43f6 on database MBD01 due to unusual activity in the mailbox. The user wasn't quarantined because the *Quarantine* parameter wasn't specified. If the problem persists, manual intervention will be required.	Warning event: Continue monitoring.
5710	The database latency troubleshooter detected that disk latencies are abnormal for database MBD01. You need to replace the disk.	Error event: You need to replace the disk. Contact your hardware manufacturer for replacement instructions.
5712	The database latency troubleshooter detected high RPC average latencies for database MBD01 but was unable to determine a cause. Manual intervention is required.	Error event: The cause of the latency couldn't be determined. You should create a dump file and analyze it to determine the cause of the issue. For Windows Vista, Windows 7, or Windows Server 2008, see How to Create a user-mode process dump file. For Windows Server 2003 or earlier, see How to use the Userdump.exe tool to create a dump file.

1.8.3.16 Managing Mailbox Import and Export Requests

Managing Mailbox Import and Export Requests

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-08*

1.8.3.16.1 Add the Mailbox Import Export Role to a Role Group

Add the Mailbox Import Export Role to a Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

By default, the Mailbox Import Export management role isn't included in any of the built-in role groups, such as the Organization Management role group. To import or export mailbox data, you need to add the Mailbox Import Export management role to a role group.

You can add the Mailbox Import Export management role to a role group with no scope between the role and the role group. When you do this, the implicit read and implicit write scopes of the role apply. For details about how to add the Mailbox Import Export management role to a role group with a predefined scope, see Add a Role to a Role Group.

Looking for other management tasks related to importing and exporting mailbox data? Check out Managing Mailbox Import and Export Requests.

Prerequisites

- Because you can't add roles to built-in role groups, you need to create a role group to which you can add the Mailbox Import Export management role. For detailed instructions, see Create a Role Group.
- Read the following topics:
  - Understanding Management Role Groups
  - Understanding Management Role Assignments
  - Understanding Management Role Scopes
- Be aware that role assignments are additive. This means that all the roles are added together when they're evaluated. If two roles are assigned to a user and one role contains a cmdlet but the other doesn't, the cmdlet is still available to the user.
- By default, role assignments, including the Organization Management role, don't grant the ability (called *role delegation*) to assign roles to other users. Role delegation is an advanced task. To enable a user to assign roles to other role groups, see Delegate Role Assignments.

Use the Shell to add the Mailbox Import Export role to a role group with no scope

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:

You can't use the EMC to add the Mailbox Import Export management role to a role group with no scope.

This example assigns the Mailbox Import Export management role to the Enterprise Support security group.

```
New-ManagementRoleAssignment -Name "Import Export_Enterprise Support" -SecurityGr
```

For detailed syntax and parameter information, see New-ManagementRoleAssignment.

Other Tasks

After you add the Mailbox Import Export management role to a role group, you may also want to:

- Add Members to a Role Group
- Change the Scope of Role Assignments to a Role Group
- Create a Mailbox Import Request
- Create a Mailbox Export Request

1.8.3.16.2 Create a Mailbox Export Request

Create a Mailbox Export Request

Mailbox > Managing Mailbox Servers > Managing Mailbox Import and Export Requests >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-21*

A mailbox export request is a process of exporting mailbox or archive data to a .pst file. You can create more than one mailbox export request per mailbox, and each request must have a unique name. Microsoft Exchange automatically generates up to 10 unique names for a mailbox. To create more than 10 export requests for a mailbox, you must specify a unique name when you create the request.

Note:
Although you can create multiple export requests per mailbox at one time, you can create only one request at a time per .pst file. This is because the .pst file is locked as *in-use* when the request begins to run.

Alternatively, you can remove existing export requests by using the **Remove-MailboxExportRequest** cmdlet, and then start the new request by using `MailboxExportX` as the default value for the *Name* parameter (where *X* equals 0–9). For more information, see Remove a Mailbox Export Request.

Note:
You can't use the Exchange Management Console (EMC) to create a mailbox export request. You must use the Exchange Management Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Note:
When you use the **New-MailboxExportRequest** cmdlet to export a mailbox to a .pst file, the .pst file can be opened only by using Microsoft Outlook 2010 or a later version.

Prerequisites

To export a mailbox or archive, you must first create a network shared folder. You need to grant read/write permission to the group Exchange Trusted Subsystem to the network share where you'll export or import mailboxes. If you don't grant this permission, you'll receive an error message stating that Exchange is unable to establish a connection to the target mailbox. For more information, see Set Permissions for Shared Folders.

Use the Shell to export a user's primary mailbox to a .pst file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

You need to grant read/write permission to the group Exchange Trusted Subsystem to the network share where you'll export or import mailboxes. If you don't grant this permission, you'll receive an error message stating that Exchange is unable to establish a connection to the target mailbox.

This example exports Ayla Kol's primary mailbox to a .pst file on the network shared folder PSTFileShare on server MBX-01.

Note:
The command doesn't create directories. If you specify a directory that doesn't exist, the command fails.

```
New-MailboxExportRequest -Mailbox AylaKol -FilePath \\MBX-01\PSTFileShare\Ayla_Re
```

For detailed syntax and parameter information, see New-MailboxExportRequest.

Use the Shell to export a user's personal archive to a .pst file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

You need to grant read/write permission to the group Exchange Trusted Subsystem to the network share where you'll export or import mailboxes. If you don't grant this permission, you'll receive an error message stating that Exchange is unable to establish a connection to the target mailbox.

This example exports Kweku's archive to a .pst file on the network shared folder PSTFileShare.

```
New-MailboxExportRequest -Mailbox Kweku -IsArchive -FilePath "\\SERVER01\PSTFileS
```

For detailed syntax and parameter information, see New-MailboxExportRequest.

Use the Shell to export data from a user's mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

You need to grant read/write permission to the group Exchange Trusted Subsystem to the network share where you'll export or import mailboxes. If you don't grant this permission, you'll receive an error message stating that Exchange is unable to establish a connection to the target mailbox.

This example exports Tony's messages that were received before January 1, 2010, and contain the words "company" and "profit" in the message body.

For more information about how to use the *ContentFilter* parameter, see Filterable Properties for the -ContentFilter Parameter.

```
New-MailboxExportRequest -Mailbox Tony -ContentFilter {(body -like "*company*") -
```

For detailed syntax and parameter information, see New-MailboxExportRequest.

Use the Shell to export data from a well-known folder

Well-known folders are mailbox folders known by a specific name, regardless of the folder's name in another language. For example, #Inbox# denotes the Inbox folder even if it's localized in Turkish as Gelen Kutusu. Well-known folders include the following types:

- Inbox
- SentItems
- DeletedItems
- Calendar
- Contacts
- Drafts

- Journal
- Tasks
- Notes
- JunkEmail
- CommunicationHistory
- Voicemail
- Fax
- Conflicts
- SyncIssues
- LocalFailures
- ServerFailures

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

You need to grant read/write permission to the group Exchange Trusted Subsystem to the network share where you'll export or import mailboxes. If you don't grant this permission, you'll receive an error message stating that Exchange is unable to establish a connection to the target mailbox.

This example exports all messages from Kweku's Inbox to the .pst file LitigationHold.

```
New-MailboxExportRequest -Mailbox Kweku -IncludeFolders "#Inbox#" -FilePath \\PST
```

For detailed syntax and parameter information, see New-MailboxExportRequest.

Other Tasks

After you export mailboxes or archives, you may also want to:

- View Mailbox Export Request Properties
- Remove a Mailbox Export Request

1.8.3.16.3 Create a Mailbox Import Request

Create a Mailbox Import Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A mailbox import request is a process of importing mailbox data from a .pst file into a mailbox or archive. You can create more than one mailbox import request per mailbox, and each request must have a unique name. Microsoft Exchange automatically generates up to 10 unique names for a mailbox. However, to create more than 10 import requests for a mailbox, you need to specify a unique name when creating the request.

Note:

Although you can create multiple import requests per mailbox at one time, you can create only one request at a time per .pst file. This is because the .pst file is locked as *in-use* when the request begins to run.

Alternatively, you can remove existing import requests by using the **Remove-**

MailboxImportRequest cmdlet, and then start the new request by using `MailboxImportX` as the default value for the *Name* parameter (where *X* equals 0–9). For more information, see Remove a Mailbox Import Request.

Note:
You can't use the Exchange Management Console (EMC) to create a mailbox import request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to import a .pst file into a user's primary mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

You need to grant read/write permission to the group Exchange Trusted Subsystem to the network share where you'll export or import mailboxes. If you don't grant this permission, you'll receive an error message stating that Exchange is unable to establish a connection to the target mailbox.

This example imports a recovered .pst file into Ayla's primary mailbox. Only data in the .pst file's Inbox is imported. The data is imported into the RecoveredFiles folder of Ayla's target mailbox.

```
New-MailboxImportRequest -Mailbox Ayla -FilePath \\SERVER01\PSTFiles\Recovered.ps
```

For detailed syntax and parameter information, see New-MailboxImportRequest.

Use the Shell to import a .pst file into a user's archive

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

You need to grant read/write permission to the group Exchange Trusted Subsystem to the network share where you'll export or import mailboxes. If you don't grant this permission, you'll receive an error message stating that Exchange is unable to establish a connection to the target mailbox.

This example imports a .pst file into Kweku's archive folder. The *TargetRootFolder* parameter isn't specified. Therefore, content is merged into existing folders, and folders are created if they don't already exist in the target folder structure.

```
New-MailboxImportRequest -Mailbox Kweku -IsArchive -FilePath \\SERVER01\PSTFiles\
```

For detailed syntax and parameter information, see New-MailboxImportRequest.

Use the Shell to import multiple .pst files

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

You need to grant read/write permission to the group Exchange Trusted Subsystem to

the network share where you'll export or import mailboxes. If you don't grant this permission, you'll receive an error message stating that Exchange is unable to establish a connection to the target mailbox.

This example imports all the .pst files in a shared folder. Each .pst file is named after a corresponding user's alias. The command creates an import request for all the .pst files and imports the data into the matching mailbox.

```
Dir \\SERVER01\PSTshareRO\Recovered\*.pst | %{ New-MailboxImportRequest -Name Rec
```

For detailed syntax and parameter information, see New-MailboxImportRequest.

1.8.3.16.4 Configure Mailbox Export Request Properties

Configure Mailbox Export Request Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

After you create a mailbox export request, the request could possibly fail (for example, if the bad item limit is exceeded). If the request fails, you can edit the properties of the mailbox export request to increase the bad item limit. After the mailbox export request is initiated, you can edit the settings until it reaches a status of Completed.

Note:

You can't use the Exchange Management Console (EMC) to change the properties of an export request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to change the bad item limit of a single mailbox export request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example changes the mailbox export request Ayla\MailboxExport to accept up to 10 corrupted mailbox items.

```
Set-MailboxExportRequest -Identity "Ayla\MailboxExport" -BadItemLimit 10
```

For detailed syntax and parameter information, see Set-MailboxExportRequest.

Use the Shell to change the properties of multiple mailbox export requests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example finds all mailbox export requests that have a status of Failed, changes the

bad item limit to accept up to five corrupted mailbox items, and then gives the requests a batch name of BadItemLimitTo5.

```
Get-MailboxExportRequest -Status Failed | Set-MailboxExportRequest -BadItemLimit
```

For detailed syntax and parameter information, see Get-MailboxExportRequest and Set-MailboxExportRequest.

1.8.3.16.5 Configure Mailbox Import Request Properties

Configure Mailbox Import Request Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

After you create a mailbox import request, the request could possibly fail (for example, if the bad item limit is exceeded). If the request fails, you can edit the properties of the mailbox import request to increase the bad item limit. After the mailbox import request is initiated, you can edit the settings until it reaches a status of Completed.

Note:

You can't use the Exchange Management Console (EMC) to change the properties of an import request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to change the bad item limit of a single mailbox import request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example changes the mailbox import request Kweku\Import to accept up to five corrupted mailbox items.

```
Set-MailboxImportRequest -Identity "Kweku\Import" -BadItemLimit 5
```

For detailed syntax and parameter information, see Set-MailboxImportRequest.

Use the Shell to change the properties of multiple mailbox import requests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example finds all mailbox import requests that have a status of Suspended, and then gives the requests a batch name of April14.

```
Get-MailboxImportRequest -Status Suspended | Set-MailboxImportRequest -BatchName
```

For detailed syntax and parameter information, see Get-MailboxImportRequest and Set-MailboxImportRequest.

1.8.3.16.6 Suspend a Mailbox Export Request

Suspend a Mailbox Export Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can suspend a mailbox export request any time after the request is created, but before the request reaches the status of Completed. You can resume the request by using the Resume-MailboxExportRequest cmdlet.

Note:
You can't use the Exchange Management Console (EMC) to suspend an export request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to suspend a mailbox export request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example suspends the mailbox export request Ayla\MailboxExport.

```
Suspend-MailboxExportRequest -Identity "Ayla\MailboxExport"
```

For detailed syntax and parameter information, see Suspend-MailboxExportRequest.

Use the Shell to suspend multiple mailbox export requests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example suspends all mailbox export requests in progress by using the **Get-MailboxExportRequest** cmdlet to retrieve all requests that have a status of `InProgress`, and then pipelines the output to the **Suspend-MailboxExportRequest** cmdlet with the suspend comment "Resume after 10 P.M."

```
Get-MailboxExportRequest -Status InProgress | Suspend-MailboxExportRequest -Suspe
```

For detailed syntax and parameter information, see Get-MailboxExportRequest and Suspend-MailboxExportRequest.

Other Tasks

After you suspend the mailbox export request, you may also want to resume it. For detailed steps, see Resume a Mailbox Export Request.

1.8.3.16.7 Suspend a Mailbox Import Request

Suspend a Mailbox Import Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can suspend a mailbox import request any time after the request is created, but before the request reaches the status of Completed. You can resume the request by using the Resume-MailboxImportRequest cmdlet.

Note:
You can't use the Exchange Management Console (EMC) to suspend an import request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to suspend a mailbox import request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example suspends the mailbox import request Ayla\MailboxImport.

```
Suspend-MailboxImportRequest -Identity "Ayla\MailboxImport"
```

For detailed syntax and parameter information, see Suspend-MailboxImportRequest.

Use the Shell to suspend multiple mailbox import requests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example suspends all mailbox import requests in progress by using the **Get-MailboxImportRequest** cmdlet to retrieve all requests that have a status of `InProgress`, and then pipelines the output to the **Suspend-MailboxImportRequest** cmdlet with the suspend comment "Resume after 10 P.M."

```
Get-MailboxImportRequest -Status InProgress | Suspend-MailboxImportRequest -Suspe
```

For detailed syntax and parameter information, see Get-MailboxImportRequest and Suspend-MailboxImportRequest.

Other Tasks

After you suspend the mailbox import request, you may also want to resume it. For detailed steps, see Resume a Mailbox Import Request.

1.8.3.16.8 Resume a Mailbox Export Request

Resume a Mailbox Export Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can resume a mailbox export request that has a status of Suspended or Failed.

Note:
You can't use the Exchange Management Console (EMC) to resume an export request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to resume a mailbox export request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example resumes the mailbox export request Kweku\Export.

```
Resume-MailboxExportRequest -Identity Kweku\Export
```

For detailed syntax and parameter information, see Resume-MailboxExportRequest.

Use the Shell to resume multiple mailbox export requests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example resumes all mailbox export requests that have a status of Failed.

```
Get-MailboxExportRequest -Status Failed | Resume-MailboxExportRequest
```

For detailed syntax and parameter information, see Get-MailboxExportRequest and Resume-MailboxExportRequest.

1.8.3.16.9 Resume a Mailbox Import Request

Resume a Mailbox Import Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can resume a mailbox import request that has a status of Suspended or Failed.

Note:
You can't use the Exchange Management Console (EMC) to resume an import request. You must use the shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to resume a mailbox import request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example resumes the mailbox import request Kweku\MailboxImport.

```
Resume-MailboxImportRequest -Identity Kweku\MailboxImport
```

For detailed syntax and parameter information, see Resume-MailboxImportRequest.

Use the Shell to resume multiple mailbox import requests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example resumes all mailbox import requests that have a status of Failed.

```
Get-MailboxImportRequest -Status Failed | Resume-MailboxImportRequest
```

For detailed syntax and parameter information, see Get-MailboxImportRequest and Resume-MailboxImportRequest.

1.8.3.16.10 View Mailbox Import Request Properties

View Mailbox Import Request Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A mailbox import request is the process of importing mailbox data from a .pst file to a

mailbox or archive. You can view the properties of a mailbox import request, or you can view the statistics. The properties provide you with basic information about the status of a mailbox import request. The statistics provide you with detailed information that can be used for troubleshooting purposes.

The search criteria for the **Get-MailboxImportRequest** and **Get-MailboxImportRequestStatistics** cmdlets is a Boolean **And** statement. If you use multiple parameters, you can narrow your search and reduce your search results.

Note:
You can't use the Exchange Management Console (EMC) to view the properties of a mailbox import request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to view mailbox import request properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example returns the default information about the status of the ongoing mailbox import request Tony\Recovered. By default, the type of information returned includes the name of the request, the mailbox for which the request is being performed, and the status of the request.

```
Get-MailboxImportRequest -Identity "Tony\Recovered"
```

This example returns detailed information about the status of the ongoing mailbox import request Tony\Recovered by using the *IncludeReport* parameter and by pipelining the results to the **Format-List** command.

```
Get-MailboxImportRequest -Identity "Tony\Recovered" -IncludeReport | Format-List
```

This example returns the information about mailbox import requests that have a status of In Progress for mailboxes or archives that reside on database DB01.

```
Get-MailboxImportRequest -Status InProgress -Database DB01
```

This example returns information about mailbox import requests in the ImportingDB1PSTs batch that have a status of Completed.

```
Get-MailboxImportRequest -BatchName "ImportingDB1PSTs" -Status Completed
```

This example returns all mailbox import requests that have the name Recovered and have a status of Suspended.

```
Get-MailboxImportRequest -Name "Recovered" -Suspend $true
```

For detailed syntax and parameter information, see Get-MailboxImportRequest.

Get-MailboxImportRequest Output

By default, the **Get-MailboxImportRequest** cmdlet returns the name of the request, the alias of the target mailbox, and the status of the request. The following table lists the information that's returned if you pipeline the **Format-List** command.

Value	Description
FilePath	This value specifies the file path of the .pst

	file from which data is being exported.
TargetDatabase	This value specifies the database that contains the mailbox or archive to which the .pst file is being imported.
Mailbox	This value specifies the user whose mailbox or archive is being imported.
Name	This value specifies the name of the mailbox import request.
RequestGUID	This value specifies the GUID of the mailbox import request.
RequestQueue	This value specifies the database on which the Microsoft Exchange Mailbox Replication service (MRS) stores the detailed status of the mailbox import request.
Flags	This value specifies flags that the cmdlet automatically sets when creating the mailbox import request.
BatchName	This value specifies a batch name. If you didn't provide a batch name, this field is blank.
Status	This value specifies the status of the request.
Suspend	This value specifies whether the request was created to be automatically suspended before completion.
Direction	This value specifies whether the request is a push or a pull. For mailbox import requests, this value is always `Pull`.
RequestStyle	This value specifies whether the request is `IntraOrg` or `CrossOrg`. For Exchange Server 2010 Service Pack 1 (SP1), this value is always `IntraOrg`.
Identity	This value specifies the identity of the mailbox import request.

Use the Shell to view mailbox import request statistics

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example returns the default statistics for the mailbox import request for Tony Smith. By default, the type of information returned includes the name of the request, the mailbox for which the request is being performed, and the status of the request.

```
Get-MailboxImportRequestStatistics -Identity Tony\MailboxImport
```

This example returns additional information about the mailbox import request

LitigationHold for Ayla's mailbox by using the *IncludeReport* parameter and by pipelining the results to the **Format-List** command.

```
Get-MailboxImportRequestStatistics -Identity Ayla\LitigationHold -IncludeReport |
```

This example returns detailed statistics for the mailbox import request Tony\MailboxImport and exports the report to a .csv file.

```
Get-MailboxImportRequestStatistics -Identity Tony\MailboxImport | Export-CSV \\SE
```

This example returns additional information for all the mailbox import requests that have a status of Failed by using the *IncludeReport* parameter, and then saves the information to the text file AllImportReports.txt.

```
Get-MailboxImportRequest -Status Failed | Get-MailboxImportRequestStatistics -Inc
```

For detailed syntax and parameter information, see Get-MailboxImportRequestStatistics and Get-MailboxImportRequest.

Get-MailboxImportRequestStatistics Output

By default, the **Get-MailboxImportRequestStatistics** cmdlet returns the name of the request, the status of the request, the alias of the target mailbox, and the percentage completed. The following table lists the information that's returned if you pipeline the **Format-List** command.

Value	Description
Name	This value specifies the name of the request.
Status	This value specifies the status of the request.
StatusDetail	This value specifies more detailed status information about the request.
Flags	This value specifies flags that the cmdlet automatically sets when creating the mailbox import request.
RequestStyle	This value specifies whether the request is `IntraOrg` or `CrossOrg`. For Exchange 2010 SP1, this value is always `IntraOrg`.
Suspend	If set to `$true`, this value specifies whether an administrator suspended this request or whether the request failed.
FilePath	This value specifies a file path from where the .pst file is imported.
TargetAlias	This value specifies the alias of the target mailbox.
TargetIsArchive	This value specifies whether the .pst file is being imported into an archive.
TargetExchangeGuid	This value specifies the GUID of the target mailbox or archive.
TargetRootFolder	This value specifies the name of the root folder in the mailbox's or archive's hierarchy

	to which data is imported. If this value is blank, data is imported to the folder Top of Information Store.
TargetDatabase	This value specifies the target database to which the .pst file is being imported.
IncludeFolders	This value specifies the list of folders to include during the import. If this value is blank, no folders were specified when the request was created, and all folders will be imported to the mailbox or archive (unless the *ExcludeFolders* parameter is used to exclude specific folders).
ExcludeFolders	This value specifies the list of folders to exclude during the import. If this value is blank, no folders were specified when the request was created, and all folders will be imported to the mailbox or archive (unless the *IncludeFolders* parameter is used to include specific folders).
ExcludeDumpster	This value specifies whether the Recoverable Items folder was excluded when the request was created.
ConflictResolutionOption	This value specifies the action for MRS to take if there are matching messages in the target and source folders.
AssociatedMessagesCopyOption	This value specifies whether the associated messages are copied when the request is processed. Associated messages are special messages that contain hidden data with information about rules, views, and forms.
BatchName	This value specifies a batch name. If you don't provide a batch name, this field is blank.
BadItemLimit	This value specifies the number of bad items that MRS will skip if the request encounters corrupted messages.
BadItemsEncountered	This value specifies the number of corrupted messages encountered by the command. If the *BadItemsEncountered* value is greater than the *BadItemLimit* value, the request fails.
QueuedTimestamp	This value specifies the date and time at which the request was initiated to MRS.
StartTimestamp	This value specifies the date and time at which the import started being processed by MRS.
LastUpdateTimeStamp	This value specifies the date and time at which the last change was made to the request. The change could have been made

	by an administrator or by MRS.
CompletionTimeStamp	This value specifies the date and time at which the request completed.
SuspendedTimeStamp	This value specifies the date and time at which the request was suspended. If the request wasn't suspended, this value is blank.
OverallDuration	This value specifies the amount of time it took to complete the request. If the request is in a Failed state, this value specifies the amount of time between the request being initiated and the request failing. If the request hasn't completed, this value specifies the amount of time between the request being initiated and the **Get-MailboxImportRequestStatistics** cmdlet being run.
TotalSuspendedDuration	This value specifies the amount of time the request was in the Suspended state.
TotalFailedDuration	This value specifies the amount of time the request was in the Failed state.
TotalQueuedDuration	This value specifies the amount of time the request was in the Queued state.
TotalInProgressDuration	This value specifies the amount of time the request was in the In Progress state.
TotalStalledDueToHADuration	This value specifies the amount of time the request was stalled due to high availability.
TotalTransientFailureDuration	This value specifies the amount of time that the request was stalled due to a transient failure, such as a database failure or network connectivity issues.
MRSServerName	This value specifies the name of the Client Access server that processed the request.
EstimatedTransferSize	This value specifies the file size that was imported or the file size that MRS expects to import if the mailbox import request is in the In Progress state.
EstimatedTransferItemCount	This value specifies the number of items that were imported or the number of items that MRS expects to import if the request is in the In Progress state.
BytesTransferred	This value specifies the number of bytes that have been transferred.
BytesTransferredPerMinute	This value specifies the average number of bytes that have been transferred per minute.
ItemsTransferred	This value specifies the number of items that

	have been transferred.
PercentComplete	This value specifies the percentage of the request that has been completed.
PositionInQueue	If the request hasn't started, this value specifies the request's position in the queue.
FailureCode	If there was a failure, this value specifies the failure code.
FailureType	If there was a failure, this value specifies the failure type.
Message	If there was a failure, this value specifies the failure message. This value can also specify the suspend comment.
FailureTimestamp	If the request failed, this value specifies the date and time at which the request failed.
IsValid	This value specifies whether the mailbox import request was valid.
ValidationMessage	If the mailbox import request wasn't valid, this value specifies the reason.
RequestGUID	This value specifies the GUID of the mailbox import request.
RequestQueue	This value specifies the database on which MRS stores the detailed status of the mailbox import request.
Identity	This value specifies the identity of the request.
Report	If you specified the *IncludeReport* parameter when using the **Get-MailboxImportRequest** cmdlet, this value specifies information that can be used to troubleshoot the request.

1.8.3.16.11 View Mailbox Export Request Properties

View Mailbox Export Request Properties

Mailbox > Managing Mailbox Servers > Managing Mailbox Import and Export Requests >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A mailbox export request is the process of exporting mailbox or archive data to a .pst file. You can view the properties of an export request, or you can view the statistics. The properties provide you with basic information about the status of an export request. The statistics provide you with detailed information that can be used for troubleshooting purposes.

Note:

You can't use the Exchange Management Console (EMC) to view the properties of a mailbox export request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

View Export Request Properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example returns the default information about the status of the ongoing export request Tony\DB01toPST. By default, the type of information includes the name of the request, the mailbox for which the request is being performed, and the status of the request.

```
Get-MailboxExportRequest -Identity "Tony\DB01toPST"
```

This example returns additional information about the status of the ongoing export request Tony\DB01toPST by pipelining the results to the **Format-List** command.

```
Get-MailboxExportRequest -Identity "Tony\DB01toPST" | Format-List
```

This example returns information about export requests that have a status of In Progress and are exporting data from a mailbox or archive that resides on database DB01.

```
Get-MailboxExportRequest -Status InProgress -Database DB01
```

This example returns information about export requests in the Attachment_CompanyReport batch that have a status of Completed.

```
Get-MailboxExportRequest -BatchName "Attachment_CompanyReport" -Status Completed
```

This example returns all export requests that have the name DB01toPST and have a status of Suspended.

```
Get-MailboxExportRequest -Name "DB01toPST" -Suspend $true
```

For detailed syntax and parameter information, see Get-MailboxExportRequest.

Get-MailboxExportRequest Output

By default, the **Get-MailboxExportRequest** cmdlet returns the name of the request, the mailbox for which the request is being performed, and the status of the request. The following table lists the information that's returned if you pipeline the **Format-List** command:

Value	Description
FilePath	This value specifies file path where the .pst file will be exported.
SourceDatabase	This value specifies the database that contains the mailbox or archive that's being exported.
Mailbox	This value specifies the user whose mailbox or archive is being exported.
Name	This value specifies the name of the export request.
RequestGUID	This value specifies the GUID of the export

	request.
RequestQueue	This value specifies the database on which the Microsoft Exchange Mailbox Replication service (MRS) stores the detailed status of the export request.
Flags	This value specifies flags that the cmdlet automatically sets when creating the export request.
BatchName	This value specifies a batch name. If you didn't provide a batch name, this field will be blank.
Status	This value specifies the status of the request.
Suspend	This value specifies if the request was created to be automatically suspended before completion.
Direction	This value specifies if the request is a push or a pull. For export requests, this value is always `Push`.
RequestStyle	This value specifies if the request is `IntraOrg` or `CrossOrg`. For Exchange 2010 SP1, this value is always `IntraOrg`.
Identity	This value specifies the identity of the export request.

View Export Request Statistics

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example returns the default export request statistics for Tony\MailboxExport. By default, the type of information returned includes the name of the request, the mailbox for which the request is being performed, and the status of the request.

```
Get-MailboxExportRequestStatistics -Identity Tony\MailboxExport
```

This example returns additional information about the export request Tony\MailboxExport by using the *IncludeReport* parameter and by pipelining the results to the **Format-List** command.

```
Get-MailboxExportRequestStatistics -Identity Tony\MailboxExport -IncludeReport |
```

This example returns detailed statistics for the export request Tony\MailboxExport and exports the report to a .csv file.

```
Get-MailboxExportRequestStatistics -Identity Tony\MailboxExport | Export-CSV \\Ex
```

This example returns additional information for all the export requests that have a status of Failed by using the *IncludeReport* parameter, and then saves the information to the text file AllExportReports.txt.

```
Get-MailboxExportRequest -Status Failed | Get-MailboxExportRequestStatistics -Inc
```

For detailed syntax and parameter information, see Get-MailboxExportRequestStatistics and Get-MailboxExportRequest.

Get-MailboxExportRequestStatistics Output

By default, the **Get-MailboxExportRequestStatistics** cmdlet returns the name of the request, the status of the request, the alias of the source mailboxes, and the percentage completed. The following table lists the information that's returned if you pipeline the **Format-List** command:

Value	Description
Name	This value specifies the name of the request.
Status	This value specifies the status of the request.
StatusDetail	This value specifies more detailed status information about the request.
Flags	This value specifies flags that the cmdlet automatically sets when creating the export request.
RequestStyle	This value specifies if the request is `IntraOrg` or `CrossOrg`. For Exchange 2010 SP1, this value is always `IntraOrg`.
Suspend	If set to `true`, this value specifies whether an administrator suspended this request or if the request failed.
FilePath	This value specifies file path from where the .pst file is exported.
SourceAlias	This value specifies the alias of the source mailbox.
SourceExchangeGuid	This value specifies the GUID of the source mailbox or archive.
SourceRootFolder	This value specifies the name of the root folder in the mailbox's or archive's hierarchy from which the data is exported. If this value is blank, the data is exported from the folder "Top of Information Store".
IncludeFolders	This value specifies the list of folders to include during the export. If this value is blank, no folders were specified when the request was created and all folders will be exported (unless the *ExcludeFolders* parameter is used to exclude specific folders).
ExcludeFolders	This value specifies the list of folders to exclude during the export. If this value is blank, no folders were specified when the request was created and all folders will be exported (unless the *IncludeFolders* parameter is used to include specific folders).

ExcludeDumpster	This value specifies if the Recoverable Items folder was excluded when the request was created.
ConflictResolutionOption	This value specifies the action for MRS to take if there are matching messages in the target and source folders.
AssociatedMessagesCopyOption	This value specifies whether the associated messages are copied when the request is processed. Associated messages are special messages that contain hidden data with information about rules, views, and forms.
BatchName	This value specifies a batch name. If you don't provide a batch name, this field will be blank.
ContentFilter	This value specifies the OPATH content filter used to search for message content. For more information, see Filterable Properties for the -ContentFilter Parameter.
ContentFilterLanguage	This value specifies the language used in the content filter string searches.
BadItemLimit	This value specifies the number of bad items that MRS will to skip if the request encounters corrupted messages.
BadItemsEncountered	This value specifies the number of corrupted messages encountered by the command. If the number of *BadItemsEncountered* is greater than the *BadItemLimit*, the request will fail.
QueuedTimeStamp	This value specifies the time at which the request was initiated to MRS.
StartTimestamp	This value specifies the date and time at which the export started being processed by MRS.
LastUpdateTimeStamp	This value specifies the date and time at which the last change was made to the request. The change could have been made by an administrator or by MRS.
CompletionTimeStamp	This value specifies the date and time at which the request completed.
SuspendedTimeStamp	This value specifies the date and time at which the request was suspended. If the request wasn't suspended, this value will be blank.
OverallDuration	This value specifies the amount of time it took to complete the request. If the request is in a Failed state, this value specifies the amount of time between the request being initiated and the request failed. If the request hasn't completed, this value

	specifies the amount of time between the request being initiated and the **Get-MailboxExportRequestStatistics** cmdlet being run.
TotalSuspendedDuration	This value specifies the amount of time the request was in the Suspended state.
TotalFailedDuration	This value specifies the amount of time the request was in the Failed state.
TotalQueuedDuration	This value specifies the amount of time the request was in the queued state.
TotalInProgressDuration	This value specifies the amount of time the request was in the In Progress state.
TotalStalledDueToHADuration	This value specifies the amount of time the request was stalled due to high availability.
TotalTransientFailureDuration	This value specifies the amount of time the request was in the Stalled state due to a transient database failure.
MRSServerName	This value specifies the name of the Client Access server that processed the request.
EstimatedTransferSize	This value specifies the file size that was exported or MRS expects to export if the export request is still in progress.
EstimatedTransferItemCount	This value specifies the number of items that were exported or that MRS expects to export if the request is in the In Progress state.
BytesTransferred	This value specifies the number of bytes that have been transferred.
BytesTransferredPerMinute	This value specifies the average number of bytes that have been transferred per minute.
ItemsTransferred	This value specifies the number of items that have been transferred.
PercentComplete	This value specifies the percentage of the request that has been completed.
PositionInQueue	If the request hasn't started, this value specifies the request's position in the queue.
FailureCode	If there was a failure, this value specifies the failure code.
FailureType	If there was a failure, this value specifies the failure type.
Message	If there was a failure, this value specifies the failure message. This value can also specify the suspend comment.

FailureTimestamp	If the request failed, this value specifies the date and time at which the request failed.
IsValid	This value specifies if the export request was valid.
ValidationMessage	If the export request wasn't valid, this value specifies the reason.
RequestGUID	This value specifies the GUID of the export request.
RequestQueue	This value specifies the database on which MRS stores the detailed status of the export request.
Identity	This value specifies the identity of the request.
Report	If you specified the *IncludeReport* parameter when using the **Get-MailboxExportRequest** cmdlet, this value specifies information that can be used to troubleshoot the request.

1.8.3.16.12 Remove a Mailbox Import Request

Remove a Mailbox Import Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Completed mailbox import requests aren't cleared automatically. You can remove fully or partially completed mailbox import requests by using the **Remove-MailboxImportRequest** cmdlet.

Note:
If you remove a partially completed mailbox import request, the request is removed from the Microsoft Exchange Mailbox Replication service (MRS) job queue. Any import progress made before the removal won't be reverted back.

Note:
You can't use the Exchange Management Console (EMC) to remove an import request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to remove a mailbox import request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example removes the mailbox import request Ayla\MailboxImport.

```
Remove-MailboxImportRequest -Identity "Ayla\MailboxImport"
```

This example cancels a mailbox import request by using the *RequestGuid* parameter for a mailbox or archive on MBXDB01.

Note:
You should use the *RequestGuid* parameter only for debugging or troubleshooting purposes.

```
Remove-MailboxImportRequest -RequestQueue MBXDB01 -RequestGuid 25e0eaf2-6cc2-4353
```

For detailed syntax and parameter information, see Remove-MailboxImportRequest.

Use the Shell to remove multiple mailbox import requests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example removes all mailbox import requests that have a status of Completed.

```
Get-MailboxImportRequest -Status Completed | Remove-MailboxImportRequest
```

For detailed syntax and parameter information, see Get-MailboxImportRequest and Remove-MailboxImportRequest.

1.8.3.16.13 Remove a Mailbox Export Request

Remove a Mailbox Export Request

Mailbox > Managing Mailbox Servers > Managing Mailbox Import and Export Requests >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Completed mailbox export requests aren't cleared automatically. You can remove fully or partially completed mailbox export requests by using the **Remove-MailboxExportRequest** cmdlet.

Note:
If you remove a partially completed mailbox export request, content already exported isn't removed from the .pst file. If you want to start a new mailbox export request to the same file and start with an empty .pst file, you must rename or delete the previous .pst file.

Note:
You can't use the Exchange Management Console (EMC) to remove an export request. You must use the Shell.

Looking for other management tasks related to mailbox import or export requests? Check out Managing Mailbox Import and Export Requests.

Use the Shell to remove a mailbox export

request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example removes the mailbox export request Ayla\MailboxExport.

```
Remove-MailboxExportRequest -Identity "Ayla\MailboxExport"
```

This example cancels a mailbox export request by using the *RequestGuid* parameter for a mailbox or archive on MBXDB01.

Note:

You should use the *RequestGuid* parameter only for debugging or troubleshooting purposes.

```
Remove-MailboxExportRequest -RequestQueue MBXDB01 -RequestGuid 25e0eaf2-6cc2-4353
```

For detailed syntax and parameter information, see Remove-MailboxExportRequest.

Use the Shell to remove multiple mailbox export requests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Import Export" entry in the Mailbox Permissions topic.

This example removes all mailbox export requests that have a status of Completed.

```
Get-MailboxExportRequest -Status Completed | Remove-MailboxExportRequest
```

For detailed syntax and parameter information, see Get-MailboxExportRequest and Remove-MailboxExportRequest.

1.8.3.17 Managing Repair Requests

Managing Repair Requests

Exchange Server 2010 > Mailbox > Managing Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-16*

Create a Mailbox Repair Request

View Mailbox Repair Request Entries in Event Viewer

Create a Public Folder Database Repair Request

Create a Mailbox Repair Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Use the **New-MailboxRepairRequest** cmdlet to detect and repair mailbox corruptions. You can run this command against a specific mailbox or against a mailbox database. While this task is running, mailbox access is disrupted for the mailbox being repaired. If you're running this command against a mailbox database, only the mailbox being repaired is disrupted. All other mailboxes in the database remain operational.

Note:
You can't perform these procedures in the Exchange Management Console (EMC). You must use the Shell.

The **New-MailboxRepairRequest** cmdlet detects and repairs the following types of mailbox corruptions:

- Search folder corruptions (using the `SearchFolder` value of the *CorruptionType* parameter)
- Aggregate counts on folders that aren't reflecting correct values (using the `AggregateCounts` value of the *CorruptionType* parameter)
- Views on folders that aren't returning the correct content (using the `FolderView` value of the *CorruptionType* parameter)
- Provisioned folders that are incorrectly pointing into parent folders that aren't provisioned (using the `ProvisionedFolder` value of the *CorruptionType* parameter)

To avoid any performance problems, Exchange enforces limits on the number of simultaneous repair requests that can be submitted per server. Only one request can be active for a database-level repair; up to 100 requests can be active for a mailbox-level repair per server.

Note:
After you start the repair request, it can't be stopped unless you dismount the database. For more information, see Dismount a Database.

Looking for other management tasks related to creating a mailbox repair request? Check out Managing Repair Requests.

New-MailboxRepairRequest Output

When you run the **New-MailboxRepairRequest** cmdlet, the following output is displayed:

- **RepairTaskID** This value specifies a unique identifier for the repair task.
- **Mailbox** This value specifies the mailbox being repaired. If you specified a database-level repair, this value is blank.
- **Database** This value specifies the database that contains the mailbox being repaired.
- **Server** This value specifies the Mailbox server hosting the active copy of the database that contains the mailbox being repaired.

Use the Shell to detect corruptions and repair a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox repair request" entry in the Mailbox Permissions topic.

This example detects and repairs the folder view for the mailbox tony@contoso.com.

```
New-MailboxRepairRequest -Mailbox tony@contoso.com -CorruptionType FolderView
```

For detailed syntax and parameter information, see New-MailboxRepairRequest.

Use the Shell to detect corruptions and repair a set of mailboxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox repair request" entry in the Mailbox Permissions topic.

This example detects and repairs all corruption types for mailboxes that have CustomAttribute2 set to Repair Required.

```
Get-Mailbox -Filter {CustomAttribute2 -like "Repair Required"} | New-MailboxRepai
```

For detailed syntax and parameter information, see Get-Mailbox and New-MailboxRepairRequest.

Use the Shell to detect corruptions for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox repair request" entry in the Mailbox Permissions topic.

This example detects and reports only on `ProvisionedFolder` and `SearchFolder` corruption issues in Ayla Kol's mailbox. This command doesn't repair the mailbox.

```
New-MailboxRepairRequest -Mailbox ayla -CorruptionType ProvisionedFolder,SearchFo
```

For detailed syntax and parameter information, see New-MailboxRepairRequest.

Use the Shell to repair all mailboxes in a database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox repair request" entry in the Mailbox Permissions topic.

This example detects and repairs the corruption type `AggregateCounts` for the mailbox database MBX-DB01.

```
New-MailboxRepairRequest -Database MBX-DB01 -CorruptionType AggregateCounts
```

For detailed syntax and parameter information, see New-MailboxRepairRequest.

Other Tasks

After you perform these procedures, you may also want to see which mailboxes had corruptions and were repaired. For details, see View Mailbox Repair Request Entries in Event Viewer.

1.8.3.17.2 View Mailbox Repair Request Entries in Event Viewer

View Mailbox Repair Request Entries in Event Viewer

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-29*

After you run the New-MailboxRepairRequest cmdlet, you can use Event Viewer to view the details of the request.

This topic lists the events that are logged and also provides steps for creating a custom view in Event Viewer in which you can view the repair request events.

Event IDs for Mailbox Repair Requests

The events are logged in Event Viewer under the **MSExchangeIS Mailbox Store** source. The following event IDs are logged for repair requests.

Event ID	Description
10044	The mailbox repair request failed for provisioned folders. This event ID is created in conjunction with event ID 10049.
10045	The database repair request failed for provisioned folders. This event ID is created in conjunction with event ID 10049.
10046	The provisioned folders repair request completed successfully.
10047	A mailbox-level repair request started.
10048	The mailbox or database repair request completed successfully.
10049	The mailbox or database repair request failed because Exchange encountered a problem with the database or another task is running against the database. To fix this issue, perform the following steps: 1. Run the command again. 2. If the problem persists, run Eseutil (Exchange Server Database Utilities) to check the drive for errors. 3. Run the Microsoft Exchange Troubleshooting Assistant v1.1 (ExTRA) with the **tagISINTEG** property. Save the ExTRA log trace information and then contact Microsoft support

<table>
<tr><td></td><td>services.</td></tr>
<tr><td>10050</td><td>The database repair request couldn't run against the database because the database doesn't support the corruption types specified in the command. This issue can occur when you run the command from a server that's running a later version of Exchange than the database you're scanning.</td></tr>
<tr><td>10051</td><td>The database repair request was cancelled because the database was dismounted.</td></tr>
<tr><td>10059</td><td>A database-level repair request started.</td></tr>
<tr><td>10062</td><td>Corruption was detected. View the repair log details to see what the corruption type was and if it was repaired.

The following is an example of the information you would get if the repair request detected and repaired a mailbox with event ID 10062.

Corruptions detected during online integrity check for request 321c88e0-0ad2-4e15-b93b-197a94efd1bd

Mailbox:C51AB7C3-9EB7-40C9-AAC6-953FD084AF59

Database:MBD01
<table>
<tr><th>Corruption</th><th>Is fixed</th><th>FID</th><th>Resolution</th></tr>
<tr><td>Folder Backlinks</td><td>Yes</td><td>1c7c-BC72D267870102</td><td>Update</td></tr>
<tr><td>Folder Aggregate Count</td><td>Yes</td><td>1c7c-BC72D267870102</td><td>Update</td></tr>
</table>
</td></tr>
</table>

Looking for other management tasks related to mailbox repair requests? Check out Managing Repair Requests.

Use Event Viewer to create a custom view for mailbox repair requests

1. Open **Event Viewer**.
2. In the console tree, click **Event Viewer**
3. On the **Action** menu, click **Create Custom View**.
4. In **Create Custom View**, click **By source**, and then, in the **Event sources** list, select **MSExchangeIS Mailbox Store**.
5. In the box labeled **<All Event IDs>**, add the event IDs for the repair request events that you want to see. For example if you want to see all of the events, enter **10044,10045,01146,10047,10048,10049,10050,10051,10059,10062**.
6. Click **OK**.
7. In **Save Filter to Custom View**, type the name of the view. For example, **Mailbox Repair Events**.

8. Click **OK**.
9. The view is created in the **Custom Views** node of the Event Viewer console tree.

1.8.3.17.3 Create a Public Folder Database Repair Request

Create a Public Folder Database Repair Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the **New-PublicFolderDatabaseRepairRequest** cmdlet to detect and fix replication issues in a public folder database. While the request is running, only access to the public folder being repaired is disrupted. All other public folders are available.

Note:
After you start the repair request, you can't stop it unless you dismount the database. For more information, see Dismount a Database.

Looking for other management tasks related to repair requests? Check out Managing Repair Requests.

New-PublicFolderDatabaseRepairRequest Output

When you run the **New-PublicFolderDatabaseRepairRequest** cmdlet, the following output is displayed:

- **RequestID** This value specifies a unique identifier for the repair request.
- **Database** This value specifies the public folder database on which the repair is being made.
- **Server** This value specifies the Mailbox server hosting the public folder database being repaired.

Use the Shell to create a public folder database repair request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the" Public folder database repair request" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to create a public folder database repair request.

This example detects and repairs replication issues in public folder database PFDB01.

```
New-PublicFolderDatabaseRepairRequest -Database PFDB01 -CorruptionType ReplState
```

This example only detects and reports replication issues in public folder database PFDB02. No issues are repaired.

```
New-PublicFolderDatabaseRepairRequest -Database PFDB02 -CorruptionType ReplState
```

For detailed syntax and parameter information, see New-PublicFolderDatabaseRepairRequest.

1.8.3.18 Managing Meeting Items

Managing Meeting Items

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-17*

Enable or Disable the Automatic Processing of Meeting Messages

Enable or Disable the Automatic Removal of Older Versions of Meeting Messages

1.8.3.18.1 Enable or Disable the Automatic Processing of Meeting Messages

Enable or Disable the Automatic Processing of Meeting Messages

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable the Calendar Attendant function to process meeting messages for a user. A *meeting message* is any meeting item used in the meeting workflow to update calendar items.

By default, the Calendar Attendant performs the following actions on a user's calendar:

- Updates the time of the meeting on an attendee's calendar after receiving an update from the organizer.
- Updates the attendee's response on the organizer's calendar after receiving a response from the attendee.

For more information about how to disable the automatic removal of older meeting messages on a per-user basis in Microsoft Office Outlook Web App, see "Automatic Processing" in Calendar Tab.

Looking for other management tasks related to meeting items? Check out Managing Meeting Items.

Use the Shell to enable automatic processing of meeting messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar processing" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to enable automatic processing of meeting messages.

This example enables the automatic processing of meeting messages for Ellen Adam's mailbox.

```
Set-CalendarProcessing -Identity "Ellen Adams" -AutomateProcessing AutoUpdate
```

For detailed syntax and parameter information, see Set-CalendarProcessing.

Use the Shell to disable automatic processing of meeting messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar processing" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to disable automatic processing of meeting messages.

This example disables the automatic processing of meeting messages for Kevin's mailbox.

```
Set-CalendarProcessing -Identity "Kevin" -AutomateProcessing:None
```

For detailed syntax and parameter information, see Set-CalendarProcessing.

1.8.3.18.2 Enable or Disable the Automatic Removal of Older Versions of Meeting Messages

Enable or Disable the Automatic Removal of Older Versions of Meeting Messages

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

By default, the Calendar Attendant removes older versions of meeting messages (such as meeting requests, cancellations, and updates) delivered to recipients' Inboxes. Removing these items helps reduce the number of meeting messages that users have to manage.

When the Calendar Attendant performs this task, the following actions occur:

- Out-of-date meeting updates are deleted.
- Redundant meeting responses that don't contain text are deleted.
- Meeting messages that contain text (for example, responses with additional text or attachments) are preserved.

For example, Tony sends a meeting request to Ayla, and Ayla tentatively accepts the meeting. Tony receives a meeting message stating that Ayla has tentatively accepted the meeting. Ayla later declines the meeting. Tony receives the newer e-mail message stating that Ayla has declined the meeting. The Calendar Attendant moves the older, tentative meeting message into Tony's Deleted Items folder.

For more information about how to disable the automatic removal of older meeting messages on a per-user basis in Microsoft Office Outlook Web App, see "Automatic

Processing" in Calendar Tab.

Looking for other management tasks related to meeting items? Check out Managing Meeting Items.

Use the Shell to disable automatic removal of meeting messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar processing" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to disable automatic removal of meeting messages.

This example disables the process by setting the *RemoveOldMeetingMessages* parameter to `false` for Ayla Kol's mailbox.

```
Set-CalendarProcessing -Identity "Ayla Kol" -RemoveOldMeetingMessages $false
```

For detailed syntax and parameter information, see Set-CalendarProcessing.

Use the Shell to enable automatic removal of meeting messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar processing" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to enable automatic removal of meeting messages.

This example enables the process by setting the *RemoveOldMeetingMessages* parameter to `true` for Tony Smith's mailbox.

```
Set-CalendarProcessing -Identity "Tony Smith" -RemoveOldMeetingMessages $true
```

For detailed syntax and parameter information, see Set-CalendarProcessing.

1.8.3.19 Managing Move Requests

Managing Move Requests

Exchange Server 2010 > Mailbox > Managing Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-05-16*

Create a Local Move Request

Complete or Resume a Move Request

Configure Move Request Properties

Move Mailboxes by Using the MoveMailbox.ps1 Script in the Shell

Clear or Remove Move Requests

Suspend Move Requests

View Move Request Properties

Test Mailbox Replication Service Health

Throttling the Mailbox Replication Service

Managing Remote Move Requests

Troubleshooting Mailbox Moves

1.8.3.19.1 Create a Local Move Request

Create a Local Move Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A move request is the process of moving a mailbox from one mailbox database to another. A local move request is a mailbox move that occurs within a single forest. For more information, see Understanding Move Requests.

In Microsoft Exchange Server 2010 Service Pack 1 (SP1), mailboxes and personal archive mailboxes can reside on separate databases. Using the move request functionality, you can move the primary mailbox and the associated archive to the same database or to separate ones. For more information about personal archive mailboxes, see Understanding Personal Archives.

Note:
If you're moving a mailbox from an Exchange 2003 database, the mailbox move will be offline.

Note:
To view all move requests in a multiple-domain environment in the Exchange Management Console, the recipient scope needs to be modified to view the entire forest. For more information, see Change the Recipient Scope.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

What Do You Want to Do?

- Use the EMC to create a local move request
- Use the Shell to create a local move request

Use the EMC to create a local move

request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select one or more mailboxes that you want to move.
3. In the action pane, click **New Local Move Request**.

4. On the **Introduction** page, configure the following settings:
   - **A new move request will be placed for the following mailboxes** This box displays the mailboxes that you selected in the result pane. If you want to add or remove mailboxes, click **Cancel**, and then make the changes in the result pane.
   - **Target mailbox database** Click **Browse** to open the **Select Mailbox Database** dialog box. Use this dialog box to select the mailbox database to which you want to move the mailboxes. Click **OK** to return to the wizard.

     If the mailbox has an archive associated with it, the following options are displayed:

     Move only the user mailbox Click this button if you want to move only the user's primary mailbox to the new database. This is selected by default.

     Move only the archive mailbox Click this button if you want to move only the user's archive mailbox to the new database.

     Move both the mailbox and the archive Click this button if you want to move both the user's primary mailbox and the associated archive mailbox to the new database.

5. On the **Move Settings** page, specify how you want to manage corrupted messages:
   - **Skip the mailbox** Click this button to specify that mailboxes containing corrupted messages won't be moved. We recommend selecting this option.
   - **Skip the corrupted messages** Click this button to move the mailbox, but not to move any corrupted messages. If you select this option, you need to set the **Maximum number of messages to skip**. We recommend selecting this option only if the move request failed in a previous attempt.
   - **Maximum number of messages to skip** If you select **Skip the corrupted messages**, use this list to specify a number from **1** through **50**.

     Note:

     If you specify a value higher than 50, the task will fail, and you need to use the Shell to create the move request. For details, see Move a user's primary mailbox and allow a large bad item limit later in this topic.

   - **Suspend this move when it is ready to complete** Select this check box to suspend the move request before the completion stage begins. You can resume the move request at a later time. For details, see Complete or Resume a Move Request.

   Note:

   You can use this feature only for online mailbox moves and when moving mailboxes from Exchange 2007 and Exchange 2010 mailbox databases. You can't use this feature for offline moves or when moving from Exchange 2003 mailbox databases.

6. On the **New Local Move Request** page, review your configuration settings. Click **New** to create the move request. Click **Back** to make changes.

7. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task

successfully.
- A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a local move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

Test whether a mailbox is ready to move

This example uses the *WhatIf* switch to test whether Tony Smith's mailbox is ready to move to the new database DB01 and if there are any errors within the command. When you use the *WhatIf* switch, the system performs checks on the mailbox. If the mailbox isn't ready to move, you receive an error.

```
New-MoveRequest -Identity 'tony@alpineskihouse.com' -TargetDatabase DB01 -WhatIf
```

For detailed syntax and parameter information, see New-MoveRequest.

Create a local move request

This example moves Tony Smith's mailbox to the new database DB01. If Tony's mailbox has an associated archive, it's also moved to the same database.

```
New-MoveRequest -Identity 'tony@alpineskihouse.com' -TargetDatabase DB01
```

For detailed syntax and parameter information, see New-MoveRequest.

Create a batch move request

This example creates a batch move request for all mailboxes on the database DB01 and moves them to the database DB02 with the *BatchName* parameter value DB01toDB02.

```
Get-Mailbox -Database DB01 | New-MoveRequest -TargetDatabase DB02 -BatchName "DB0
```

For detailed syntax and parameter information, see Get-Mailbox and New-MoveRequest.

Create a move request that suspends before completion

This example creates a move request that's suspended after the initial content is moved, but before the mailbox is locked down and switched over to the new location.

```
New-MoveRequest -Identity 'tony@alpineskihouse.com' -TargetDatabase DB01 -Suspend
```

For detailed syntax and parameter information, see New-MoveRequest.

Create a move request processed by a specific server

This example creates a move request processed by the Client Access server CAS1.contoso.com, which has the Microsoft Exchange Mailbox Replication service installed.

```
New-MoveRequest -Identity 'tony@alpineskihouse.com' -TargetDatabase DB01 -MRSServ
```

For detailed syntax and parameter information, see New-MoveRequest.

Create a suspended move requests

This example creates a batch move request that's suspended for all mailboxes on database DB01. Run this command if you want to create the move request during business hours, and then resume at a later time, when e-mail traffic is low.

```
Get-Mailbox -Database DB01 | New-MoveRequest -TargetDatabase DB02 -BatchName "26A
```

For detailed syntax and parameter information, see Get-Mailbox and New-MoveRequest.

Move only a user's primary mailbox

This example moves only Tony Smith's primary mailbox to DB01. The archive isn't moved.

```
New-MoveRequest -Identity 'tony@alpineskihouse.com' -PrimaryOnly -TargetDatabase
```

For detailed syntax and parameter information, see New-MoveRequest.

Move only an archive mailbox

This example moves only Tony Smith's archive mailbox to DB03. The primary mailbox isn't moved.

```
New-MoveRequest -Identity 'tony@alpineskihouse.com' -ArchiveOnly -ArchiveTargetDa
```

For detailed syntax and parameter information, see New-MoveRequest.

Move a user's primary mailbox and archive mailbox to separate databases

This example moves Ayla's primary mailbox and archive mailbox to separate databases. The primary database is moved to DB01, and the archive is moved to DB03.

```
New-MoveRequest -Identity 'ayla@humongousinsurance.com' -TargetDatabase DB01 -Arc
```

For detailed syntax and parameter information, see New-MoveRequest.

Move a user's primary mailbox and allow a large bad item limit

This example moves Kweku's primary mailbox to mailbox database DB01 and sets the bad item limit to 100. To set a large bad item limit, you must use the *AcceptLargeDataLoss* parameter.

```
New-MoveRequest -Identity 'Kweku' -PrimaryOnly -TargetDatabase "DB01" -BadItemLim
```

For detailed syntax and parameter information, see New-MoveRequest.

Other Tasks

After you move the mailboxes, you may also want to:

- View Move Request Properties
- Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010
- Complete or Resume a Move Request

1.8.3.19.2 Complete or Resume a Move Request

Complete or Resume a Move Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can complete a move request that failed or was suspended.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Prerequisites

Before you can complete a move request, it must have a move request status of **Suspended**, **Automatically suspended**, or **Failed**. For more information, see Suspend Move Requests.

Use the EMC to complete a move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Move Requests**.
2. In the result pane, select one or more mailboxes that have a move request status of **Failed**, **Suspended**, or **Automatically suspended**.
3. In the action pane, click **Complete Move Request**.
4. In **Complete Move Request**, confirm that you want to complete the move request by clicking **Yes**.

Use the Shell to complete a move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

This example completes the move request for Tony Smith's mailbox.

```
Resume-MoveRequest -Identity "Tony@contoso.com"
```

This example resumes any failed move requests.

```
Get-MoveRequest -MoveStatus Failed | Resume-MoveRequest
```

This example resumes any move requests that have the suspend comment "Resume after 10 P.M."

```
Get-MoveRequest -MoveStatus Suspended | Get-MoveRequestStatistics |Where {$_.Mess
```

For detailed syntax and parameter information, see the following topics:

- Resume-MoveRequest
- Get-MoveRequest
- Get-MoveRequestStatistics

1.8.3.19.3 Configure Move Request Properties

Configure Move Request Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

After you create a move request, the request could fail due to bad item limit errors or rule

limit errors. If the move request fails because of those errors, you can edit the move request settings to increase the bad item limit or to ignore rule limit errors. After the move request is initiated, you can edit it until it has a status of Completed.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Use the Shell to change the bad item limit

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to change the bad item limit.

This example changes the move request for Ayla's mailbox to accept up to five corrupted mailbox items.

```
Set-MoveRequest -Identity "Ayla" -BadItemLimit 5
```

For detailed syntax and parameter information, see Set-MoveRequest.

Use the Shell to ignore rule limit errors

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to ignore rule limit errors.

This example ignores rule limit errors by not moving any rules associated with Tony's mailbox.

```
Set-MoveRequest -Identity "Tony" -IgnoreRuleLimitErrors $true
```

For detailed syntax and parameter information, see Set-MoveRequest.

1.8.3.19.4 Move Mailboxes by Using the MoveMailbox.ps1 Script in the Shell

Move Mailboxes by Using the MoveMailbox.ps1 Script in the Shell

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Similar to the **Move-Mailbox** cmdlet in Microsoft Exchange Server 2007, the MoveMailbox.ps1 script provides a synchronous management experience for moving mailboxes. By default, scripts are installed at C:\Program Files\Microsoft\Exchange Server

\V14\Scripts.

Note:
You can use this script for local moves only. You can't use this script for remote (cross-forest) moves. For information about remote mailbox moves, see Prepare Mailboxes for Cross-Forest Move Requests.

MoveMailbox.ps1 performs the following tasks:

1. Creates a local move request.
2. Waits for the mailbox move to complete.
3. Clears the move request after it completes.

MoveMailbox.ps1 includes two parameter sets. The first parameter set moves a single mailbox, or you can pipeline mailboxes into the command. The second parameter set moves all mailboxes hosted on a specified database, or you can pipeline database objects into the command to move all mailboxes that reside on those mailbox databases.

Note:
The Shell doesn't load scripts automatically. You must precede all scripts with "**.**" For example, to run the MoveMailbox.ps1 script, type `.\MoveMailbox.ps1`.

For more information about using and writing scripts, see Scripting with the Exchange Management Shell.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Using MoveMailbox.ps1 to move specific mailboxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

The following parameter syntax set and table lists the parameters that you can use to move specific mailboxes.

```
MoveMailbox.ps1 -Identity <Object> -DatabaseMap <Hashtable> -TargetDatabase <Obje
```

Parameter	Required	Description
DatabaseMap	Required	The *DatabaseMap* parameter specifies the map between the databases you're moving to and from. Use this parameter if you're using the pipelining method to identify the mailboxes you're moving to. The *DatabaseMap* parameter requires the following: • Use the following syntax: `@{"<SourceDatabase>"="<TargetDatabase>"}` • The *SourceDatabase* name must match the database name as reported by the Get-Mailbox cmdlet. • You can include multiple database maps. Separate multiple maps with a semicolon (;), for example,

		@{"DB1"="DBA";"DB2"="DBB"} **Note:** You can't use this parameter in conjunction with the *TargetDatabase* parameter. If you're pipelining the command, and a user matches the identity in the Get-Mailbox cmdlet but doesn't match the source database in the *DatabaseMap* cmdlet, that user's mailbox will be skipped.
Identity	Required	The *Identity* parameter specifies the identity of the mailbox that you want to move. This parameter accepts the following values: • ADObjectID • Alias • Distinguished name (DN) • *Domain\Account* • GUID • LegacyExchangeDN • SmtpAddress • User principal name (UPN) **Note:** You can pipeline the *Identity* parameter by using the **Get-Mailbox** cmdlet.
TargetDatabase	Required	The *TargetDatabase* parameter specifies the identity of the database that you're moving the mailbox to. This parameter accepts the following values: • GUID • Distinguished name (DN) • *Server\database name* • Database name **Note:** You can't use this parameter in conjunction with the *DatabaseMap* parameter.
AutoSuspend	Optional	The *AutoSuspend* switch specifies whether to suspend the move request before it reaches the status of `CompletionInProgress`. After the move is suspended, it has a status of `AutoSuspended`. If you use this parameter, you must complete the move by using the Resume-MoveRequest cmdlet.
BadItemLimit	Optional	The *BadItemLimit* parameter specifies the number of bad items to skip if the move request encounters corruption in the mailbox. Use the value 0 if you

		don't want to skip bad items. Use the value -1 to skip an unlimited number of bad items. The valid input range for this parameter is from -1 through 2,147,483,647. The default value is 0. We recommend that you keep the default value 0 and only change the *BadItemLimit* parameter value if the move request fails.
DomainController	Optional	The *DomainController* parameter specifies the fully qualified domain name (FQDN) of the domain controller that writes this configuration change to Active Directory.
PollInterval	Optional	The *PollInterval* parameter specifies, in seconds, the amount of time to wait before checking if a move request is completed. For example, if the *PollInterval* is set to 180, the MoveMailbox.ps1 script will check the move requests status every 3 minutes to see if the move has the status of Completed. The default time is 10 seconds.
StartBatchSize	Optional	The *StartBatchSize* parameter specifies how often to start mailbox moves for load balancing purposes. The parameter applies only when moving multiple mailboxes at one time. For example, if this parameter is set to 10 and you're moving 15 mailboxes, the script will invoke the **New-MoveRequest** cmdlet when it sees that 10 mailboxes are being moved to the same target database.

Examples

EXAMPLE 1

This example moves the mailboxes that begin with "ay". If these mailboxes reside on the mailbox database DB1, this example uses the *DatabaseMap* parameter to move them to mailbox database DBA. If these mailboxes reside on DB2, this example moves them to mailbox database DBB.

```
Get-Mailbox ay* | .\MoveMailbox.ps1 -DatabaseMap @{"DB1"="DBA";"DB2"="DBB"}
```

EXAMPLE 2

This example moves Tony Smith's mailbox to DB2.

```
.\MoveMailbox.ps1 -Identity "Tony@Contoso.com" -TargetDatabase "DB2"
```

Using MoveMailbox.ps1 to move mailboxes homed on a specific database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

The following parameter syntax set and table lists the parameters that will move mailboxes based on the database.

```
MoveMailbox.ps1 -MailboxDatabase <Object> [-DatabaseMap <Hashtable>] [-TargetData
```

Parameter	Required	Description
MailboxDatabase	Required	The *MailboxDatabase* parameter specifies the mailbox database from which you're moving mailboxes. This parameter accepts the following values: • GUID • Distinguished name (DN) • *Server\database name* • Database name **Note:** You can't use this parameter in conjunction with the *DatabaseMap* parameter.
AutoSuspend	Optional	The *AutoSuspend* switch specifies whether to suspend the move request before it reaches the status of `CompletionInProgress`. After the move is suspended, it has a status of `AutoSuspended`. If you use this parameter, you must complete the move by using the Resume-MoveRequest cmdlet.
BadItemLimit	Optional	The *BadItemLimit* parameter specifies the number of bad items to skip if the move request encounters corruption in the mailbox. Use the value 0 if you don't want to skip bad items. Use the value -1 to skip an unlimited number of bad items. The valid input range for this parameter is -1 to `2,147,483,647`. The default value is 0. We recommend that you keep the default value 0 and only change the *BadItemLimit* parameter value if the move request fails.
DatabaseMap	Optional	The *DatabaseMap* parameter specifies the map between the databases you're moving to and from. Use this parameter if you're using the pipelining method to identify the mailboxes you're moving to. The *DatabaseMap* parameter requires the following: • Use the following syntax: `@{"<SourceDatabase>"="<TargetDatabase>"}` • The *SourceDatabase* name must match the database name as reported by the

		Get-Mailbox cmdlet. • You can include multiple database maps. Separate multiple maps with a semicolon (;), for example, @{"DB1"="DBA";"DB2"="DBB"} **Note:** You can't use this parameter in conjunction with the *TargetDatabase* parameter. If you're pipelining the command, and a user matches the identity in the Get-Mailbox cmdlet but doesn't match the source database in the *DatabaseMap* cmdlet, that user's mailbox will be skipped.
DomainController	Optional	The *DomainController* parameter specifies the fully qualified domain name (FQDN) of the domain controller that writes this configuration change to Active Directory.
PollInterval	Optional	The *PollInterval* parameter specifies, in seconds, the amount of time to wait before checking if a move request is completed. For example, if the *PollInterval* is set to 180, the MoveMailbox.ps1 script will check the move requests status every 3 minutes to see if the move has the status of Completed. The default time is 10 seconds.
StartBatchSize	Optional	The *StartBatchSize* parameter specifies how often to start mailbox moves for load balancing purposes. The parameter applies only when moving multiple mailboxes at one time. For example, if this parameter is set to 10 and you're moving 15 mailboxes, the script will invoke the **New-MoveRequest** cmdlet when it sees that 10 mailboxes are being moved to the same target database.
TargetDatabase	Optional	The *TargetDatabase* parameter specifies the identity of the database that you're moving the mailbox to. This parameter accepts the following values: • GUID • Distinguished name (DN) • *Server\database name* • Database name **Note:** You can't use this parameter in conjunction with the *DatabaseMap*

		parameter.

Examples

EXAMPLE 1

This example moves all mailboxes that reside on mailbox database DB1 to database DB2.

```
.\MoveMailbox.ps1 -MailboxDatabase DB1 -TargetDatabase DB2
```

EXAMPLE 2

This example uses the **Get-MailboxDatabase** cmdlet to retrieve all mailbox database objects whose mailbox database begins with "DB1", and then pipelines the result to the MoveMailbox.ps1 script.

```
Get-MailboxDatabase DB1* | .\MoveMailbox.ps1 -DatabaseMap @{"DB10"=DBA;"DB11"="DB
```


1.8.3.19.5 Clear or Remove Move Requests

Clear or Remove Move Requests

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When a move request reaches a status of **Completed** or **Completed with warning**, you must clear the move request to remove the **InTransit** flag from the mailbox. You won't be able to move the mailbox again until you clear the previous move request. To learn more about the **Completed with warning** status, see Troubleshooting Mailbox Moves.

In addition, you can remove a move request that's in progress. When you remove a move request in progress, mailbox replication stops, and the replica is deleted from the target database. If you remove the move request and later decide to move the mailbox, you must start the move request process at the beginning.

Note:
To view all move requests in a multiple-domain environment in the Exchange Management Console, the recipient scope needs to be modified to view the entire forest. For more information, see Change the Recipient Scope.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Use the EMC to clear a move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Move Request**.
2. In the result pane, select a recipient that has a **Move Request Status** of **Completed** or **Completed with warning**.

   Note:
   You can select multiple recipients in the result pane.

3. In the action pane, click **Clear Move Request**.
4. A warning message appears confirming that you want to clear the move request. Click **Yes**.

Use the EMC to remove a move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Move Request**.
2. In the result pane, select a recipient that has a **Move Request Status** of **Automatically Suspended**, **In Progress**, **Queued**, or **Completing**.

   Note:
   You can select multiple recipients in the result pane.

3. In the action pane, click **Remove Move Request**.
4. A warning appears confirming that you want to remove the move request. Click **Yes**.

Use the Shell to clear or remove a move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

This example clears the move request from all mailboxes that have a status of Completed.

```
Get-MoveRequest -MoveStatus Completed | Remove-MoveRequest
```

This example removes the move request for Ayla's mailbox.

```
Remove-MoveRequest -Identity 'Ayla@humongousinsurance.com'
```

For detailed syntax and parameter information, see Remove-MoveRequest or Get-MoveRequest.

Other Tasks

After you clear the move request, you can no longer view move request statistics for those mailboxes. For information about how to view the move history for a mailbox, see View Move Request Properties.

1.8.3.19.6 Suspend Move Requests

Suspend Move Requests

Mailbox > Managing Mailbox Servers > Managing Move Requests >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the **Suspend-MoveRequest** cmdlet to suspend a move request any time after the move request is created, but before it reaches the status of CompletionInProgress, Completing, or Completed. You can also automatically suspend a move request by using the **New-MoveRequest** cmdlet with the *SuspendWhenReadyToComplete* parameter.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Use the Shell to suspend a move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to suspend a move request.

This example suspends a move request for Tony Smith's mailbox and includes the suspend comment "Move suspended per user request. Do not resume until Sunday."

```
Suspend-MoveRequest -Identity 'Tony@humongousinsurance.com' -SuspendComment "Move
```

This example suspends all move requests that have the target database DB02 and includes the suspend comment "Pending final approval."

```
Get-MoveRequest -TargetDatabase DB02 | Suspend-MoveRequest -SuspendComment "Pendi
```

For detailed syntax and parameter information, see Suspend-MoveRequest and Get-MoveRequest.

Use the Shell to automatically suspend a move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

This example automatically suspends a move request when the request reaches a status of ReadyToComplete.

```
New-MoveRequest -Identity Ayla@alpineskihouse.com -TargetDatabase DB05 -SuspendWh
```

For detailed syntax and parameter information, see New-MoveRequest.

1.8.3.19.7 View Move Request Properties

View Move Request Properties

Mailbox > Managing Mailbox Servers > Managing Move Requests >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

A move request is the process of moving a mailbox from one mailbox database to another. After starting the move request process, you must wait until the Microsoft Exchange Mailbox Replication service replicates the mailbox from the source database to the target database, and the move request status is **Completed** or **Completed with warning**.

During this waiting period, you can view the move request status by using the EMC or the **Get-MoveRequest** cmdlet in the Shell. (For a more detailed report, you can run the **Get-MoveRequestStatistics** cmdlet with the *IncludeReport* parameter.)

After the move request is complete, you can view the move history of the completed move request by running the **Get-MailboxStatistics** cmdlet with the *IncludeMoveHistory*

parameter. You can also get the complete move request report by running the **Get-MailboxStatistics** cmdlet with the *IncludeMoveReport* parameter. Use this information to troubleshoot any errors or failures that may have occurred during the move.

Note:
Move requests won't display in the result pane of the **Move Request** node until they're in the **Queued** status.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

What Do You Want to Do?

- Use the EMC to view the status of an in-progress or completed move request
- Use the Shell to view the status of an in-progress move request
- Use the Shell to view a completed move request report

Use the EMC to view the status of an in-progress or completed move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Move Request**.

   Note:
   If you have multiple forests in the EMC, you need to navigate to the target forest's **Move Request** node.

2. In the result pane, select a move request.
3. In the action pane, click **Properties**.
4. Use the **General** tab to view the following information about the move request:
   - **Move request status** This read-only field displays one of the following move request statuses:

     Automatically Suspended This status specifies that the move is ready to complete, but that the move request was suspended when it was created. This can be done either by selecting the **Suspend this move when it is ready to complete** check box in the EMC or by specifying the *SuspendWhenReadyToComplete* switch in the Shell. You can resume the move request by using the **Resume-MoveRequest** cmdlet or by using the **Complete Move Request** action in the action pane. For more information, see Complete or Resume a Move Request.

     Completed This status specifies that the move request was completed successfully without any warnings.

     Completed with warning This status specifies that the move request completed, but that there were warnings. For more information, see Troubleshooting Mailbox Moves.

     Completion in progress This status specifies that the mailbox is in its final stages of being moved. If the move was an online move, at this point, the user's mailbox may become unavailable.

     Failed This status specifies that the move request has failed. To view the message that describes why the move failed, click **View** located next to the **Failed Message** field.

     In progress This status specifies that the move is still in progress. If this is an online mailbox move, the user can still

access the mailbox. If this is an offline mailbox move, the user's mailbox is unavailable.
Queued This status specifies that the move has been queued and is waiting to be picked up by the Microsoft Exchange Mailbox Replication service.
Ready to complete This status specifies that the move is ready to complete. You need to manually complete the move. For more information, see Complete or Resume a Move Request.
Suspended This status specifies that the move was suspended by using the **Suspend-MoveRequest** cmdlet. You can resume the move request by using the **Resume-MoveRequest** cmdlet or by using the **Complete Move Request** action in the action pane. For more information, see Complete or Resume a Move Request.

- **Percent complete** This field displays the completion percentage for the move request.
- **Duration** This field displays how long it took the move to complete.
- **Mailbox size** This field displays the size of the mailbox being moved.
- **Number of corrupted items** This field displays the number of corrupted items detected during the move.
- **Source database** This field displays the database from which the mailbox is being moved.
- **Target database** This field displays the database to which the mailbox is being moved.
- **Last updated time** This field displays the date and time at which the last change was made to the request. The change could've been made by an administrator or by the Microsoft Exchange Mailbox Replication service (MRS).
- **Suspend this move when it is ready to complete** If the move has the move request status of **In Progress** or **Queued**, you can select this check box, and then click **Apply** to suspend the move when it's ready to complete. You can then manually complete the move request at a later time. For more information, see Complete or Resume a Move Request. If you select this check box, a **Suspended Comment** appears on the **Details** tab.

5. Use the **Details** tab to view the following information about the move request:
   - **Remote host name** If you're moving the mailbox across Exchange forests, this field displays the fully qualified domain name (FQDN) of the remote host. If this is a local move, this field is blank.
   - **Move request server name** This field displays the FQDN of the Client Access server that processed the move request.
   - **Source version** This field displays the version of Exchange on which the source database resides.
   - **Target version** This field displays the version of Exchange on which the target database resides.
   - **Move request queued time** This field displays the time the move request was queued. The time may not be the same as the time the move request was created.
   - **Queued duration** This field displays the amount of time the move request remained in the **Queued** status.
   - **Move request start time** This field displays the time at which the move request began.
   - **Move request completion time** This field displays the time at which the move request completed. If the move request isn't completed, this field is blank.
   - **Suspended time** This field displays the time at which the request was suspended. If the request wasn't suspended, this field is blank.

- **Suspended comment** This field displays the comment added by the administrator who suspended the move request. By default, if the move request was set to be suspended before completion, the comment includes the following text:

  Informational: The move request for mailbox <mailbox GUID> is ready to complete and has been automatically suspended because the SuspendWhenReadyToComplete parameter is set to $true

6. Use the **Log** tab to view the move request log. Click **View** to display the log. The move request log can be used for debugging purposes if a move request fails or is having transient issues. You can press Ctrl+C to copy the contents of the log file.

Use the Shell to view the status of an in-progress move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

This example retrieves the status of the ongoing move for Tony Smith's mailbox (tony@contoso.com).

```
Get-MoveRequest -Identity 'tony@contoso.com'
```

This example retrieves the status of ongoing moves for user mailboxes in the Marketing department.

```
Get-User -Filter {Department -like 'Marketing'} | Get-MoveRequest
```

This example retrieves the status of ongoing mailbox moves to the target database DB05.

```
Get-MoveRequest -MoveStatus InProgress -TargetDatabase DB05
```

This example retrieves the status for completed move requests in the FromDB01toDB02 batch that had warnings.

```
Get-MoveRequest -BatchName "FromDB01ToDB02" -MoveStatus CompletedWithWarning
```

For detailed syntax and parameter information, see Get-MoveRequest or Get-User.

Use the Shell to view a completed move request report

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

This example uses the *IncludeMoveHistory* parameter to retrieve the move history of a completed move request for Tony Smith's mailbox.

```
Get-MailboxStatistics -Identity tony@contoso.com -IncludeMoveHistory
```

This example uses the *IncludeMoveReport* parameter to retrieve a detailed move report for a failed move request of Ayla Kol's mailbox.

```
Get-MailboxStatistics -Identity ayla@contoso.com -IncludeMoveReport
```

For detailed syntax and parameter information, see Get-MailboxStatistics.

Other Tasks

After the move is complete, you may also want to clear the move requests from the result pane of the EMC. For detailed instructions, see Clear or Remove Move Requests.

If the move failed, you may also want to troubleshoot the move to determine the cause of the failure. For more information, see Troubleshooting Mailbox Moves.

1.8.3.19.8 Test Mailbox Replication Service Health

Test Mailbox Replication Service Health

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Microsoft Exchange Mailbox Replication service (MRS) runs on Client Access servers. You can test MRS health to make sure that MRS is running and that it responds to a remote procedure call (RPC) ping check. Use this procedure to troubleshoot problems that occur when moving mailboxes.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Use the Shell to test MRS health

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to test MRS health.

This example tests the health of MRS on all Client Access servers.

```
Get-ClientAccessServer | Test-MRSHealth
```

This example tests the health of MRS on the Client Access server CAS01.

```
Test-MRSHealth -Identity CAS01
```

This example tests the health of MRS on the Client Access server CAS02 and also includes monitoring events and performance counters in the results. The results are then exported to the .xml file CAS02_MRSHealth.xml.

```
Test-MRSHealth -Identity CAS02 -MonitoringContext $true | Export-CliXml "C:\CAS02
```

For detailed syntax and parameter information, see Get-ClientAccessServer or Test-MRSHealth.

Throttling the Mailbox Replication Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-13*

The Mailbox Replication Service (MRS), which resides on all Microsoft Exchange Server 2010 Client Access servers, is the service responsible for moving mailboxes, importing and exporting .pst files, and restoring disabled and soft-deleted mailboxes.

Because MRS performs several tasks, you can throttle it to maintain the overall health of your Exchange organization. Although each instance of MRS has its own configuration settings, each instance of MRS is aware of the tasks that other instances of MRS are processing. MRS throttling is controlled by the configuration file MSExchangeMailboxReplication.exe.config. By default, this configuration file is located on all Client Access servers in the same folder where Exchange is installed: *<Exchange Installation Path>*\Program Files\Microsoft\Exchange Server\V14\Bin\MSExchangeMailboxReplication.exe.config.

Note:

When you open the configuration file, you can find the minimum, maximum, and default values for the configuration settings in the section titled **! Mailbox Replication Service configuration**.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Throttle MRS

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Text editor" entry in the Client Access Permissions topic.

1. Navigate to *<Exchange Installation Path>*\Program Files\Microsoft\Exchange Server\V14\Bin**.**
2. Open the MSExchangeMailboxReplication.exe.config file using a text editor such as Notepad.
3. Navigate to the **MRSConfiguration** section. You can edit the following properties:
   - **MaxRetries** This property specifies the maximum number of times MRS will attempt to perform a task after encountering a transient failure. You can specify a value from 0 through 1000. The default value is 60.
   - **MaxCleanupRetries** This property specifies the number of times that MRS should attempt to clean up a task. If the maximum number of attempts is reached, the task fails. You can specify a value from 0 through 100. The default value is 5.
   - **MaxStallRetryPeriod** This property specifies the maximum duration for which MRS pauses while waiting for the Microsoft Exchange Information Store service to bring the target mailbox database into compliance with its configured data redundancy constraints. If the Microsoft Exchange Information Store service reports that the mailbox database is unhealthy, MRS will pause. If the maximum time is reached, the task fails. You can specify a value from 00:00:10 (10 seconds) through 05:00:00 (5 hours). The default value is 00:15:00 (15 minutes).
   - **RetryDelay** This property specifies the amount of time MRS will wait before it attempts to perform a task again after a transient failure. You can specify a value from 00:00:10 (10 seconds) through 00:30:00 (30 minutes). The default value is 00:00:30 (30 seconds).

- **MaxMoveHistoryLength** This property specifies the maximum number of move histories to maintain in the mailbox. You can specify a value from 0 through 100. The default value is 2 move histories per mailbox.
- **MaxActiveMovesPerSourceMDB** This property specifies the total number of tasks MRS can perform that involve the mailbox database as a data source. Types of tasks include moving mailboxes located on the database, exporting mailbox data from mailboxes located on the database, and restoring mailbox data from the database. You can specify a value from 0 through 100. The default value is 5 concurrent tasks.
- **MaxActiveMovesPerTargetMDB** This property specifies the total number of tasks MRS can perform that involve the mailbox database as a data target. Types of tasks include moving mailboxes to the database, importing mailbox data into a mailbox located on the database, and restoring mailbox data to a mailbox located on the database. You can specify a value from 0 through 100. The default value is 2 concurrent tasks.
- **MaxActiveMovesPerSourceServer** This property specifies the total number of tasks MRS can perform that include the server as a data source. You can specify a value from 0 through 1000. The default value is 50 concurrent moves.
- **MaxActiveMovesPerTargetServer** This property specifies the total number of tasks MRS can perform that involve the server as a data target. You can specify a value from 0 through 1000. The default value is 5 concurrent moves.
- **MaxTotalMovesPerMRS** This property specifies the total number of tasks that a single instance of MRS can perform at a time. You can specify a value from 0 through 1000. The default value is 100 concurrent moves.
- **FullScanMoveJobsPollingPeriod** This property specifies how often each instance of MRS scans for new tasks. You can specify a value from 00:03:00 (3 minutes) through 1.00:00:00 (1 day). The default value is 00:10:00 (10 minutes).

In addition to the preceding properties, you can also configure the following properties. However, you should only change these settings when directed by support personnel.

- **MinimumTimeBeforePickingJobsFromSameDatabase**
- **ServerCountsNotOlderThan**
- **MRSAbandonedMoveJobDetectionTime**
- **BackoffIntervalForProxyConnectionLimitReached**
- **DataGuaranteeCheckPeriod**
- **DataGuaranteeTimeout**
- **DataGuaranteeLogRollDelay**
- **MailboxLockoutTimeout**
- **MailboxLockoutRetryInterval**
- **EnableDataGuaranteeCheck**
- **DisableMrsProxyCompression**
- **DisableMrsProxyBuffering**
- **MinBatchSize**
- **MinBatchSizeKB**

4. Make sure any changes you make are also applied to the MSExchangeMailboxReplication.exe.config file on all other Client Access servers.

1.8.3.19.10 Managing Remote Move Requests

Managing Remote Move Requests

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-02*

Create a Remote Move Request That has Exchange 2010 in Both Forests

Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010

Prepare Mailboxes for Cross-Forest Move Requests

Prepare Mailboxes for Cross-Forest Moves Using the Prepare-MoveRequest.ps1 script in the Shell

Prepare Mailboxes for Cross-Forest Moves Using Sample Code

Start the MRSProxy Service on a Remote Client Access Server

1.8.3.19.10.1 Create a Remote Move Request That has Exchange 2010 in Both Forests

Create a Remote Move Request That has Exchange 2010 in Both Forests

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Remote mailbox moves are also known as cross-forest mailbox moves. Microsoft Exchange Server 2010 supports two types of remote mailbox moves:

- **Remote mailbox moves that have Exchange 2010 in both forests** In this scenario, one forest is an Exchange 2010 forest, and the other forest has at least one Exchange 2010 Client Access server. You can use the Exchange Management Console (EMC) or the Exchange Management Shell to perform these mailbox moves.
- **Remote mailbox moves with a legacy Exchange forest** In this scenario, one forest contains Exchange 2010, and the other forest contains Exchange Server 2003 Service Pack 2 (SP2), Exchange Server 2007 SP3, or a combination of both. No Exchange 2010 Client Access server is installed in the legacy forest. You can't use the EMC to perform these mailbox moves. You must use the Shell. For more information, see Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010.

When you move Exchange 2003 mailboxes, the mailbox move is offline. During the move, the users won't be able to access their mailboxes. When you move Exchange 2007 SP2 mailboxes or Exchange 2010 mailboxes, the move is online, and the users can access their mailboxes during the move.

While performing remote mailbox moves, the Microsoft Exchange Mailbox Replication service (MRS) maintains the Send As and Receive As permissions. MRS maps the trustee to the matching user in the destination forest. This functionality relies on the destination

forest having all recipient objects being represented and having their corresponding **msExchMailboxGUID** attributes stamped.

Important:
Maintaining permissions may not be possible in split permission deployments. This is because in split permission deployments the **ExchangeTrustedSubsystem** group attribute isn't included in the Exchange Windows Permissions security group.

MRS also uses the **msExchMailboxGUID** attribute to attempt to maintain mailbox and mailbox folder permissions. MRS maps the permissions to point to the matching user in the destination forest. The security identifiers (SIDs) in the access control entries (ACEs) are replaced. If a SID isn't mapped, the permissions aren't maintained.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Prerequisites

For the complete list of prerequisites to move mailboxes across forests, see Prepare Mailboxes for Cross-Forest Move Requests.

What Do You Want to Do?

- Use the EMC to create a remote move request
- Use the Shell to create a remote move request

Use the EMC to create a remote move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

If the source forest is an Exchange 2007 or Exchange 2003 forest, the administrator performing the move must have the following remote credentials on the Exchange 2007 server:

- Exchange Server Administrator role
- Exchange Recipient Administrator role

Important:
You can't move mailboxes by using the EMC if the source forest doesn't have at least one Exchange 2010 Client Access server installed. Instead, you must use the Shell to perform the task. For more information, see Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox** of the remote forest.

   Note:
   All remote moves need to be initiated from the target forest.

2. In the result pane, select one or more mailboxes that you want to move.
3. In the action pane, click **New Remote Move Request**.
4. On the **Introduction** page, view the mailboxes that you selected in the result pane. If you want to remove or add recipients, click **Cancel**, and then make the changes in the result pane.

   Note:

The option to select a target database from the EMC isn't available. A target database is automatically selected. For more information about how database automatic selection is determined, see Understanding Move Requests.

5. On the **Connection Configurations** page, view or specify the following settings:
   - **Source Forest** This read-only field displays the source forest on which the mailboxes that you're moving reside.
   - **Target Forest** Select the target forest from the list. This field is populated with the forests that have been added to the EMC. If this field is blank, see View Local Forest Properties for information about how to add forests.
   - **FQDN of the Microsoft Exchange Mailbox Replication Service proxy server in the source forest** Type the fully qualified domain name (FQDN) for the server on which the MRS proxy resides. This is a Client Access server in the remote forest, for example, CAS01.contoso.com.
   - **Use the following source forest's credential** To move mailboxes across forests, you must supply the credentials of a recipient administrator who has permission to move mailboxes from the source forest:
     User Name Type the domain name and password of a recipient administrator who has permission to move mailboxes from the source forest.
     Password Type the administrator's password.

6. On the **Move Settings** page, specify the following settings:
   - **Target Delivery Domain** Type the FQDN of the external e-mail address created in the source forest for the mail-enabled user when the move request is complete, for example, the FQDN of the target forest. Mail-enabled users must have a proxy address that has this FQDN as the SMTP domain of the address. At move completion, this proxy address is stamped as the mail-enabled user's external e-mail address in the source forest to ensure that mail flow will return to the new mailbox.
   - **Archive Domain** Type the FQDN of the domain on which the archive will reside.
   - **Target Database** Type the name of the target database in the remote forest.

7. On the **New Remote Move Request** page, review the settings for this remote move request, and then click **New**.

8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a remote move request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

If the source forest is an Exchange 2007 or Exchange 2003 forest, the administrator performing the move must have the following remote credentials on the Exchange 2007 or Exchange 2003 server:

- Exchange Server Administrator role

- Exchange Recipient Administrator role

Test whether a mailbox is ready to move across forests

This example uses the *WhatIf* switch to test whether a mailbox is ready to move across forests and whether any errors are within the command. When you use the *WhatIf* switch, the system performs checks on the mailbox. If the mailbox isn't ready, an error is returned. This command is run on the target forest.

```
New-MoveRequest -Identity 'tony@humongousinsurance.com' -Remote -TargetDatabase D
```

For detailed syntax and parameter information, see New-MoveRequest or Get-Credential.

Move a mailbox from a remote forest

This example moves Tony Smith's mailbox into the forest where the command is run. When the move is completed, the new **ExternalEmailAddress** property in the source forest will be Tony's proxy address with the SMTP domain mail.contoso.com.

```
New-MoveRequest -Identity 'tony@humongousinsurance.com' -Remote -TargetDatabase D
```

For detailed syntax and parameter information, see New-MoveRequest.

Move a mailbox to a remote forest

This example pushes Tony Smith's mailbox to the remote forest. Use this command when you initiate the move from the source forest. When initiating moves from the source forest, you must use the *RemoteTargetDatabase* parameter to specify the database that you're moving the mailbox to. When the move is complete, the new **ExternalEmailAddress** property in the source forest will be Tony's proxy address with the SMTP domain mail.contoso.com.

```
New-MoveRequest -Identity 'tony@humongousinsurance.com' -Remote -RemoteTargetData
```

For detailed syntax and parameter information, see New-MoveRequest.

Create a batch move request

This example creates a batch move request for all mailboxes in the source forest on the database DB01 and moves them to the target database DB02 in the target forest with the *BatchName* parameter value HumongousDB01ToContosoDB02.

Note:

By creating a batch, you can create a tag that identifies the mailboxes being moved. Each mailbox is moved individually when an MRS instance becomes available to perform the move. You can then filter searches using the *BatchName* parameter in the **Get-MoveRequest** and **Get-MoveRequestStatistics** cmdlets.

```
Get-MailUser -Database DB01 | New-MoveRequest -Remote -RemoteHostName 'CAS01.humo
```

For detailed syntax and parameter information, see Get-MailUser or New-MoveRequest.

Create a move request that suspends before completion

This example creates a remote move request for all mailboxes on the target forest that begin with the letter a. The request will be suspended after all the initial content is moved, but before the mailbox is locked down and switched over to the new location.

Note:

You can use the *SuspendWhenReadyToComplete* parameter only for online mailbox moves and when moving mailboxes from Exchange 2007 and Exchange 2010 mailbox databases. You can't use this parameter for offline moves or when moving from Exchange 2003 mailbox databases.

The move request will then need to be resumed by using the **Resume-MoveRequest** cmdlet.

Note:
By creating a batch, you can create a tag that identifies the mailboxes being moved. Each mailbox is moved individually when an MRS instance becomes available to perform the move. You can then filter searches using the *BatchName* parameter in the **Get-MoveRequest** and **Get-MoveRequestStatistics** cmdlets.

```
Get-MailUser -Anr a* | New-MoveRequest -Remote -RemoteHostName 'CAS01.humongousin
```

For detailed syntax and parameter information, see Get-MailUser or New-MoveRequest.

Create a move request processed by a specific server

This example creates a move request processed by the specific Client Access server CAS1.contoso.com, which has MRS installed.

Note:
The *MRSServer* parameter is reserved for debugging purposes. Use this parameter only if directed by support personnel. If you use this parameter and the specified server isn't functional, this move request isn't processed.

```
New-MoveRequest -Identity 'tony@humongousinsurance.com' -RemoteHostName 'CAS01.hu
```

For detailed syntax and parameter information, see New-MoveRequest.

Create a suspended move request

This example creates a batch move request that's suspended for all mailboxes in the target forest where the *CustomAttribute1* parameter is set to Monday. You may want to run this command if you want to create the move request now, and then resume it in the evening, when e-mail traffic is low.

Note:
By creating a batch, you can create a tag that identifies the mailboxes being moved. Each mailbox is moved individually when an MRS instance becomes available to perform the move. You can then filter searches using the *BatchName* parameter in the **Get-MoveRequest** and **Get-MoveRequestStatistics** cmdlets.

```
Get-MailUser -Filter {CustomAttribute1 -eq 'Monday'} | New-MoveRequest -RemoteHos
```

For detailed syntax and parameter information, see Get-MailUser or New-MoveRequest.

1.8.3.19.10.2 Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010

Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010

Managing Mailbox Servers > Managing Move Requests > Managing Remote Move Requests >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Remote mailbox moves are also known as cross-forest mailbox moves. There are two types of remote mailbox moves that Microsoft Exchange Server 2010 supports:

- **Remote mailbox moves with a legacy Exchange forest** In this scenario, one forest contains Exchange 2010 and the other forest contains Exchange Server 2003 Service Pack 2 (SP2), Exchange Server 2007 SP2, or a combination of both. There is no Exchange 2010 Client Access server installed in the legacy forest. You must use the Shell to perform these mailbox moves.
- **Remote mailbox moves that have Exchange 2010 in both forests** In this

scenario, one forest contains Exchange 2010 and the other forest has at least one Exchange 2010 Client Access server. You can use the EMC or the Shell to perform these mailbox moves. For more information, see Create a Remote Move Request That has Exchange 2010 in Both Forests.

When you move Exchange 2003 mailboxes to Exchange 2010, the mailbox move will be offline. During the move, users won't be able to access their mailboxes. When you move Exchange 2007 SP2 mailboxes to Exchange 2010, the move will be online, and users can access their mailboxes during the move.

To perform remote legacy move requests, you must supply the following information in the command:

- Identity of the mail-enabled user
- *RemoteLegacy* switch
- Fully qualified domain name (FQDN) of the remote global catalog server
- FQDN of the external e-mail address that's created in the source forest for the mail-enabled user when the move request is complete
- Target database when moving mailboxes to Exchange 2010 or remote target database when moving mailboxes from Exchange 2010 to the remote legacy database

While performing remote mailbox moves, the Microsoft Exchange Mailbox Replication service (MRS) uses the **msExchMailboxGUID** attribute to find matching users, thereby maintaining the Send As and Receive As permissions. MRS then maps the trustee to the matching user in the destination forest.

Important:

Maintaining permissions may not be possible in split-permission deployments. The **ExchangeTrustedSubsystem** attribute isn't included in the Exchange Windows Permissions security group.

MRS also uses the **msExchMailboxGUID** attribute to attempt to maintain mailbox and mailbox folder permissions. MRS then maps the permissions to point to the matching user in the destination forest.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Prerequisites

For the complete list of prerequisites to move mailboxes across forests, see Prepare Mailboxes for Cross-Forest Move Requests.

Use the Shell to create remote legacy move requests

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to create remote legacy move requests.

In addition to the permissions listed previously, the administrator performing the move must have the following remote credentials on the Exchange 2003 or Exchange 2007 server:

- Exchange Server Administrator role
- Exchange Recipient Administrator role

Note:
The following examples use the *RemoteCredential* parameter. This parameter requires the creation and passing of a credential object. This credential object is created by using the **Get-Credential** cmdlet. For more information, see Get-Credential.

Move a mailbox from a remote legacy forest

This example moves Tony Smith's mailbox into the Exchange 2010 forest from an Exchange 2007 SP2 or Exchange 2003 SP2 forest. When the move is complete, the new *ExternalEmailAddress* in the source forest will be Tony's proxy address with the SMTP domain mail.contoso.com.

```
New-MoveRequest -Identity 'tony@humongousinsurance.com' -RemoteLegacy -TargetData
```

Move a mailbox to a remote legacy forest

This example moves Tony Smith's mailbox to the remote forest. Use this command when you initiate the move from the source Exchange 2010 forest. When initiating moves from the source forest, you must use the *RemoteTargetDatabase* parameter to specify the database that you're moving the mailbox to. When the move is complete, the new *ExternalEmailAddress* in the source forest will be Tony's proxy address with the SMTP domain mail.contoso.com.

```
New-MoveRequest -Identity 'tony@humongousinsurance.com' -RemoteLegacy -RemoteTarg
```

Create a remote legacy batch move request

This example creates a batched move request for all mailboxes in the source forest that have **CustomAttribute2** set to Washington and moves them to the target database DB02 in the target forest with the *BatchName* parameter value Washington_HumongousToContoso.

Note:
Creating a batch move request allows you to create a tag that identifies which mailboxes are being moved. When an MRS instance becomes available to perform the move, each mailbox will be moved individually. You can then filter in searches using the *BatchName* parameter in the **Get-MoveRequest** and **Get-MoveRequestStatistics** cmdlets.

```
Get-MailUser -Filter {CustomAttribute2 -eq "Washington"} | New-MoveRequest -Remot
```

Create a remote legacy move request that suspends before completion

This example creates a remote move request for all mailboxes that begin with the letter 'a' in the target forest. The request will be suspended after the initial content is moved, but before the mailbox is locked down and switched over to the new location.

Note:
You can use the *SuspendWhenReadyToComplete* parameter only for online mailbox moves and when moving mailboxes from Exchange 2007 and Exchange 2010 mailbox databases. You can't use this parameter for offline moves or when moving from Exchange 2003 mailbox databases.

The move request will then need to be resumed by using the **Resume-MoveRequest** cmdlet.

Note:
Only online moves can be suspended by using the *SuspendWhenReadyToComplete* parameter.

Note:
Creating a batch move request allows you to create a tag that identifies which mailboxes are being moved. When an MRS instance becomes available to perform the move, each mailbox will be moved individually. You can then filter in searches using the *BatchName* parameter in the **Get-MoveRequest** and **Get-MoveRequestStatistics** cmdlets.

```
Get-MailUser -ANR a* | New-MoveRequest -RemoteLegacy -RemoteGlobalCatalog 'GC01.h
```

Create a remote legacy move request that's processed by a specific server

This example creates a move request that's processed by the Client Access server CAS1.contoso.com, which has MRS installed.

Note:

The *MRSServer* parameter is reserved for debugging purposes. Use this parameter only if directed by support personnel. If you use this parameter and the specified server isn't functional, the move request won't be processed.

```
New-MoveRequest -Identity 'tony@humongousinsurance.com' -RemoteLegacy -RemoteGlob
```

Create a suspended remote legacy move request

This example creates a batch move request that's suspended for all mailboxes in the target forest where **CustomAttribute1** is set to Monday. You may want to run this command if you want to create the move request now and then resume it in the evening, when e-mail traffic is low.

Note:

Creating a batch move request allows you to create a tag that identifies which mailboxes are being moved. When an MRS instance becomes available to perform the move, each mailbox will be moved individually. You can then filter in searches using the *BatchName* parameter in the **Get-MoveRequest** and **Get-MoveRequestStatistics** cmdlets.

```
Get-MailUser -Filter {CustomAttribute1 -eq 'Monday'} | New-MoveRequest -RemoteLeg
```

For More Information

For detailed syntax and parameter information, see the following cmdlet reference topics:

- New-MoveRequest
- Get-MailUser
- Get-MoveRequest
- Get-MoveRequestStatistics

1.8.3.19.10.3 Prepare Mailboxes for Cross-Forest Move Requests

Prepare Mailboxes for Cross-Forest Move Requests

Managing Mailbox Servers > Managing Move Requests > Managing Remote Move Requests >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 supports remote mailbox moves via the **New-MoveRequest** cmdlet. To move a mailbox from an Exchange Server 2010, Exchange Server 2007, or Exchange Server 2003 forest to another Exchange 2010 forest, the Exchange 2010 target forest must contain a valid mail-enabled user with a specified set of Active Directory attributes. (Exchange 2010 doesn't support moving an Exchange 2000 Server mailbox.) If there is at least one Exchange 2010 Client Access server deployed in the forest, the forest is considered an Exchange 2010 forest.

To prepare for the mailbox move, you must create mail-enabled users with the required attributes in the target forest. Here are two recommended approaches to creating mail-enable users with the necessary attributes:

- If you deployed Microsoft Identity Lifecycle Manager (ILM) for cross-forest

global address list (GAL) synchronization, the recommended approach to creating the mail-enabled user is to use Service Pack 1 (SP1) for ILM 2007 Feature Pack 1 (FP1). We've created sample code that you can use to learn how to customize ILM to synchronize the source mailbox user and target mail user.
For more information, including how to download the sample code, see Prepare Mailboxes for Cross-Forest Moves Using Sample Code.

- If you created the target mail user using an Active Directory tool other than ILM/MIIS, use the **Update-Recipient** cmdlet with the *Identity* parameter to run the Address List service to generate the **LegacyExchangeDN** for the target mail user. We have created a sample Windows PowerShell script that reads from and writes to Active Directory and calls the **Update-Recipient** cmdlet. For more information about using the sample script, see Prepare Mailboxes for Cross-Forest Moves Using the Prepare-MoveRequest.ps1 script in the Shell.

After creating the target mail user, you can then run the **New-MoveRequest** cmdlet to move the mailbox to the target Exchange 2010 forest.

For more information about remote move requests, see the following topics:

- Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010
- Create a Remote Move Request That has Exchange 2010 in Both Forests
- New-MoveRequest

For more information about remote mailbox moves and remote legacy moves, see Understanding Move Requests.

The remainder of this topic describes the Active Directory mail user attributes that are required for a mailbox move. These attributes are configured for you when you use either the code or script to prepare for the mailbox move. However, you can manually copy these attributes using an Active Directory editor.

Active Directory User Attributes Required for a Mailbox Move

To support a remote mailbox move, the mail user object in the target Exchange 2010 forest must have the Active Directory attributes that are described in this section:

- Mandatory attributes
- Optional attributes
- Linked attributes
- Linked user attributes
- Resource mailbox attributes
- Additional attributes

Mandatory Attributes

The following table lists the minimum set of attributes that need to be configured in ILM on the target mail user for the **New-MoveRequest** cmdlet to function correctly.

Mail user's attributes

Mail user's Active Directory attributes	Action
displayName	Copy the corresponding attribute of the source mailbox or generate a new value.
Mail	Directly copy the corresponding attribute of the source mailbox.
mailNickname	Copy the corresponding attribute of the

	source mailbox or generate a new value.
msExchArchiveGUID and msExchArchiveName	Directly copy the corresponding attribute of the source mailbox. Attributes are only available if the source mailbox is Exchange 2010.
msExchMailboxGUID	Directly copy the corresponding attribute of the source mailbox.
msExchRecipientDisplayType	-2147483642 (decimal) //equivalent to 0x80000006 (hex).
msExchRecipientTypeDetails	128 (decimal) /0x80 (hex).
msExchUserCulture	Directly copy the corresponding attribute of the source mailbox.
msExchVersion	44220983382016 (decimal).
cn	Copy the corresponding attribute of the source mailbox or generate a new value.
proxyAddresses	Copy source mailbox's **proxyAddresses** attribute. Additionally, copy source mailbox's **LegacyExchangeDN** as an X500 address in the **proxyAddresses** attribute of the target mail user. **Note:** The **proxyAddresses** of the source mailbox user must contain an SMTP address that matches the authoritative domain of the target forest. This allows the **New-MoveRequest** cmdlet to correctly select the **targetAddress** of the source mail-enabled user (converted from the source mailbox user after the mailbox move request is complete) to ensure that mail routing is still functional.
sAMAccountName	Copy the corresponding attribute of the source mailbox or generate a new value. Ensure that the value is unique within the target forest domain that the target mail user belongs to.
targetAddress	Set to an SMTP address in the **proxyAddresses** attribute of the source mailbox. This SMTP address must belong to the authoritative domain of the source forest.
userAccountControl	Constant: 514 //equivalent to 0x202, ACCOUNTDISABLE | NORMAL_ACCOUNT.
userPrincipalName	Copy the corresponding attribute of the source mailbox or generate a new value. Because the mail user is logon disabled, this **userPrincipalName** isn't used.

Optional Attributes

It isn't mandatory that the following attributes are configured for the **New-MoveRequest** cmdlet to function correctly; however, synchronizing them provides a better end-to-end user experience after moving the mailbox. Because the GAL in the target forest displays this target mail user, you should set the following GAL-related attributes.

GAL-related attributes

Mail user's Active Directory attributes	Action
c	Directly copy the corresponding attribute of the source mailbox.
co	Directly copy the corresponding attribute of the source mailbox.
countryCode	Directly copy the corresponding attribute of the source mailbox.
company	Directly copy the corresponding attribute of the source mailbox.
department	Directly copy the corresponding attribute of the source mailbox.
facsimileTelephoneNumber	Directly copy the corresponding attribute of the source mailbox.
givenName	Directly copy the corresponding attribute of the source mailbox.
homePhone	Directly copy the corresponding attribute of the source mailbox.
info	Directly copy the corresponding attribute of the source mailbox.
initials	Directly copy the corresponding attribute of the source mailbox.
l	Directly copy the corresponding attribute of the source mailbox.
mobile	Directly copy the corresponding attribute of the source mailbox.
msExchAssistantName	Directly copy the corresponding attribute of the source mailbox.
msExchHideFromAddressLists	Directly copy the corresponding attribute of the source mailbox.
otherHomePhone	Directly copy the corresponding attribute of the source mailbox.
otherTelephone	Directly copy the corresponding attribute of the source mailbox.
pager	Directly copy the corresponding attribute of the source mailbox.
physicalDeliveryOfficeName	Directly copy the corresponding attribute of the source mailbox.

postalCode	Directly copy the corresponding attribute of the source mailbox.
sn	Directly copy the corresponding attribute of the source mailbox.
st	Directly copy the corresponding attribute of the source mailbox.
streetAddress	Directly copy the corresponding attribute of the source mailbox.
telephoneAssistant	Directly copy the corresponding attribute of the source mailbox.
telephoneNumber	Directly copy the corresponding attribute of the source mailbox.
title	Directly copy the corresponding attribute of the source mailbox.

Linked Attributes

A linked attribute is an Active Directory attribute that references other Active Directory objects in the local forest. You can't directly copy the linked attribute values from a mailbox in the source forest to a mail user in the target forest. First, you must find the Active Directory objects in the source forest that the source mailbox attribute refers to. Then, you must find the corresponding Active Directory objects in the target forest for the above-mentioned Active Directory object in the source forest. And finally, set the target mail user's attribute to refer to the Active Directory objects in the target forest.

Linked attributes

Mail User's Active Directory attributes	Action
altRecipient	Correspond to the source mailbox's **altRecipient** attribute.
deliverAndRedirect	Directly copy the corresponding attribute of the source mailbox. This attribute is a Boolean value that should be set along with **altRecipient**.
Manager (and its backlinks)	Correspond to the source mailbox's manager attribute.
MemberOf (backlinks)	This is the backlink of group member attribute.
publicDelegates (and its backlinks)	Correspond to the source mailbox's **publicDelegates** attribute.

Linked User Attributes

If you want to move a mailbox to an Exchange 2010 resource forest, the mailbox in the resource forest is considered a *linked mailbox*. In this scenario, you need to create a linked mail user in the (target) resource forest. To create a linked mail user, you need to set the attributes shown in the following table.

Linked mail user attributes

Mail user's Active Directory attributes	Action
msExchMasterAccountHistory	Directly copy the corresponding attribute of the source mailbox.

msExchMasterAccountSid	If the source mailbox has **msExchMasterAccountSid**, copy it. Otherwise, copy the source mailbox's **objectSid**.
msExchRecipientDisplayType	Constant:-1073741818 (decimal) // equivalent to *unsigned* 0xC0000006.

Note:
A linked mailbox can only be created if there's forest trust between the source forest and target forest.

If the source object is disabled and the **msExchMasterAccountSid** attribute is set to self (resource mailbox, shared mailbox), don't stamp anything on the target user.

If the source object is disabled and the **msExchMasterAccountSid** attribute isn't set, the mailbox is invalid.

If the source object is enabled and the **msExchMasterAccountSid** attribute is set, the mailbox is invalid.

Resource Mailbox Attributes

If you want to move a resource mailbox to an Exchange 2010 forest, you need to set the attributes shown in the following table on the target mail user.

Resource mailbox attributes

Mail user's Active Directory attributes	Action

msExchRecipientDisplayType	If the source mailbox is a conference room:
	• **Constant** -2147481850 (decimal) // equivalent to *unsigned* 0x80000706.
	
	If the source mailbox is an equipment mailbox:
	• **Constant** -2147481594 (decimal) // equivalent to *unsigned* 0x80000806.

msExchResourceCapacity	Directly copy the corresponding attribute of the source mailbox.
msExchResourceDisplay	Directly copy the corresponding attribute of the source mailbox.
msExchResourceMetaData	Directly copy the corresponding attribute of the source mailbox.
msExchResourceSearchProperties	Directly copy the corresponding attribute of the source mailbox.

Additional Attributes

In Exchange 2007, the **Move-Mailbox** cmdlet also copied the attributes shown in the following table when moving a mailbox. You can optionally copy these attribute if required by your organization.

Resource mailbox attributes

Mail User's Active Directory attributes	Description
comment	Directly copy the corresponding attribute of the source mailbox.

deletedItemFlags	Directly copy the corresponding attribute of the source mailbox.
delivContLength	Directly copy the corresponding attribute of the source mailbox.
departmentNumber	Directly copy the corresponding attribute of the source mailbox.
description	Directly copy the corresponding attribute of the source mailbox.
division	Directly copy the corresponding attribute of the source mailbox.
employeeID	Directly copy the corresponding attribute of the source mailbox.
employeeNumber	Directly copy the corresponding attribute of the source mailbox.
employeeType	Directly copy the corresponding attribute of the source mailbox.
extensionAttribute1-15	Directly copy the corresponding attribute of the source mailbox.
homePostalAddress	Directly copy the corresponding attribute of the source mailbox.
internationalISDNNumber	Directly copy the corresponding attribute of the source mailbox.
ipPhone	Directly copy the corresponding attribute of the source mailbox.
language	Directly copy the corresponding attribute of the source mailbox.
lmPwdHistory	Directly copy the corresponding attribute of the source mailbox.
localeID	Directly copy the corresponding attribute of the source mailbox.
mAPIRecipient	Directly copy the corresponding attribute of the source mailbox.
middleName	Directly copy the corresponding attribute of the source mailbox.
msDS-PhoneticCompanyName	Directly copy the corresponding attribute of the source mailbox.
msDS-PhoneticDepartment	Directly copy the corresponding attribute of the source mailbox.
msDS-PhoneticDisplayName	Directly copy the corresponding attribute of the source mailbox.
msDS-PhoneticFirstName	Directly copy the corresponding attribute of the source mailbox.

msDS-PhoneticLastName	Directly copy the corresponding attribute of the source mailbox.
msExchBlockedSendersHash	Directly copy the corresponding attribute of the source mailbox.
msExchELCExpirySuspensionEnd	Directly copy the corresponding attribute of the source mailbox.
msExchELCExpirySuspensionStart	Directly copy the corresponding attribute of the source mailbox.
msExchELCMailboxFlags	Directly copy the corresponding attribute of the source mailbox.
msExchExternalOOFOptions	Directly copy the corresponding attribute of the source mailbox.
msExchMessageHygieneFlags	Directly copy the corresponding attribute of the source mailbox.
msExchMessageHygieneSCLDeleteThreshold	Directly copy the corresponding attribute of the source mailbox.
msExchMessageHygieneSCLJunkThreshold	Directly copy the corresponding attribute of the source mailbox.
msExchMessageHygieneSCLQuarantineThreshold	Directly copy the corresponding attribute of the source mailbox.
msExchMessageHygieneSCLRejectThreshold	Directly copy the corresponding attribute of the source mailbox.
msExchMDBRulesQuota	Directly copy the corresponding attribute of the source mailbox.
msExchPoliciesExcluded	Directly copy the corresponding attribute of the source mailbox.
msExchSafeRecipientsHash	Directly copy the corresponding attribute of the source mailbox.
msExchSafeSendersHash	Directly copy the corresponding attribute of the source mailbox.
msExchUMSpokenName	Directly copy the corresponding attribute of the source mailbox.
otherFacsimileTelephoneNumber	Directly copy the corresponding attribute of the source mailbox.
otherIpPhone	Directly copy the corresponding attribute of the source mailbox.
otherMobile	Directly copy the corresponding attribute of the source mailbox.
otherPager	Directly copy the corresponding attribute of the source mailbox.
preferredDeliveryMethod	Directly copy the corresponding attribute of the source mailbox.

personalPager	Directly copy the corresponding attribute of the source mailbox.
personalTitle	Directly copy the corresponding attribute of the source mailbox.
photo	Directly copy the corresponding attribute of the source mailbox.
pOPCharacterSet	Directly copy the corresponding attribute of the source mailbox.
pOPContentFormat	Directly copy the corresponding attribute of the source mailbox.
postalAddress	Directly copy the corresponding attribute of the source mailbox.
postOfficeBox	Directly copy the corresponding attribute of the source mailbox.
primaryInternationalISDNNumber	Directly copy the corresponding attribute of the source mailbox.
primaryTelexNumber	Directly copy the corresponding attribute of the source mailbox.
showInAdvancedViewOnly	Directly copy the corresponding attribute of the source mailbox.
street	Directly copy the corresponding attribute of the source mailbox.
terminalServer	Directly copy the corresponding attribute of the source mailbox.
textEncodedORAddress	Directly copy the corresponding attribute of the source mailbox.
thumbnailLogo	Directly copy the corresponding attribute of the source mailbox.
thumbnailPhoto	Directly copy the corresponding attribute of the source mailbox.
url	Directly copy the corresponding attribute of the source mailbox.
userCert	Directly copy the corresponding attribute of the source mailbox.
userCertificate	Directly copy the corresponding attribute of the source mailbox.
userSMIMECertificate	Directly copy the corresponding attribute of the source mailbox.
wWWHomePage	Directly copy the corresponding attribute of the source mailbox.

Prepare Mailboxes for Cross-Forest Moves Using the Prepare-MoveRequest.ps1 script in the Shell

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-20*

Microsoft Exchange Server 2010 supports an online mailbox move using the **New-MoveRequest** cmdlet. You can move a mailbox from a source Exchange forest to a target Exchange 2010 forest.

To run the **New-MoveRequest** cmdlet, a mail user must exist in the target Exchange forest, and the mail user must have a minimum set of required Active Directory attributes.

The sample Windows PowerShell script described in this topic supports this task by synchronizing mailbox users from an Exchange 2010, Exchange Server 2007, or Exchange Server 2003 source forest to Exchange 2010 target forests as mail-enabled users. The script copies the Active Directory attributes of the mailbox users in the source forest to the target forest, and then uses the **Update-Recipient** cmdlet to turn the target objects into mail-enabled users.

For more information about using and writing scripts, see Scripting with the Exchange Management Shell. For more information about preparing for cross-forest moves, see Prepare Mailboxes for Cross-Forest Move Requests.

Looking for other management tasks related to remote move requests? Check out Managing Remote Move Requests.

Prerequisites

- Locate the script in the following location: Program Files\Microsoft\Exchange Server\V14\Scripts.
- To run the sample script, you need the following:
  - A source forest running Exchange 2010, Exchange 2007, or Exchange 2003, where the mailbox currently resides.
  - A target forest with Exchange 2010 installed, where the mailbox will be moved to.

Use the Prepare-MoveRequest.ps1 script to prepare mailboxes for cross-forest moves

Run the script from the Shell on a server role running Exchange 2010 in the target Exchange 2010 forest. The script copies the mailbox attributes from the source forest.

To assign a specific authentication credential for the remote forest domain controller, you must first run the Windows PowerShell **Get-Credential** cmdlet and store the user input in

a temporary variable. When you run the **Get-Credential** cmdlet, the cmdlet asks for the user name and password of the account used during authentication with the remote forest domain controller. You can then use the temporary variable in the Prepare-MoveRequest.ps1 script. For more information about the **Get-Credential** cmdlet, see Get-Credential.

Note:
Make sure that you use two separate credentials for the local forest and the remote forest when calling this script.

First, run the following commands to get the local forest and remote forest credentials.

```
$LocalCredentials = Get-Credential
$RemoteCredentials = Get-Credential
```

Then, run the following commands to pass the credential information to the *LocalForestCredential* and *RemoteForestCredential* parameters in the Prepare-MoveRequest.ps1 script.

```
Prepare-MoveRequest.ps1 -Identity JohnSmith@Fabrikan.com -RemoteForestDomainContr
```

The following table describes the parameter set for the script.

Parameter set of the Prepare-MoveRequest.ps1 script

Parameter	Required	Description
Identity	Required	The *Identity* parameter uniquely identifies a mailbox in the source forest. Identity can be any of the following: • Common name (CN) • Alias • **proxyAddress** property • **objectGuid** property • **DisplayName** property
RemoteForestCredential	Required	The *RemoteForestCredential* parameter specifies the administrator who has permissions to copy data from the source forest Active Directory.
RemoteForestDomainController	Required	The *RemoteForestDomainController* parameter specifies a domain controller in the source forest where the mailbox resides.
DisableEmailAddressPolicy	Optional	The *DisableEmailAddressPolicy* parameter specifies whether the Email Address Policy (EAP) should be disabled when creating a **MailUser** object in the target forest. When you specify this parameter, the EAP in the target forest won't be applied. **Note:** When you specify this parameter, the **MailUser** object won't have e-mail address mapping in the local forest domain stamped. This is usually

		stamped by the EAP.
LinkedMailUser	Optional	The *LinkedMailUser* switch specifies whether to create a linked MailUser in the local forest for the mailbox user in the remote forest. If the switch is provided, the script creates a target **MailUser** object linked to the source mailbox. If the switch is omitted, the script creates a regular target **MailUser** object. For more information, see Create a Linked Mailbox.
LocalForestCredential	Optional	The *LocalForestCredential* parameter specifies the administrator with permissions to write data to the target forest Active Directory. We recommend that you explicitly specify this parameter to avoid Active Directory permission issues. If the remote forest and the local forest have a trusted relationship configured, don't use a user account from the remote forest as the local forest credential, even though the remote user account may have permission to modify Active Directory in the local forest.
LocalForestDomainController	Optional	The *LocalForestDomainController* parameter specifies a domain controller in the target forest where the mail-enabled user will be created. We recommend that you specify this parameter to avoid possible domain controller replication delay issues in the local forest that could occur if a random domain controller is selected.
MailboxDeliveryDomain	Optional	The *MailboxDeliveryDomain* parameter specifies an authoritative domain of the source forest so that the script can select the correct source mailbox user's **proxyAddress** property as the target mail-enabled user's **targetAddress** property. By default, the primary SMTP address of the source mailbox user is set as the **targetAddress** property of the target mail-enabled user.
OverWriteLocalObject	Optional	The *OverWriteLocalObject* parameter is used for users created by the Active Directory Migration Tool. The

		properties are copied from the existing mail contact to the newly created mail user. However, after this copy, the script also copies the properties from the source forest user to the newly created mail user.
TargetMailUserOU	Optional	The *TargetMailuserOU* parameter specifies the organizational unit (OU) under which the target mail-enabled user will be created.
UseLocalObject	Optional	The *UseLocalObject* parameter specifies whether to convert the existing local object to the required target mail-enabled user if the script detects an object in the local forest that conflicts with the to-be-created mail-enabled user.

Examples

This section contains several examples of how you can use the Prepare-MoveRequest.ps1 script.

Example 1

This example provisions a single linked mail-enabled user in the local forest, when there is forest trust between the remote forest and local forest.

First, run the following commands to get the local forest and remote forest credentials.

```
$LocalCredentials = Get-Credential
$RemoteCredentials = Get-Credential
```

Then, run the following command to pass the credential information to the *LocalForestCredential* and *RemoteForestCredential* parameters in the Prepare-MoveRequest.ps1 script.

```
Prepare-MoveRequest.ps1 -Identity JamesAlvord@Contoso.com -RemoteForestDomainCont
```

Example 2

This example supports pipelining if you supply a list of mailbox identities.

First, run the following command.

```
$UserCredentials = Get-Credential
```

Then, run the following command to pass the credential information to the *RemoteForestCredential* parameter in the Prepare-MoveRequest.ps1 script.

```
"IanP@Contoso.com", "JoeAn@Contoso.com" | Prepare-MoveRequest.ps1 -RemoteForestDo
```

Example 3

You can generate a CSV file containing a list of mailbox identities from the source forest, which allows you to pipe the content of this file into the script to bulk create the target mail-enabled users.

For example, the content of the CSV file can be:

Identity

Ian@contoso.com

John@contoso.com

Cindy@contoso.com

This example calls a CSV file to bulk create the target mail-enabled users.

First, run the following command to get the remote forest credentials.

```
$UserCredentials = Get-Credential
```

Then, run the following command to pass the credential information to the *RemoteForestCredential* parameter in the Prepare-MoveRequest.ps1 script.

```
Import-Csv Test.csv | Prepare-MoveRequest.ps1 -RemoteForestDomainController DC001
```

Script Behavior per Target Object

This section describes how the script performs in relation to the following scenarios for target objects:

- Duplicate target mail-enabled object
- Mail-enabled user
- Mail-enabled contact
- **LegacyExchangeDN** attribute

Duplicate Target Mail-Enabled Object

When the script attempts to create a target mail-enabled user from the source mailbox user, and it detects a duplicate local mail-enabled object, it uses the following logic:

- If the source mailbox user's **masterAccountSid** attribute equals any target object's **objectSid** or **masterAccountSid** attribute:
  - If the target object isn't mail-enabled, the script returns an error because the script doesn't support converting an object that isn't mail-enabled to a mail-enabled user.
  - If the target object is mail-enabled, the target object is a duplicate.
- If an address in the source mailbox user's **proxyAddress** properties (smtp/x500 only) equals an address in a target object's **proxyAddress** properties (smtp/x500 only), the target object is a duplicate.

The script prompts the user about the duplicate objects.

If the target mail-enabled object is a mail-enabled user or contact, which is most likely created by a cross-forest (Identity Lifecycle Management 2007 Service Pack 1-based) global address list (GAL) synchronization deployment, the user can run the script again with the *UseLocalObject* parameter to use the target mail-enabled object for mailbox migration.

Mail-Enabled User

If the target object is a mail-enabled user, the script copies the following attributes from the source mailbox user to the target mail-enabled user:

- **msExchMailboxGUID**
- **msExchArchiveGUID**
- **msExchArchiveName**

If the *LinkedMailUser* parameter is set, the script copies the source **objectSid**/**masterAccountSid** attribute.

Mail-Enabled Contact

If the target object is a mail-enabled contact, the script deletes the existing contact and copies all its attributes to a new mail-enabled user. The script also copies the following attributes from the source mailbox user:

- **msExchMailboxGUID**
- **msExchArchiveGUID**
- **msExchArchiveName**
- **sAMAccountName**
- **userAccountControl** (set to 514 //equivalent to 0x202, ACCOUNTDISABLE | NORMAL_ACCOUNT)
- **userPrincipalName**

If the *LinkedMailUser* parameter is set, the script copies the source **objectSid**/ **masterAccountSid** attribute.

LegacyExchangeDN Attribute

When the **Update-Recipient** cmdlet is called to convert the target object into a mail-enabled user, a new **LegacyExchangeDN** attribute is generated for the target mail-enabled user. The script copies the **LegacyExchangeDN** attribute of the target mail-enabled user as an x500 address to the **proxyAddress** properties of the source mailbox user. This action ensures the correct resolution of recipients when messages are sent between the source and target forests.

1.8.3.19.10.5 Prepare Mailboxes for Cross-Forest Moves Using Sample Code

Prepare Mailboxes for Cross-Forest Moves Using Sample Code

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-02*

Microsoft Exchange Server 2010 supports an online mailbox move using the **New-MoveRequest** cmdlet in the Exchange Management Shell. You can move a mailbox from a source Exchange forest to a target Exchange 2010 forest. To run **New-MoveRequest**, a mail user must exist in the target Exchange forest and the mail user must have a minimum set of required Active Directory attributes.

You can create the required mail user in the target Exchange forest by customizing your Microsoft Identity Lifecycle Manager (ILM) 2007 deployment. The ILM-based rules extension sample code described in this topic demonstrates how to customize your current ILM deployment to create the required mail-enabled users in the target Exchange 2010 forest.

For more information about preparing for cross-forest moves, including descriptions of the required Active Directory attributes, see Prepare Mailboxes for Cross-Forest Move Requests.

Prerequisites

- Download the sample code from the Prepare for Online Mailbox Move page in the Microsoft Download Center.
- To run the sample code, you need ILM 2007 Feature Pack 1 SP1. To download the feature pack, see Microsoft Knowledge Base article 977791, Service Pack 1 (build 3.3.1139.2) is available for Identity Lifecycle Manager 2007 Feature Pack 1.
- You also need the following:

- A source forest running Exchange 2003, Exchange 2007 or Exchange 2010, where the mailbox currently resides

  Note:
  Exchange 2010 doesn't support moving an Exchange 2000 mailbox.

- A target forest with Exchange 2010 installed, where the mailbox will be moved to

- To connect to the Exchange 2010 target forest, you must have the appropriate permission to call the **UpdateRecipient** cmdlet. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Contents of Sample Code

In Microsoft Visual Studio 2008, open Microsoft.Exchange.Sample.OneWayGALSync.sln to view the sample code. The sample code includes the following:

- Microsoft.MetadirectoryServicesEx.dll is the binary file that is shipped with ILM 2007 FP1 SP1 under "\Program Files\Microsoft Identity Integration Server\Bin \Assemblies". It's referenced by the sample code.
- OneWaySync.xml is referenced by the sample code.
- The ILMServerConfig folder contains the ILM configuration files for the source management agent (MA), target MA, and the ILM Metaverse (MV).
- Microsoft.Exchange.Sample.OneWayGALSync.MARules.dll and Microsoft.Exchange.Sample.OneWayGALSync.MVRules.dll (built from the sample code) are under "\obj\Debug"

Install the ILM sample code

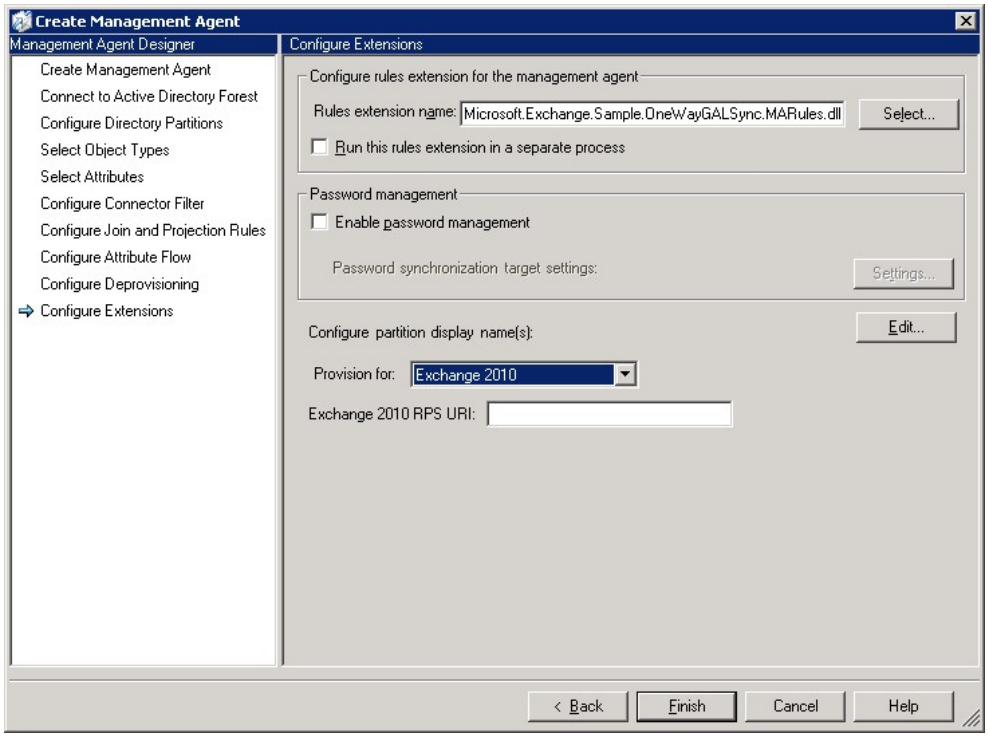
1. On the ILM server, copy the following to \Program Files\Microsoft Identity Integration Server\Extensions:
   - OneWaySync.xml
   - Microsoft.Exchange.Sample.OneWayGALSync.MARules.dll
   - Microsoft.Exchange.Sample.OneWayGALSync.MVRules.dll
2. Edit the file OneWaySync.xml that you copied to the ILM Extensions folder in step 1 to specify the distinguishedName (DN) of the TargetOU container in the target Exchange forest in which you want to create the mail users. You can use LDP.exe or ADSIEdit.exe to browse for the TargetOU container if you don't know what its name is.

   Note:
   If you're using this sample together with ILM GalSync 2007 exclude this container from the list of containers managed by GalSync2007.

3. On the ILM Identity Manager Console, go to **File** > **Import Server Configuration** to import the ILM server configuration from the folder ILMServerConfig. This action will import two Active Directory Management Agents along with the Metaverse schema and the provisioning rule.

   Note:
   During the import, you must provide the forest name and credentials and match the partitions of the imported Active Directory Management Agent (ADMA) to the partition name in your configuration for both the source and target ADMAs.

4. For the ADMA to support the Exchange 2010 target forest, on the **Create Management Agent** page, on the **Configure Extensions** pane, select **Exchange 2010** in the **Provision for** drop-down and then enter the remote Windows PowerShell URI of an Exchange 2010 Client Access server in **Exchange 2010 RPS URI**.



5. On the ILM Identity Manager Console on the **Create Management Agent** pane, open the **Properties** for the Source Forest Management Agent. Select the **Configure Directory Partitions** wizard, and then click **Containers** to select the container that will contain the mailboxes you will be moving to the target forest. Clear the selections for all other containers, that is, scope the management agent to only manage this one container. Similarly, for the target forest MA, select the container to which mail-enabled user's will be provisioned, that is, the TargetOU specified in step 2.

Note:
If you're using this sample together with ILM GalSync 2007, exclude both of these containers from the list of containers managed by GalSync 2007.

6. Perform an initial Full Import (stage only) on the target MAs so that ILM can discover the TargetOU specified in step 2.

Create Mail User in Target Exchange Forest

Now that you've installed the sample code, use the following procedure to create the required mail user in the target Exchange forest so that **New-MoveRequest** can be run to perform an online mailbox move.

1. In the source forest, use the Exchange Management Console to create mailbox users in the container selected in step 4 of "Install the ILM sample code". You can also use Active Directory Users and Computers to move existing mailbox users to the container.
2. Perform Delta Import and Delta Sync run on the source MA to discover the mailboxes added to the source container, and provision mail users to the target MA.
3. Perform Export run on the target MA to export the mail users provisioned in step 1 to the target Active Directory.
4. Perform Delta Import on the target MA to confirm the changes exported in step 2.
5. In the target forest, open the Exchange Management Shell and use the

New-MoveRequest cmdlet to move mailboxes from the source forest.

For more information related to the preceding steps, see the following topics:

- Prepare Mailboxes for Cross-Forest Move Requests
- Create a Remote Move Request That has Exchange 2010 in Both Forests
- Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010

1.8.3.19.10.6 Start the MRSProxy Service on a Remote Client Access Server

Start the MRSProxy Service on a Remote Client Access Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-22*

The Mailbox Replication Proxy (MRSProxy) service is installed on every Microsoft Exchange Server 2010 Client Access server. MRSProxy helps to facilitate cross-forest move requests and runs on the remote forest's Exchange 2010 Client Access server. However, MRSProxy is disabled by default.

Note:

All Client Access servers in the Network Load Balancing (NLB) array must have MRSProxy started. When you create a remote move request, and specify the fully qualified domain name (FQDN) of the *RemoteHostName* parameter, the load balancers that share the same name space as the FQDN you specified can direct the move request to any of the Client Access servers in that array. If you don't have MRSProxy started on one of the Client Access servers, and a move request is directed to that server, the move request fails. For more information about the NLB array, see "Availability Service Network Load Balancing" in Understanding the Availability Service.

Looking for other management tasks related to move requests? Check out Managing Move Requests.

Use the Shell to Enable MRSProxy in the Remote Forest

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange Web Services virtual directory settings" entry in the Client Access Permissions topic.

This example enables MRSProxy on the Exchange Web Services (EWS) default Web site. It also modifies the maximum number of simultaneous connections that an MRSProxy instance accepts by changing the value to 50. The default value is 100.

```
Set-WebServicesVirtualDirectory -Identity "EWS (Default Web Site)" -MRSProxyEnabl
```

1.8.3.19.10.7 Modify the Maximum Number of Recipients to Display in the Result Pane

Modify the Maximum Number of Recipients to Display in the Result Pane

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the **Maximum Number of Recipients to Display** dialog box to specify how many recipients you want to display in the result pane of the Exchange Management Console (EMC).

By default, a maximum of 1,000 recipients is displayed. Increasing this value can be beneficial in large environments. However, increasing the value also increases the time it takes to display the results. Depending on the size of your organization, it may also have a performance impact on the domain controller to which you are connected.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Provisioning Recipients Permissions" section in the Mailbox Permissions topic.

1. In the EMC console tree, click **Recipient Configuration**.
2. In the action pane, click **Modify the Maximum Number of Recipients to Display**.
3. In the **Maximum number of recipients to display** box, type the number of recipients that you want to display in the result pane. The number must be between 1 and 100,000.
4. Click **OK**.

1.8.3.20 Managing Offline Address Books

Managing Offline Address Books

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-30*

Add or Remove an Address List from an Offline Address Book

Change the Default Offline Address Book

Create an Offline Address Book

Configure Offline Address Book Properties

Provision Recipients for Offline Address Book Downloads

Remove an Offline Address Book

Update the Offline Address Book

Create an Offline Address Book Virtual Directory

Configure Offline Address Book Distribution Properties

Move the Offline Address Book Generation Process to Another Server

Remove, Re-Create, and Reconnect an Offline Address Book Virtual Directory

Require SSL for Offline Address Book Distribution

1.8.3.20.1 Add or Remove an Address List from an Offline Address Book

Add or Remove an Address List from an Offline Address Book

[This topic is in progress.]

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to add or remove an address list from an offline address book (OAB). By default, there is an OAB named the Default Offline Address Book that contains the global address list (GAL). OABs are generated based on the address lists that they contain. To create custom OABs that users can download, you can add or remove address lists from OABs.

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

Note:

The changes to the address list aren't available for client download until after the OAB in which the address list resides has been generated. For more information, see Update the Offline Address Book.

Use the EMC to add or remove an address list from an offline address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Offline Address Book** tab, and then click the OAB that you want to edit.
3. In the action pane, click **Properties**.
4. In **<Offline Address Book Name> Properties**, click the **Address Lists** tab.
5. To add an address list to the OAB or remove an address list from the OAB, select the **Include the following address lists** check box, and then perform one of the following tasks:
   - Click **Add** to select one or more address lists to add to the OAB. You can select one or multiple address lists.
   - Click **Remove** ( ) to remove the selected address list from the OAB.
6. Click **Apply** to save your changes without closing, or click **OK** to save your changes and close **<Offline Address Book Name> Properties**.

Use the Shell to add or remove an address

list from an offline address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

To add an address list to an OAB, use the following syntax.

```
Set-OfflineAddressBook -Identity <OfflineAddressBookIdParameter> -AddressLists <A
```

When using the *AddressLists* parameter, any address lists that currently exist will be overwritten. You must include existing address lists when you use the *AddressLists* parameter to continue to generate those address lists in your OAB. This example, in which you have AddressList1 and AddressList2, adds AddressList3.

```
Set-OfflineAddressBook -Identity "My OAB" -AddressLists AddressList1,AddressList2
```

To remove an address list from an OAB, omit that address list from the list of addresses. This example, in which you have AddressList1, AddressList2, and AddressList3, removes AddressList3.

```
Set-OfflineAddressBook -Identity "My OAB" -AddressLists AddressList1,AddressList2
```

For detailed syntax and parameter information, see Set-OfflineAddressBook.

1.8.3.20.2 Change the Default Offline Address Book

Change the Default Offline Address Book

Mailbox > Managing Mailbox Servers > Managing Offline Address Books >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

By default, when you install the Mailbox server role, a Web-based default offline address book (OAB) named Default Offline Address Book is created. You can set any OAB in your Exchange organization as the default OAB. This new default OAB is associated with all newly created mailbox databases. You can have only one default OAB in your organization. If you delete the default OAB, Microsoft Exchange doesn't automatically assign another OAB as the default. You must manually designate another OAB as the default.

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

Use the EMC to change the default offline address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Offline Address Book** tab, and then click the OAB that you want to set as the default OAB.
3. In the action pane, click **Set as Default**. A warning appears. Click **Yes** to

confirm that you want to set this OAB as the default OAB.

Use the Shell to change the default offline address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

To change the default OAB, use the following syntax.

```
Set-OfflineAddressBook -Identity <OfflineAddressBookIdParameter> -IsDefault <$tru
```

This example sets the OAB named My OAB as the default OAB.

```
Set-OfflineAddressBook -Identity "My OAB" -IsDefault $true
```


1.8.3.20.3 Create an Offline Address Book

Create an Offline Address Book

Mailbox > Managing Mailbox Servers > Managing Offline Address Books >

[This topic is in progress.]

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

An offline address book (OAB) in Exchange Server 2010 is a copy of an address book that has been downloaded so that an Outlook user can access the information it contains while disconnected from the server. Exchange administrators can choose which address books are made available to users who work offline, and they can also configure the method by which the address books are distributed (Web-based distribution or public folder distribution).

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

What Do You Want to Do?

- Use the EMC to create an OAB
- Use the Shell to create an OAB with web-based distribution
- Use the Shell to create an OAB with public folder distribution

Use the EMC to create an OAB

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Offline Address Book**.
3. On the **Introduction** page, complete the following fields:
   - **Name** Use this box to provide a name for the OAB.
   - **Offline address book generation server** Click **Browse** to specify the location where the OAB generation server will be located. The OAB generation server is the Mailbox server on which the OABs are generated.

- **Include the default Global Address List** The OAB is a snapshot of the Active Directory information that's available in the GAL. Select this check box to include the default GAL in the OAB.
- **Include the following address lists** Select this check box to add address lists to or remove address lists from the OAB.
  Click **Add** to open the **Select Address List** dialog box. Use this dialog box to select one or more address lists to add to the OAB.
  Click  to remove the selected address list from the OAB.

4. On the **Distribution Points** page, complete the following fields:
   - **Enable Web-based distribution** Select this check box to distribute the OAB from selected virtual directories. Web-based distribution is the distribution method by which Outlook 2007 or later clients that are working offline or through a dial-up connection access OABs. Clients will download the OAB over HTTPS from the virtual directory you specify.
     Click **Add** to open the **Select OAB Virtual Directory** dialog box. Use this dialog box to add virtual directories from which to distribute the OAB.
     Click  to delete the Web-based distribution point.
   - **Enable public folder distribution** Select this check box to enable public folder distribution. Public folder distribution is the distribution method by which Outlook 2003 or earlier clients that are working offline or through a dial-up connection access OABs.

5. On the **New Offline Address** Book page, review your configuration settings. Click **New** to create the OAB or click **Back** to make changes. Click **Cancel** to close the wizard without creating a new OAB.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. Click **Finish** the close the wizard.

Use the Shell to create an OAB with web-based distribution

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

This example creates the OAB New OAB that uses Web-based distribution for Outlook 2007 or later clients on SERVER01 by using the default virtual directory.

```
New-OfflineAddressBook -Name "New OAB" -AddressLists "\Default Global Address Lis
```

Use the Shell to create an OAB with public folder distribution

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

This example creates the OAB Legacy OAB that uses public folder distribution for Outlook 2003 SP1 and Outlook 98 Service Pack 2 (SP2) clients on SERVER01.

```
New-OfflineAddressBook -Name "Legacy OAB" -AddressLists "Default Global Address L
```

Note:
If you configure OABs to use public folder distribution, but your organization doesn't have any public folder infrastructure, an error will be returned. For more information, see Managing Public Folders.
For detailed syntax and parameter information, see New-OfflineAddressBook.

For More Information

Understanding Offline Address Books

Configure Offline Address Book Properties

Configure Offline Address Book Distribution Properties

1.8.3.20.4 Configure Offline Address Book Properties

Configure Offline Address Book Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-17*

An offline address book (OAB) in Exchange Server 2010 is a copy of an address book that's been downloaded so that an Outlook user can access the information it contains while disconnected from the server. Exchange administrators can choose which address books are made available to users who work offline, and they can also configure the method by which the address books are distributed (Web-based distribution or public folder distribution).

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

What Do You Want to Do?

- Use the EMC to configure OAB properties
- Use the Shell to configure OAB properties

Use the EMC to configure OAB properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Offline Address Book** tab, and then select the offline address book that you want to configure.
3. In the action pane, click **Properties**.
4. Use the **General** tab to view OAB properties and to set the update interval for the OAB.

- **Name** This unlabeled box at the top of the tab displays the OAB name. You can modify this name.
- **Generation server** This read-only field displays the OAB generation server. The OAB generation server is the Mailbox server on which the OABs are generated. If you want to specify a different generation server, use the **Move-OfflineAddressBook** cmdlet with the *Server* parameter. For more information, see Move-OfflineAddressBook.
- **Default offline address book** This read-only field displays a **True** or **False** status to indicate whether the selected OAB is the default OAB. If this isn't the default OAB, and you want to set it as the default, right-click the OAB in the result pane, and then click **Set as Default**.
- **Modified** This read-only field displays the last date and time that the OAB was modified.
- **Update Schedule** This list displays the time and interval for the regularly scheduled update.

  To customize the schedule, select **Use Custom Schedule** from the list, and then click **Customize** to open the **Schedule** dialog box and specify the schedule you want.

5. Use the **Address Lists** tab to select the address lists you want to include in the OAB. If you want to include a global address list (GAL) other than the default GAL, you must use the Shell.
   - **Include the default Global Address List** Select this check box to include the default GAL in the OAB.
   - **Include the following address lists** Select this check box to add address lists to or remove address lists from the OAB.

     Click **Add** to select one or more address lists to add to the OAB.

     Click  to remove the selected address list from the OAB.

6. Use the **Distribution** tab to specify the client support and OAB distribution points for the OAB.

   Client Support Select the OAB version that will be generated for the version of Outlook that is used by your Exchange organization. If you have more than one version of Outlook in your organization, you can select one or more of the following versions:
   - **Outlook 98 SP1 or earlier (Version 2)**
   - **Outlook 98 SP2 or later (Version 3)**
   - **Outlook 2003 SP2 or later (Version 4)**

   If you don't select one of the **Client Support** options, Version 4 will be generated.

   Distribution Points OAB distribution is the method by which the OAB can be accessed by users when they are working remotely or over a dial-up connection. To distribute the OAB, administrators can use Web-based distribution, public folder distribution, or both. An OAB distribution point is the HTTP Web address or public folder where client computers can download an OAB.

   You can select one or both of the following check boxes:
   - **Enable Web-based distribution** Select this check box to enable Web-based distribution. Web-based distribution is the distribution method by which Outlook 2007 or later clients that are working offline or through a dial-up connection access the OAB. With Web-based distribution, a Client Access server will contain an OAB virtual directory for Web distribution purposes.

     Click **Add** to specify the virtual directory or directories from which you want to distribute the OAB.

     Click  to remove the selected virtual directory from the OAB.
   - **Enable public folder distribution** Select this check box to enable public folder distribution. Public folder distribution is the distribution method by which Outlook 2003 or earlier clients that are working offline or through a

dial-up connection access OABs.

Use the Shell to configure OAB properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

This example modifies the time and date at which the OAB generation occurs for the OAB My OAB.

```
Set-OfflineAddressBook -Identity "My OAB" -Schedule "Sun.1:15 AM-Sun.1:30 AM"
```

Note:
The *Schedule* parameter takes the following format and must include a range: Weekday.Hour:Minute[AM/PM]-Weekday.Hour:Minute[AM/PM].

For More Information

Understanding Offline Address Books

Configure Offline Address Book Distribution Properties

1.8.3.20.5 Provision Recipients for Offline Address Book Downloads

Provision Recipients for Offline Address Book Downloads

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you use multiple offline address books (OABs) in your organization, there are several ways to specify which recipients download which OABs:

- **Per mailbox database** You can use the EMC or the Shell to provision recipients for OAB downloads by linking a mailbox database to a public folder database (for Microsoft Outlook 2003 clients), to a default OAB (for Office Outlook 2007 and Outlook 2010 clients), or both.
- **Per recipient** You can use the **Set-Mailbox** cmdlet in the Shell to specify which OAB is downloaded by linking the OAB directly to a recipient's mailbox. You can't specify the public folder database at the per-recipient level.
- **Per multiple recipients** You can use a pipelined command in the Shell to specify the OAB that multiple recipients download, based on common attributes.
- **Per address book policy** You can assign an address book policy (ABP) to a mailbox user's account to specify which OAB is downloaded to a recipient's mailbox. If you assign an ABP to a user account that already has an OAB assigned, the OAB that is explicitly assigned to the mailbox will take precedence. For more information, see Assign an Address Book Policy to a Mail User.

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

Provision recipients for OAB downloads

by linking their mailbox database to a public folder database or to a default OAB

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

Use the EMC

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab, and then select the mailbox database you want.
3. In the action pane, click **Properties**.
4. In **<Mailbox Database Name>** **Properties**, on the **Client Settings** tab, use the following boxes to select the default public folder database, the default OAB, or both:
   - **Default public folder database** This box displays the location of the default public folder database. The public folder database stores public folder data, OAB information, and free/busy information for Outlook 2003 and earlier clients. To change the location of the default public folder database, click **Browse**.
   - **Offline address book** This box displays the location of the OAB that this database uses as the default OAB for Outlook 2007 and Outlook 2010 clients. To change the OAB, click **Browse**.
5. Click **Apply** to save your changes without closing, or click **OK** to save your changes and close **<Mailbox Database Name> Properties**.

Use the Shell

To specify the public folder database and OAB, use the following syntax.

```
Set-MailboxDatabase -Identity <DatabaseIdParameter> -OfflineAddressBook <OfflineA
```

This example sets up the Web-based distribution of My OAB for the default mailbox database.

```
Set-MailboxDatabase -Identity "Mailbox Database" -OfflineAddressBook "My OAB"
```

For detailed syntax and parameter information, see Set-MailboxDatabase.

Use the Shell to specify which OAB will be downloaded by linking the OAB directly to a recipient's mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

You can't use the EMC to complete this procedure.

To specify which OAB is downloaded by linking the OAB directly to a recipient's mailbox, use the following syntax.

```
Set-Mailbox -Identity <MailboxIDParameter> -OfflineAddressBook <OfflineAddressBoo
```

Note:

The *Identity* parameter identifies the mailbox and can take the following values: GUID, ADObjectID, distinguished name (DN), *domain**account*, user principal name (UPN), LegacyExchangeDN, SmtpAddress, and alias.

This example specifies that the user Kim will download the OAB My OAB.

```
Set-Mailbox -Identity Kim -OfflineAddressBook "My OAB"
```

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to specify the OAB that multiple recipients will download

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:
You can't use the EMC to complete this procedure.

To specify the OAB that multiple recipients download, use the following syntax.

```
Get-User -Filter <String> | Set-Mailbox -OfflineAddressBook <OfflineAddressBookId
```

This example specifies that all user mailboxes in the United States for the Contoso company download the OAB Contoso United States.

```
Get-User -ResultSize Unlimited -Filter { Company -eq "Contoso" -and RecipientType
```

Note:
For more information about using filters to limit the scope of a command, see Creating Filters in Recipient Commands.

For detailed syntax and parameter information, see Get-User and Set-Mailbox.

1.8.3.20.6 Remove an Offline Address Book

Remove an Offline Address Book

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to remove an offline address book (OAB).

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

Note:
After you remove an OAB that's linked to a user or to a mailbox database, the recipient will download the default OAB until you assign a new OAB for that user. If you remove the default OAB, you must assign a different OAB as the default OAB. For instructions about how to change the default OAB, see Change the Default Offline Address Book.

Use the EMC to remove an offline address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Offline Address Book** tab, and then click the OAB that you want to remove.
3. In the action pane, click **Remove**. A warning appears. Click **Yes** to confirm that you want to remove the OAB.

Use the Shell to remove an offline address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

To remove an OAB, use the following syntax.

```
Remove-OfflineAddressBook -Identity <OfflineAddressBookIdParameter>
```

This example removes an OAB named My OAB.

```
Remove-OfflineAddressBook -Identity "My OAB"
```

Type **Y** to confirm that you want to remove the OAB, and then press ENTER.

For detailed syntax and parameter information, see Remove-OfflineAddressBook.

1.8.3.20.7 Update the Offline Address Book

Update the Offline Address Book

Mailbox > Managing Mailbox Servers > Managing Offline Address Books >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC or the Shell to update an offline address book (OAB). After you create an OAB or modify OAB settings, the changes aren't available to users until the OAB generation (OABGen) process has completed.

For information about how to create OABs, see Create an Offline Address Book.

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

Use the EMC to update an offline address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Offline Address Book** tab, and then click the OAB that you want to update.
3. In the action pane, click **Update**.
4. A warning appears. Click **Yes** to update the OAB.

Use the Shell to update an offline address book

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

To update an OAB, use the following syntax.

```
Update-OfflineAddressBook -Identity <OfflineAddressBookIdParameter>
```

This example updates the OAB named My OAB.

```
Update-OfflineAddressBook -Identity "My OAB"
```

For detailed syntax and parameter information, see Update-OfflineAddressBook.

1.8.3.20.8 Create an Offline Address Book Virtual Directory

Create an Offline Address Book Virtual Directory

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can use the Shell to create an offline address book (OAB) virtual directory.

The OAB virtual directory is the distribution point used by the Web-based distribution method of the OAB. By default, when Microsoft Exchange Server 2010 is installed, a new virtual directory named OAB is created in the default internal Web site in Internet Information Services (IIS). If you have client-side users that connect to Microsoft Outlook from outside your organization's firewall, you can add an external Web site. Alternatively, when you run the **New-OABVirtualDirectory** cmdlet in the Shell, a new virtual directory named OAB is created in the default IIS Web site on the local Exchange server.

Although Web-based distribution is enabled by default and doesn't require further configuration, we recommend that you enable Secure Sockets Layer (SSL) for the OAB distribution point. For more information, see Require SSL for Offline Address Book Distribution.

Creating an OAB virtual directory isn't a common task. Exchange allows for one OAB virtual directory named OAB, and you should create an OAB virtual directory only if there is a problem with the existing OAB virtual directory, and the previous OAB virtual directory was removed. For more information, see Remove, Re-Create, and Reconnect an Offline Address Book Virtual Directory.

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

Important:
Before you create an OAB virtual directory, make sure that your users are aware of the changes you are making. This procedure may interrupt the OAB downloading process for your users.

Prerequisites

- The local Exchange server has the Client Access server role installed.
- There is a default IIS Web site, for example, /w3svc/1/root.
- A virtual directory named OAB doesn't already exist.

Use the Shell to create an OAB virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "OAB virtual directory" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to create an OAB virtual directory.

To create an OAB virtual directory with all of the default settings, you can run the **New-OABVirtualDirectory** cmdlet without any parameters. Use the following procedure to create an OAB virtual directory with custom settings.

Note:
When creating an OAB virtual directory, we recommend that you have SSL enabled.

To create an OAB virtual directory, use the following syntax.

```
New-OABVirtualDirectory -DomainController <Fqdn> -ExternalUrl <Url> -InternalUrl
```

This example creates an OAB virtual directory on the Client Access server named CAS_SERVER01 that has SSL enabled and an external URL.

```
New-OABVirtualDirectory -RequireSSL $true -ExternalURL "https://www.contoso.com/O
```

After you create a new OAB virtual directory, you must edit the settings on each OAB that uses Web-based distribution to reconnect to the OAB virtual directory. For more information, see Configure Offline Address Book Properties.

For detailed syntax and parameter information, see New-OABVirtualDirectory.

1.8.3.20.9 Configure Offline Address Book Distribution Properties

Configure Offline Address Book Distribution Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

For each offline address book (OAB) distribution point in Exchange Server 2010, you can configure two URLs—an internal URL that can be accessed only from your internal corporate network and an external URL that can be accessed from the Internet.

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

What Do You Want to Do?

- Use the EMC to view or configure OAB distribution properties
- Use the Shell to configure OAB distribution properties

Use the EMC to view or configure OAB distribution properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address book distribution" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Client Access**.
2. In the result pane, select the Client Access server you want.
3. In the work pane, click the **Offline Address Book Distribution** tab, and then select the OAB distribution point you want to configure.
4. In the action pane, click **Properties**.
5. Use the **General** tab to view information about the OAB and to configure the polling interval.
   - **Server** This read-only field displays the name of the server that hosts the OAB.
   - **Path** This read-only field displays the path to the location where the OAB is stored.
   - **Modified** This read-only field displays the date and time when the last configuration change was made to this OAB distribution point.
   - **Polling interval (minutes)** Use this box to configure your polling interval (in minutes). The distribution point will use this interval to poll for updated OAB files. The default setting is eight hours (480 minutes).
6. Use the **URLs** tab to view and modify the URLs to which users connect to download OAB updates.
   - **Internal URL** Use this box to type the URL that Outlook users on the corporate network can use to download OAB updates.
   - **External URL** Use this box to type the URL that Outlook users can use to download OAB updates from the Internet.

Use the Shell to configure OAB distribution properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address book distribution" entry in the Mailbox Permissions topic.

This example sets the polling interval for OAB distribution on the OAB virtual directory OAB (Default Web Site) to six hours.

```
Set-OABVirtualDirectory "OAB (Default Web Site)" -PollInterval 360
```

This example sets the external distribution point to https://contoso.com/OAB for the

default OAB virtual directory OAB (Default Web Site).

```
Set-OABVirtualDirectory "OAB (Default Web Site)" -ExternalUrl https://contoso.com
```

For More Information

Understanding Offline Address Books

1.8.3.20.10 Move the Offline Address Book Generation Process to Another Server

Move the Offline Address Book Generation Process to Another Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Offline address book (OAB) generation is the process by which Exchange creates and updates the OAB. When OAB generation occurs, Exchange generates new OAB files, compresses the files, and then places the files on a local share.

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

Cautions

- If you use Web-based distribution, the Client Access server replicates the files. If you use public folder distribution, the OAB generation process places the files directly in one of the public folders, and then the Exchange store replication copies the data to other public folder distribution points.
- Client computers that are running Outlook periodically check for and download OAB updates. For information about how to modify when OAB generation occurs, see Configure Offline Address Book Properties.
- If your organization contains Exchange Server 2003 servers, you can generate the OAB from an Exchange 2003 server provided that public folder distribution is enabled. However, if you generate the OAB from an Exchange 2003 server, you will lose the following functionality:
  - Japanese phonetic display name
  - Japanese phonetic surname
  - Japanese phonetic given name
  - Japanese phonetic company name
  - Japanese phonetic department name
  - PR_DISPLAY_TYPE_EX, which is used by Office Outlook 2007 and later to render the correct icon for objects that are replicated across the forest.

What Do You Want to Do?

- Use the EMC to move OAB generation to another server
- Use the Shell to move OAB generation to another server

Use the EMC to move OAB generation to

another server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "OAB virtual directories" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Offline Address Book** tab, and then select the OAB for which you want to move the generation to a new server.
3. In the action pane, click **Move**.
4. On the **Move Offline Address Book** page, click **Browse** to open the **Select Mailbox Server** dialog box. Select the server to which you want to move the OAB generation process, and then click **OK**.
5. Click **Move** to move the OAB generation process to the new server.
6. View the status of the move operation. The wizard will move the generation of your OAB to the new server and copy the existing files for the OAB to the new server. Click **Back** to make configuration changes.
7. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
8. Click **Finish** to close the wizard.

Use the Shell to move OAB generation to another server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "OAB virtual directories" entry in the Mailbox Permissions topic.

This example moves the OAB generation process to SERVER01 for the OAB MyOAB.

```
Move-OfflineAddressBook -Identity "My OAB" -Server SERVER01
```

For detailed syntax and parameter information, see Move-OfflineAddressBook.

For More Information

Understanding Offline Address Books

1.8.3.20.11 Remove, Re-Create, and Reconnect an Offline Address Book Virtual Directory

Remove, Re-Create, and Reconnect an Offline Address Book Virtual Directory

Mailbox > Managing Mailbox Servers > Managing Offline Address Books >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to remove, re-create, and then reconnect an offline address book (OAB) virtual directory. The OAB virtual directory is the distribution point used by the Web-based distribution method of the OAB. By default, when Microsoft Exchange Server 2010 is installed, a virtual directory named OAB is created in the default internal Web site in Internet Information Services (IIS).

When you remove an OAB virtual directory, the OABs that use Web-based distribution will lose their connection to the OAB virtual directory. After you re-create the virtual directory, you must edit the settings on each OAB that uses Web-based distribution to reconnect to the OAB virtual directory. For information about how to edit OAB settings, see Configure Offline Address Book Properties.

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

Important:

Before you remove, re-create, and reconnect an OAB virtual directory, make sure that your users are aware of the changes. These procedures may interrupt the OAB downloading process for your users.

Use the Shell to remove, re-create, and reconnect an OAB virtual directory

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to remove an OAB virtual directory.

1. To get the default OAB virtual directory's settings, run the following command.

```
Get-OABVirtualDirectory -Identity "OAB (Default Web Site)" | fl | Out-
```

2. Record the settings for the *PollInterval*, *OfflineAddressBooks*, *RequireSSL*, *Path*, *InternalURL*, and *ExternalURL* parameters.
3. To delete the default OAB virtual directory, run the following command.

```
Remove-OABVirtualDirectory -Identity "OAB (Default Web Site)"
```

4. Type **Y** to confirm that you want to remove the OAB virtual directory, and then press ENTER. If the OAB virtual directory that you are removing has OABs connecting to it, you will receive another warning indicating that you must designate another OAB virtual directory.
5. Create an OAB virtual directory that has the same settings as the OAB that you removed, except the settings for the *OfflineAddressBooks* parameter. You will reconnect the OABs in the next step. For instructions about how to create an OAB virtual directory, see Create an Offline Address Book Virtual Directory.
6. Reconnect any OABs that use the Web-based distribution method to the new OAB virtual directory. For instructions about how to reconnect OABs to a virtual directory, see Configure Offline Address Book Properties.

For detailed syntax and parameter information, see Remove-OABVirtualDirectory.

Require SSL for Offline Address Book Distribution

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use Internet Information Services (IIS) Manager and the Shell to configure the virtual directory to use Secure Sockets Layer (SSL) for an offline address book (OAB). By default, when you install the Client Access server role on a computer running Microsoft Exchange Server 2010, a virtual directory named OAB is created on the default IIS Web site on the Exchange server.

When SSL is enabled, both SSL and unencrypted requests to the OAB virtual directory are allowed. You can disallow unencrypted requests by performing the procedures detailed later in this topic.

Looking for other management tasks related to OABs? Check out Managing Offline Address Books.

Prerequisites

- To learn more about the various security and authentication related options that are available, we recommend that you first read Securing Client Access Servers.
- After you obtain a valid SSL certificate to use with the Client Access server on the OAB default Web site or on the Web site where you host your OAB virtual directory, you should test SSL connectivity by issuing an HTTPS request. Using your browser, type the following URL in the address bar: **https://<server name>/**. The request should return your server's home page. You can configure the Web site to require SSL. You can also enable SSL for one or more Web sites hosted by the Client Access server. For more information, see Securing Client Access Servers.

Step 1: Use Internet Information Services 7 Manager to set up the default Web site for OAB to require SSL

To perform this procedure, you must be a member of the Administrators group on the local computer.

1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the console tree of **Internet Information Services (IIS) 7 Manager**, expand the Client Access server on which you are going to configure IIS.
3. Expand **Sites**, expand **Default Web Site**, and then click **OAB**.
4. In the result pane, double-click **SSL Settings**.
5. In the **SSL Settings** property page, select the **Require SSL** check box, and then select the **Require 128-bit SSL** check box.
6. In the action pane, click **Apply**.

Step 2: Use the Shell to set up the OAB virtual directory to require SSL

verification and to use an SSL-enabled external Web site

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "OAB virtual directory" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to set up the OAB virtual directory to require SSL verification and to use an SSL-enabled external Web site.

To set up the OAB virtual directory to require SSL verification and to use an SSL-enabled external Web site, use the following syntax.

```
Set-OABVirtualDirectory -Identity <VirtualDirectoryIdParameter> -RequireSSL <$tru
```

This example requires SSL for the OAB default Web site with an external URL for the Contoso company.

```
Set-OABVirtualDirectory -Identity "OAB (Default Web Site)" -RequireSSL $true -Ext
```

For detailed syntax and parameter information, see Set-OABVirtualDirectory.

1.8.3.21 Managing Public Folders

Managing Public Folders

Exchange Server 2010 > Mailbox > Managing Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-20*

Change the Default Public Folder Database for a Mailbox Database

Create a Public Folder

Configure Public Folder Properties

Configure Public Folder Referrals

Configure Public Folder Replication

Mail-Disable a Public Folder

Mail-Enable a Public Folder

Managing Public Folder Databases

Remove Public Folders

Resume Public Folder Content Replication

Scripts for Managing Public Folders in the Exchange Management Shell

Set the Size Limit for Public Folder Replication Messages

Suspend Public Folder Content Replication

Update a Public Folder Hierarchy

Update Public Folders

View Public Folder Item Statistics

View Public Folder Statistics

1.8.3.21.1 Change the Default Public Folder Database for a Mailbox Database

Change the Default Public Folder Database for a Mailbox Database

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Each mailbox database is configured with a default public folder database. MAPI client applications, such as Microsoft Outlook, open a connection to the default public folder database and perform all hierarchy-based operations against the server that contains that database. These operations include viewing public folders, creating and deleting public folders, and querying for the location of public folder content.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Use the EMC to change the default public folder database for a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, select the mailbox database for which you want to change the default public folder database.
3. In the action pane, under the mailbox database name, click **Properties**.
4. In **<Mailbox Database Name> Properties**, click the **Client Settings** tab.
5. Next to the **Default public folder database** box, click **Browse**.
6. In **Select Public Folder Database**, select the public folder database from the list of public folder databases, and then click **OK**.
7. Click **OK**.

Use the Shell to change the default public folder database for a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database" entry in the Mailbox Permissions topic.

This example sets the public folder database PublicFolderDB1 as the default public folder database for the mailbox database Mailbox Database.

```
Set-MailboxDatabase -Identity "Mailbox Database" -PublicFolderDatabase "PublicFol
```

For detailed syntax and parameter information, see Set-MailboxDatabase.

1.8.3.21.2 Create a Public Folder

Create a Public Folder

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Public folders are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization. Public folders are hierarchically organized, stored in dedicated databases, and can be replicated between Exchange servers.

When you create a public folder, the only required attribute is the folder name. After the folder has been created, you can edit the public folder to configure other folder properties. For more information, see Configure Public Folder Properties.

Caution:

By default, a public folder inherits the settings of its parent folder, including the permissions settings.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Prerequisite

You can't create public folders until you have created a public folder database. For detailed instructions, see Create a Public Folder Database.

What Do You Want to Do?

- Use the EMC to create a public folder
- Use the Shell to create a public folder

Note:

You can also create public folders by using a client program such as Outlook.

Use the EMC to create a public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the public folder tree of the Public Folder Management Console, navigate to **Default Public Folders**, and then select the parent public folder for the public folder you want to create.
4. In the action pane, click **New Public Folder**.
5. On the **Introduction** page, complete the following fields:

- **Name** Use this box to type the name of the new public folder.
- **Path** Use this read-only box to verify the path to the public folder. If this box displays a backslash (****), the public folder that you are creating will be a top-level public folder.

Note:
To change the path, close the wizard, and then, in the Public Folder Management Console, select the public folder under which you want to create this public folder, and start the wizard again.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. Click **Finish** to close the wizard.

Use the Shell to create a public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

This example creates a public folder in the root of the public folder tree on the closest Mailbox server that has a public folder database.

```
New-PublicFolder -Name "My Public Folder"
```

Note:
If you don't specify a server, the cmdlet checks if the local server is an Exchange 2007 or later Mailbox server that has a public folder database. If it is, the public folder is created locally. If it isn't, Exchange finds the closest (by site cost) Exchange 2007 or later Mailbox server that has a public folder database on which to create the public folder.

This example creates the public folder Pending in the existing public folder Legal on the Mailbox server My Server.

```
New-PublicFolder -Name "Pending" -Path \Legal -Server "My Server"
```

For syntax and parameter information, see New-PublicFolder.

Other Tasks

After you create a public folder, you may also want to:

- Mail-Enable a Public Folder
- Configure Public Folder Properties

For More Information

Understanding Public Folders

Managing Public Folders

1.8.3.21.3 Configure Public Folder Properties

Configure Public Folder Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Public folders in Exchange Server 2010 are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization. Public folders are hierarchically organized, stored in dedicated databases, and can be replicated between Exchange servers.

Note:
By default, a public folder inherits the settings of its parent folder, including the permissions settings.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

What Do You Want to Do?

- Use the EMC to configure public folder properties
- Use the EMC to overwrite child public folder settings with the parent public folder settings
- Use the Shell to configure public folder properties

Use the EMC to configure public folder properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the console tree of the Public Folder Management Console, expand **Default Public Folders**, and then click the parent public folder of the public folder you want to configure.
4. In the result pane, click the public folder you want, and then, in the action pane, click **Properties**.
5. Use the **General** tab to view the properties of a public folder or to change the public folder's name.
   - **Name** Use this unlabeled box to view or modify the display name for the public folder.
   - **Path** This read-only field displays the path to the public folder.
   - **Total items** This read-only field displays the number of items in the public folder.
   - **Size (KB)** This read-only field displays the public folder's size in kilobytes (KB).
   - **Public folder database** This read-only field displays the name of the public folder database that contains this public folder.
   - **Modified** This read-only field displays the last date and time a configuration change was made.

     Note:
     Configuration changes made through any other method, such as

the Exchange Management Shell or Active Directory Service Interfaces (ADSI) Edit, will also update this field.

- **Maintain per-user read and unread information for this folder** Select this check box to allow the user to see if a public folder message has been read or unread in Outlook.

6. Use the **Statistics** tab to view the number of associated items in a public folder, the total size of associated and deleted items, the owner and contact count, and the last time the public folder was accessed.
   - **Associated items** This read-only field displays the number of associated items in a public folder. Associated items include rules configured on the public folder, categories that are set on posts in a public folder, and more.
   - **Total size of associated items (KB)** This read-only field displays the size, in kilobytes, of the associated items in a public folder.
   - **Total size of deleted items (KB)** This read-only field displays the size, in kilobytes, of the deleted items in a public folder. The size of a public folder's deleted items is calculated independently of the public folder size displayed on the **General** tab.
   - **Owner count** This read-only field displays the number of owners specified on a public folder.
   - **Contact count** This read-only field displays the number of contacts specified on a public folder.
   - **Last access time** This read-only field displays the last time the public folder was accessed.

7. Use the **Replication** tab to view and set the content replication schedule and to specify the databases on which the public folder content will be replicated. To learn more, see Understanding Public Folder Replication.
   - **Replicate content to these public folder databases**

     Add Click this button to open the **Select Public Folder Database** dialog box. Use this dialog box to specify which public folder databases this public folder should be replicated to. Select the public folder database, and then click **OK**.

      Select a database from the list, and then click this button to remove it from the replication list.
   - **Use public folder database replication schedule** Select this check box to use the replication schedule that is set on the public folder database. This check box is selected by default. To manually set the replication schedule, clear this check box and then select from the options in the corresponding list. If you select **Use Custom Schedule**, click **Customize** to open the **Schedule** dialog box, and then specify the times that you want replication to occur.
   - **Local replica age limit (days)** Use this text box to specify the age limit for items in this public folder. Items that have reached the specified age limit are deleted.

8. Use the **Limits** tab to view or configure storage quotas, deleted item retention, and age limits for the public folder.

   Storage quotas
   - **Use database quota defaults** Select this check box to use the public folder database quota limits on which the public folder resides. If you clear this check box, the **Issue warning at (KB)**, **Prohibit post at (KB)**, and **Maximum item size (KB)** check boxes are made available.
   - **Issue warning at (KB)** Select this check box to automatically warn public folder owners that the public folder is approaching its storage limit.

     To specify this limit, select the check box, and then specify the size of the public folder in kilobytes (KB) at which you want to prohibit posting. You can enter a value between 0 and 2,147,483,647 KB (2.1 terabytes).

- **Prohibit post at (KB)** Select this check box to prevent posting to the public folder after the size of the folder reaches the specified limit.
  To specify this limit, select the check box, and then specify the size of the public folder in KB at which you want to prohibit posting. You can enter a value between 0 and 2,147,483,647 KB (2.1 terabytes).
- **Maximum item size (KB)** Select this check box to limit the maximum size of items that users can post to the public folder.
  To specify the size, select the check box, and then specify the maximum size of items in KB that users can post to the public folders. You can enter a value between 0 and 2,097,151 KB.

Deleted item retention

- **Use database retention defaults** Select this check box to use the public folder database item retention limits on which this public folder resides. If you clear this check box, the **Retain deleted items for (days)** check box is made available.
- **Retain deleted items for (days)** Select this check box to set the number of days that deleted items are retained in a public folder. You can enter a value between 0 and 24,855 days.

Age limits

- **Use database age defaults** Select this check box to use the public folder database age limits on which this public folder resides. If you clear this check box, the **Age limit for replicas (days)** check box is made available.
- **Age limit for replicas (days)** Select this check box to limit the age of the public folder. Use the corresponding text box to specify the age limit in days. Replicas of this public folder are automatically deleted when the age limit is exceeded. You can enter a value between 0 and 24,855 days.

9. Use the **Permissions** tab to add user permissions to or remove user permissions from the selected public folder.
   - **Add** Click this button to add a user. After you add the user, you must select the permissions you want them to have.
   -  Click this button to remove a user's permissions to the public folder.
   - **Permission Level** Use this list and the associated check boxes to assign permissions to the selected user. For more information about the permissions and the level of access that each one grants, see the "Client User Access Rights and Roles" section of Understanding Public Folder Permissions.

10. (This tab appears only for mail-enabled public folders.)
    Use the **Exchange General** tab to view and configure the general settings of a mail-enabled public folder.
    - **Alias** Use this box to view or modify the alias for the mail-enabled public folder.
    - **Display name** Use this box to view or modify the display name for the public folder. This is the name that the public folder displays in the global address list (GAL).
    - **Simple display name** Use this box to view or modify the simple display name for the mail-enabled public folder. This field accepts only ASCII characters.
      The **Display name** field (located on the **General** tab) can contain Unicode characters. However, third-party applications and older client applications may not support Unicode characters. If the system that is displaying the public folder doesn't support Unicode characters, the simple display name can be used. For more information about Unicode characters, see Unicode.
    - **Hide from Exchange address lists** Select this check box to prevent the recipient from appearing in the global address list (GAL) and other address lists that are defined in your Exchange organization.

After you select this check box, users in your Exchange organization can still send messages to the recipient by using the e-mail address.

- **Custom Attributes** Click this button to open the **Custom Attributes** dialog box. You can specify up to 15 custom attributes for the recipient. To specify the custom attribute values, use the corresponding boxes, and then click **OK**. To learn more, see Understanding Custom Attributes.

11.(This tab appears only for mail-enabled public folders.)
Use the **E-Mail Addresses** tab to configure the e-mail addresses for the recipient. You can modify the existing addresses or create additional ones. Each recipient must have at least one primary STMP address that is internal to your Exchange organization and one external address.

- **Add** Click **Add** to add a new e-mail address for this recipient. Use the drop-down box to select from the following address types:
  SMTP Address This is the default address type. Click this button and use the corresponding dialog box to add an SMTP address.
  EUM Address This address type is available only for user mailboxes. It's not available for mail users, mail contacts, distribution groups, or mail-enabled public folders. An EUM (Exchange Unified Messaging) address is used by Unified Messaging servers to locate UM-enabled users within an Exchange 2010 organization. EUM addresses contain the extension number and the UM dial plan for the UM-enabled user. Click this button and use the corresponding dialog box to add an EUM address.
  Custom Address Click this button and use the corresponding dialog box to add a custom address (for example, fax or X.400).

  Note:
  With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.

- **Edit** Click this button to modify the selected e-mail address.
-  Click this button to remove the selected e-mail address.
- **Set as Reply** Click this button to set your selected address as the "reply to" address. A recipient can have multiple e-mail addresses for a specific address type. This allows the recipient to receive messages that are addressed to any one of these e-mail addresses. However, a single address must be used for any messages that are sent by the recipient. If a recipient has multiple e-mail addresses, the primary address is used for any messages sent by the recipient.
  This button is available only when an address other than the primary address is selected. Primary addresses for each address type are displayed in bold type.
  If an e-mail address policy in your Exchange organization applies to this mailbox, the **Set as Reply** setting will be controlled by that policy. To change the primary address for a specific address type, you must clear the **Automatically update e-mail addresses based on e-mail address policy** check box.
- **Set as External** This button is available only for mail users and mail contacts. It's not available for user mailboxes, distribution groups, or mail-enabled public folders. Click **Set as External** to designate the selected e-mail address as the external e-mail address for the recipient.

  Note:
  This button is enabled when an address other than the external e-mail address is selected.

- **Automatically update e-mail addresses based on e-mail address policy** Select this check box to have the recipient's e-mail addresses automatically updated based on changes made to e-mail address policies in your organization. This box is selected by default.

12.(This tab appears only for mail-enabled public folders.)
Use the **Member Of** tab to view a list of the groups to which this recipient belongs. Some of these groups may not be mail-enabled. Mail-enabled groups will have an envelope icon next to them. You can't use this tab to modify membership information. The recipient may match the criteria for one or more dynamic distribution groups in your organization. However, dynamic distribution groups aren't displayed on this tab because their membership is calculated each time they are used. For more information, see Managing Distribution Groups.

13.(This tab appears only for mail-enabled public folders.)
Use the **Mail Flow Settings** tab to configure delivery options and message size or message delivery restrictions for the mail-enabled public folder.

- **Delivery Options** Select this setting and then click **Properties** to open the **Delivery Options** dialog box. Use this dialog box to configure the following settings:
  Send on behalf Click **Add** to open the **Select Mailbox or Mail-Enabled User** dialog box. Use this dialog box to grant a recipient the permissions to send e-mail on behalf of the selected public folder. Click  to remove a recipient from the list.
  Forward to Select this check box, and then click **Browse** to open the **Select Recipient** dialog box. Use this dialog box to select a recipient to whom you want to forward all e-mail messages that are sent to this public folder.
  Deliver message to both forwarding address and mailbox If you selected the **Forward to** check box, you can select this check box to specify that e-mail messages be delivered to both the public folder and to the forwarding address.
- **Message Size Restrictions** Select this setting and then click **Properties** to open the **Message Size Restrictions** dialog box. In this dialog box, use the **Maximum message size (in KB)** check boxes to set the maximum size for messages that can be sent and received by this recipient. Use the corresponding text boxes to type the maximum message size allowed (in KB). The message size must be between 0 and 2,097,151 KB. If a message larger than the specified size is sent to the recipient, the message will be returned to the sender with a descriptive error message.
- **Message Delivery Restrictions** Select this setting and then click **Properties** to open the **Message Delivery Restrictions** dialog box. Use this dialog box to configure the following settings:
  All senders Click this button to specify that the recipient can accept messages from all senders. This includes senders in both your Exchange organization and external senders. This button is selected by default. This option includes external users only if you clear the **Require that all senders are authenticated** check box. If you select this check box, messages from external users will be rejected.
  Only senders in the following list Click this button to specify that the recipient can accept messages only from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.

Require that all senders are authenticated Select this check box to prevent anonymous users from sending messages to the recipient.
No senders Click this button to specify that the recipient will not reject messages from any senders in the Exchange organization. This button is selected by default.
Senders in the following list Click this button to specify that the recipient will reject messages from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now.**

Use the EMC to overwrite child public folder settings with the parent public folder settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder client permissions" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, double-click **Public Folder Management Console**.
3. In the public folder tree of the Public Folder Management Console, expand **Default Public Folders**, and then click the parent public folder of the public folder you want to configure.
4. In the result pane, click the public folder you want to configure.
5. In the action pane, click **Manage Settings**.
6. On the **Introduction** page, click **Overwrite Settings** to override the child public folder settings with the selected parent public folder settings. You can overwrite the age limits, keep per-user read/unread state, replicas, and replication schedule. This option is available only if the public folder that you're modifying has one or more child public folders.
7. On the **Select Settings** page, select the settings to overwrite. For more information about the settings you can configure, see Configure Public Folder Properties.
   - **Age limits** Select this check box to copy the selected public folder's age limits to the child public folders.
   - **Keep per user read/unread state** Select this check box to copy the selected public folder's per-user read/unread settings to the child public folders. This setting allows users to see if a public folder message has been read or unread in Microsoft Outlook.
   - **Replicas** Select this check box to copy the selected public folder's replica settings to the child public folders.
   - **Replication schedule** Select this check box to copy the selected public folder's replication schedule to the child public folders.
8. On the **Overwrite Settings** page, review your configuration settings. Click **Overwrite** to overwrite the child public folder settings with the selected public folder. Click **Back** to make configuration changes.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

10.Click **Finish** to close the wizard.

Use the Shell to configure public folder properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

Use the **Set-MailPublicFolder** cmdlet to configure public folder properties.

This example sets the primary SMTP address of the public folder Sales to MyMailPublicFolder@contoso.com.

```
Set-MailPublicFolder -Identity "\Sales" -PrimarySmtpAddress MyMailPublicFolder@co
```

Note:
You cannot change the primary SMTP e-mail address if the *EmailAddressEnabled* parameter is set to true.

This example disables the e-mail address policy of the mail-enabled public folder Sales.

```
Set-MailPublicFolder -Identity "\Sales" -EmailAddressEnabled $False
```

This example assigns a value (string) to the first custom attribute of the mail-enabled public folder Sales.

```
Set-MailPublicFolder -Identity "\Sales" -CustomAttribute1 "This string is the val
```

This example sets a 200 megabyte (MB) size limit for the mail-enabled public folder Sales, after which the folder can no longer send e-mail messages.

```
Set-MailPublicFolder -Identity "\Sales" -SendStorageQuota 200MB
```

For More Information

Understanding Recipients

Mail-Enable a Public Folder

Managing Public Folders

1.8.3.21.4 Configure Public Folder Referrals

Configure Public Folder Referrals

Mailbox > Managing Mailbox Servers > Managing Public Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Public folder referrals have an associated *cost number*. The numbers range from 1 through 100. This cost number is used to optimize message flow. Specifically, e-mail messages are routed according to lowest cost number. If two or more routes are available with the same cost, the load is distributed as equally as possible between them. This cost is also used to calculate the most appropriate route that the client application (such as Microsoft Outlook) can use to access public folders on remote servers.

The maximum public folder referral cost that you can set for a public folder database is 100. However, by setting the maximum referral cost for a server to 100, the server may still be used for referrals. If you want to decrease the chances of the server being used for referrals, you should work with your domain administrator or enterprise administrator to configure site link costs.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Use the EMC to configure public folder referrals

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder databases" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, select the public folder database that you want to modify.
3. In the action pane, under the name of the public folder database, click **Properties**.
4. In **<Public Folder Database> Properties**, click the **Public Folder Referral** tab.
5. To specify that Exchange uses the cost data from the Active Directory site to compute the connection cost for public folder referrals, click **Use Active Directory site costs**. This is the default option.

   Note:

   If the custom list contains public folder referrals and you click **Use Active Directory sites costs**, the list is unavailable and is cleared when this tab is refreshed.

6. To create a custom public folder referrals list and the associated costs, click **Use custom list**, click **Add**, and then perform following steps:
   6.a. Click **Browse**.
   6.b. In **Select Referral Server**, select the Mailbox server on which a public folder database resides, and then click **OK**.

   Note:

   You can't select a server that's already in the list of servers that appear in the **Name** column on the **Public Folder Referral** tab, nor can you select the server on which the specified public folder database resides.

   6.c. In the **Cost** box, assign a cost number from **1** through **100**, and then click **OK**. The number 1 represents the lowest cost, which means that Exchange routing is more likely to use this as the replica server. The number 100 represents the highest cost, which means that Exchange routing is less likely to use this as the replica server.
7. To add additional servers to the referral list, on the **Public Folder Referral** tab, click **Add**, and then repeat Steps a through c.
8. Click **OK** to close **<Public Folder Database> Properties**.

Use the Shell to configure public folder referrals

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder databases" entry in the Mailbox Permissions topic.

This example configures public folder referrals.

```
Set-PublicFolderDatabase -Identity "Server1\PublicFolderDatabase01" -UseCustomRef
```

Note:
The *CustomReferralServerList* parameter accepts an array in the following format: **serverID:cost**. Separate multiple servers with a comma.

For detailed syntax and parameter information, see Set-PublicFolderDatabase.

1.8.3.21.5 Configure Public Folder Replication

Configure Public Folder Replication

Mailbox > Managing Mailbox Servers > Managing Public Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) or the Exchange Management Shell to configure public folder replication and to set the public folder replication schedule for a specific public folder. For information about how to configure the public folder replication schedule for a public folder database, see Set the Replication Schedule for a Public Folder Database.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Use the EMC to configure public folder replication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder replication" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Public Folder Management Console**.
3. In the action pane, click **Open Tool**. The Public Folder Management Console appears.
4. In the public folder tree, click or expand **Default Public Folders**, and then select the parent public folder of the public folder that you want to configure.

   Note:
   To configure replication for the offline address book (OAB) or for Schedule+ free and busy information, expand **System Public Folders**, and then click **OFFLINE ADDRESS BOOK** or **SCHEDULE+ FREE BUSY**.
5. In the result pane, select the public folder for which you want to configure replication.
6. In the action pane, click **Properties.**
7. In **<Public Folder> Properties**, click the **Replication** tab.
8. To add a public folder database to the list of replicas, click **Add**.
9. In **Select Public Folder Database**, select the public folder database on which to replicate the public folder, and then click **OK**.
10. By default, Exchange uses the replication schedule set on the public folder database. To create a custom replication schedule for the public folder, clear the **Use public folder database replication schedule** check box and use the

following settings in the corresponding list:

- **Never Run** The public folder is not replicated.
- **Always Run** The replication process is initiated during the replication interval set for the public folder database.
- **Run every hour** The replication process is initiated every hour.
- **Run every 2 hours** The replication process is initiated every 2 hours.
- **Run every 4 hours** The replication process is initiated every 4 hours.
- **Use Custom Schedule** The replication process uses the customized schedule that you create in Step 12.

11. To create a customized schedule, click **Customize**.

Note:
If you want to use a customized schedule, you must select **Use Custom Schedule** from the interval list.

12. To set the schedule, click the time grid in the **Schedule** dialog box. Public folder replication will run during the time slots that you specify. You can select the same time slot every day by clicking a column header for a specific time slot. You can select an entire day by clicking the name of that day.

Note:
The default time slot for the grid is one hour. For finer control, you can change the schedule grid to 15 minute intervals by clicking **15 minute**. Scheduled intervals must be at least 15 minutes apart.

13. Click **OK** to close the **Schedule** dialog box.
14. To specify the age limit for items in this public folder, type the number of days in the **Local replica age limit (days)** box. Items that have reached the age limit are deleted.
15. Click **OK** to close **<Public Folder> Properties** and to save your changes.

Use the Shell to configure public folder replication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder replication" entry in the Mailbox Permissions topic.

This example sets the public folder My Public Folder so that it doesn't use the default replication schedule of the public folder database and replicates to PFDatabase02 on Server02 and PFDatabase03 on Server03.

```
Set-PublicFolder "\My Public Folder" -UseDatabaseReplicationSchedule: $False -Rep
```

This example sets a public folder so that it always uses the default replication schedule of the public folder database.

```
Set-PublicFolder "\My Public Folder" -ReplicationSchedule Always
```

This example sets a public folder so that it replicates only during the weekend.

```
Set-PublicFolder \MyPublicFolder -ReplicationSchedule "Saturday.12:00 AM-Monday.1
```

Note:
The public folder replication schedule uses the format: "Weekday.Hour:Minute [AM/PM]-Weekday.Hour:Minute [AM/PM]"

For detailed syntax and parameter information, see Set-PublicFolder.

1.8.3.21.6 Mail-Disable a Public Folder

Mail-Disable a Public Folder

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) or the Exchange Management Shell to mail-disable a public folder.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Use the EMC to mail-disable a public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Public Folder Management Console**.
3. In the action pane, click **Open Tool**. The Public Folder Management Console appears.
4. In the public folder tree, click or expand **Default Public Folders**, and then if any public folders are displayed in the result pane, select the parent folder of the public folder that you want to mail-disable.
5. In the result pane, select the public folder that you want to mail-disable.
6. In the action pane, click **Mail Disable**. A warning dialog box appears.
7. Click **Yes** to confirm that you want to mail-disable the public folder.
8. To indicate that this is a mail-disabled public folder, the icon for the public folder changes.
   Mail-disabled public folders are represented by the following icon.
   
   Mail-enabled public folders are represented by the following icon.
   

Use the Shell to mail-disable a public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

This example mail-disables the public folder My Public Folder.

```
Disable-MailPublicFolder -Identity "\My Public Folder"
```

This example mail-disables the public folder My Public Folder on the server Server01.

```
Disable-MailPublicFolder -Identity "\My Public Folder" -Server "Server01"
```

For detailed syntax and parameter information, see Disable-MailPublicFolder.

1.8.3.21.7 Mail-Enable a Public Folder

Mail-Enable a Public Folder

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Shell or the Exchange Management Console (EMC) to mail-enable public folders.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Important:

To ensure that users can send e-mail messages to a mail-enabled public folder, the public folder must have at least the *CreateItems* access right granted to the Anonymous account.

Use the EMC to mail-enable a public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Public Folder Management Console**.
3. In the action pane, click **Open Tool**. The Public Folder Management Console appears.
4. In the public folder tree, click or expand **Default Public Folders**, and then if any public folders are displayed in the result pane, select the parent folder of the public folder that you want to mail-enable.
5. In the result pane, select the public folder that you want to mail-enable.
6. In the action pane, click **Mail Enable**.
7. To indicate that this is a mail-enabled public folder, the icon for the public folder changes.
   Mail-enabled public folders are represented by the following icon.

Public folders that aren't mail-enabled are represented by the following icon.

Use the Shell to mail-enable a public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

This example mail-enables the public folder My Public Folder.

```
Enable-MailPublicFolder -Identity "\My Public Folder"
```

This example mail-enables the public folder My Public Folder on the server Server01.

```
Enable-MailPublicFolder -Identity "\My Public Folder" -Server "Server01"
```

Note:

If you don't specify a server, the cmdlet checks whether the local server is an Exchange Mailbox server that contains a public folder database. If it is, the public folder is created

locally. If it isn't, Exchange finds the closest (by site cost) Exchange Mailbox server that has a public folder database on which to create the public folder.

This example mail-enables the public folder My Public Folder, but hides the folder from address lists.

```
Enable-MailPublicFolder -Identity "\My Public Folder" -HiddenFromAddressListsEnab
```

For detailed syntax and parameter information, see Enable-MailPublicFolder.

1.8.3.21.8 Managing Public Folder Databases

Managing Public Folder Databases

Mailbox > Managing Mailbox Servers > Managing Public Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-14*

1.8.3.21.8.1 Create a Public Folder Database

Create a Public Folder Database

Managing Mailbox Servers > Managing Public Folders > Managing Public Folder Databases >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Public folders are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization. A public folder database is a database that stores public folders, indexes their contents, and assists in the replication of the folders with other servers. A public folder database is stored as an Exchange database (.edb) file.

Important:

Before you perform this procedure, be aware that a server can contain only one public folder database.

Looking for other management tasks related to public folder databases? Check out Managing Public Folder Databases.

What Do You Want to Do?

Use the EMC to create a public folder database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder databases" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Public Folder Database**.
3. On the **Introduction** page, complete the following fields:
   - **Public folder database name** Use this box to type the name of the new public folder database.
   - **Server name** This box lets you specify where to create the public folder database. To specify a location click **Browse** to open the **Select Mailbox Server** dialog box. Use this dialog box to select the server where you want to create the public folder database, and then click **OK**.
4. On the **Set Paths** page, complete the following fields:
   - **Database file path** This box is automatically populated with the default path to the database file. To specify a different location or file name, type the location in the box.
   - **Log folder path** This box is automatically populated with the default path to the database log files. To specify a different location, type the location in the box.
   - **Mount this database** Select this check box to mount the database immediately after it is created.
5. On the **New Public Folder Database** page, review your configuration settings. Click **New** to create the public folder database. Click **Back** to make changes. Click **Cancel** to close the wizard without creating the public folder database.
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
7. Click **Finish** to close the wizard.

Use the Shell to create a public folder database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder databases" entry in the Mailbox Permissions topic.

Use the **New-PublicFolderDatabase** cmdlet to create a new public folder database. When you create a new public folder database, you must specify the server on which to

create it. If you don't specify the public folder database file path, database file name, or the database log file path, the following default values are used:

- **Public folder database and filename** <installation location>\V14 \Mailbox\<database name>\<database name>.edb
- **Public folder database log file path** <installation location>\V14 \Mailbox\<database name>

By default, public folder databases are dismounted when created. You must mount the database manually after it's created by using the **Mount-Database** cmdlet.

This example creates the public folder database Public Folders on the server SERVER01 with the default database locations.

```
New-PublicFolderDatabase "Public Folders" -Server SERVER01
```

This example mounts the database Public Folders.

```
Mount-Database "Public Folders"
```

To specify database and database log locations you can use the *EdbFilePath* and *LogFilePath* parameters respectively. This example creates the public folder database Support on the server SERVER02 with alternate database and log locations.:

```
New-PublicFolderDatabase Support -Server SERVER02 -EdbFilePath E:\Databases\Suppo
```

This example mounts the database Support.

```
Mount-Database Support
```

For More Information

Understanding Public Folders

View or Configure Public Folder Database Properties

1.8.3.21.8.2 View or Configure Public Folder Database Properties

View or Configure Public Folder Database Properties

Managing Mailbox Servers > Managing Public Folders > Managing Public Folder Databases >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Public folders are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization. A public folder database is a database that stores public folders, indexes their contents, and assists in the replication of the folders with other servers. A public folder database is stored as an Exchange database (.edb) file.

Looking for other management tasks related to public folder databases? Check out Managing Public Folder Databases.

What Do You Want to Do?

- Use the EMC to view or configure public folder database properties

- Use the Shell to configure public folder database properties
- Use the Shell to view public folder database properties

Use the EMC to view or configure public folder database properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder databases" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab, and then select the public folder database you want to configure.
3. In the action pane, click **Properties**.
4. Use the **General** tab to view or configure the properties of a public folder database, to change its name, and to customize its maintenance schedule.
   - **Name** This unlabeled box at the top of the tab displays the name of the public folder database. You can modify this name.
   - **Database path** This read-only field displays the full path to the Exchange database (.edb) file for the selected public folder database. To view the entire path, you may have to click the path and use the RIGHT ARROW key.
     You cannot use this field to change the path. To change the location of the database files, close **Properties**, right-click the public folder database, and then click **Move Database Files**. You can also change the location by using the Move-DatabasePath cmdlet in the Exchange Management Shell.
   - **Last full backup** This read-only field displays the date and time of the last complete backup of the public folder database.
   - **Last incremental backup** This read-only field displays the date and time of the last incremental backup of the public folder database.
   - **Status** This read-only field displays whether the public folder database is mounted or dismounted.
     For information about how to mount or dismount a database, see the following topics:
     Mount a Database
     Dismount a Database
   - **Modified** This read-only field displays the last date and time that the public folder database was modified.
   - **Maintenance schedule** Use this list to select one of the preset maintenance schedules.
     You can also configure a custom schedule. To configure a custom schedule, in the **Maintenance schedule** list, select **Use Custom Schedule**, and then click **Customize**.
   - **Enable background database maintenance (24 x7 ESE scanning)** Select this check box to enable background database maintenance. If you select this check box, the Extensible Storage Engine (ESE) performs the database maintenance, and the public folder database reads the object during database mount and initializes the database to perform the background database maintenance. If you don't select this check box, the public folder database reads the object during database mount and initializes the database without the option to perform the background database maintenance.
   - **Don't mount this database at startup** Select this check box to prevent Exchange from mounting this public folder database when it starts.
   - **This database can be overwritten by a restore** Select this check box to allow the public folder database to be overwritten during a restore process.
   - **Enable circular logging** Click this check box to enable circular logging.

Circular logging overwrites and reuses a single log file after the data it contains has been written to the database. Circular logging is disabled by default. By enabling circular logging, you reduce drive storage space requirements. However, you can't recover anything more recent than the last full (normal) backup because the transaction logs no longer contain all the transactions that were completed since the last backup. Therefore, in a normal production environment, circular logging isn't recommended.

5. Use the **Replication** tab to specify the public folder database replication interval and the replication message size limit.
   - **Replication interval** Use this list to set the interval at which replication of public folders or content updates may occur.
     To schedule a custom replication interval, select **Use Custom Schedule** from the list, and then click **Customize**. Use the **Schedule** dialog box to customize the replication schedule, and then click **OK** to return to the **Replication** tab.
   - **Replication interval for "Always Run" (minutes)** If you set the replication interval to **Always Run**, this box displays the time interval (in minutes) during which replication of public folders or contents may occur. You can modify this interval. The value range is from 1 through 2,147,483,647 minutes.
   - **Replication message size limit (KB)** This box displays the size limit in kilobytes (KB) of a replication message. Small items may be aggregated into a single replication message that can be as large as this setting, but items larger than this setting are replicated with messages larger than this size. You can modify this size limit. The value range is from 1 through 2,097,151 KB.

6. Use the **Limits** tab to specify the storage limits, warning message interval, deletion settings, and age limits for all public folders in the selected public folder database.
   - **Issue warning at (MB)** Select this check box to automatically warn public folder owners that the public folder is approaching its storage limit.
     To specify the storage limit, select the check box, and then specify in megabytes (MB) how much content can be stored in the public folder before a warning e-mail message is sent to the folder's owner. You can enter a value from 0 through 2,097,151 MB (2.0 terabytes)
   - **Prohibit post at (MB)** Select this check box to prevent posting to the public folders in the database after the size of folder reaches the specified limit.
     To specify this limit, select the check box, and then specify the size of the public folder in megabytes (MB) at which you want to prohibit posting. You can enter a value from 0 through 2,097,151 MB (2.0 terabytes)
   - **Maximum item size (MB)** Select this check box to limit the maximum size of items that users can post to the public folders in the database.
     To specify the size, select the check box, and then specify the maximum size of items in megabytes (MB) that users can post to the public folders. You can enter a value from 0 through 2,097,151 MB (2.0 terabytes)
     Warning message interval Use this list to display the interval at which you want warning messages to be generated. To select one of the default intervals, click the list, and then select one of the following:
     Run daily at midnight
     Run daily at 1:00 AM
     Run daily at 2:00 AM
     Use Custom Schedule
     If you select **Use Custom Schedule**, you must click **Customize**

to set the schedule.

- **Keep deleted items for (days)** Use this box to set the numbers of days that deleted items are retained in a public folder. You can enter a value between 0 and 24,855 days.
- **Don't permanently delete items until the database has been backed up** Select this check box to prevent items from being permanently deleted until after the public folder database is backed up.
- **Age limit for all folders in this public folder database (days)** Select this check box to limit the age of all folders in this public folder database. Use the text box to specify the age limit in days. You can enter a value between 0 and 24,855 days.

7. Use the **Public Folder Referral** tab to configure the folder replica that will be accessed by the client application. To learn more, see Understanding Public Folder Referrals.
   - **Use Active Directory site costs** Click this button to specify that Exchange uses the cost data from the Active Directory site to compute the connection cost for public folder referrals. This is the default option.

     Note:
     If the custom list contains public folder referrals, and you click **Use Active Directory site costs**, the list is unavailable and is cleared when this tab is refreshed.

   - **Use custom list** Click this button to create a custom list of public folder referrals and the associated costs.

     When you click **Use custom list**, the following features are made available:

     Note:
     If you click **Use Active Directory site costs**, these features are unavailable.

     Add Click this button to open the **Server Referral Cost** dialog box.
     Click **Browse** to open the **Select Referral Server** dialog box. Use this dialog box to select the referral server from the list of available servers that contain a public folder database and click OK.
     In the **Cost** box, assign a cost number between **1** and **100**. The number **1** represents the lowest cost, which means that Exchange routing is more likely to use this as the replica server. The number **100** represents the highest cost, which means that Exchange routing is less likely to use this as the replica server.
     Edit Select a server from the list, and then click this button to edit a public folder referral. This button is disabled if no servers are listed in the custom list.
      Click this button to remove a public folder referral from the custom list. This button is disabled if no servers are listed in the custom list.

Use the Shell to configure public folder database properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder databases" entry in the Mailbox Permissions topic.

This example changes the size of the maximum post that can be stored in the Sales public folder database to 1 GB and issues a warning when the post size reaches 900 MB.

```
Set-PublicFolderDatabase  Sales -IssueWarningQuota 900MB -ProhibitPostQuota 1GB
```

This example sets the database maintenance schedule on PFDB01 to run daily from 02:00 (2:00 A.M.) until 06:00 (6:00 A.M.).

```
Set-PublicFolderDatabase -Identity 'PFDB01'-MaintenanceSchedule 'Sun.2:00 AM-Sun.
```

This example sets the deleted items retention on the public folder database PFDB01 to 10 days.

```
Set-PublicFolderDatabase -Identity 'PFDB01' -DeletedItemRetention '10.00:00:00'
```

This example prevents the deleted items in the public folder database PFDB01 from being permanently deleted until after the database has been backed up.

```
Set-PublicFolderDatabase -RetainDeletedItemsUntilBackup $true -Identity 'PFDB01'
```

For syntax and parameter information, see Set-PublicFolderDatabase.

Use the Shell to view public folder database properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder databases" entry in the Mailbox Permissions topic.

Use the **Get-PublicFolderDatabase** cmdlet to view the properties of a public folder database. This command returns all the public folder databases in your organization.

```
Get-PublicFolderDatabase
```

To view all of the properties of a single public folder database, you can pipe the results of the **Get-PublicFolderDatabase** cmdlet to the **Format-List** cmdlet. This example gets the properties of the public folder database Support.

```
Get-PublicFolderDatabase Support | Format-List
```

For syntax and parameter information, see Get-PublicFolderDatabase.

1.8.3.21.8.3 Move Public Folder Content from One Public Folder Database to Another Public Folder Database

Move Public Folder Content from One Public Folder Database to Another Public Folder Database

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use scripts to move public folders to a different database or server.

Looking for other management tasks related to public folder databases? Check out Managing Public Folder Databases.

Use the MoveAllReplicas.ps1 script to move all public folder content from one server to another server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

To move all public folders in a public folder database on one server to a public folder database on another server, use the MoveAllReplicas.ps1 script. This script replaces a server with a new server in the replication list for all public folders, including system folders. For more information about using public folder scripts, see Scripts for Managing Public Folders in the Exchange Management Shell.

This example moves all public folder content from Server01 to Server02.

```
.\MoveAllReplicas.ps1 -Server Server01 -NewServer Server02
```

Use the ReplaceReplicaOnPFRecursive.ps1 script to move replicas in a public folder subtree to another server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

To move all the replicas of a public folder subtree from one server to another server, use the ReplaceReplicaOnPFRecursive.ps1 script. This script adds a new server to the replication list for a public folder and all the folders within that hierarchy. If the server is already listed in the replication list for a folder, nothing is changed for that folder. For more information about using public folder scripts, see Scripts for Managing Public Folders in the Exchange Management Shell.

This example moves the public folder replica Legal and all the folders within that hierarchy from Server01 to Server02.

```
.\ReplaceReplicaOnPFRecursive.ps1 -TopPublicFolder "\Legal" -ServerToAdd Server02
```


1.8.3.21.8.4 Remove Multiple Public Folders from a Public Folder Database

Remove Multiple Public Folders from a Public Folder Database

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to remove all the public folders from a public folder database.

This procedure removes all the user and system public folders from a public folder database. If you only want to remove one public folder from a public folder database, see Remove Public Folders. This procedure is required if you are removing the last public folder

database in your Exchange organization. For detailed instructions about how to remove public folder databases, see Remove Public Folder Databases.

Caution:
The **Remove-PublicFolder** cmdlet removes the public folder data from all servers in your organization. If you only want to remove data from one server, use the **Set-PublicFolder** cmdlet with the *Replicas* parameter. For more information, see Set-PublicFolder.

Looking for other management tasks related to public folder databases? Check out Managing Public Folder Databases.

Use the Shell to delete user public folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to delete user public folders.

This example removes all user public folders.

```
Get-PublicFolder -Server <server containing the public folder database> "\" -Recu
```

For detailed syntax and parameter information, see Get-PublicFolder and Remove-PublicFolder.

Use the Shell to delete system public folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to delete system public folders.

This example removes all system public folders.

```
Get-PublicFolder -Server <server containing the public folder database> "\Non_Ipm
```

For detailed syntax and parameter information, see Get-PublicFolder and Remove-PublicFolder.

1.8.3.21.8.5 Remove Public Folder Databases

Remove Public Folder Databases

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove a public folder database using the steps in this procedure. Links to detailed topics will help you complete the task.

The process for removing a public folder database requires several steps. Because this process is different if you're removing the last public folder database in your organization, consider the following scenarios before you begin:

- **Removing a public folder database from a Mailbox server** If you want to remove a public folder database from a Mailbox server, you must first move the data within the public folder database to a public folder database on another server, and then you remove the public folder database.
- **Removing the last public folder database from the organization** If you want to remove the last public folder database in your organization, you must first make sure that your organization doesn't contain any servers running Microsoft Exchange Server 2003 or earlier versions.

Caution:

If you remove the last public folder database, only users who are running Microsoft Office Outlook 2007 or later versions, or who are running Microsoft Office Outlook Web App, will be able to connect to your Exchange organization.

Important:

Don't remove the last public folder database if your organization uses public folders to distribute organizational forms or to replicate free/busy information to or from another Exchange organization.

Migrating public folders from Exchange 2003 to Exchange Server 2010? If so, you can use either Exchange System Manager in Exchange 2003 or the Exchange Management Console (EMC) in Exchange 2010 to move Exchange 2003 public folders to an Exchange 2010 server.

Looking for other management tasks related to public folder databases? Check out Managing Public Folder Databases.

Remove a public folder database from a Mailbox server

To remove a public folder database from a Mailbox server, perform the following steps.

Note:

If you have a mixed Exchange 2003 or Exchange Server 2007 and Exchange 2010 organization, we recommend that you perform these procedures against an Exchange 2010 server. For more information about performing public folder management tasks in mixed environments, see Understanding Public Folders.

Step 1: Delete unnecessary public folders

You can't delete a public folder database that contains data. To remove data from a public folder database, delete any unnecessary public folders. For detailed instructions, see Remove Public Folders. To determine which public folders are unnecessary, see View Public Folder Item Statistics.

Step 2: Move the public folder replicas to another server

After you delete any unnecessary public folders, you must move the remaining folder replicas in that database to a public folder database on another server.

Note:

Depending on the number of public folders, the amount of information in the database, and the replication interval, this process may take several hours to complete.

For detailed instructions, see Move Public Folder Content from One Public Folder Database to Another Public Folder Database.

Important:
Don't remove the public folder database until public folder replication has completed.

Step 3: Associate mailbox databases with another default public folder database

If the public folder database you're removing is being used as the default public folder database by any mailbox databases, you must configure another public folder database as the default public folder database.

This example identifies the public folder databases associated with all mailbox databases.

```
Get-MailboxDatabase | ft Name,PublicFolderDatabase
```

For more information about how to change the default public folder database, see Change the Default Public Folder Database for a Mailbox Database.

Step 4: Remove the public folder database

Note:
If you successfully perform Step 1 through Step 4 and you receive an error message stating that the public folder database can't be removed because it contains replicas, you may need to wait several hours for public folder replication to finish.

Use the EMC to remove a public folder database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. Click the **Database Management** tab.
3. In the result pane, select the public folder database that you want to remove.
4. In the action pane, click **Remove**. A message appears confirming that you want to remove the database. Click **Yes**.

   Note:
   If you haven't moved the public folder replicas to another server, or if you haven't removed all the public folders in the public folder database, you'll receive an error stating that the public folder database can't be removed because it contains public folder replicas.

5. A warning appears, indicating that the database was successfully removed and reminding you to manually remove the database file. The default location for these files is <Exchange Installation Path>\V14\Mailbox\<*public folder database name*>.

Use the Shell to remove a public folder database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. This example removes a public folder database named PFDB01:

   ```
   Remove-PublicFolderDatabase -Identity "PFDB01"
   ```

   Note:
   If you haven't moved the public folder replicas to another server, or if you haven't removed all the public folders in the public folder database, you'll receive an error stating that the public folder database can't be removed because it contains public folder replicas.

2. A message appears asking you to confirm that you want to perform this action. Enter **Y**.
3. A warning appears, indicating that the database was removed and reminding you to manually remove the database file. The default location for these files is <*Exchange installation path*>\v14\Mailbox\<*public folder database name*>.

Step 5: Delete the public folder database files manually

When you remove a public folder database, the Exchange database (.edb) file for the database and other files associated with the database aren't automatically deleted. You must delete the public folder database files manually. The default location for these files on an Exchange 2010 server is *<Exchange installation path>*\v14\Mailbox*<public folder database name>*. The default location for these files on an Exchange 2007 server is C:\Program Files\Microsoft\ExchangeServer\Mailbox*<storage group name>**<public folder database name>*.

Remove the last public folder database from an organization

To remove the last public folder database from an organization, perform the following steps.

Note:

If you have a mixed Exchange 2003 or Exchange 2007 and Exchange 2010 organization, we recommend that you perform these procedures against an Exchange 2010 server. For more information about performing public folder management tasks in mixed environments, see Understanding Public Folders.

Step 1: Verify that no OABs in your organization are configured for public folder distribution

If any offline address books (OABs) are configured for public folder distribution, you can't remove the last public folder database in your organization. For instructions about how to reconfigure OABs, see Managing Offline Address Books.

Step 2: Remove all public folders from the public folder database

You can't delete a public folder database that contains data. To remove data from a public folder database, delete any unnecessary public folders. For detailed instructions about how to remove all the public folders in a public folder database, see Remove Multiple Public Folders from a Public Folder Database.

Step 3: Remove the last public folder database

Note:

If you successfully perform Step 1 and Step 2 and you receive an error message stating that the public folder database can't be removed because it contains replicas, repeat Step 2 of the procedure Remove Multiple Public Folders from a Public Folder Database. In addition, you can verify that all public folders have been removed by running the **Get-PublicFolderStatistics** cmdlet. For more information about this cmdlet, see Get-PublicFolderStatistics.

Use the EMC to remove a public folder database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. Click the **Database Management** tab.
3. In the result pane, select the public folder database that you want to remove.
4. In the action pane, click **Remove**. A message appears confirming that you want to remove the database. Click **Yes**.

Note:

If you haven't moved the public folder replicas to another server, or if you haven't removed all the public folders in the public folder database, you'll receive an error stating that the public folder database can't be removed because it contains public folder replicas.

5. A warning appears, indicating that the database was successfully removed and reminding you to manually remove the database file. The default location for these files is <Exchange Installation Path>\V14\Mailbox*<public folder database name>*.

Use the Shell to remove a public folder database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. This example removes a public folder database named PFDB01:

```
Remove-PublicFolderDatabase -Identity "PFDB01"
```

Note:
If you haven't moved the public folder replicas to another server, or if you haven't removed all the public folders in the public folder database, you'll receive an error stating that the public folder database can't be removed because it contains public folder replicas.

2. A message appears asking you to confirm that you want to perform this action. Enter **Y**.
3. A warning appears, indicating that the database was removed and reminding you to manually remove the database file. The default location for these files is *<Exchange installation path>*\v14\Mailbox*<public folder database name>*.

Step 4: Delete the public folder database files manually

When you remove a public folder database, the Exchange database (.edb) file for the database and other files associated with the database aren't automatically deleted. You must delete the public folder database files manually. The default location for these files on an Exchange 2010 server is *<Exchange installation path>*\v14\Mailbox*<public folder database name>*. The default location for these files on an Exchange 2007 server is C:\Program Files\Microsoft\ExchangeServer\Mailbox*<storage group name>**<public folder database name>*.

Note:
When the last public folder database in the organization is removed, the default public folder database for all mailbox databases is automatically set to null.

1.8.3.21.8.6 Set the Replication Schedule for a Public Folder Database

Set the Replication Schedule for a Public Folder Database

Managing Mailbox Servers > Managing Public Folders > Managing Public Folder Databases >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

After you determine which public folders you want to replicate and the databases on which they will be replicated, you can set the public folder database replication schedule. By default, public folder replication is scheduled to run every 15 minutes. You can select precanned replication intervals, or you can create a custom schedule. For more information about how to configure the list of public folder databases to which public folders will replicate, see Configure Public Folder Replication.

This topic shows you how to use the Exchange Management Console (EMC) or the Exchange Management Shell to set the public folder replication schedule for a public folder database.

Looking for other management tasks related to managing public folder databases? Check out Managing Public Folder Databases.

Use the EMC to set the replication schedule for a public folder database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder replication" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab, and then click the public folder database you want to configure.
3. In the action pane, click **Properties**.
4. In **<Public Folder Database> Properties**, click the **Replication** tab.
5. In the **Replication interval** list, the following options are available:
   - **Always Run** The replication process is initiated during the replication interval that's specified in the **Replication interval for "Always Run" (minutes)** box.
   - **Never Run** The public folder database isn't replicated.
   - **Run every hour** The replication process is initiated every hour.
   - **Run every 2 hours** The replication process is initiated every 2 hours.
   - **Run every 4 hours** The replication process is initiated every 4 hours.
   - **Use Custom Schedule** The replication process uses the customized schedule that you create in Step 8.
6. Click **Customize** to create a customized schedule.

   Note:
   If you use a customized schedule, you must select **Use Custom Schedule** from the **Replication interval** list.

7. To set the schedule, click the time grid in the **Schedule** dialog box. Public folder replication will run during the time slots that you specify. You can select the same time slot every day by clicking a column header for a specific time slot. You can select an entire day by clicking the name of that day.

   Note:
   The default time slot for the grid is one hour. For finer control, you can change the schedule grid to 15 minute intervals by clicking **15 minute**. Scheduled intervals must be at least 15 minutes apart.

8. Click **OK** to close the **Schedule** dialog box.
9. Click **OK** to close the **<Public Folder Database> Properties** dialog box and to save your changes.

Use the Shell to set the replication schedule for a public folder database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder replication" entry in the Mailbox Permissions topic.

This example creates a customized public folder replication schedule for the public folder database PFDatabase that resides on Server01.

```
Set-PublicFolderDatabase -Identity "Server01\PFDatabase" -ReplicationSchedule "Su
```

For detailed syntax and parameter information, see Set-PublicFolderDatabase.

1.8.3.21.9 Remove Public Folders

Remove Public Folders

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) or the Exchange Management Shell to remove a public folder. To help determine which public folders should be removed, see View Public Folder Item Statistics.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Caution:

The **Remove-PublicFolder** cmdlet removes the public folder data from all servers in your organization. If you only want to remove data from one server, use the **Set-PublicFolder** cmdlet with the *Replicas* parameter. For more information, see Set-PublicFolder.

Use the EMC to remove public folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Public Folder Management Console**.
3. In the action pane, click **Open Tool**. The Public Folder Management Console appears.
4. In the console tree, expand **Default Public Folders**, and then select the parent public folder of the public folder that you want to remove.
5. In the result pane, select the public folder that you want to remove.
6. In the action pane, click **Remove**. A warning appears. Click **Yes** to confirm that you want to remove the public folder.

Use the Shell to remove public folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

This example removes the public folder My Public Folder.

```
Remove-PublicFolder -Identity "\My Public Folder"
```

This example removes the public folder My Public Folder and specifies the server from which to remove it.

```
Remove-PublicFolder -Identity "\My Public Folder" -Server "My Server"
```

This example tests the previous command without making any modifications.

```
Remove-PublicFolder -Identity "\My Public Folder" -WhatIf
```

This example removes the public folder My Public Folder and all of its subfolders because the command runs recursively.

```
Remove-PublicFolder -Identity "\My Public Folder" -Recurse: $True
```

For detailed syntax and parameter information, see Remove-PublicFolder.

1.8.3.21.10 Resume Public Folder Content Replication

Resume Public Folder Content Replication

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Exchange Management Shell to resume public folder content replication.

You need to resume public folder content replication if public folder content replication has stopped or if you have suspended replication due to a configuration error pertaining to the replication of the public folder hierarchy. If you suspend replication due to a configuration error, you must first correct the error, and then let the change replicate throughout the public folder hierarchy.

For more information about how to suspend public folder content replication, see Suspend Public Folder Content Replication.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Use the Shell to resume public folder content replication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder replication" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to resume public folder content replication.

This command resumes public folder content replication.

```
Resume-PublicFolderReplication
```

For detailed syntax and parameter information, see Resume-PublicFolderReplication.

1.8.3.21.11 Scripts for Managing Public Folders in the Exchange Management Shell

Scripts for Managing Public Folders in the Exchange Management Shell

See Also

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-29*

Running scripts in the Exchange Management Shell can make public folder administration faster and easier by automating complex or frequently performed tasks. You can use scripts that are installed with Microsoft Exchange Server 2010 and described in this topic (as well as other scripts), or you can write your own scripts.

Note:
The Shell doesn't load scripts automatically. You must precede all scripts with **.** (a period, followed by a backslash). For example, to run the AggregatePFData.ps1 script, type **.\AggregatePFData.ps1**.

The collection of Shell scripts described in this topic is installed, by default, at <*Exchange Installation Path*>\v14\ Server\Scripts.

For more information about using and writing scripts, see Scripting with the Exchange Management Shell.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Administrative Scripts

The following table lists the administrative scripts included with Exchange 2010.

Task	Script	Description
Add a server to the replication list.	AddReplicaToPFRecursive.ps1	This script adds a new server to the replication list for a public folder and all the folders beneath it in the hierarchy. If the server is already listed in the replication list for a folder, nothing is changed for that folder. This script accepts the following parameters: • **Help** This parameter displays the Help file for the script. • **Server** (Optional) This parameter specifies the server to operate against. This server must be an Exchange Mailbox server that has a public folder database. If you don't use the *Server* parameter to specify a server, the script defaults to the local server. • **TopPublicFolder** (Required) This parameter specifies the identity of the folder at the top of the public folder tree. • **ServerToAdd** (Required) This parameter specifies the server identity to add to the replica list. This server must contain a

		public folder database.
Aggregate data across all public folder replicas.	AggregatePFData.ps1	This script aggregates and captures information collected from the following cmdlets: • **Get-PublicFolderItemStatistics** • **Get-PublicFolderStatistics** • **Get-PublicFolder** The following information is aggregated at the public folder level, and not at the item level: • Last user access and last user modification times • Owner of the public folder • Other properties such as MailEnabled, HasRules, ItemCount, FolderType, HasModerator, and TotalItemSize This script accepts the following parameters: • **Help** This parameter displays the Help file for the script. • **Public Folder** (Required) This parameter specifies the identity of the public folder. For more information, see View Public Folder Item Statistics.
Remove a server from the replication list.	RemoveReplicaFromPFRecursive.ps1	This script removes a server from the replication list for a public folder and all the folders beneath it in the hierarchy. If the server isn't listed in the replication list for a folder, nothing is changed for that folder. If the server is the only server on the replication list, the list isn't changed. This script accepts the following parameters: • **Help** This parameter displays the Help file for the script. • **Server** (Optional) This parameter specifies the server to operate against. This server must be an Exchange Mailbox server that has a public folder database. If you don't use the *Server* parameter to

		specify a server, the script defaults to the local server. • **TopPublicFolder** (Required) This parameter specifies the identity of the folder at the top of the public folder tree. • **ServerToRemove** This parameter specifies the server identity to remove from the replica list. This server must have a public folder database.
Replace a server in the replication list.	MoveAllReplicas.ps1	This script replaces a server with a new server in the replication list for all public folders, including system folders. This script accepts the following parameters: • **Help** This parameter displays the Help file for the script. • **Server** (Required) This parameter specifies the server to remove. This server must be an Exchange Mailbox server that contains a public folder database. • **NewServer** (Required) This parameter specifies the identity of the server to add to the replica list. This server must contain a public folder database.
Replace a server in the replication list with a new server.	ReplaceReplicaOnPFRecursive.ps1	This script replaces a server with a new server in the replication list for a public folder and all the folders beneath it in the hierarchy. If the server that you want to remove isn't listed in the replication list for a particular folder, nothing is changed for that folder. This script accepts the following parameters: • **Help** This parameter displays the Help file for the script. • **Server** (Optional) This parameter specifies the server to operate against. This server must be an Exchange Mailbox server that contains a public folder database. If you don't use the *Server* parameter to specify a server, the script defaults to the local server. • **TopPublicFolder**

		(Required) This parameter specifies the identity of the folder at the top of the public folder tree. • **ServerToRemove** This parameter specifies the server identity to remove from the replica list. This server must contain a public folder database. •

User Management Scripts

The following table lists the user management scripts included with Exchange 2010.

Task	Script	Description
Add a user to the client permissions list.	AddUsersToPFRecursive.ps1	This script adds a user and that user's permissions to the client permissions list for a public folder and all the folders beneath it in the hierarchy. If the user is already listed in the client permissions list for a folder, the user's permissions are updated to the new set specified in the script. This script accepts the following parameters: • **Help** This parameter displays the Help file for the script. • **Server** (Optional) This parameter specifies the server to operate against. This server must be an Exchange Mailbox server that contains a public folder database. If you don't use the *Server* parameter to specify a server, the script defaults to the local server. • **TopPublicFolder** (Required) This parameter specifies the identity of the folder at the top of the public folder tree. • **User** (Required) This parameter specifies the identity of the user to whom to add client permissions. • **Permissions** (Required) This parameter specifies the client permissions to apply to the user.
Replace a user with a new user in the client	ReplaceUserWithUserOnPFRecursive.ps1	This script replaces a user with a new user in the client permissions list for a

permissions list.		public folder and all the folders beneath it in the hierarchy. Existing permissions for the first user are retained. Public folders that don't contain permissions for the user aren't modified. This script accepts the following parameters: • **Help** This parameter displays the Help file for the script. • **Server** (Optional) This parameter specifies the server to operate against. This server must be an Exchange Mailbox server that has a public folder database. If you don't use the *Server* parameter to specify a server, the script defaults to the local server. • **TopPublicFolder** (Required) This parameter specifies the identity of the folder at the top of the public folder tree. • **UserOld** (Required) This parameter specifies the identity of the user from whom to remove client permissions. • **UserNew** (Required) This parameter specifies the identity of the user to whom to add client permissions.
Replace a user's permissions.	ReplaceUserPermissionOnPFRecursive.ps1	This script replaces the permissions of a user in the client permissions list for a public folder with a new set of permissions. It also replaces the permissions for all the folders in the hierarchy beneath that folder. Public folders that don't contain permissions for the user aren't modified. This script accepts the following parameters: • **Help** This parameter displays the Help file for the script. • **Server** (Optional) This parameter specifies the server to operate against. This server must be an Exchange Mailbox server that contains a public folder database. If you don't use the *Server* parameter to specify a server, the script defaults

		to the local server. • **TopPublicFolder** (Required) This parameter specifies the identity of the folder at the top of the public folder tree. • **User** (Required) This parameter specifies the identity of the user for whom to replace client permissions. • **Permissions** (Required) This parameter specifies the client permissions to apply to the user.
Remove a user from the client permissions list.	RemoveUserFromPFRecursive.ps1	This script removes a user from the client permissions list for a public folder and from all the folders beneath it in the hierarchy. This script accepts the following parameters: • **Help** This parameter displays the Help file for the script. • **Server** (Optional) This parameter specifies the server to operate against. This server must be an Exchange Mailbox server that contains a public folder database. If you don't use the *Server* parameter to specify a server, the script defaults to the local server. • **TopPublicFolder** (Required) This parameter specifies the identity of the folder at the top of the public folder tree. • **User** (Required) This parameter specifies the identity of the user from whom to remove client permissions. **Note:** The users Default and Anonymous can't be removed from the permissions list. Any attempt to do so effectively replaces their permissions with None.

See Also

Concepts

Understanding Public Folders

Managing Public Folders
Exchange Management Shell

1.8.3.21.12 Set the Size Limit for Public Folder Replication Messages

Set the Size Limit for Public Folder Replication Messages

Mailbox > Managing Mailbox Servers > Managing Public Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you modify a public folder or its contents, the database that contains the replica of the public folder that was changed sends a descriptive e-mail message to the other public folder databases that host a replica of the public folder. To reduce traffic on your network, Exchange includes information about multiple changes in one e-mail message. The amount of information included in these messages depends on the size limit you set for replication messages. If any message exceeds the specified size limit, that message is sent as a separate replication message.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Use the EMC to set the size limit for public folder replication messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, select the public folder database you want to configure.
3. In the action pane, click **Properties**.
4. In **<Public Folder Database> Properties**, click the **Replication** tab.
5. In the **Replication message size limit (KB)** box, type the message size limit. The value range is from 1 through 2,097,151 kilobytes (KB). The default message size is 300 KB.
6. Click **OK** to close the **<Public Folder Database> Properties** dialog box and to save your changes.

Use the Shell to set the size limit for public folder replication messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folder" entry in the Mailbox Permissions topic.

This example sets the public folder replication message size limit to 500 KB for the public folder database PFDatabase that resides on Server01.

```
Set-PublicFolderDatabase -Identity "Server01\PFDatabase" -ReplicationMessageSize
```

For detailed syntax and parameter information, see Set-PublicFolderDatabase.

1.8.3.21.13 Suspend Public Folder Content Replication

Suspend Public Folder Content Replication

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Exchange Management Shell to suspend the replication of public folder content.

Note:
Suspending public folder replication applies only to content replication. Hierarchical replication will continue normally.

If you experience a configuration error pertaining to the replication of the public folder hierarchy, you must suspend the replication of public folder content and correct the error. You can resume the replication of public folder content after you have fixed the error, and then let the change replicate throughout the public folder hierarchy. For more information about how to resume public folder replication, see Resume Public Folder Content Replication.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Use the Shell to suspend public folder content replication

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to suspend public folder content replication.

This command suspends content replication.

```
Suspend-PublicFolderReplication
```

For detailed syntax and parameter information, see Suspend-PublicFolderReplication.

1.8.3.21.14 Update a Public Folder Hierarchy

Update a Public Folder Hierarchy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console or the Exchange Management Shell to update a public folder hierarchy.

Perform this procedure to synchronize the public folder hierarchy from one server to the other servers on which public folder replicas exist. This procedure is helpful in cases

where the public folder hierarchy on one server is different from the public folder hierarchy on other servers in your organization.

Note:

In Microsoft Exchange Server 2003, this procedure is known as *manually replicating the public folder*.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Caution:

Performing this procedure only allows the server running Exchange to begin any outstanding replication actions. The process may take several hours to complete.
Because factors not controlled by replication can prevent the hierarchy from becoming immediately synchronized, performing this procedure doesn't ensure that the public folder hierarchy will be completely synchronized.
This procedure only updates the public folder hierarchy. It doesn't update public folder content. For instructions about how to update public folder content, see Update Public Folders.

Use the EMC to update a public folder hierarchy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Public Folder Management Console**.
3. In the action pane, click **Open Tool**. The Public Folder Management Console appears.
4. In the public folder tree, click the **Public Folders - <Server Name>** node.
5. In the action pane, click **Update Hierarchy**.

Use the Shell to update a public folder hierarchy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

This example updates the public folder hierarchy on the server Server01.

```
Update-PublicFolderHierarchy -Server "Server01"
```

For detailed syntax and parameter information, see Update-PublicFolderHierarchy.

1.8.3.21.15 Update Public Folders

Update Public Folders

Mailbox > Managing Mailbox Servers > Managing Public Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) or the Exchange Management Shell to update the public folder content in a specified public folder's replication list.

For more information about how to update the public folder hierarchy, see Update a Public Folder Hierarchy.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Use the EMC to update public folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

1. In the console tree, click **Toolbox**.
2. In the result pane, click **Public Folder Management Console**.
3. In the action pane, click **Open Tool**. The Public Folder Management Console appears.
4. In the public folder tree, click or expand **Default Public Folders**, and then if any public folders are displayed in the result pane, select the parent folder of the public folder that you want to update.
5. In the result pane, click the public folder that you want to update.
6. In the action pane, click **Update Content**.

Use the Shell to update public folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

This example updates the folders in the replication list of the public folder My Public Folder that resides on the server My Server.

```
Update-PublicFolder "\My Public Folder" -Server "My Server"
```

Note:

The *Server* parameter specifies the identity of a Mailbox server with a public folder database that's the source of the replication.

For detailed syntax and parameter information, see Update-PublicFolder.

1.8.3.21.16 View Public Folder Item Statistics

View Public Folder Item Statistics

Mailbox > Managing Mailbox Servers > Managing Public Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can view the following information about items within a specific public folder:

- Type of item
- Subject
- Last user modification time
- Last user access time
- Creation time

- Attachments
- Message size

You can use this information to make decisions about what actions to take for your public folders, such as which public folders to delete. For example, you may want to delete a public folder if the items haven't been accessed for over two years, or you may want to convert a public folder that's being used as a document repository to another client access application.

Looking for other management tasks related to public folders? Check out Managing Public Folders.

Use the Shell to view item statistics for a specific public folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to view item statistics for a specific public folder.

This example returns default statistics for all items in the public folder Pamphlets under the \Marketing\2010 path. Default information includes item identity, creation time, and subject.

```
Get-PublicFolderItemStatistics -Identity "\Marketing\2010\Pamphlets"
```

This example returns additional information about the items within the public folder Pamphlets, such as subject, last modification time, creation time, attachments, message size, and the type of item by piping the results of the **Get-PublicFolderItemStatistics** cmdlet to the **Format-List** cmdlet.

```
Get-PublicFolderItemStatistics -Identity "\Marketing\2010\Pamphlets" | Format-Lis
```

For detailed syntax and parameter information, see Get-PublicFolderItemStatistics.

Use the Shell to export the output of the Get-PublicFolderItemStatistics cmdlet to a .csv file

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to export the output of the **Get-PublicFolderItemStatistics** cmdlet to a .csv file.

This example exports the output of the **Get-PublicFolderItemStatistics** cmdlet to the PFItemStats.csv file that includes the following information for all items within the public folder \Marketing\Reports:

- Subject of the message (Subject)
- Date and time that the item was last modified (LastModificationTime)
- Whether the item has attachments (HasAttachments)
- Type of item (ItemType)
- Size of the item (MessageSize)

```
Get-PublicFolderItemStatistics -Identity "\Marketing\Reports" | Select Subject,La
```

For detailed syntax and parameter information, see Get-PublicFolderItemStatistics.

Use AggregatePFData.ps1 to aggregate public folder statistics across all replicas

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

The AggregatePFData.ps1 script aggregates and captures information collected from three cmdlets:

- **Get-PublicFolderItemStatistics**
- **Get-PublicFolderStatistics**
- **Get-PublicFolder**

The following information is aggregated at the public folder level, and not at the item level:

- Last user access and last user modification times
- Owner of the public folder
- Properties such as MailEnabled, HasRules, ItemCount, FolderType, HasModerator, and TotalItemSize

This example returns the aggregated data from the public folder Pamphlets under the \Marketing\2008 path.

Note:

The Shell doesn't load scripts automatically. You must precede all scripts with a period followed by a backslash (.\) For example, to run the AggregatePFData.ps1 script, type `.\AggregatePFData.ps1`. For more information, see Scripting with the Exchange Management Shell.

```
.\AggregatePFData.ps1 -Publicfolder "\Marketing\2008\Pamphlets"
```


1.8.3.21.17 View Public Folder Statistics

View Public Folder Statistics

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Exchange Management Shell to retrieve statistics about a public folder, such as the display name, creation time, last user modified time, last user access, and item size. You can use this information to make decisions about deleting or keeping public folders.

You can also use the **Get-PublicFolderItemStatistics** cmdlet and the **AggregatePFDAta.ps1** script to view additional information about public folders and their contents. For more information, see View Public Folder Item Statistics.

Looking for other management tasks related to managing public folders? Check out Managing Public Folders.

Use the Shell to retrieve public folder statistics

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to retrieve public folder statistics.

This example returns the statistics for the public folder Marketing with a piped command to format the list.

```
Get-PublicFolderStatistics -Identity \Marketing | fl
```

Note:
The value for the *Identity* parameter must include the path. For example, if the public folder Marketing existed under the parent folder Business, you would provide the following value: \Business\Marketing

For detailed syntax and parameter information, see Get-PublicFolderStatistics.

1.8.3.21.18 Create an Organizational Forms Library

Create an Organizational Forms Library

Mailbox > Managing Mailbox Servers > Managing Public Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

An organizational forms library is a repository for forms generally accessed by all users in a company. Forms are templates that help users to enter and view information. For example, a standard supply request form can be stored in an organizational forms library. Provided that you granted all users permissions to the library, all users in your organization can access the forms within the library.

An organizational forms library is a special type of public folder listed only under the NON_IPM_SUBTREE systems folder. You can have only one organizational forms library for each language in your organization.

You can add a form to the organizational forms library when you want to use the same custom form in more than one public folder. This library is frequently used for e-mail message forms because they typically aren't based on a specific public folder. When you publish a form, you can maintain only a single published form.

Important:
By default, the organizational forms library isn't required for Microsoft Exchange Server 2010 to operate correctly. Create the organizational forms library only if you must support custom forms already developed or if a third-party application requires the library.

Looking for other management tasks related to managing public folders? Check out Managing Public Folders.

Step 1: Create a public folder for the organizational forms library Public Folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Public folders" entry in the Mailbox Permissions topic.

Use the Shell to create the public folder for the organization forms library

This example creates the public folder for the organizational forms library in the EFORMS REGISTRY branch of your public folder hierarchy.

```
New-PublicFolder -Path "\NON_IPM_SUBTREE\EFORMS REGISTRY" -Name "Organizational F
```

For detailed syntax and parameter information, see New-PublicFolder.

Use the Public Folder Management Console to create the public folder for the organizational forms library

1. In the console tree of the EMC, click **Toolbox**.
2. In the result pane, click **Public Folder Management Console**.
3. In the action pane, click **Open Tool**.
4. In the public folder tree of the Public Folder Management Console, expand **System Public Folders**, and then click **EFORMS REGISTRY**.
5. In the action pane, click **New Public Folder**.
6. On the **Introduction** page, complete the following fields:
   - **Name** Use this box to type the name of the new public folder, for example, **Organizational Forms Library**.
   - **Path** Use this read-only box to verify the path to the public folder. The path should read: **\Non_IPM_SUBTREE\EFORMS REGISTRY**.
7. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Step 2: Use the ExFolders tool to add the PR_URL_NAME property to the organizational forms library

To perform this procedure, the ExFolders tool (ExFolders.exe) must exist in the *<Exchange Installation Path>*\V14\Bin directory. You can download the tool from one of the following locations:

- If you're running Exchange 2010 Service Pack 1 (SP1), see ExFolders tool (Compatible with Exchange 2010 SP1 version).
- If you're running the release to manufacturing (RTM) version of Exchange 2010, see ExFolders tool (Compatible with Exchange 2010 RTM version).

After the download, be sure to copy the ExFolders.exe file to the *<Exchange Installation Path>*\V14\Bin directory.

To perform this procedure, you must have administrative permissions to the public folders you're modifying. For more information, see Understanding Public Folder Permissions.

1. Navigate to the **<Exchange Installation Path>\V14\Bin** directory, and then double-click **ExFolders.exe**.

Note:
You must run the ExFolders tool from an Exchange 2010 server. You can't run it from a workstation as you could with the PFDAVAdmin tool. To learn more about the ExFolders tool, see the Exchange Server Team Blog article Exchange, Meet ExFolders.

2. In the ExFolders management console, navigate to **File** > **Connect**.
3. In **Connect**, click **Public Folders**.
4. Next to the **Global Catalog** box, click **Select**, and then select a global catalog server you want to use.
5. Next to the **Database(s)** box, click **Select**, select the public folder database you want to use, and then click **OK**. A public folder hierarchy will appear in the ExFolders console tree.
6. Expand **System Folders**, expand **EFORMS REGISTRY**, right-click the public folder you created for the organizational forms library, and then click **Property Editor**.
7. On the **Property** menu, click **Add Property To View**.
8. In **Add Property To View**, type **0x6707001E**, and then click **OK**.
9. Sort the **Name** column to find the **PR_URL_NAME** property you just added.
10. Right-click **PR_URL_NAME**, and then click **Edit Value**.
11. In the **Value** box, type **/NON_IPM_SUBTREE/EFORMS REGISTRY**, and then click **OK**.
12. Close the ExFolders tool.

Step 3: Use MAPI Editor (Mfcmapi.exe) to add the PR_EFORMS_LOCALE_ID property to the organizational forms library

To perform this procedure, you must use the Microsoft Exchange Server MAPI Editor (MFCMAPI) tool on a computer that's running the 64-bit version of Microsoft Outlook 2010. To download MFCMAPI, see Microsoft Exchange Server MAPI Editor.

1. In MFCMAPI, on the **Session** menu, click **Logon and Display Store Table**.

Note:
If this is your first time using MAPI Editor, you're prompted to create a profile.

2. On the **MDB** menu, click **Open Public Folder Store**, and then click **OK**. The Public Folder Management Console appears.
3. In the console tree, expand **Public Root**, expand **NON_IPM_SUBTREE**, expand **EFORMS REGISTRY**, and then click the public folder that you created for the organizational forms library.
4. In the result pane, in the **Property Name(s)** column, click the **PR_URL_NAME** property.
5. On the **Property Pane** menu, click **Modify 'Extra' Properties**.
6. In **Extra Properties**, click **Add**.
7. In **Property Tag Editor**, click **Select Property Tag**.
8. In **Property Selector**, click **PR_EFORMS_LOCALE_ID**, and then click **OK**.
9. Click **OK** to close **Property Tag Editor**, and then click **OK** to close **Extra Properties**.
10. To verify that the property was added, in the Public Folder Management Console, locate the newly created **PR_EFORMS_LOCALE_ID** property in the **Property Name(s)** column. A red exclamation point (!) is displayed as its icon.
11. Double-click **PR_EFORMS_LOCALE_ID** to open **Property Editor**.
12. In the **Unsigned Decimal** box, type the desired locale ID, and then click **OK**. For example, type **1033** for English, **1040** for Italian, and so on.

Note:
For more information about determining the locale ID, see languagecode

Field.

13.Close MFCMAPI.

Other Tasks

After you create the organizational forms library, you may also want to:

- Use the Set-PublicFolder cmdlet to set storage limits.
- Use the following cmdlets to set permissions for each user:
  - Add-PublicFolderClientPermission
  - Add-PublicFolderAdministrativePermission

1.8.3.22 Managing Recoverable Items

Managing Recoverable Items

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-05-24*

Enable Single Item Recovery for a Mailbox

Configure Deleted Item Retention and Recoverable Items Quotas

Perform Single Item Recovery

Get Recoverable Items Folder Statistics

Clean Up the Recoverable Items Folder

1.8.3.22.1 Enable Single Item Recovery for a Mailbox

Enable Single Item Recovery for a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Exchange Management Shell to enable single item recovery on a mailbox.

Looking for other management tasks related to recovery items? Check out Managing Recoverable Items.

Use the Shell to enable recoverable items

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Retention and legal holds" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to enable recoverable items.

This example uses the **Set-Mailbox** command to enable single item recovery and sets the number of days that deleted items are retained.

```
Set-Mailbox -Identity MBX01 -SingleItemRecoveryEnabled $True -RetainDeletedItemsF
```

Note:
By default, the mailbox uses the deleted item retention settings of the mailbox database, but you can override the default can be overridden by setting it at the mailbox level for specific mailboxes.

For detailed syntax and parameter information, see Set-Mailbox.

1.8.3.22.2 Configure Deleted Item Retention and Recoverable Items Quotas

Configure Deleted Item Retention and Recoverable Items Quotas

Mailbox > Managing Mailbox Servers > Managing Recoverable Items >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When a user deletes items from the Deleted Items default folder by using the Delete, Shift+Delete, or **Empty Deleted Items Folder** actions, the items are moved to the **Recoverable Items\Deletions** folder. The duration that deleted items remain in this folder is based on the deleted item retention settings configured for the mailbox database or the mailbox. By default, a mailbox database is configured to retain deleted items for 14 days, and the Recoverable Items warning quota and Recoverable Items quota are set to 20 gigabytes (GB) and 30 GB respectively.

Note:
Before the retention time for deleted items elapses, Microsoft Outlook and Microsoft Office Outlook Web App users can recover deleted items by using the Recover Deleted Items feature. To learn more about these features, see the "Recover deleted items" topic for Outlook or Outlook Web App.

You can use the Shell to configure deleted item retention settings and Recoverable Items quotas for a mailbox or mailbox database. These values are ignored when a mailbox is placed on litigation hold.

Note:
You can't use the EMC to configure deleted item retention and recoverable items quotas.

To learn more about deleted item retention, the Recoverable Items folder, and litigation hold, see the following topics:

- Understanding Recoverable Items
- Understanding Litigation Hold

Looking for other management tasks related to recoverable items? Check out Managing Recoverable Items.

Use the Shell to configure deleted item

retention for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Retention and legal holds" entry in the Mailbox Permissions topic.

This example configures April Stewart's mailbox to retain deleted items for 30 days.

```
Set-Mailbox -Identity - "April Stewart" -RetainDeletedItemsFor 30
```

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to configure Recoverable Items quotas for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Retention and legal holds" entry in the Mailbox Permissions topic.

This example configures a Recoverable Items warning quota of 12 GB and a Recoverable Items quota of 15 GB for April Stewart's mailbox.

```
Set-Mailbox -Identity "April Stewar"t -RecoverableItemsWarningQuota 12GB -Recover
```

Note:

To configure a mailbox to use different Recoverable Items quotas than the mailbox database in which it resides, you must set the *UseDatabaseQuotaDefaults* parameter to `$false`.

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to configure deleted item retention for a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Retention and legal holds" entry in the Mailbox Permissions topic.

This example configures a deleted item retention period of 10 days for the mailbox database MDB2.

```
Set-MailboxDatabase -Identity MDB2 -DeletedItemRetention 10
```

For detailed syntax and parameter information, see Set-MailboxDatabase.

Use the Shell to configure Recoverable Items quotas for a mailbox database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Retention and legal holds" entry in the Mailbox Permissions topic.

This example configures a Recoverable Items warning quota of 15 GB and a Recoverable

Items quota of 20 GB on mailbox database MDB2.

```
Set-MailboxDatabase -Identity MDB2 -RecoverableItemsWarningQuota 15GB -Recoverabl
```

For detailed syntax and parameter information, see Set-MailboxDatabase.

1.8.3.22.3 Perform Single Item Recovery

Perform Single Item Recovery

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Single item recovery provides an additional layer of protection so that you can recover items accidentally deleted by a user or by automated processes such as the Managed Folder Assistant. Single item recovery simplifies recovery and reduces recovery time because you can recover items without recovering an entire mailbox or mailbox database from backup media.

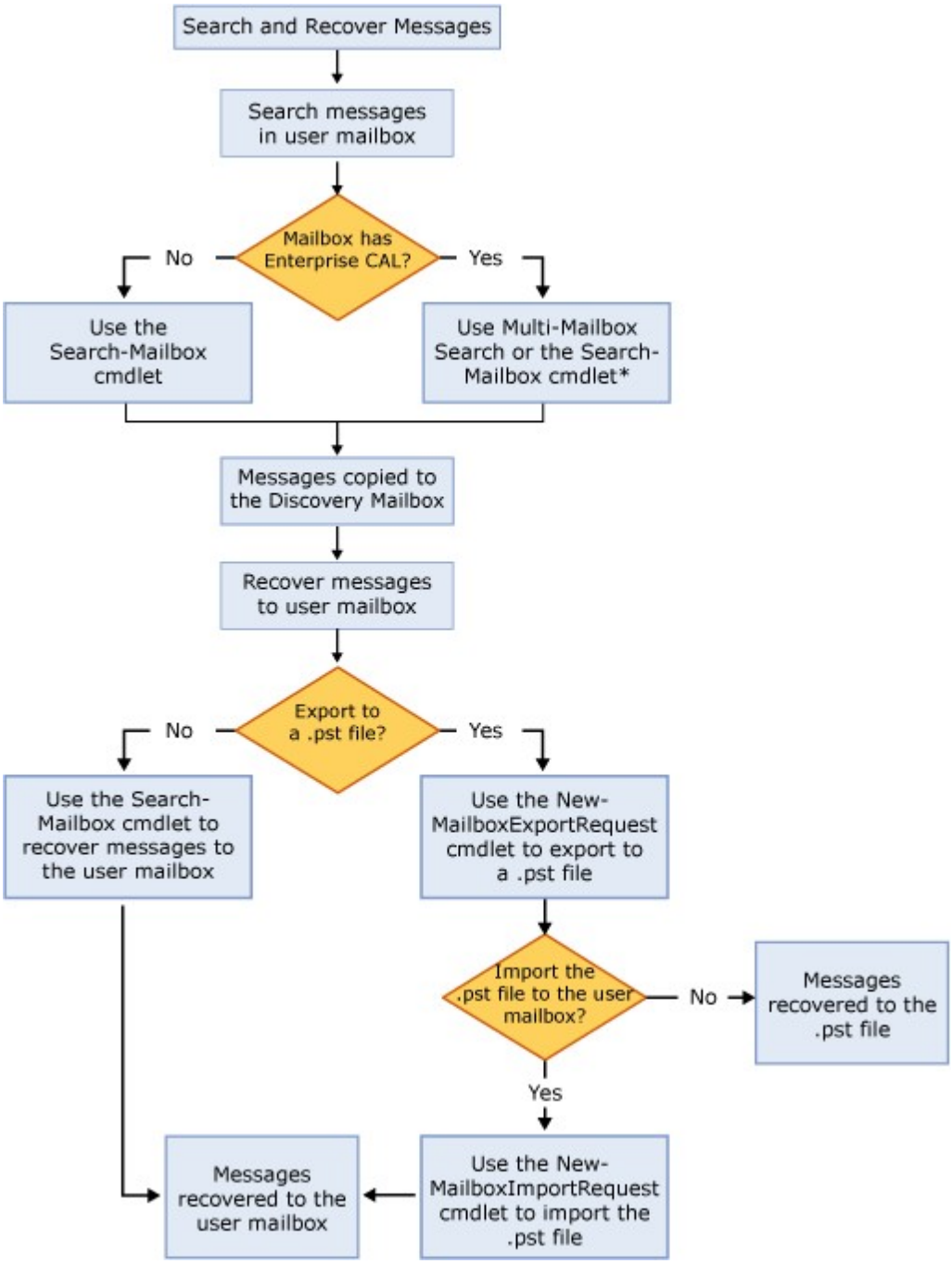
Note:

In addition to using this procedure to search for and recover deleted items (which are moved to the Recoverable Items\Purges folder if either single item recovery or litigation hold is enabled), you can also use this procedure to search for items residing in other folders in the mailbox and to delete items from the source mailbox (also known as *search and destroy*). For details, see Use Mailbox Search to Delete Messages.

The method you use to search for and recover missing items depends on the client access license (CAL) for the mailbox you're searching. If the mailbox has an enterprise CAL, you can use the Multi-Mailbox Search feature in the Exchange Control Panel (ECP) or the **New-MailboxSearch** cmdlet in the Shell. These features also allow you to search multiple mailboxes simultaneously.

You can also use the **Search-Mailbox** cmdlet in the Shell to search for and recover missing items. If the mailbox has a standard CAL, this is the only method you can use. If you use this cmdlet, you can search only one mailbox at a time.

The following flowchart illustrates the different methods available for performing single item recovery.



To search for and recover items, you must have the following information:

- **Source mailbox** This is the mailbox being searched.
- **Target mailbox** This is the discovery mailbox in which messages will be recovered. Exchange Setup creates a default discovery mailbox. If required, you can create additional discovery mailboxes. For details, see Create a Discovery Mailbox.

Note:

When using the **Search-Mailbox** cmdlet, you can also specify a target mailbox that isn't a discovery mailbox. However, you can't specify the same mailbox as the source and target mailbox.

- **Search criteria** Criteria include sender or recipient, or keywords (words or phrases) in the message.

The process consists of two steps:

1. **Search** Searching for the missing items and recovering them to a discovery mailbox.
2. **Restore** Restoring the items to the user's mailbox or a .pst file.

Looking for other management tasks related to recoverable items? Check out Managing Recoverable Items.

Prerequisites

Before the item you want to recover is deleted, single item recovery must be enabled for a mailbox. For details, see Enable Single Item Recovery for a Mailbox.

Step 1: Search for and recover missing items

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Multi-Mailbox Search" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to search for and recover missing items.

The first step in the recovery process is to search for messages in the source mailbox. Use one of the following methods to search a user mailbox and copy messages to a discovery mailbox.

Use the Shell

This example searches for messages in April Stewart's mailbox that meet the following criteria:

- Sender: Ken Kwok
- Keyword: Seattle

```
Search-Mailbox "April Stewart" -SearchQuery "from:'Ken Kwok' AND seattle" -Target
```

Note:
When using the **Search-Mailbox** cmdlet, you can scope the search by using the *SearchQuery* parameter to specify a query formatted using Advanced Query Syntax (AQS). You can also use the *SearchDumpsterOnly* switch to search only items in the dumpster.

For detailed syntax and parameter information, see Search-Mailbox.

Use Multi-Mailbox Search in the ECP

For details about how to perform a Multi-Mailbox Search in the ECP, see Multi-Mailbox Searches.

Step 2: Restore recovered items

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Multi-Mailbox Search" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to restore recovered items.

After messages have been recovered to a discovery mailbox, you can restore them to the user's mailbox by using the **Search-Mailbox** cmdlet. You can also use the **New-MailboxExportRequest** and **New-MailboxImportRequest** cmdlets to export the messages to or import the messages from a .pst file.

Use the Shell to restore messages

This example restores messages to April Stewart's mailbox and deletes them from the Discovery Search Mailbox.

```
Search-Mailbox "Discovery Search Mailbox" -SearchQuery "from:'Ken Kwok' AND seatt
```

For detailed syntax and parameter information, see Search-Mailbox.

Use the Shell to export and import messages from a .pst file

In Microsoft Exchange Server 2010 Service Pack 1 (SP1), you can export messages from and import messages to .pst files without requiring the installation of Microsoft Outlook. To learn more about mailbox import and export, see Understanding Mailbox Import and Export Requests.

This example uses the following settings to export messages from the folder April Stewart Recovery in the Discovery Search Mailbox to a .pst file:

- **Mailbox** Discovery Search Mailbox
- **Source folder** April Stewart Recovery
- **ContentFilter** april travel plans
- **PST file path** \\MYSERVER\HelpDeskPst\AprilStewartRecovery.pst

```
New-MailboxExportRequest -Mailbox "Discovery Search Mailbox" -SourceRootFolder "A
```

For detailed syntax and parameter information, see New-MailboxExportRequest.

This example uses the following settings to import messages from a .pst file to the folder Recovered By Helpdesk in April Stewart's mailbox:

- **Mailbox** April Stewart
- **Target folder** Recovered By Helpdesk
- **PST file path** \\MYSERVER\HelpDeskPst\AprilStewartRecovery.pst

```
New-MailboxImportRequest -Mailbox "April Stewart" -TargetRootFolder "Recovered By
```

For detailed syntax and parameter information, see New-MailboxImportRequest.

1.8.3.22.4 Get Recoverable Items Folder Statistics

Get Recoverable Items Folder Statistics

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Recoverable Items folder contains items deleted by Microsoft Outlook and Microsoft Office Outlook Web App users or by the Mailbox Assistant. The duration that deleted items remain in this folder is based on the deleted item retention settings configured for the mailbox database or the mailbox. By default, a mailbox database is configured to retain deleted items for 14 days, and the Recoverable Items warning quota and Recoverable Items quota are set to 20 gigabytes (GB) and 30 GB respectively. However, if litigation hold is enabled for the mailbox, the Recoverable Items folder can accumulate deleted items beyond the specified retention period and can also maintain different versions of

modified mailbox items.

When the Recoverable Items folder reaches the Recoverable Items warning quota, a warning event is logged in the Application event log. If the mailbox isn't on litigation hold, items are then removed on a first in, first out (FIFO) basis. However, if the mailbox is on litigation hold, the mailbox is never emptied and upon reaching the Recoverable Items quota, mailbox functionality is impacted.

Therefore, it's important to monitor the event log for alerts generated when mailboxes reach the Recoverable Items quotas. You can also use this procedure to report statistics for the Recoverable Items folder, particularly for mailboxes placed on litigation hold.

To learn more, see the following topics:

- Understanding Recoverable Items
- Understanding Litigation Hold

Looking for other management tasks related to recoverable items? Check out Managing Recoverable Items.

Use the Shell to get Recoverable Items folder statistics for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox folders" entry in the Mailbox Permissions topic.

Note:

You can't use the Exchange Management Console (EMC) to get Recoverable Items folder statistics for a mailbox.

This example gets folder statistics for Soumya Singhi's Recoverable Items folder and displays the output in a list format.

```
Get-MailboxFolderStatistics -Identity "Soumya Singhi" -FolderScope RecoverableIte
```

This example gets folder statistics for Soumya Singhi's Recoverable Items folder and displays the folder name, folder path, number of items in the folder, and folder size in a table format.

```
Get-MailboxFolderStatistics -Identity "Soumya Singhi" -FolderScope RecoverableIte
```

For detailed syntax and parameter information, see Get-MailboxFolderStatistics.

Use the Shell to get Recoverable Items folder statistics for all mailboxes on litigation hold

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox folders" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to get Recoverable Items folder statistics for all mailboxes on litigation hold.

This example retrieves a list of all mailboxes placed on litigation hold and retrieves mailbox folder statistics for the Recoverable Items folder and its subfolders for each

mailbox. The **Identity** (mailbox folder identity) and the **FolderAndSubfolderSize** properties are displayed in a table format.

```
Get-Mailbox -ResultSize Unlimited -Filter {LitigationHoldEnabled -eq $true} | Get
```

For detailed syntax and parameter information, see Get-Mailbox and Get-MailboxFolderStatistics.

Other Tasks

After you get Recoverable Items folder statistics for a mailbox, you may also want to:

- Configure Deleted Item Retention and Recoverable Items Quotas
- Clean Up the Recoverable Items Folder

1.8.3.22.5 Clean Up the Recoverable Items Folder

Clean Up the Recoverable Items Folder

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Recoverable Items folder (known in earlier versions of Exchange as the dumpster) exists to protect from accidental or malicious deletions and to facilitate discovery efforts commonly undertaken before or during litigation or investigations. To learn more about the Recoverable Items folder, see Understanding Recoverable Items.

How you clean up a mailbox's Recoverable Items folder depends on whether the mailbox is placed on litigation hold or had single item recovery enabled:

- If a mailbox isn't placed on litigation hold or doesn't have single item recovery enabled, you can simply delete items from the Recoverable Items folder. After being deleted, you can't use single item recovery to recover the items.
- If the mailbox is placed on litigation hold or has single item recovery enabled, it's important to preserve the mailbox data until the litigation hold is removed or single item recovery is disabled. Therefore, you need to perform more detailed steps to clean up the Recoverable Items folder.

To learn more about litigation hold and single item recovery, see Understanding Litigation Hold or "Single Item Recovery" inUnderstanding Recoverable Items.

Looking for other management tasks related to recoverable items? Check out Managing Recoverable Items.

Prerequisites

Because incorrectly cleaning up the Recoverable Items folder can result in data loss, it’s important that you're familiar with the Recoverable Items folder and the impact of removing its contents. Before performing this procedure, we recommend that you review the information in Understanding Recoverable Items.

Use the Shell to delete items from the Recoverable Items folder for mailboxes that aren't placed on litigation hold or don't have single item recovery enabled

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Delete mailbox content" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to delete items from the Recoverable Items folder for mailboxes that aren't placed on litigation hold or don't have single item recovery enabled.

This example permanently deletes items from Gurinder Singh's Recoverable Items folder and also copies the items to the GurinderSingh-RecoverableItems folder in the Discovery Search Mailbox (a discovery mailbox created by Exchange Setup).

```
Search-Mailbox -Identity "Gurinder Singh" -SearchDumpsterOnly -TargetMailbox "Dis
```

Note:
To delete items from the mailbox without copying them to another mailbox, use the preceding command without the *TargetMailbox* and *TargetFolder* parameters.

For detailed syntax and parameter information, see Search-Mailbox.

Use the Shell to clean up the Recoverable Items folder for mailboxes that are placed on litigation hold or have single item recovery enabled

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Delete mailbox content" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to clean up the Recoverable Items folder for mailboxes placed on litigation hold or have single item recovery enabled.

If a mailbox reaches its Recoverable Items quota, we recommend that you raise the quota and not delete items from the folder. You can also monitor events in the Application log related to the Recoverable Items warning quota and take necessary actions (such as raising the quota or investigating dumpster growth for mailboxes that reach the warning quota).

If storage constraints or similar issues prevent you from raising the Recoverable Items quota, and you need to delete messages from the Recoverable Items folder of a mailbox on litigation hold or has single item recovery enabled, we recommend that you first copy data from the user's Recoverable Items folder to another mailbox. If you're deleting items due to storage constraints on one volume, you can copy items to a mailbox located on a volume that has adequate storage.

This procedure copies items from Gurinder Singh's Recoverable Items folder to the

GurinderSingh-RecoverableItems folder in the Discovery Search Mailbox. Before you copy and delete items from the Recoverable Items folder, you must first perform several steps to make sure items aren't deleted from the Recoverable Items folder. After you copy items to a discovery or backup mailbox and clean up the folder, you can revert to the mailbox's previous settings.

1. Retrieve the following quota settings. Be sure to note the values so you can revert to these settings after cleaning up the Recoverable Items folder:
   - *RecoverableItemsQuota*
   - *RecoverableItemsWarningQuota*
   - *ProhibitSendQuota*
   - *ProhibitSendReceiveQuota*
   - *UseDatabaseQuotaDefaults*
   - *RetainDeletedItemsFor*
   - *UseDatabaseRetentionDefaults*

   Note:

   If the *UseDatabaseQuotaDefaults* parameter is set to `$true`, the previous quota settings aren't applied. The corresponding quota settings configured on the mailbox database are applied, even if individual mailbox settings are populated.

   ```
   Get-Mailbox "Gurinder Singh" | Format-List RecoverableItemsQuota, Reco
   ```

2. Retrieve the mailbox access settings for the mailbox. Be sure to note these settings for later.

   ```
   Get-CASMailbox "Gurinder Singh" | Format-List EwsEnabled, ActiveSyncEn
   ```

3. Retrieve the current size of the Recoverable Items folder. Note the size so you can raise the quotas in Step 6.

   ```
   Get-MailboxFolderStatistics "Gurinder Singh" -FolderScope RecoverableI
   ```

4. Retrieve the current Managed Folder Assistant work cycle configuration. Be sure to note the setting for later.

   ```
   Get-MailboxServer "My Mailbox Server" | Format-List Name,ManagedFolder
   ```

5. Disable client access to the mailbox to make sure no changes can be made to mailbox data for the duration of this procedure.

   ```
   Set-CASMailbox "Gurinder Singh" -EwsEnabled $false -ActiveSyncEnabled
   ```

6. To make sure no items are deleted from the Recoverable Items folder, increase the Recoverable Items quota, increase the Recoverable Items warning quota, and set the deleted item retention period to a value higher than the current size of the user's Recoverable Items folder. This is particularly important for preserving messages for mailboxes placed on litigation hold. We recommend raising these settings to twice their current size.

   ```
   Set-Mailbox "Gurinder Singh" -RecoverableItemsQuota 50Gb -RecoverableI
   ```

7. Disable the Managed Folder Assistant on the Mailbox server.

   ```
   Set-MailboxServer MyMailboxServer -ManagedFolderWorkCycle $null
   ```

   Important:

   If the mailbox resides on a mailbox database in a database availability group (DAG), you must disable the Managed Folder Assistant on each DAG member that hosts a copy of the database. If the database fails over to another server, this prevents the Managed Folder Assistant on that server from deleting mailbox data.

8. Disable single item recovery and remove the mailbox from litigation hold.

   ```
   Set-Mailbox "Gurinder Singh" -SingleItemRecoveryEnabled $false -Litiga
   ```

Important:
After you run this command, it may take up to one hour to disable single item recovery or litigation hold. We recommend that you perform the next step only after this period has elapsed.

9. Copy items from the Recoverable Items folder to a folder in the Discovery Search Mailbox and delete the contents from the source mailbox.

```
Search-Mailbox -Identity "Gurinder Singh" -SearchDumpsterOnly -TargetM
```

If you need to delete only messages that match specified conditions, use the *SearchQuery* parameter to specify the conditions. This example deletes messages that have the string "Your bank statement" in the **Subject** field.

```
Search-Mailbox -Identity "Gurinder Singh" -SearchQuery "Subject:'Your
```

Note:
It isn't required to copy items to the Discovery Search Mailbox. You can copy messages to any mailbox. However, to prevent access to potentially sensitive mailbox data, we recommend copying messages to a mailbox that has access restricted to authorized records managers. By default, access to the default Discovery Search Mailbox is restricted to members of the Discovery Management role group. For details, see Understanding Multi-Mailbox Search.

10. If the mailbox was placed on litigation hold or had single item recovery enabled earlier, enable these features again.

```
Set-Mailbox "Gurinder Singh" -SingleItemRecoveryEnabled $true -Litigat
```

Important:
After you run this command, it may take up to one hour to enable single item recovery or litigation hold. We recommend that you enable the Managed Folder Assistant and allow client access (Steps 11 and 12) only after this period has elapsed.

11. Revert the following quotas to the values noted in Step 1:
    - *RecoverableItemsQuota*
    - *RecoverableItemsWarningQuota*
    - *ProhibitSendQuota*
    - *ProhibitSendReceiveQuota*
    - *UseDatabaseQuotaDefaults*
    - *RetainDeletedItemsFor*
    - *UseDatabaseRetentionDefaults*

    In this example, the mailbox is removed from retention hold, the deleted item retention period is reset to the default value of 14 days, and the Recoverable Items quota is configured to use the same value as the mailbox database. If the values you noted in Step 1 are different, you must use the preceding parameters to specify each value and set the *UseDatabaseQuotaDefaults* parameter to `$false`. If the *RetainDeletedItemsFor and UseDatabaseRetentionDefaults* parameters were previously set to a different value, you must also revert them to the values noted in Step 1.

```
Set-Mailbox "Gurinder Singh" -RetentionHoldEnabled $false -RetainDelet
```

12. Enable the Managed Folder Assistant by setting the work cycle back to the value you noted in Step 4. This example sets the work cycle to one day.

```
Set-MailboxServer MyMailboxServer -ManagedFolderWorkCycle 1
```

13. Enable client access.

```
Set-CASMailbox -ActiveSyncEnabled $true -EwsEnabled $true -MAPIEnabled
```

For detailed syntax and parameter information, see the following topics:

- Get-Mailbox
- Get-CASMailbox

- Get-MailboxFolderStatistics
- Get-MailboxServer
- Set-CASMailbox
- Set-Mailbox
- Set-MailboxServer
- Search-Mailbox

Other Tasks

After you clean up the Recoverable Items folder, you may also want to:

- Enable Single Item Recovery for a Mailbox
- Configure Deleted Item Retention and Recoverable Items Quotas

1.8.3.23 Managing Resource Mailboxes and Scheduling

Managing Resource Mailboxes and Scheduling

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-30*

Create a Room or Equipment Mailbox

Create or Remove Custom Resource Properties

Configure Custom Resource Properties for a Resource Mailbox

Configure the Automated Booking Policies for a Resource Mailbox

Customize the Response Message for Resource Scheduling

Enable or Disable Automatic Booking on a Resource Mailbox

List Available Resource Mailboxes and Their Properties

Remove Full Access Permissions from a Resource Mailbox Schedule

Set a Delegate on a Resource Mailbox

Set Full Access Permissions to a Resource Mailbox Schedule

Add Resource Mailboxes to an Address List

1.8.3.23.1 Add Resource Mailboxes to an Address List

Add Resource Mailboxes to an Address List

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Exchange Management Shell to add a resource mailbox to an address list. Only the global address list (GAL) contains all of the recipient types. The All Rooms address list, which is one of the default address lists included with Exchange, contains only resource mailboxes that are the Recipient Display type **ConferenceRoomMailbox** or **SyncedConferencRoomMailbox**.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the Shell to add resource mailboxes to an address list

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Address lists" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to add resource mailboxes to an address list.

None of the default address lists installed with Exchange include equipment mailboxes. This example changes the name of the address list Resource Rooms to Rooms and Equipment and sets the *IncludedRecipients* parameter to ResourceMailboxes, which includes room and equipment mailboxes.

```
Set-AddressList -Identity "Resource Rooms" -Name "Rooms and Equipment" -IncludedR
```

For detailed syntax and parameter information, see Set-AddressList.

1.8.3.23.2 Create a Room or Equipment Mailbox

Create a Room or Equipment Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A *room mailbox* is a resource mailbox assigned to a meeting location, such as a conference room, auditorium, or training room. An *equipment mailbox* is a resource mailbox assigned to a resource that's not location specific, such as a portable computer, projector, microphone, or a company car. You can use the Exchange Management Console (EMC) and the Exchange Management Shell to create a room or equipment mailbox.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the EMC to create a room or equipment mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration**.

2. In the action pane, click **New Mailbox**.
3. On the **Introduction** page, click **Room Mailbox** or **Equipment Mailbox**, and then click **Next**.
4. On the **User Type** page, click **New user**, and then click **Next**.
5. On the **Mailbox Information** page, complete the following fields:
   - **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.
   - **First name**, **Initials**, and **Last name** Because this mailbox will be used as a resource, it isn't necessary to complete these fields.
   - **Name** Type a name for the user. This is the name that's listed in Active Directory. By default, this box is populated with the names you enter in the **First name**, **Initials**, and **Last name** boxes. If you didn't use those boxes, you must still type a name in this field. The name can't exceed 64 characters.
   - **User logon name (User Principal Name)** Type the name that the user will use to log on to the mailbox. The user logon name consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides.
   - **User logon name (pre-Windows 2000)** Type the name for the user that's compatible with the legacy versions of Microsoft Windows (prior to the release of Windows 2000 Server). This field is automatically populated based on the **User logon name (User Principal Name)** field. This field is required.
   - **Password** Type the password that the user must use to log on to his or her mailbox.

     Note:
     Make sure that the password you supply complies with the password length, complexity, and history requirements of the domain in which you are creating the user account.
   - **Confirm password** To confirm, type the password that you typed in the **Password** box.
   - **User must change password at next logon** Select this check box if you want the user to reset the password when the user first logs on to the mailbox.

     If you select this check box, at first logon, the new user will be prompted with a dialog box in which to change the password. The user won't be allowed to perform any tasks until the password is successfully changed.
6. On the **Mailbox Settings** page, complete the following fields:
   - **Alias** Type an alias for the mailbox. The alias can't exceed 64 characters and must be unique in the forest.
   - **Specify the mailbox database rather than using a database automatically selected** Select this check box to specify a mailbox database instead of allowing Exchange to select a database for you. Click **Browse** to open the **Select Mailbox Database** dialog box. This dialog box lists all the mailbox databases in your Exchange organization. By default, the mailbox databases are sorted by name. You can also click the title of the corresponding column to sort the databases by server name. Select the mailbox database you want to use, and then click **OK**. This is an optional

field.

- **Managed folder mailbox policy** Select this check box to specify a managed folder mailbox policy for the mailbox. A managed folder mailbox policy is a logical grouping of managed folders. When a managed folder mailbox policy is applied to a user's mailbox, all the managed folders linked to the policy are deployed in a single operation, thereby making the deployment of messaging records management (MRM) easier. To learn more, see Understanding Managed Folders.

  Click **Browse** to open the **Select Managed Folder Mailbox Policy** dialog box. Use this dialog box to select the managed folder mailbox policy to be associated with this mailbox. This is an optional field.

  Note:
  Managed custom folders are a premium feature of MRM. Mailboxes with policies that include managed custom folders require an Exchange Server Enterprise client access license (CAL).

- **Exchange ActiveSync mailbox policy** Select this check box to specify an Exchange ActiveSync mailbox policy for the mailbox. Exchange ActiveSync enables access to an Exchange mailbox from a mobile device. To learn more, see Understanding Exchange ActiveSync Mailbox Policies.

  Click **Browse** to open the **Select ActiveSync Mailbox Policy** dialog box. Use this dialog box to select the policy that you want associated with this mailbox. This is an optional field.

7. (Optional) On the **Archive Settings** page, select the **Create an archive mailbox for this account** check box if you want to link an online archive to the mailbox. If you create an archive mailbox for the mailbox, mailbox items will be moved automatically from the primary user mailbox to the archive, based on the default retention policy settings or those you define. To learn more, see Understanding Personal Archives.

   Note:
   Due to the small size of a resource mailbox, we recommend that you don't create an archive for a resource mailbox.

8. On the **New Mailbox** page, review your configuration settings. To make any configuration changes, click **Back**. To create the mailbox, click **New**.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a room mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example creates a room mailbox with the following configuration:

- The resource mailbox resides on Mailbox Database 1.
- The mailbox's name is ConfRoom1 and the name will display in the global address list (GAL) as ConfRoom1.
- The mailbox is in the Conference Rooms organizational unit.
- The user principal name (UPN) is ConfRoom1@contoso.com.
- The *Room* switch specifies that this mailbox will be created as a room mailbox.

```
New-Mailbox -database "Mailbox Database 1" -Name ConfRoom1 -OrganizationalUnit "C
```

For detailed syntax and parameter information, see New-Mailbox.

Use the Shell to create an equipment mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example creates an equipment mailbox with the following configuration:

- The equipment mailbox resides on Mailbox Database 1.
- The equipment's name is DVDPlayer01 and the name will display in the GAL as DVDPlayer01.
- The mailbox is in the Equipment organizational unit.
- The UPN is DVDPlayer01@contoso.com.
- The *Equipment* switch specifies that this mailbox will be created as an equipment mailbox.

```
New-Mailbox -Database "Mailbox Database 1" -Name DVDPlayer01 -OrganizationalUnit
```

For detailed syntax and parameter information, see New-Mailbox.

Other Tasks

After the room or equipment mailbox is created, we recommend that you perform additional configuration tasks based on the needs of your organization. For example, you can configure resource scheduling policies or assign delegates for the mailbox. For details, see Managing Resource Mailboxes and Scheduling.

1.8.3.23.3 Create or Remove Custom Resource Properties

Create or Remove Custom Resource Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to create or remove custom resource properties by modifying the resource configuration of your Exchange organization.

Custom resource properties are features for room or equipment mailboxes. You can indicate that a resource has a specific feature by assigning the corresponding custom resource property to that resource mailbox.

Important:

Custom resource properties can't include spaces.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the Shell to add custom resource

properties to the resource schema

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:
You can't use the EMC to add custom resource properties to the resource schema.

This example creates three custom resource properties for room mailboxes and two custom resource properties for equipment mailboxes. This example also demonstrates two methods for adding new custom resource properties. The syntax of both commands can be used interchangeably.

1. Use the following command to read the current resource configuration and store it in a temporary variable called `$ResourceConfiguration`.

```
$ResourceConfiguration = Get-ResourceConfig
```

2. Use the following commands to create the custom properties AV, TV, and Whiteboard for room mailboxes.

Note:
This example assumes that some of the meeting rooms in your organization have audio-visual equipment, TV, or whiteboards. It also assumes that you want to differentiate the rooms that have the specified features from others that don't.

```
$ResourceConfiguration.ResourcePropertySchema+=("Room/AV")
$ResourceConfiguration.ResourcePropertySchema.Add("Room/TV")
$ResourceConfiguration.ResourcePropertySchema+=("Room/Whiteboard")
```

3. Use the following commands to create the custom properties Car and Van for equipment mailboxes.

Note:
This example assumes that your organization uses equipment mailboxes to track the scheduling of company vehicles, and you plan to use the custom resource properties to specify the vehicle type.

```
$ResourceConfiguration.ResourcePropertySchema.Add("Equipment/Car")
$ResourceConfiguration.ResourcePropertySchema+=("Equipment/Van")
```

4. Use the following commands to update the resource configuration of your organization by using the modified resource property schema.

```
Set-ResourceConfig -ResourcePropertySchema $ResourceConfiguration.Reso
```

For detailed syntax and parameter information, see Get-ResourceConfig and Set-ResourceConfig.

Use the Shell to remove custom resource properties from the resource schema

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example removes two of the custom resource properties for room mailboxes that were created in the previous procedure. The commands also demonstrate two methods for removing a custom resource property. The syntax of both commands can be used interchangeably.

1. Use the following command to read the current resource configuration and store it in a temporary variable called $ResourceConfiguration.

```
$ResourceConfiguration = Get-ResourceConfig
```

2. Use the following commands to remove the custom properties AV and TV from room mailboxes.

```
$ResourceConfiguration.ResourcePropertySchema-=("Room/AV")
$ResourceConfiguration.ResourcePropertySchema.Remove("Room/TV")
```

3. Use the following commands to update the resource configuration of your organization by using the modified resource property schema.

```
Set-ResourceConfig -ResourcePropertySchema $ResourceConfiguration.Reso
```

For detailed syntax and parameter information, see Get-ResourceConfig and Set-ResourceConfig

Other Tasks

After you create custom resource properties, you may also want to assign them to a resource mailbox. For detailed steps, see Configure Custom Resource Properties for a Resource Mailbox.

1.8.3.23.4 Configure Custom Resource Properties for a Resource Mailbox

Configure Custom Resource Properties for a Resource Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A *resource mailbox* is a mailbox that represents conference rooms and company equipment. Resource mailboxes can be included as resources in meeting requests, providing a simple and efficient way to manage the scheduling of resources for your organization.

There are two types of resource mailboxes: room and equipment. *Room mailboxes* are assigned to a meeting location such as a conference room, auditorium, or training room. *Equipment mailboxes* are assigned to a resource that isn't location specific, such as a portable computer projector, microphone, or company car.

Custom resource properties can help users select the most appropriate room or equipment by providing additional information about the resource. For example, you can create a custom property for room mailboxes called AV. You can add this property to all rooms that have audio-visual equipment. This allows users to identify which conference rooms have audio-visual equipment available.

Note:

For every custom resource property you create in your organization, you must specify to which resource mailbox type it applies (room or equipment). When you are managing a resource mailbox, you can assign only those custom resource properties that apply to that specific resource mailbox type. For example, if you are configuring a room mailbox, you can assign only the custom resource properties that apply to room mailboxes.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Prerequisites

Before you can assign custom resource properties to a room or equipment mailbox, you must first create these properties by modifying the resource configuration of your Exchange organization. For detailed instructions, see Create or Remove Custom Resource Properties.

Use the EMC to add or remove custom resource properties for a resource mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the resource mailbox that you want to configure.
3. In the action pane, under the name of the resource mailbox, click **Properties**.
4. In **<Resource Mailbox Name> Properties**, click the **Resource General** tab.
5. Under **Resource custom properties**, perform the following tasks:
   - To add a custom resource property, click **Add**. The **Select Resource Custom Property** dialog box opens. This dialog box displays a list of all custom resource properties defined in your Exchange organization for the specific resource type. Select the custom resource properties you want to assign to this mailbox, and then click **OK**.
   - To remove a custom resource property, select the property you want to remove, and then click  .
6. Click **OK**.

Use the Shell to add custom resource properties to a resource mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example adds the resource property AV to the room mailbox Conference Room 1. This example also overwrites any existing custom resource properties on the mailbox.

```
Set-Mailbox -Identity "Conference Room 1" -ResourceCustom ("AV")
```

This example adds the custom resource properties TV and Whiteboard to the room mailbox Conference Room 1. This example adds the Whiteboard custom property and preserves any existing custom resource properties on the mailbox. This example also demonstrates the two acceptable syntaxes for adding a custom resource property.

```
$ResourceMailbox = Get-Mailbox -Identity "Conference Room 1"
$ResourceMailbox.ResourceCustom+=("TV")
$ResourceMailbox.ResourceCustom.Add("whiteboard")
Set-Mailbox -ResourceCustom $ResourceMailbox.ResourceCustom.Add
```

For detailed syntax and parameter information, see Get-Mailbox and Set-Mailbox.

Use the Shell to remove custom resource

properties from a resource mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example removes the custom resource properties AV and TV from the room mailbox Conference Room 1. This example also demonstrates the two acceptable syntaxes for removing a custom resource property.

```
$ResourceMailbox = Get-Mailbox -Identity "Conference Room 1"
$ResourceMailbox.ResourceCustom-=("AV")
$ResourceMailbox.ResourceCustom.Remove("TV")
Set-Mailbox -Identity "Converence Room 1" $ResourceMailbox.ResourceCustom.Remove
```

For detailed syntax and parameter information, see Get-Mailbox and Set-Mailbox.

1.8.3.23.5 Configure the Automated Booking Policies for a Resource Mailbox

Configure the Automated Booking Policies for a Resource Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-28*

A meeting organizer can send a meeting request to any resource mailbox, which includes conference room and equipment mailboxes. Depending on the scheduling role membership of the meeting organizer, this meeting request can be automatically approved or declined.

In some cases, the meeting request requires special handling to determine if the meeting organizer can schedule a conference room. In this case, an acknowledgement is sent to the meeting organizer, and the request is kept in the resource mailbox or forwarded to a delegate.

Meeting requests sent to the resource mailbox are categorized as one of the following:

- **In-policy meeting requests** These meeting requests don't violate any of the resource scheduling options.
- **Out-of-policy meeting requests** These meeting requests violate one or more of the resource scheduling options. For example, one reason a meeting request is considered out-of-policy is because of a conflict with an existing resource reservation.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the EMC to specify which users can send meeting requests to resource mailboxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox

Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the resource mailbox that you want to configure.
3. In the action pane, under the name of the resource mailbox, click **Properties**.
4. On the **Resource In-Policy Requests** tab, configure the following settings:
   - **All Users** Select this option to allow all users to submit requests within the resource policy's configuration.
   - **Selected recipients** Select this option to specify who can submit requests within the resource policy's configuration. If you select this option, you need to click **Add** to select the recipients. You can also remove selected recipients by clicking **Remove**.
5. On the **Resource Out-of-Policy Requests** tab, specify the users who can submit out-of-policy requests. Users who can submit out-of-policy requests won't have their request denied, but the requests will require approval by one of the resource's delegates. Configure the following settings:
   - **All users** Select this option to allow all users who submit resource requests that don't meet the resource policy's configuration.
   - **Selected recipients** Select this option to add specific users who are allowed to submit out-of-policy requests. If you select the **Selected recipients** option, you need to click the **Add** button to select the recipients. You can also remove selected recipients by clicking **Remove**.

Use the Shell to specify which users can send meeting requests to resource mailboxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

To control who can schedule a resource, use the following parameters with the **Set-CalendarProcessing** cmdlet:

- *AllBookInPolicy*
- *AllRequestInPolicy*
- *AllRequestOutOfPolicy*
- *BookInPolicy*
- *RequestInPolicy*
- *RequestOutOfPolicy*
- *ProcessExternalMeetingMessages*

Note:

When *AllRequestInPolicy* and *AllRequestOutOfPolicy* are both set to True, only out-of-policy requests are forwarded to delegates. Exchange Server automatically accepts in-policy requests, and does not forward the policy requests to a delegate.

This example allows the Calendar Attendant to approve in-policy requests from all users for the room mailbox 5th Floor Conference Room.

```
Set-CalendarProcessing -Identity "5th Floor Conference Room" -AutomateProcessing
```

This example allows all users to submit in-policy requests to the room mailbox 5th Floor Conference Room, but the request is still subject to approval by a delegate.

```
Set-CalendarProcessing -Identity "5th Floor Conference Room" -AutomateProcessing
```

This example allows the Calendar Attendant to accept out-of-policy requests from Alan Brewer to the room mailbox Room222. The request is still subject to approval by a delegate.

```
Set-CalendarProcessing -Identity "Room222" -AutomateProcessing AutoAccept -Reques
```

This example allows a list of users to submit in-policy meeting requests to the equipment mailbox Car54.

```
Set-CalendarProcessing -Identity "Car54" -AutomateProcessing AutoAccept -BookInPo
```

This example rejects meeting requests from any user who isn't a member of the Exchange organization.

```
Set-CalendarProcessing -Identity "Room222" -ProcessExternalMeetingMessages $false
```

For detailed syntax and parameter information, see Set-CalendarProcessing.

Other Tasks

After you specify which users can send meeting requests to resource mailboxes, you may also want to set a delegate on a resource mailbox. For detailed steps, see Set a Delegate on a Resource Mailbox.

1.8.3.23.6 Customize the Response Message for Resource Scheduling

Customize the Response Message for Resource Scheduling

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can create a custom response message that's included in the Accept, Decline, or Acknowledge messages sent back to a meeting organizer.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the EMC to customize the response message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Resource Mailbox Configuration Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the resource mailbox you want to configure.
3. In the action pane, under the name of the resource mailbox, click **Properties**.
4. In **<Resource Mailbox Name> Properties**, click the **Resource Information** tab.
5. Select the **Add additional text** check box to customize the message the requester receives when the meeting has been accepted, declined, or acknowledged. In the **Additional Text** field, type the custom message. For example, type **All requests for Car 54 are subject to approval**.

Use the Shell to customize the response

message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Resource Mailbox Configuration Permissions" section in the Mailbox Permissions topic.

This example sends a response message for all requests made to the equipment mailbox for Car 54.

```
Set-CalendarProcessing -Identity "Car 54" -AddAdditionalResponse:$true  -Addition
```

For detailed syntax and parameter information, see Set-CalendarProcessing.

1.8.3.23.7 Enable or Disable Automatic Booking on a Resource Mailbox

Enable or Disable Automatic Booking on a Resource Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The *Resource Booking Attendant* can accept or decline resource requests based upon policies that you create. If the Resource Booking Attendant is enabled, it uses the booking policies to determine if incoming requests will be accepted or declined. If the Resource Booking Attendant is disabled, the resource mailbox's delegate must accept or decline all requests. For more information about booking policies, see Configure the Automated Booking Policies for a Resource Mailbox.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the EMC to enable or disable automatic booking on a resource mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Resource Mailbox Configuration Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the resource mailbox that you want to configure.
3. In the action pane, under the name of the resource mailbox, click **Properties**.
4. In **<Resource Mailbox Name> Properties**, on the **Resource General** tab, do one of the following:
   - To enable the Resource Booking Attendant, select the **Enable the Resource Booking Attendant** check box. This allows the Resource Booking Attendant to process resource requests and cancellations automatically.
   - To disable the Resource Booking Attendant, clear the **Enable the Resource Booking Attendant** check box.
5. Click **Apply** to apply the changes, or click **OK** to apply the changes and close the dialog box.

Use the Shell to enable automatic booking

on a resource mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Resource Mailbox Configuration Permissions" section in the Mailbox Permissions topic.

This example enables the Resource Booking Attendant for the resource mailbox Room 222 by setting the *AutomateProcessing* parameter to **AutoAccept**. With this setting enabled, the Resource Booking Attendant will use the booking policies to determine if incoming requests will be accepted or declined.

```
Set-CalendarProcessing "Room 222" -AutomateProcessing AutoAccept
```

For detailed syntax and parameter information, see Set-CalendarProcessing.

Use the Shell to disable automatic booking on a resource mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Resource Mailbox Configuration Permissions" section in the Mailbox Permissions topic.

This example disables the Resource Booking Attendant for the resource mailbox Car 54 by setting the *AutomateProcessing* parameter to **AutoUpdate**. With this setting enabled, the Resource Booking Attendant is disabled, but the Calendar Attendant is still enabled.

```
Set-CalendarProcessing "Car 54" -AutomateProcessing AutoUpdate
```

For detailed syntax and parameter information, see Set-CalendarProcessing.

Other Tasks

After you enable automatic booking on a resource mailbox, you may also want to configure the policies for accepting or declining requests. For detailed steps, see Configure User and Resource Mailbox Properties.

1.8.3.23.8 List Available Resource Mailboxes and Their Properties

List Available Resource Mailboxes and Their Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A *resource mailbox* is a mailbox that represents conference rooms and company equipment. Resource mailboxes can be included as resources in meeting requests, providing a simple and efficient way to utilize resources for an organization. By default, the user account associated with a resource mailbox is disabled.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the EMC to list available resource mailboxes and their properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Resource Mailbox Configuration Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, click **Create Filter**.
3. Use the drop-down lists to create a filter that displays the resource mailboxes you want:
   - If you want to display conference room mailboxes, select **Recipient Type Details**, select **Equals**, and then select **Conference Room Mailbox**.
   - If you want to display equipment mailboxes, select **Recipient Type Details**, select **Equals**, and then select **Equipment Mailbox**.
4. Click **Apply Filter** to display the results.

Use the Shell to list available resource mailboxes and their properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Resource Mailbox Configuration Permissions" section in the Mailbox Permissions topic.

This example lists available room mailboxes.

```
Get-Mailbox -RecipientTypeDetails RoomMailbox
```

This example lists available equipment mailboxes.

```
Get-Mailbox -RecipientTypeDetails EquipmentMailbox
```

For detailed syntax and parameter information, see Get-Mailbox.

1.8.3.23.9 Publish Free/Busy Information for More Than Two Months in Exchange 2010

Publish Free/Busy Information for More Than Two Months in Exchange 2010

Mailbox > Managing Mailbox Servers > Managing Resource Mailboxes and Scheduling >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-03*

This topic explains how to configure Microsoft Exchange Server 2010 so that published Free/Busy information for a mailbox is displayed for more than a two-month period. To do this, you must configure the registry on the server that is running both Microsoft Exchange and Resource Booking Attendant.

By default, Microsoft Office Outlook displays the Free/Busy information for a mailbox for a two-month period. If you want to display Free/Busy information for a longer period, you must add the **Excdo\Parameters** subkey to the registry, and then add the value for the period in which you want to display Free/Busy information. After you make this change, restart the Internet Information Services (IIS) Admin service and the Microsoft Exchange

System Attendant service.

To change the amount of Free/Busy information that is displayed for mailboxes

1. Start Registry Editor.
2. Expand the following subkey:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
3. Right-click **Microsoft**, point to **New**, and then click **Key**.
4. Type **Excdo**, and then press ENTER to name the new key.
5. Right-click **Excdo**, point to **New**, and then click **Key**.
6. Type **Parameters**, and then press ENTER to name the new subkey.
7. Right-click **Parameters**, point to **New**, and then click **DWORD (32-bit) Value**.
8. Type **FBPublishMonths**, and then press ENTER to name the new value.
9. Right-click **FBPublishMonths**, and then click **Modify**.
10. Click Decimal. Then, in the **Value data** box, type the number of months for which you want to publish Free/Busy information. For example, if you want to publish Free/Busy data for four months, type **4** in the **Value data** box.
11. Click **OK**, and then exit Registry Editor.
12. Restart the IIS Admin service and the Microsoft Exchange System Attendant service. To do this, type the following commands at a command prompt, and then press ENTER after each command:
    iisreset
    net stop msexchangesa && net start msexchangesa

For More Information

For more information about managing resource mailboxes or scheduling, see Managing Resource Mailboxes and Scheduling.

1.8.3.23.10 Remove Full Access Permissions from a Resource Mailbox Schedule

Remove Full Access Permissions from a Resource Mailbox Schedule

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to remove Full Access permissions from a resource mailbox schedule. A *resource mailbox* is a mailbox that represents conference rooms and company equipment and is used for conference room or equipment scheduling. The user account associated with a resource mailbox is disabled.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the Shell to remove Full Access permissions from a resource mailbox schedule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to remove Full Access permissions from a resource mailbox schedule.

This example removes Tony's permissions to access the resource mailbox Car 54.

```
Remove-MailboxPermission -AccessRights FullAccess -Identity "Car 54" -User Tony@c
```

For detailed syntax and parameter information, see Remove-MailboxPermission.

1.8.3.23.11 Set a Delegate on a Resource Mailbox

Set a Delegate on a Resource Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can set a delegate on a resource mailbox to control the scheduling options for that resource mailbox and to have all requests forwarded to the delegate.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the EMC to set a delegate on a resource mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Resource Mailbox Configuration Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the resource mailbox that you want to configure.
3. In the action pane, under the name of the resource mailbox, click **Properties**.
4. In **<Resource Mailbox Name> Properties**, click the **Resource Policy** tab.
5. Under **Specify delegates of this mailbox**, perform the following tasks:
   - To add a resource delegate, click **Add**, and then select the recipient.
   - To remove a resource delegate, select the delegate, and then click **Remove**.
6. If you want to forward all meeting requests to the delegates listed, select the **Forward meeting requests to delegates** check box.
7. Click **Apply** to save your changes, or click **OK** to save your changes and close the dialog box.

Use the Shell to set a delegate on a resource mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Resource Mailbox Configuration Permissions" section in the Mailbox Permissions topic.

This example uses the primary SMTP address for Ed, Ayla, and Tony to set them as the delegates for the resource mailbox Room222

```
Set-CalendarProcessing -Identity "Room222" -ResourceDelegates "ed@contoso.com","a
```

Note:
Don't run this cmdlet on a user mailbox. This causes the user's mail to be forwarded to the assigned delegate.

For detailed syntax and parameter information, see Set-CalendarProcessing.

1.8.3.23.12 Set Full Access Permissions to a Resource Mailbox Schedule

Set Full Access Permissions to a Resource Mailbox Schedule

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to set Full Access permissions to a resource mailbox schedule. A *resource mailbox* is a mailbox that represents conference rooms and company equipment and is used for conference room or equipment scheduling. The user account associated with a resource mailbox is disabled.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Use the Shell to set Full Access permissions to a resource mailbox schedule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Permissions and delegation" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to set Full Access permissions to a resource mailbox schedule.

This example grants Tony Full Access permissions to Car54's schedule.

```
Add-MailboxPermission -AccessRights FullAccess -Identity Car54 -User Tony
```

For detailed syntax and parameter information, see Add-MailboxPermission.

1.8.3.23.13 Upgrade Exchange 2003 Auto Accept Agent-Based Resource Mailboxes to Exchange 2010

Upgrade Exchange 2003 Auto Accept Agent-Based Resource Mailboxes to Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A *resource mailbox* is a mailbox that represents conference rooms and company equipment. Resource mailboxes are used for conference room or equipment scheduling. The Auto Accept agent is an Exchange store event sink that automatically processes meeting requests for resource mailboxes. In Microsoft Exchange Server 2003, you must use the Auto Accept agent for resource mailboxes. Because Exchange Server 2010 supports automatic booking for resource mailboxes, the Auto Accept agent isn't required.

Upgrading Exchange 2003 Auto Accept agent-based resource mailboxes to Exchange 2010 involves the following steps:

1. Unregister the Exchange 2003 Auto Accept agent-based resource mailboxes from the Exchange 2003 store.
2. Move the resource mailboxes from the Exchange 2003 server to an Exchange 2010 Mailbox server.
3. Convert the Exchange 2003 Auto Accept agent-based mailbox to an Exchange 2010 resource mailbox.
4. Configure automated processing for the Exchange 2010 resource mailbox.

Looking for other management tasks related to resource mailboxes? Check out Managing Resource Mailboxes and Scheduling.

Step 1: Use a command prompt to unregister the Exchange 2003 Auto Accept agent

To perform this procedure, the account you use must be an Exchange Admin account and have Local Administrator rights.

From a Command Prompt window on an Exchange 2003 computer, use the following example to unregister the Exchange 2003 Auto Accept agent-based resource mailboxes from the Exchange 2003 store.

```
cscript RegisterMailbox.vbs /u /m:"Room2@Fabrikam.Contoso.com"
```

This script is located in the Auto Accept agent installation directory (usually %Program Files%\Exchsrvr\Agents\AutoAccept).

Step 2: Use the EMC or the Shell to move the mailbox to an Exchange 2010 Mailbox server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox moves" entry in the Mailbox Permissions topic.

You can use the EMC or the Shell to move the Auto Accept agent-based resource mailboxes from the Exchange 2003 server to an Exchange 2010 Mailbox server. For detailed instructions, see the following topics:

- Create a Local Move Request
- Create a Remote Move Request That has Exchange 2010 in Both Forests
- Create a Remote Legacy Move Request Where One of the Forests Doesn't Have Exchange 2010

Step 3: Use the Shell to convert the Auto

Accept agent-based mailbox to an Exchange 2010 resource mailbox

After you move the Exchange 2003 resource mailbox to Exchange 2010, it's considered a shared mailbox. You must convert the shared mailbox to an Exchange 2010 resource mailbox.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:
You can't use the EMC to convert the Auto Accept agent-based mailbox.

This example converts the mailbox Room222 to a room mailbox.

```
Set-Mailbox Room222 -Type Room
```

For more information, see Convert a Mailbox.

Step 4: Use the Shell to configure automatic processing of the Exchange 2010 resource mailbox

After you convert the mailbox to an Exchange 2010 resource mailbox, you may want to configure the resource mailbox to automate the processing of meeting requests.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Calendar processing" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure automatic processing of resource mailboxes.

This example configures the automatic processing of the room mailbox Room222 to approve in-policy requests from all users.

```
Set-CalendarProcessing -Identity Room222 -AutomateProcessing AutoAccept -AllBookI
```

For more information, see the following topics:

- Enable or Disable Automatic Booking on a Resource Mailbox
- Configure the Automated Booking Policies for a Resource Mailbox

1.8.3.24 Managing User Mailboxes

Managing User Mailboxes

Exchange Server 2010 > Mailbox > Managing Mailbox Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-16*

1.8.3.24.1 Add an E-Mail Address for a User Mailbox

Add an E-Mail Address for a User Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) and the Exchange Management Shell to add an e-mail address for a user mailbox.

Looking for other management tasks related to managing user mailboxes? Check out Managing User Mailboxes.

Use the EMC to add an e-mail address for a user mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox for which you want to add an e-mail address.
3. In the action pane, under the mailbox name, click **Properties**.
4. In **<User Mailbox > Properties**, click the **E-Mail Addresses** tab.
5. To create an e-mail address, under **E-mail Addresses**, click the arrow next to **Add** and select from the following address types:
   - **SMTP Address** This is the default address type. Click this button and use the corresponding dialog box to add an SMTP address.
   - **EUM Address** An Exchange Unified Messaging (EUM) address is used by Unified Messaging (UM) servers to locate UM-enabled users within a Microsoft Exchange Server 2010 organization. EUM addresses contain the extension number and the UM dial plan for the UM-enabled user. Click this button and use the corresponding dialog box to add an EUM address.
   - **Custom Address** Click this button and use the corresponding dialog box to add a custom address (for example, fax or X.400).

   Note:
   With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.
6. Click **Apply**, and then click **OK**.

Use the Shell to add an e-mail address for a user mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example shows how to add an additional address to the user john@contoso.com. For more information about adding and removing values from multivalued properties, see Modifying Multivalued Properties.

```
Set-Mailbox john@contoso.com -EmailAddresses @{add="john@northamerica.contoso.com
```

For detailed syntax and parameter information, see Set-Mailbox or Get-Mailbox.

1.8.3.24.2 Change the Languages for a User Mailbox

Change the Languages for a User Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Exchange Management Shell to change the languages for a user mailbox.

In Microsoft Exchange Server 2010, you can specify multiple languages for a mailbox, in order of preference. Several Exchange components display information to a mailbox user in the preferred language, if that language is supported. These components include quota messages, non-delivery reports (NDRs), the Microsoft Office Outlook Web App user interface, and Unified Messaging (UM) voice prompts.

Note:
For Exchange Server 2003, the language for quota messages and NDRs wasn't determined by the Exchange server. Instead, the language for these messages was determined by the language setting on the Outlook client computer used to view the NDR. To make sure that users who migrated from Exchange 2003 or earlier versions continue to receive these messages in their preferred language, set the language to match the language settings configured on their Outlook client computer.

The language for a mailbox can be set by using the *Languages* parameter of the **Set-Mailbox** cmdlet. An acceptable value for this parameter is a combination of an ISO 639 two-letter lowercase culture code associated with a language and an ISO 3166 two-letter uppercase subculture code associated with a country or region. To learn more about culture codes and to view a complete list of acceptable values, see CultureInfo Class in the MSDN Library.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the Shell to change the languages for a user mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "User mailboxes users" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to change the languages for a user mailbox.

This example sets the language for the user Katarina Larsson to Finnish.

```
Set-Mailbox -Identity "Katarina Larsson" -Languages "fi-FI"
```

Note:
This command overwrites any existing languages for the mailbox.

This example adds the language Turkish to the user mailbox Cigdem Akin without overwriting any existing languages.

```
$Mailbox = Get-Mailbox -Identity "Cigdem Akin"
$Mailbox.Languages += "tr-TR"
Set-Mailbox -Identity "Cigdem Akin" $Mailbox.languages
```

For detailed syntax and parameter information, see Set-Mailbox.

Create a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-16*

Mailboxes are the most common recipient type used by information workers in an Exchange organization. Each mailbox is associated with an Active Directory user account. The user can use the mailbox to send and receive messages, and to store messages, appointments, tasks, notes, and documents. You can also create mailboxes for resources such as meeting rooms and equipment. Mailboxes are the primary messaging and collaboration tools for the users in your organization. To learn more about mailboxes, see Understanding Recipients.

Looking for other management tasks related to mailboxes? See Managing User Mailboxes.

What Do You Want to Do?

- Use the EMC to create a mailbox
- Use the Shell to create a single new mailbox
- Use the Shell to mail-enable existing users
- Use the Shell to create a linked mailbox

Use the EMC to create a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox users" entry in the Mailbox Permissions topic.

If you want to create mailboxes for new users, you'll have to use this wizard for each new user mailbox; you can't use the wizard to create multiple user mailboxes. However, you can use the wizard to create multiple mailboxes for existing users.

Note:

If you create mailboxes for multiple existing users, you must create mailboxes of the same type.

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Mailbox**.

3. On the **Introduction** page, select one of the following options:
   - **User Mailbox** Click this button to create a mailbox that is owned by a user to send and receive e-mail messages. User mailboxes can't be used for resource scheduling.

     The Active Directory account that is associated with user mailboxes must reside in the same forest as the Exchange server. To use an account in a trusted forest, select **Linked Mailbox**.
   - **Room Mailbox** Click this button to create a mailbox that will be used as a location resource for scheduling meetings. Room mailboxes can be included in meeting requests as resources and can be configured to automatically process incoming requests.

     If you create a new user account for the room mailbox in Active Directory, it will be disabled. If you plan to associate the room mailbox with an existing account, you must select a disabled account.
   - **Equipment Mailbox** Click this button to create a mailbox that will be used

as a resource for scheduling meetings. Equipment mailboxes can be included in meeting requests as resources and can be configured to automatically process incoming requests.

As a best practice, create mailboxes for shared meeting equipment, such as projectors or audio equipment, which can be moved to different meeting rooms.

If you create a new user account for the equipment mailbox in Active Directory, it will be disabled. If you plan to associate the equipment mailbox with an existing account, you must select a disabled account.

- **Linked Mailbox** Click this button to create a user mailbox that is accessed by a user in a separate, trusted forest. You must still create a user account in the forest in which Exchange Server resides. This is required to create the necessary Active Directory object for storing the mailbox information.

  Linked mailboxes might be necessary for organizations that choose to deploy Exchange in a resource forest. The resource forest scenario allows an organization to centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests.

  Note:
  You cannot create linked mailboxes for multiple existing users. You can only use this wizard to create one linked mailbox at a time.

4. On the **User Type** page, select one of the following options:
   - **New User** Click this button to simultaneously create a new user in Active Directory and mail-enable the user.

     If you click this button, you'll need to provide the required user account information on the **User Information** page of this wizard.
   - **Existing users** Click this button to mail-enable one or more existing users.

     Click **Add** to open the **Select User** dialog box. This dialog box displays a list of user accounts in the forest that aren't mail-enabled or don't have Exchange mailboxes. Select the user accounts you want to mail-enable, and then click **OK** to return to the wizard.

     To remove a user from the list, select the user name, and then click  .

5. If you selected **New User** in Step 4, complete the following fields on the **User Information** page. Otherwise skip to Step 6:
   - **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.
   - **First name** Use this box to type the first name of the user. This field is optional.
   - **Initials** Use this box to type the initials of the user. This field is optional.
   - **Last name** Use this box to type the last name of the user. This field is optional.
   - **Name** Use this box to type a name for the user. This is the name that's

listed in Active Directory. By default, this box is populated with the names you enter in the **First name**, **Initials**, and **Last name** boxes. If you didn't use those boxes, you must still type a name in this field. The name can't exceed 64 characters.

Note:
In Exchange 2010, the mailbox's alias is generated based on the Name property. Invalid characters in the name will be replaced with a question mark (?) when the alias is generated.

- **User logon name (User Principal Name)** Use this box to type the name that the user will use to log on to the mailbox. The user logon name consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides.
- **User logon name (pre-Windows 2000)** Use this box to type the name for the user that is compatible with the legacy versions of Microsoft Windows (prior to the release of Windows 2000 Server). This field is automatically populated based on the **User logon name (User Principal Name)** field. This field is required.
- **Password** Use this box to type the password that the user must use to log on to his or her mailbox. This box won't be available if you're creating a room, equipment, or linked mailbox.

Note:
Make sure that the password you supply complies with the password length, complexity, and history requirements of the domain in which you are creating the user account.

- **Confirm password** Use this box to confirm the password that you typed in the **Password** box. This box won't be available if you're creating a room, equipment, or linked mailbox.
- **User must change password at next logon** Select this check box if you want the user to reset the password when they first logon to the mailbox. This box won't be available if you're creating a room, equipment or linked mailbox.

  If you select this check box, at first logon, the new user will be prompted with a dialog box in which to change the password. The user won't be allowed to perform any tasks until the password is successfully changed.

6. On the **Mailbox Settings** page, complete the following fields:
   - **Alias** This field is automatically populated with the text that you specified in the **Name** box. If you're creating a new user, or if you selected a single existing user to mail-enable, you can modify the alias for the mailbox. If you're mail-enabling more than one existing user, you can't specify a value for this field. The alias can't exceed 64 characters and must be unique in the forest.
   - **Specify the mailbox database rather than using a database automatically selected** Select this check box to specify a mailbox database instead of allowing Exchange to select a database for you. Click **Browse** to open the **Select Mailbox Database** dialog box. This dialog box lists all the mailbox databases in your Exchange organization. By default, the mailbox databases are sorted by name. You can also click the title of the corresponding column to sort the databases by server name. Select the mailbox database you want to use, and then click **OK**. This is an optional field.
   - **Retention policy** Select this check box to specify a retention policy for the mailbox. Retention policies allow you to group one or more retention tags and apply them to mailboxes to enforce message retention settings. A mailbox can't have more than one retention policy. To learn more, see Understanding Retention Tags and Retention Policies.

     Click **Browse** to open the **Select Retention Policy** dialog box.

Use this dialog box to select the retention policy to be associated with this mailbox. This is an optional field.

- **Exchange ActiveSync mailbox policy** Select this check box to specify an Exchange ActiveSync mailbox policy for the mailbox. Exchange ActiveSync enables access to an Exchange mailbox from a mobile device. To learn more, see Understanding Exchange ActiveSync Mailbox Policies.

  Click **Browse** to open the **Select ActiveSync Mailbox Policy** dialog box. Use this dialog box to select the policy that you want associated with this mailbox. This is an optional field.
- **Address book policy** Select this check box to specify an address book policy (ABP) for the mailbox. ABPs contain a GAL, an offline address book (OAB), a room list, and a set of address lists. When assigned to mailbox users, an ABP provides them with access to a customized GAL in Outlook and Outlook Web App. To learn more, see Understanding Address Book Policies.

  Click **Browse** to open the **Select Address Book Policy** dialog box. Use this dialog box to select the policy that you want associated with this mailbox.

7. On the **Archive Settings** page, complete the following fields:

Note:
This page isn't available if you're creating a room, equipment, or linked mailbox.

- **Don't create an archive** Click this button if you don't want to create an archive for the mailbox.
- **Create a local archive** Click this button to create a personal (also known as a *local* or *on-premises* archive) for the mailbox.

  If you create a personal archive, mailbox items will be moved automatically from the primary mailbox to the archive, based on the default retention policy settings or those you define. If you click this button, the following settings are available:

  Select a specific mailbox database rather than having one selected automatically Select this check box and then click **Browse** to select a database that resides in the local forest. To learn more, see Understanding Personal Archives.
- **Create a remote hosted archive** Click this button to create a cloud-based archive. To create a cloud-based archive, you must first configure Exchange Online Archiving. For details, see Configure Exchange Online Archiving. If you've already configured Exchange Online Archiving, click **Browse** to select the domain name of the cloud-based organization. To learn more, see Understanding Exchange Online Archiving.

8. If you selected **Linked Mailbox** in Step 3, complete the following fields on the **Master Account** page. Otherwise skip to Step 9.
   - **Trusted forest or domain** Click **Browse** to open the **Select Trusted Forest or Domain** dialog box. Use this dialog box to select the forest or domain that contains the master account, and then click **OK**. This enables the **Browse** button for the **Linked domain controller** field.
   - **Use the following Windows user account to access linked domain controller** To access the domain controller in the trusted forest or domain, you can use credentials other than the ones with which you are currently logged on. If you want to specify a different user account, select this check box, and then use the **User name** and **Password** boxes to type your credentials.
   - **Linked domain controller** Click **Browse** to open the **Select Domain Controller** dialog box. Use this dialog box to select the linked domain controller that you want to use, and then click **OK**. Selecting a valid linked domain controller enables the **Browse** button for **the Linked master account** field.

- **Linked master account** Click **Browse** to open the **Select Master Account** dialog box. Use this dialog box to select the user account that you want to use as the master account for the linked mailbox, and then click **OK**.

9. On the **New Mailbox** page, review your configuration settings. To make any configuration changes, click **Back**. To create the new mailbox, click **New**.

10. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a single mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox users" entry in the Mailbox Permissions topic.

This example creates a mailbox for the user Chris Ashton with the following details:

- The mailbox's alias is Chris
- The user's first name is Chris and the last name is Ashton
- The name and display name is Chris Ashton
- The user principal name (UPN) is ChrisAshton@contoso.com
- The mailbox will be created in the Users container of the organizational unit

```
New-Mailbox -Alias chris -Name "Chris Ashton" -FirstName Chris -LastName Ashton -
```

This example creates a mailbox for the 3rd floor conference room with the following details:

- The room mailbox's alias is 3rdfloorconf
- The first name is 3rd Floor and the last name is Conference Room
- The name and display name is 3rdFloor Conference Room
- The UPN is 3rdfloorconf@contoso.com
- The mailbox will be created in the Room container of the organizational unit

```
New-Mailbox -Alias 3rdfloorconf -Name "3rd Floor Conference Room" -FirstName "3rd
```

For syntax and parameter information, see New-Mailbox.

Use the Shell to mail-enable existing users

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox users" entry in the Mailbox Permissions topic.

This example mail-enables the user john@contoso.com on the database Sales

```
Enable-Mailbox john@contoso.com -Database Sales
```

You can also use the **Enable-Mailbox** cmdlet to mail-enable multiple users. You can do this by piping the results of the **Get-User** cmdlet to the **Enable-Mailbox** cmdlet. When you run the **Get-User** cmdlet, you must return only users that aren't already mail-enabled. To do this, you need specify the value User with the *RecipientTypeDetails* parameter. You can also limit the results returned by using the *Filter* parameter to request only users that meet the criteria you specify. You then pipe the results to the **Enable-Mailbox** cmdlet.

For example, this command mail-enables users who aren't already mail-enabled and that contain the text "Contoso" in the Company user field.

```
Get-User -RecipientTypeDetails User -Filter { Company -Eq 'Contoso' } | Enable-Ma
```

For syntax and parameter information, see Enable-Mailbox and Get-User.

For more information about pipelining, see Pipelining.

Use the Shell to create a linked mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox User" entry in the Mailbox Permissions topic.

When you create a linked mailbox, you must use the *LinkedMasterAccount* parameter to specify the account in the account forest. You must also use the *LinkedDomainController* parameter to specify the domain controller of the account domain you want to contact and the *LinkedCredential* parameter to specify the credentials that allow access to the account domain. For example, this command creates a mailbox for the user John Peoples and links the mailbox to John's account on the domain controller DC01fabrikam.

```
New-Mailbox -Database "Mailbox Database 1" -Name "John Peoples" -LinkedDomainCont
```

For syntax and parameter information, see New-Mailbox.

1.8.3.24.4 Create a Mailbox for an Existing User

Create a Mailbox for an Existing User

Mailbox > Managing Mailbox Servers > Managing User Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) and the Exchange Management Shell to create a mailbox for an existing user. After you mailbox-enable an existing user on a specified Mailbox server, the user can send and receive e-mail messages.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the EMC to create a mailbox for an existing user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "User mailboxes" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration**.
2. In the action pane, click **New Mailbox**.
3. On the **Introduction** page, click **User Mailbox**, and then click **Next**.
4. On the **User Type** page, click **Existing user**, and then click **Add**.
5. In **Select User**, select the user for whom you want to create a mailbox, and then click **OK**.
6. Click **Next**.

7. On the **Mailbox Settings** page, complete the following fields:
   - **Alias** Use this box to type the alias for the user mailbox. If the user logon name contains any characters that aren't valid for the alias field, they will be replaced by underscore characters (_). The alias can't exceed 64 characters and must be unique in the forest. If you're creating mailboxes for multiple existing users, this box will be unavailable and will display the following message: **An alias will be automatically generated for each new mailbox**.
   - **Specify the mailbox database rather than using a database automatically selected** Select this check box to specify a mailbox database instead of allowing Exchange to select a database for you. Click **Browse** to open the **Select Mailbox Database** dialog box. This dialog box lists all the mailbox databases in your Exchange organization. By default, the mailbox databases are sorted by name. You can also click the title of the corresponding column to sort the databases by server name. Select the mailbox database you want to use, and then click **OK**. This is an optional field.
   - **Managed folder mailbox policy** Select this check box to specify a managed folder mailbox policy for the mailbox. A managed folder mailbox policy is a logical grouping of managed folders. When a managed folder mailbox policy is applied to a user's mailbox, all the managed folders linked to the policy are deployed in a single operation, thereby making the deployment of messaging records management (MRM) easier. To learn more, see Understanding Managed Folders.

     Click **Browse** to open the **Select Managed Folder Mailbox Policy** dialog box. Use this dialog box to select the managed folder mailbox policy to be associated with this mailbox. This is an optional field.

     Note:
     Managed custom folders are a premium feature of MRM. Mailboxes with policies that include managed custom folders require an Exchange Server Enterprise client access license (CAL).
   - **Exchange ActiveSync mailbox policy** Select this check box to specify a Microsoft Exchange ActiveSync mailbox policy for the mailbox. Exchange ActiveSync enables access to an Exchange mailbox from a mobile device. To learn more, see Understanding Exchange ActiveSync Mailbox Policies.

     Click **Browse** to open the **Select ActiveSync Mailbox Policy** dialog box. Use this dialog box to select the policy that you want associated with this mailbox. This is an optional field.
8. On the **New Mailbox** page, review the **Configuration Summary**. This summary contains information about the options you have selected for the mailbox. To make changes to these options, click **Back**. To create the new mailbox, click **New**.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a mailbox for an existing user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "User mailboxes" entry in the Mailbox Permissions topic.

This example creates a mailbox for the existing user John in the contoso.com domain.

```
Enable-Mailbox john@contoso.com -Database "MyServer\Mailbox Database"
```

For detailed syntax and parameter information, see Enable-Mailbox.

Other Tasks

After you create a mailbox, you may want to:

- Configure Anti-Spam Features on a Mailbox
- Configure Message Size Limits for a Mailbox or a Mail-Enabled Public Folder
- Configure Storage Quotas for a Mailbox
- Restrict the Number of Recipients per Message
- Configure resource mailbox settings (if this is a resource mailbox). For more information about the different configuration options on a resource mailbox, see Managing Resource Mailboxes and Scheduling.

1.8.3.24.5 Create a Linked Mailbox

Create a Linked Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A linked mailbox is a mailbox associated with an external account. The resource forest scenario is an example of when you would want to associate a mailbox with an external account. In a resource forest scenario, user objects in the Exchange forest have mailboxes, but the user objects are disabled for logon. You must associate these disabled user accounts in the Exchange forest with enabled user objects in the external accounts forest.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the EMC to create a linked mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration**.
2. In the action pane, click **New Mailbox**.
3. On the **Introduction** page, click **Linked Mailbox**, and then click **Next**.
4. On the **User Type** page, click **New User**.

   Note:

   Every mailbox must have a user account associated with it. However, the user account that will access the linked mailbox doesn't exist in the forest where Exchange is deployed. Therefore, a disabled user account that exists in the same forest as Exchange must be created and associated with each linked mailbox, which is the new user account to which this wizard page is referring.

5. Click **Next**.

6. On the **User Information** page, complete the following fields. These fields are for the disabled user account that will be associated with the linked mailbox, and not for the actual user account in the remote forest that will be accessing the mailbox:
   - **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.
   - **First name** Use this box to type the first name of the user. This field is optional.
   - **Initials** Use this box to type the initials of the user. This field is optional.
   - **Last name** Use this box to type the last name of the user. This field is optional.
   - **Name** Use this box to type a name for the user. This is the name that's listed in Active Directory. By default, this box is populated with the names you enter in the **First name**, **Initials**, and **Last name** boxes. If you didn't use those boxes, you must still type a name in this field. The name can't exceed 64 characters.
   - **User logon name (User Principal Name)** Use this box to type the name that the user will use to log on to the mailbox. The user logon name consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides.
   - **User logon name (pre-Windows 2000)** Use this box to type the name for the user that's compatible with the legacy versions of Microsoft Windows (prior to the release of Windows 2000 Server). This field is automatically populated based on the **User logon name (User Principal Name)** field. This field is required.
   - **Password** Use this box to type the password that the user must use to log on to his or her mailbox.

     Note:
     Make sure that the password you supply complies with the password length, complexity, and history requirements of the domain in which you're creating the user account.

   - **Confirm password** Use this box to confirm the password that you typed in the **Password** box.
   - **User must change password at next logon** Select this check box if you want the user to reset the password when first logging on to the mailbox. If you select this check box, at first logon, the new user will be prompted with a dialog box in which to change the password. The user won't be allowed to perform any tasks until the password is successfully changed.
7. Click **Next**.
8. On the **Mailbox Settings** page, complete the following fields:
   - **Alias** Use this box to type an alias for the mailbox. The alias can't exceed 64 characters and must be unique in the forest.
   - **Specify the mailbox database rather than using a database automatically selected** Select this check box to specify a mailbox database instead of allowing Exchange to select a database for you. Click **Browse** to open the **Select Mailbox Database** dialog box. This dialog box lists all the mailbox databases in your Exchange organization. By default, the mailbox databases are sorted by name. You can also click the title of the corresponding column to sort the databases by storage group name or

server name. Select the mailbox database you want to use, and then click **OK**. This is an optional field.

- **Managed folder mailbox policy** Select this check box to specify a managed folder mailbox policy for the mailbox. A managed folder mailbox policy is a logical grouping of managed folders. When a managed folder mailbox policy is applied to a user's mailbox, all the managed folders linked to the policy are deployed in a single operation, thereby making the deployment of messaging records management (MRM) easier. To learn more, see Understanding Managed Folders.

  Click **Browse** to open the **Select Managed Folder Mailbox Policy** dialog box. Use this dialog box to select the managed folder mailbox policy to be associated with this mailbox. This is an optional field.

  Note:
  Managed custom folders are a premium feature of MRM. Mailboxes with policies that include managed custom folders require an Exchange Server Enterprise client access license (CAL).

- **Exchange ActiveSync mailbox policy** Select this check box to specify a Microsoft Exchange ActiveSync mailbox policy for the mailbox. Exchange ActiveSync enables access to an Exchange mailbox from a mobile device. To learn more, see Understanding Exchange ActiveSync Mailbox Policies.

  Click **Browse** to open the **Select ActiveSync Mailbox Policy** dialog box. Use this dialog box to select the policy that you want associated with this mailbox. This is an optional field.

9. Click **Next**.
10. On the **Master Account** page, complete the following fields:
    - **Trusted forest or domain** Click **Browse** to open the **Select Trusted Forest or Domain** dialog box. Use this dialog box to select the forest or domain that contains the master account, and then click **OK**. This enables the **Browse** button for the **Linked domain controller** field.
    - **Use the following Windows user account to access linked domain controller** To access the domain controller in the trusted forest or domain, you can use credentials other than the ones with which you are currently logged on. If you want to specify a different user account, select this check box, and then use the **User name** and **Password** boxes to type your credentials.
    - **Linked domain controller** Click **Browse** to open the **Select Domain Controller** dialog box. Use this dialog box to select the linked domain controller that you want to use, and then click **OK**. Selecting a valid linked domain controller enables the **Browse** button for **the Linked master account** field.
    - **Linked master account** Click **Browse** to open the **Select Master Account** dialog box. Use this dialog box to select the user account that you want to use as the master account for the linked mailbox, and then click **OK**.
11. Click **Next**.
12. On the **New Mailbox** page, review the **Configuration Summary**. To change the configuration, click **Back**. To create the new linked mailbox, click **New**.
13. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a linked mailbox

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example creates a linked mailbox for John Peoples. The fabrikam domain is in the accounts forest. The user account fabrikam\Admin01 is used to access the linked domain controller.

```
New-Mailbox -Database "Mailbox Database 1" -Name "John Peoples" -LinkedDomainCont
```

For detailed syntax and parameter information, see New-Mailbox.

1.8.3.24.6 Create a Remote Mailbox

Create a Remote Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the New Remote Mailbox wizard to create a mail-enabled user in your Microsoft Exchange Server 2010 on-premises organization with an associated mailbox in the cloud-based service.

A remote mailbox consists of a mail-enabled user that exists in the on-premises Active Directory and an associated mailbox that exists in the cloud-based service. When you create a new remote mailbox, the mail-enabled user is created in your on-premises Active Directory. Then, directory synchronization, if it's configured, automatically synchronizes this new user object to the cloud-based service which then converts it to a user mailbox. You can create remote mailboxes as regular user mailboxes or as resource mailboxes for meeting rooms and equipment.

Directory synchronization and mail flow should be configured correctly for a mailbox to be created in the service. Creation of the mailbox in the service isn't immediate and depends on the directory synchronization schedule.

To learn more about remote mailboxes, see Understanding Recipients.

Looking for other management tasks related to remote mailboxes? See Managing User Mailboxes.

Use the EMC to create a remote mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote mailboxes" entry in the Mailbox Permissions topic.

If you want to create remote mailboxes, you'll have to use this wizard for each remote mailbox. You can't use the wizard to create multiple remote mailboxes.

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Remote Mailbox**.
3. On the **Introduction** page, select one of the following options:
   - **User Mailbox** Click this button to create a remote mailbox in the cloud-based service that is owned by a user to send and receive e-mail messages. User remote mailboxes can't be used for resource scheduling.
   - **Room Mailbox** Click this button to create a remote mailbox in the cloud-based service that will be used as a location resource for scheduling

meetings. Room remote mailboxes can be included in meeting requests as resources and can be configured to automatically process incoming requests.

- **Equipment Mailbox** Click this button to create a remote mailbox in the cloud-based service that will be used as a resource for scheduling meetings. Equipment remote mailboxes can be included in meeting requests as resources and can be configured to automatically process incoming requests.

  As a best practice, create mailboxes for shared meeting equipment, such as projectors or audio equipment, which can be moved to different meeting rooms.

4. On the **User Information** page, complete the following fields:
   - **Specify the on-premises organization unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope).
   - **First name** Use this box to type the first name of the user. This field is optional.
   - **Initials** Use this box to type the initials of the user. This field is optional.
   - **Last name** Use this box to type the last name of the user. This field is optional.
   - **Name** Use this box to type a name for the user. This is the name that's listed in Active Directory. By default, this box is populated with the names you enter in the **First name**, **Initials**, and **Last name** boxes. If you didn't use those boxes, you must type a name in this field. The name can't exceed 64 characters.
   - **User logon name (User Principal Name)** Use this box to type the name that the user will use to log on to the remote mailbox. The user logon name consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides. This field is required.
   - **Password** Use this box to type the password that the user must use to log on to his or her remote mailbox.

     Note:
     Make sure that the password you supply complies with the password length, complexity, and history requirements of the domain in which you are creating the user account.

   - **Confirm password** Use this box to confirm the password that you typed in the **Password** box.
   - **User must change password at next logon** Select this check box if you want the user to reset the password when they first log on to the remote mailbox.

     If you select this check box, at first logon, the new user will be prompted with a dialog box in which to change the password. The user won't be allowed to perform any tasks until the password is successfully changed.

5. On the **Archive Mailbox** page, select the **Add an archive mailbox** check box if you want to link an archive mailbox to the remote mailbox in the cloud-based service. The archive mailbox is also created in the cloud-based service. If you create an archive mailbox for the remote mailbox, mailbox items will be moved automatically from the primary user mailbox to the archive, based on the default retention policy settings or those settings that you define. To learn more, see Understanding Personal Archives.

6. On the **New Remote Mailbox** page, review your configuration settings. To make any configuration changes, click **Back**. To create the new remote mailbox, click **New**.

7. On the **Completion** page, review the following, and then click **Finish** to close

the wizard:

- A status of **Completed** indicates that the wizard completed the task successfully.
- A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a single remote mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote mailboxes" entry in the Mailbox Permissions topic.

This example creates a mail-enabled user in the on-premises Active Directory and an associated remote mailbox in the cloud-based service for the user Chris Ashton with the following details:

- The remote mailbox's alias is Chris.
- The user's first name is Chris and the last name is Ashton.
- The name and display name is Chris Ashton.
- The user principal name (UPN) is ChrisAshton@contoso.com.
- The mail-enabled user will be created in the Users container of the on-premises organizational unit.

```
New-RemoteMailbox -Alias chris -Name "Chris Ashton" -FirstName Chris -LastName As
```

Because the *RemoteRoutingAddress* parameter isn't specified, Exchange calculates the SMTP address of the remote mailbox in the cloud-based service automatically. This assumes mail flow has been configured between the on-premises organization and the cloud-based service. This example also assumes that directory synchronization has been configured.

This example creates a mailbox for the third floor conference room with the following details:

- The room remote mailbox's alias is 3rdfloorconf.
- The first name is 3rd Floor and the last name is Conference Room.
- The name and display name is 3rdFloor Conference Room.
- The UPN is 3rdfloorconf@contoso.com.
- The mail-enabled user will be created in the Room container of the on-premises organizational unit.

```
New-RemoteMailbox -Alias 3rdfloorconf -Name "3rdFloor Conference Room" -FirstName
```

Because the *RemoteRoutingAddress* parameter isn't specified, Exchange calculates the SMTP address of the remote mailbox in the cloud-based service automatically. This assumes mail flow has been configured between the on-premises organization and the cloud-based service. This example also assumes that directory synchronization has been configured.

Use the Shell to mail-enable existing users

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote mailboxes" entry in the Mailbox Permissions topic.

This example mail-enables the on-premises user john@contoso.com and creates an associated remote mailbox in the cloud-based service.

```
Enable-Mailbox john@contoso.com
```

You can also use the **Enable-RemoteMailbox** cmdlet to mail-enable multiple users and create their remote mailboxes in the cloud-based service. You can do this by piping the results of the **Get-User** cmdlet to the **Enable-RemoteMailbox** cmdlet. When you run the **Get-User** cmdlet, you must return only users that aren't already mail-enabled. To do this, specify the value User with the *RecipientTypeDetails* parameter. You can also limit the results returned by using the *Filter* parameter to request only users that meet the criteria you specify. You then pipe the results to the **Enable-RemoteMailbox** cmdlet.

For example, this command mail-enables users who aren't already mail-enabled and that contain the text "Contoso" in the Company user field.

```
Get-User -RecipientTypeDetails User -Filter { Company -Eq 'Contoso' } | Enable-Re
```

Because the *RemoteRoutingAddress* parameter isn't specified, Exchange calculates the SMTP address of the remote mailboxes in the cloud-based service automatically. This assumes mail flow has been configured between the on-premises organization and the cloud-based service. These examples also assume that directory synchronization has been configured.

For more information about pipelining, see Pipelining.

Other Tasks

View or Configure Remote Mailbox Properties

1.8.3.24.7 View or Configure Remote Mailbox Properties

View or Configure Remote Mailbox Properties

Mailbox > Managing Mailbox Servers > Managing User Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the **Properties** dialog box to configure the settings for the remote mailboxes in your Microsoft Exchange Server 2010 organization.

A remote mailbox consists of a mail-enabled user that exists in the on-premises Active Directory and an associated mailbox that exists in the cloud-based service. When you create a new remote mailbox, the mail-enabled user is created in your on-premises Active Directory. Then, directory synchronization, if it's configured, automatically synchronizes this new user object to the cloud-based service and is converted to a user mailbox. You can create remote mailboxes as regular user mailboxes or as resource mailboxes for meeting rooms and equipment.

Directory synchronization and mail flow should be configured correctly for a mailbox to be created in the service. Creation of the mailbox in the service isn't immediate and depends on the directory synchronization schedule.

To learn more about remote mailboxes, see Understanding Recipients.

Looking for other management tasks related to remote mailboxes? See Managing User Mailboxes.

Use the EMC to view or configure remote mailbox properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote mailboxes" section in the Mailbox Permissions topic.

Properties specific to a remote mailbox are controlled by the **Set-RemoteMailbox** cmdlet. The EMC allows you to set additional properties and the permissions may vary depending upon the feature that you're configuring. The permissions listed above grant permission to edit all the properties of the **< Remote Mailbox> Properties** dialog box.

1. In the console tree, navigate to **Recipient Configuration** > **Mail Contact**.
2. In the result pane, select the remote mailbox you want to configure.
3. In the action pane, click **Properties**.

4. Use the **General** tab to view or modify the following settings:
   - **Display name** Use this unlabeled box at the top of the page to view or change the display name.
   - **On-Premises organizational unit** This read-only field displays the on-premises organizational unit (OU) that contains the mail-enabled user.
   - **Modified** This read-only field displays the last date and time that a configuration change was made to the remote mailbox.
     Configuration changes made through any other method, such as the Exchange Management Shell or Active Directory Service Interfaces (ADSI) Edit, will also update this field.
   - **Alias** Use this text box to view or change the remote mailbox's alias. The alias can't exceed 64 characters and must be unique in the forest.
   - **Use MAPI rich text format** Select one of the following options from the corresponding list:
     Never If you select this option, messages sent to this recipient are converted to plain text.
     Always If you select this option, messages sent to this recipient are in the MAPI rich text format (RTF).
     Use Default Settings If you select this option, messages sent to this recipient are sent in either MAPI RTF or plain text, depending on the settings of the client computer from which the message is sent.
   - **Hide from Exchange address lists** Select this check box to prevent the recipient from appearing in the global address list (GAL) and other address lists that are defined in your Exchange organization.
     After you select this check box, users in your Exchange organization can still send messages to the recipient by using the e-mail address.
   - **Custom Attributes** Click this button to open the **Custom Attributes** dialog box. You can specify up to 15 custom attributes for the recipient. To specify the custom attribute values, use the corresponding boxes, and then click **OK**. To learn more, see Understanding Custom Attributes.

5. Use the **User Information** tab to modify the following fields.
   - **First name** Use this box to modify the recipient's first name.
   - **Initials** Use this box to modify the recipient's middle initials.
   - **Last name** Use this box to modify the recipient's last name.
   - **Name** Use this box to modify the recipient's directory name. This is the name that's listed in Active Directory.
   - **Simple display name** Use this box to modify the recipient's simple display name. The simple display name field accepts only ASCII characters.
     In Exchange 2010, the **Display name** field (located on the

General tab) can contain Unicode characters. However, third-party applications and older clients may not support Unicode characters. If the system that is displaying the recipient properties doesn't support Unicode characters, you can use the simple display name. For more information about Unicode characters, see Unicode.

- **Web page** Use this box to modify the recipient's Web page address.
- **Notes** Use this box to modify administrative notes about the recipient. These notes are also visible in Outlook. When a user views the recipient's properties in Outlook, the notes will be displayed on the **Phone/Notes** tab.

6. Use the **Address and Phone** tab to view or modify the following fields:
   - **Street address** Use this box to view or change the recipient's street.
   - **City** Use this box to view or change the city where the recipient is located.
   - **State/Province** Use this box to view or change the state or province where the recipient is located. You can use the **State/Province** field as a condition for dynamic distribution groups and e-mail address policies. If you plan to use this field as a condition, you must devise and follow a consistent naming convention to ensure accurate results for dynamic distribution groups and e-mail address policies.
   - **ZIP/Postal code** Use this box to view or change the ZIP code or the postal code where the recipient is located.
   - **Country/region** Use this list to view or change the country or region where the recipient is located.
   - **Business** Use this box to view or change the recipient's business phone number.
   - **Pager** Use this box to view or change the recipient's pager number.
   - **Fax** Use this box to view or change the recipient's fax number.
   - **Home** Use this box to view or change the recipient's home phone number.
   - **Mobile** Use this box to view or change the recipient's mobile phone number.

7. Use the **Organization** tab to view or change the information about the recipient's role in your organization.
   - **Title** Use this box to view or change the recipient's title.
   - **Company** Use this box to view or change the company for which the recipient works. You can use this field to create recipient conditions for dynamic distribution groups, e-mail address policies, or address lists.
   - **Department** Use this box to view or change the department in which the recipient works. You can use this field to create recipient conditions for dynamic distribution groups, e-mail address policies, or address lists.
   - **Office** Use this box to view or change the office location for the recipient.
   - **Manager** Select this check box if you want to specify this recipient's manager. By specifying the manager for each recipient in your organization, you can create a virtual organization chart that is accessible from e-mail clients such as Outlook. Click **Browse** to open the **Select Recipient User or Contact** dialog box. Select the recipient's manager, and then click **OK** to return to the property page.
   - **Direct Reports** Use this box to view the list of mailbox users and contacts that are managed by this recipient. This field is read-only and is populated automatically when this recipient is designated as a manager for another recipient.

8. Use the **Account** tab to modify the logon names for the Active Directory domain service user account that is associated with the recipient:
   - **User logon name (User Principal Name)** The user logon name consists

of a user name and a suffix. Use this box to type the user name that the user will use to log on to the Active Directory domain. The user logon name cannot exceed 1,024 characters and must be unique in the forest.

Use the corresponding drop-down list to select the suffix for this user. Typically, the suffix is the Active Directory domain name in which the user account resides. To view or change the list of available domain suffixes in your forest, use Active Directory Domains and Trusts. In the Active Directory Domains and Trusts console tree, right-click **Active Directory Domains and Trusts**, and then click **Properties**. In the property page, use the **UPN suffixes** tab to view the list of available domain suffixes in the forest.

- **User logon name (pre-Windows 2000)** Use this box to type a user name that is compatible with legacy versions of Windows (prior to the release of Windows 2000 Server). The user logon name for a version of Windows earlier than Windows 2000 Server can't exceed 20 characters and can't contain any of the following characters: **\/ [] : | <> + = ; ? , ***.

  When the user account is first created, this field is automatically populated based on the **User logon name (User Principal Name)** field.
- **User must change password at next logon** Select this check box if you want the user to change the password at next logon. The user won't be able to log on until the password is successfully changed.

9. Use the **Mail Flow Settings** tab to configure delivery options and message size or message delivery restrictions for the remote mailbox.
   - **Message Size Restrictions** Select this setting and then click **Properties** to open the **Message Size Restrictions** dialog box. In this dialog box, use the **Maximum message size (in KB)** check boxes to set the maximum size for messages that can be sent and received by this recipient. Use the corresponding text boxes to type the maximum message size allowed (in KB). The message size must be between 0 and 2,097,151 KB. If a message larger than the specified size is sent to the recipient, the message will be returned to the sender with a descriptive error message.
   - **Message Delivery Restrictions** Select this setting and then click **Properties** to open the **Message Delivery Restrictions** dialog box. Use this dialog box to configure the following settings:

     All senders Click this button to specify that the recipient can accept messages from all senders. This includes senders in both your Exchange organization and external senders. This button is selected by default. This option includes external users only if you clear the **Require that all senders are authenticated** check box. If you select this check box, messages from external users will be rejected.

     Only senders in the following list Click this button to specify that the recipient can accept messages only from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.

     Require that all senders are authenticated Select this check box to prevent anonymous users from sending messages to the recipient.

     No senders Click this button to specify that the recipient will not reject messages from any senders in the Exchange organization. This button is selected by default.

     Senders in the following list Click this button to specify that the recipient will reject messages from a specified set of

senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now.**

10. Use the **Member Of** tab to view a list of the groups to which this recipient belongs. Some of these groups may not be mail-enabled. Mail-enabled groups will have an envelope icon next to them. You can't use this tab to modify membership information. The recipient may match the criteria for one or more dynamic distribution groups in your organization. However, dynamic distribution groups aren't displayed on this tab because their membership is calculated each time they are used. For more information, see Managing Distribution Groups.

11. Use the **E-Mail Addresses** tab to configure the e-mail addresses for the remote mailbox. You can modify the existing addresses or create additional ones. Each remote mailbox must have at least one primary STMP address that is internal to your Exchange organization and one remote routing address. The remote routing address should contain the SMTP address of the mail-enabled user's associated remote mailbox in the cloud-based service.
    - **Add** Click **Add** to add a new e-mail address for this recipient. Use the drop-down box to select from the following address types:
      SMTP Address This is the default address type. Click this button, and use the corresponding dialog box to add an SMTP address.
      Custom Address Click this button, and use the corresponding dialog box to add a custom address (for example, fax or X.400).

      Note:
      With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.
    - **Edit** Click this button to modify the selected e-mail address.
    - **Set as Reply** Click this button to set your selected address as the "reply to" address. A recipient can have multiple e-mail addresses for a specific address type. This allows the recipient to receive messages that are addressed to any one of these e-mail addresses. However, a single address must be used for any messages that are sent by the recipient. If a recipient has multiple e-mail addresses, the primary address is used for any messages sent by the recipient.
      This button is available only when an address other than the primary address is selected. Primary addresses for each address type are displayed in bold type.
      If an e-mail address policy in your Exchange organization applies to this mailbox, the **Set as Reply** setting will be controlled by that policy. To change the primary address for a specific address type, you must clear the **Automatically update e-mail addresses based on e-mail address policy** check box.
    - **Set as Routing Address** Click **Set as Routing Address** to designate the selected e-mail address as the remote routing address for the recipient.

      Note:
      This button is enabled when an address other than the remote routing address is selected.
    - **Automatically update e-mail addresses based on e-mail address policy** Select this check box to have the recipient's e-mail addresses automatically updated based on changes made to e-mail address policies in your

organization. This box is selected by default.

Use the Shell to configure remote mailbox properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote mailboxes" section in the Mailbox Permissions topic.

This example shows how to change the type of the Resource1 remote mailbox to `Equipment`.

```
Set-RemoteMailbox Resource1 -Type Equipment
```

This example uses the **Get-RemoteMailbox** command to find all the mailboxes in the Marketing on-premises organizational unit, and then uses the **Set-RemoteMailbox** command to configure these remote mailboxes. The custom maximum send and receive message sizes are set to 10 MB. You can use this command to configure a specific set of mailboxes to have larger or smaller message size limits than other mailboxes in the organization.

```
Get-RemoteMailbox -OnPremisesOrganizationalUnit "Marketing" | Set-RemoteMailbox -
```

This example sets the MailTip translation in French and Chinese.

```
Set-RemoteMailbox JohnD@contoso.com -MailTipTranslations ("FR: C'est la langue fr
```


1.8.3.24.8 Configure Anti-Spam Features on a Mailbox

Configure Anti-Spam Features on a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to configure anti-spam features on a mailbox. All messages that come into the Exchange organization from the Internet are filtered by the anti-spam agents that are enabled on the Edge Transport server. As the messages are filtered, metadata is added to the messages.

Legitimate messages that haven't been filtered are delivered to the recipient's mailbox.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Prerequisites

Before you perform these procedures, review Understanding Anti-Spam and Antivirus Functionality to confirm that you understand the general strategy for configuring all anti-spam agents so that they work together efficiently for your organization.

Use the Shell to configure anti-spam features on mailboxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to configure anti-spam features on mailboxes.

You use the following parameters to configure anti-spam features with the **Set-Mailbox** cmdlet:

- *AntispamBypassEnabled*
- *RequireSenderAuthenticationEnabled*
- *SCLDeleteEnabled*
- *SCLDeleteThreshold*
- *SCLJunkEnabled*
- *SCLJunkThreshold*
- *SCLQuarantineEnabled*
- *SCLQuarantineThreshold*
- *SCLRejectEnabled*
- *SCLRejectThreshold*

Note:
With the exception of the junk e-mail settings, the spam confidence level (SCL) settings on the mailbox are the same as the settings that you apply on the Content Filter agent. The content filtering settings are applied to the organization. The mailbox settings are applied to the individual mailbox user. The mailbox settings override the organization-wide content filtering settings.
The *SCLDeleteEnabled*, *SCLJunkEnabled*, *SCLQuarantineEnabled*, and *SCLRejectEnabled* parameters have three possible values: `$true`, `$false`, and `$null`. If a parameter has the value of `$true` or `$false`, that parameter overrides the settings on the Content Filter agent. If the setting is `$null`, the settings on the Content Filter agent are applied.

Use the Shell to configure anti-spam features on a single mailbox

To configure all the anti-spam settings on a mailbox, use the following syntax.

```
Set-Mailbox -Identity <MailboxIdParameter> -AntispamBypassEnabled <$true | $false
```

This example configures John Peoples' mailbox to bypass all the anti-spam filters and to have messages that meet or exceed an SCL Junk E-mail folder threshold of 5 delivered to his Junk E-mail folder in Microsoft Outlook.

```
Set-Mailbox -Identity John -AntispamBypassEnabled $true -SCLJunkEnabled $true -SC
```

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to configure anti-spam features on multiple mailboxes by using a piped command

To configure all the anti-spam settings on multiple mailboxes by using a piped command, use the following syntax.

```
Get-Mailbox | Set-Mailbox
```

This example enables the SCL quarantine threshold with a value of 7 on all mailboxes in the Users container in the Contoso.com domain.

```
Get-Mailbox -OrganizationalUnit Contoso.com\Users | Set-Mailbox -SCLQuarantineEna
```

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to configure anti-spam

features for all mailboxes in your organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" entry in the Transport Permissions topic.

Note:

You can't use the EMC to configure anti-spam features for all mailboxes in your organization.

To configure all the anti-spam features on multiple mailboxes by using the **Set-OrganizationConfig** cmdlet, use the following syntax.

```
Set-OrganizationConfig -SCLJunkThreshold <Int32>
```

This example sets the organization's junk e-mail threshold to 5.

```
Set-OrganizationConfig -SCLJunkThreshold 5
```

For detailed syntax and parameter information, see Set-OrganizationConfig.

1.8.3.24.9 Configure Deleted Mailbox and Disabled Personal Archive Retention

Configure Deleted Mailbox and Disabled Personal Archive Retention

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When you delete a mailbox or disable a personal archive, the mailbox or archive is kept in the mailbox database for a specified period of time. When that time expires, the mailbox database maintenance permanently deletes the mailbox or personal archive. By default, mailbox databases are configured to retain mailboxes and personal archives for 30 days. Before the time expires, mailboxes and personal archives are in a disconnected state. You can reconnect them by associating them with an existing user.

For more information, see the following topics:

- Connect or Restore a Disabled Mailbox
- Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive

Looking for other management tasks related to mailboxes? Check out Managing User Mailboxes.

Use the Shell to configure deleted mailbox and disabled personal archive retention

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to configure deleted mailbox and disabled personal archive retention.

This example changes the mailbox retention to 45 days for the mailbox database MBX01.

```
Set-MailboxDatabase -Identity MBX01 -MailboxRetention 45
```

Note:

To specify a value for the *MailboxRetention* parameter, enter it as a time span: dd.hh:mm:ss where d = days, h = hours, m = minutes, and s = seconds.

For detailed syntax and parameter information, see Set-MailboxDatabase.

1.8.3.24.10 Configure Mail Forwarding

Configure Mail Forwarding

Mailbox > Managing Mailbox Servers > Managing User Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) or the Exchange Management Shell to configure mail forwarding for a mailbox.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the EMC to configure mail forwarding for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, right-click the mailbox for which you want to configure mail forwarding, and then click **Properties**.
3. In **<Mailbox> Properties**, on the **Mail Flow Settings** tab, click **Delivery Options**, and then click **Properties**.
4. Select the **Forward to** check box, and then click **Browse**.
5. In **Select Recipient**, select the recipient to whom you want to forward messages, and then click **OK**.

   Note:

   By default, the dialog box displays all recipients that are in the current recipient scope specified in the **Recipient Configuration** node. To learn more about the recipient scope and its impact on the recipient work center, see Understanding Recipient Scope.

6. If you want incoming messages to be delivered to the mailbox as well as to the forwarding address you specified, select the **Deliver message to both forwarding address and mailbox** check box. Clear this check box to forward all incoming messages without retaining copies in the mailbox.
7. Click **OK** to return to **<Mailbox> Properties**.

Use the Shell to configure mail forwarding for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example forwards all mail for John Smith's mailbox to sara@contoso.com.

```
Set-Mailbox -Identity "John Smith" -ForwardingAddress "sara@contoso.com"
```

This example delivers mail to John Smith's mailbox and at the same time forwards all mail for John Smith's mailbox to sara@contoso.com.

```
Set-Mailbox -Identity "John Smith" -ForwardingAddress "sara@contoso.com" -Deliver
```

For detailed syntax and parameter information, see Set-Mailbox.

1.8.3.24.11 Configure Message Size Limits for a Mailbox or a Mail-Enabled Public Folder

Configure Message Size Limits for a Mailbox or a Mail-Enabled Public Folder

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) and the Exchange Management Shell to configure message size limits for a mailbox-enabled user or a mail-enabled public folder.

Keep in mind that there are other settings in an Exchange organization that determine the maximum message size a mailbox can send and receive (for example, the maximum message size configured on a Hub Transport server). To learn more about the message size restrictions in Microsoft Exchange Server 2010, including their scope and the order of precedence, see Understanding Message Size Limits.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the EMC to configure message size limits

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. For mailboxes, perform the following steps:
   1.a. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
   1.b. In the result pane, select the mailbox for which you want to configure message size limits.
   1.c. In the action pane, under the mailbox name, click **Properties**.
   1.d. In **<Mailbox User> Properties**, click the **Mail Flow Settings** tab.
   1.e. Select **Message Size Restrictions**, and then click **Properties**.

1.f.Proceed to Step 3.

2. For mail-enabled public folders, perform the following steps:
   2.a.In the console tree, click **Toolbox**.
   2.b.In the result pane, click **Public Folder Management Console**, and then in the action pane, click **Open Tool**. The Public Folder Management Console appears.
   2.c.In the console tree, expand **Default Public Folders**, and then click the public folder that you want to configure. If the public folder you want to configure is a top-level public folder, click **Default Public Folders**.
   2.d.In the result pane, select the public folder for which you want to configure message size limits.
   2.e.In the action pane, under the public folder name, click **Properties**.
   2.f.In **<Public Folder> Properties**, click the **Mail Flow Settings** tab.
   2.g.Select **Message Size Restrictions**, and then click **Properties**.
   2.h.Proceed to Step 3.
3. In the **Message Size Restrictions** dialog box, select the **Maximum message size (in KB)** check boxes to set the maximum size for messages that can be sent and received by the mailbox or public folder. Use the corresponding text boxes to type the maximum message size allowed in kilobytes (KB). The message size must be from 0 through 2,097,151 KB. If a message larger than the specified size is sent to the mailbox or public folder, the message will be returned to the sender with a descriptive error message. Click **OK** to return to the **Mail Flow Settings** tab.
4. Click **OK**.

Use the Shell to configure message size limits

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section and the "Public folders" entry in the Mailbox Permissions topic.

This example sets both the sending and receiving message sizes for the mailbox of user John Smith to 10 megabytes (MB).

```
Set-Mailbox -Identity "John Smith" -MaxSendSize 10mb -MaxReceiveSize 10mb
```

This example sets both the sending and receiving message sizes for the mail-enabled public folder Accounting Department to 10 MB.

```
Set-MailPublicFolder -Identity "\Accounting Department" -MaxSendSize 10mb -MaxRec
```

For detailed syntax and parameter information, see Set-Mailbox or Set-MailPublicFolder.

1.8.3.24.12 Configure Storage Quotas for a Mailbox

Configure Storage Quotas for a Mailbox

Mailbox > Managing Mailbox Servers > Managing User Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) or the Exchange Management Shell to configure mailbox storage quotas for a mailbox. Storage quotas allow administrators to control the size of mailboxes and manage the growth of mailbox

databases.

Note:
Storage quotas can also be configured on a per-database basis. The quotas configured for a mailbox database apply to all mailboxes in that database, unless the mailbox is configured to not use mailbox database defaults. For details, see Configure Mailbox Database Properties.

When a mailbox size reaches or exceeds a specified storage quota limit, Exchange sends a descriptive notification to the mailbox owner.

Important:
The message associated with the **Issue warning** quota won't be sent to the user unless the value of the quota is greater than 50% of the value specified in the **Prohibit send** quota. For example, if you set the **Prohibit send** quota to 8 MB, you must set the **Issue warning** quota to at least 4 MB. If you don't, the **Issue warning** quota message won't be sent.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the EMC to configure storage quotas for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox user for whom you want to configure storage quotas.
3. In the action pane, under the mailbox user's name, click **Properties**.
4. In **<Mailbox User Name> Properties**, click the **Mailbox Settings** tab.
5. Click **Storage Quotas**, and then click **Properties**.
6. In **Storage Quotas**, clear the **Use mailbox database defaults** check box, and then complete the following fields:
   - **Issue warning at (KB)** Use this check box and use the corresponding text box to specify the maximum storage limit in kilobytes (KB) before a warning is issued to the mailbox user. The value range is from 0 through 2,147,483,647 KB. If the mailbox size reaches or exceeds the value specified, Exchange sends a warning message to the mailbox user.
   - **Prohibit send at (KB)** Use this check box and use the corresponding text box to specify a *prohibit send* limit in KB for the mailbox. The value range is from 0 through 2,147,483,647 KB. If the mailbox size reaches or exceeds the specified limit, Exchange prevents the mailbox user from sending new messages and displays a descriptive error message.
   - **Prohibit send and receive at (KB)** Use this check box and use the corresponding text box to specify a *prohibit send and receive* limit in KB for the mailbox. The value range is from 0 through 2,147,483,647 KB. If the mailbox size reaches or exceeds the specified limit, Exchange prevents the mailbox user from sending new messages and won't deliver any new messages to the mailbox. Any messages sent to the mailbox are returned to the sender with a descriptive error message.
7. Click **OK** to return to the **Mailbox Settings** tab.
8. Click **OK**.

Use the Shell to configure storage quotas

for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example sets the warning, prohibit send, and prohibit send and receive limits for John Smith's mailbox to 200 megabytes (MB), 250 MB, and 280 MB respectively.

Note:

To make sure that the custom settings for the mailbox are used rather than the mailbox database defaults, you must set the *UseDatabaseQuotaDefaults* parameter to `$false`.

```
Set-Mailbox -Identity jsmith@contoso.com -IssueWarningQuota 209715200 -ProhibitSe
```

For detailed syntax and parameter information, see Set-Mailbox.

1.8.3.24.13 Configure User and Resource Mailbox Properties

Configure User and Resource Mailbox Properties

Mailbox > Managing Mailbox Servers > Managing User Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-26*

Mailboxes are the most common recipient type used by information workers in an Exchange organization. Each mailbox is associated with an Active Directory user account. The user can use the mailbox to send and receive messages, and to store messages, appointments, tasks, notes, and documents. You can also use mailboxes for resources such as meeting rooms and equipment. Mailboxes are the primary messaging and collaboration tools for the users in your organization. To learn more about mailboxes, see Understanding Recipients.

Looking for other management tasks related to mailboxes? See Managing User Mailboxes.

What Do You Want to Do?

- Use the EMC to view or configure user mailbox properties
- Use the EMC to configure resource mailbox properties
- Use the Shell to configure user mailbox properties

Use the EMC to view or configure user mailbox properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Provisioning Recipient Permissions" section in the Mailbox Permissions topic.

Properties specific to a mailbox user are controlled by the **Set-Mailbox** cmdlet. The EMC allows you to set additional properties and the permissions may vary depending upon the feature that you're configuring. The permissions listed above grant permission to edit all of the properties of the **< User Mailbox> Properties** dialog box.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.

2. In the result pane, select the user or resource mailbox you want to configure.
3. In the action pane, click **Properties**.

4. Use the **General** tab to view or modify the following settings:
   - **Display name** Use this unlabeled box at the top of the page to view or change the display name.
   - **Organizational unit** This read-only field displays the organizational unit (OU) that contains the user account.
   - **Last logged on by** This read-only field displays the Active Directory user that last logged on to the mailbox.

     Note:
     To obtain the information that's displayed in this field, the Exchange Management Console (EMC) queries the mailbox database that hosts the mailbox. If the EMC is unable to communicate with the Exchange store that contains the mailbox database, this field will be blank. This field will also be blank if no user has logged on to the mailbox since the Microsoft Exchange Information Store service was last started.

   - **Total items** This read-only field displays the total number of items in the mailbox.

     Note:
     To obtain the information that's displayed in this field, the EMC queries the mailbox database that hosts the mailbox. If the EMC is unable to communicate with the Exchange store that contains the mailbox database, this field will be blank.

   - **Size (KB)** This read-only field displays the total size of the mailbox in kilobytes (KB).

     Note:
     To obtain the information that's displayed in this field, the EMC queries the mailbox database that hosts the mailbox. If the EMC is unable to communicate with the Exchange store that contains the mailbox database, this field will be blank.

   - **Mailbox database** This read-only field displays the name of the storage group and mailbox database that host the mailbox.
   - **Archive database** This read-only field displays the name of the mailbox database that host the archive mailbox. If an archive doesn't exist for the mailbox, this field will be blank.
   - **Modified** This read-only field displays the last date and time that a configuration change was made to the user mailbox.
     Configuration changes made through any other method, such as the Exchange Management Shell or Active Directory Service Interfaces (ADSI) Edit, will also update this field.
   - **Alias** Use this text box to view or change the user's alias. The alias cannot exceed 64 characters and must be unique in the forest. One of the reasons why the alias must be unique is because it is used to generate the SMTP address in a default installation.
   - **Hide from Exchange address lists** Select this check box to prevent the recipient from appearing in the global address list (GAL) and other address lists that are defined in your Exchange organization.
     After you select this check box, users in your Exchange organization can still send messages to the recipient by using the e-mail address.
   - **Custom Attributes** Click this button to open the **Custom Attributes** dialog box. You can specify up to 15 custom attributes for the recipient. To specify the custom attribute values, use the corresponding boxes, and then click **OK**. To learn more, see Understanding Custom Attributes.

5. Use the **User Information** tab to modify the following fields.
   - **First name** Use this box to modify the recipient's first name.
   - **Initials** Use this box to modify the recipient's middle initials.
   - **Last name** Use this box to modify the recipient's last name.
   - **Name** Use this box to modify the recipient's directory name. This is the name that's listed in Active Directory.
   - **Simple display name** Use this box to modify the recipient's simple display name. The simple display name field accepts only ASCII characters.
     In Exchange 2010, the **Display name** field (located on the **General** tab) can contain Unicode characters. However, third-party applications and older clients may not support Unicode characters. If the system that is displaying the recipient properties doesn't support Unicode characters, you can use the simple display name. For more information about Unicode characters, see Unicode.
   - **Web page** Use this box to modify the recipient's Web page address.
   - **Notes** Use this box to modify administrative notes about the recipient.
     These notes are also visible in Outlook. When a user views the recipient's properties in Outlook, the notes will be displayed on the **Phone/Notes** tab.

6. Use the **Address and Phone** tab to view or modify the following fields:
   - **Street address** Use this box to view or change the recipient's street.
   - **City** Use this box to view or change the city where the recipient is located.
   - **State/Province** Use this box to view or change the state or province where the recipient is located.
     You can use the **State/Province** field as a condition for dynamic distribution groups and e-mail address policies. If you plan to use this field as a condition, you must devise and follow a consistent naming convention to ensure accurate results for dynamic distribution groups and e-mail address policies.
   - **ZIP/Postal code** Use this box to view or change the ZIP code or the postal code where the recipient is located.
   - **Country/region** Use this list to view or change the country or region where the recipient is located.
   - **Business** Use this box to view or change the recipient's business phone number.
   - **Pager** Use this box to view or change the recipient's pager number.
   - **Fax** Use this box to view or change the recipient's fax number.
   - **Home** Use this box to view or change the recipient's home phone number.
   - **Mobile** Use this box to view or change the recipient's mobile phone number.

7. Use the **Organization** tab to view or change the information about the recipient's role in your organization.
   - **Title** Use this box to view or change the recipient's title.
   - **Company** Use this box to view or change the company for which the recipient works. You can use this field to create recipient conditions for dynamic distribution groups, e-mail address policies, or address lists.
   - **Department** Use this box to view or change the department in which the recipient works. You can use this field to create recipient conditions for dynamic distribution groups, e-mail address policies, or address lists.
   - **Office** Use this box to view or change the office location for the recipient.
   - **Manager** Select this check box if you want to specify this recipient's manager. By specifying the manager for each recipient in your organization, you can create a virtual organization chart that is accessible from e-mail clients such as Outlook.
     Click **Browse** to open the **Select Recipient User or Contact** dialog box. Select the recipient's manager, and then click **OK** to

return to the property page.

- **Direct Reports** Use this box to view the list of mailbox users and contacts that are managed by this recipient. This field is read-only and is populated automatically when this recipient is designated as a manager for another recipient.

8. Use the **Account** tab to modify the logon names for the Active Directory domain service user account that is associated with the recipient:
   - **User logon name (User Principal Name)** The user logon name consists of a user name and a suffix. Use this box to type the user name that the user will use to log on to the Active Directory domain. The user logon name cannot exceed 1,024 characters and must be unique in the forest.
     Use the corresponding drop-down list to select the suffix for this user. Typically, the suffix is the Active Directory domain name in which the user account resides. To view or change the list of available domain suffixes in your forest, use Active Directory Domains and Trusts. In the Active Directory Domains and Trusts console tree, right-click **Active Directory Domains and Trusts**, and then click **Properties**. In the property page, use the **UPN suffixes** tab to view the list of available domain suffixes in the forest.
   - **User logon name (pre-Windows 2000)** Use this box to type a user name that is compatible with legacy versions of Windows (prior to the release of Windows 2000 Server). The user logon name for a version of Windows earlier than Windows 2000 Server can't exceed 20 characters and can't contain any of the following characters: **\/ [] : | <> + = ; ? , ***.
     When the user account is first created, this field is automatically populated based on the **User logon name (User Principal Name)** field.
   - **User must change password at next logon** Select this check box if you want the user to change the password at next logon. The user won't be able to log on until the password is successfully changed.

9. Use the **Mail Flow Settings** tab to configure delivery options and message size or message delivery restrictions for the mailbox.
   - **Delivery Options** Select this setting and then click **Properties** to open the **Delivery Options** dialog box. Use this dialog box to configure the following settings:
     Send on behalf Click **Add** to open the **Select Mailbox or Mail-Enabled User** dialog box. Use this dialog box to grant a recipient the permissions to send e-mail on behalf of the selected mailbox. Click  to remove a recipient from the list.
     Forward to Select this check box, and then click **Browse** to open the **Select Recipient** dialog box. Use this dialog box to select a recipient to whom you want to forward all e-mail messages that are sent to this mailbox.
     Deliver message to both forwarding address and mailbox If you selected the **Forward to** check box, you can select this check box to specify that e-mail messages be delivered to both the mailbox and to the forwarding address.
     Maximum Recipients Select this check box to limit the number of recipients to which this mailbox can send e-mail messages at one time.
   - **Message Size Restrictions** Select this setting and then click **Properties** to open the **Message Size Restrictions** dialog box. In this dialog box, use the **Maximum message size (in KB)** check boxes to set the maximum size for messages that can be sent and received by this recipient. Use the corresponding text boxes to type the maximum message size allowed (in KB). The message size must be between 0 and 2,097,151 KB. If a message larger than the specified size is sent to the recipient, the message will be

returned to the sender with a descriptive error message.

- **Message Delivery Restrictions** Select this setting and then click **Properties** to open the **Message Delivery Restrictions** dialog box. Use this dialog box to configure the following settings:

  All senders Click this button to specify that the recipient can accept messages from all senders. This includes senders in both your Exchange organization and external senders. This button is selected by default. This option includes external users only if you clear the **Require that all senders are authenticated** check box. If you select this check box, messages from external users will be rejected.

  Only senders in the following list Click this button to specify that the recipient can accept messages only from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now**.

  Require that all senders are authenticated Select this check box to prevent anonymous users from sending messages to the recipient.

  No senders Click this button to specify that the recipient will not reject messages from any senders in the Exchange organization. This button is selected by default.

  Senders in the following list Click this button to specify that the recipient will reject messages from a specified set of senders in your Exchange organization. Click **Add** to open the **Select Recipient** dialog box. This dialog box displays a list of all recipients in the Active Directory forest. Select the recipients you want, and then click **OK**. You can also search for a specific recipient by typing its name in the **Search** box and then clicking **Find Now.**

10. Use the **Mailbox Features** tab to view or modify the following mailbox features:
    - **Outlook Web App** This feature is enabled by default. Click **Disable** to disable this feature for the mailbox. Click **Properties**, and then use the corresponding property page to add an Outlook Web App mailbox policy to the user's mailbox. Outlook Web App enables access to an Exchange mailbox from a Web browser. To learn more, see Understanding Outlook Web App Mailbox Policies.
    - **Exchange ActiveSync** This feature is enabled by default. Click **Disable** to disable this feature for the mailbox. Click **Properties**, and then use the corresponding property page to apply an Exchange ActiveSync mailbox policy to the user's mailbox. Exchange ActiveSync enables access to an Exchange mailbox from a mobile device. To learn more, see Understanding Exchange ActiveSync Mailbox Policies.
    - **Unified Messaging** This feature is disabled by default. To enable Unified Messaging (UM) for the mailbox, in the EMC result pane, select the mailbox, and then, in the action pane, click **Enable Unified Messaging**. For details, see Enable a User for Unified Messaging.

      If UM is enabled, click **Properties** and use the corresponding property page to configure UM settings for the user. For details see View or Configure the Properties of a UM-Enabled User.
    - **MAPI** This feature is enabled by default. Click **Disable** to disable this feature for the mailbox. MAPI enables access to an Exchange mailbox from a MAPI client such as Outlook. There is no property page available for this feature.
    - **POP3** and **IMAP4** These features are enabled by default. Click **Disable** to

disable these features for the mailbox. Click **Properties**, and then use the corresponding property pages to specify the MIME format of messages that are retrieved from the server.

- **Archive** If an archive doesn't exist for the mailbox, this feature is disabled . To enable an archive for this mailbox, in the EMC result pane, select the mailbox and then, in the action pane, click **Enable Archive**. If an archive does exist for the mailbox, click **Properties**, and then use the corresponding property page to specify a name for the archive associated with this mailbox. For more information, see Enable a Personal (On-Premises) or Cloud-Based Archive for an Existing Mailbox.

11. Use the **Calendar Settings** tab to modify the Calendar Attendant settings for this mailbox. The Calendar Attendant processes meeting requests as they come in, even if users are not currently logged on by means of a client such as Outlook. Meetings are automatically placed on the calendar as "Tentative" so timeslots won't be overbooked. You can use the Calendar Attendant to accept and decline requests for users.

Note:
This tab isn't displayed for resource mailboxes. To configure calendar settings for resource mailboxes, see Use the EMC to configure resource mailbox properties later in this topic.

- **Enable the Calendar attendant** Select this check box to enable the Calendar Attendant or clear the check box to disable it. It is enabled by default. When Calendar Attendant is enabled, the following settings are made available:

  Remove meeting forward notifications to the Deleted Items folder If you select this check box, meeting forwarding notifications are moved to the Deleted Items folder after they are processed by the Calendar Attendant. This setting is disabled by default.

  Remove old meeting requests and responses If you select this check box, the Calendar Attendant removes old and redundant updates and responses. This setting is enabled by default.

  Mark new meeting requests as Tentative If you select this check box, incoming meeting requests are marked as "Tentative" on the calendar. If you don't select this check box, pending requests are marked as "Free". This setting is enabled by default.

  Process meeting requests and responses originating outside the Exchange organization If you select this check box, the Calendar Attendant will process meeting requests that originate outside the Exchange organization. This setting is disabled by default.

12. Use the **Member Of** tab to view a list of the groups to which this recipient belongs. Some of these groups may not be mail-enabled. Mail-enabled groups will have an envelope icon next to them. You can't use this tab to modify membership information. The recipient may match the criteria for one or more dynamic distribution groups in your organization. However, dynamic distribution groups aren't displayed on this tab because their membership is calculated each time they are used. For more information, see Managing Distribution Groups.

13. Use the **E-Mail Addresses** tab to configure the e-mail addresses for the recipient. You can modify the existing addresses or create additional ones. Each recipient must have at least one primary STMP address that is internal to your Exchange organization and one external address.

- **Add** Click **Add** to add a new e-mail address for this recipient. Use the

drop-down box to select from the following address types:

SMTP Address This is the default address type. Click this button and use the corresponding dialog box to add an SMTP address.

EUM Address This address type is available only for user mailboxes. It's not available for mail users, mail contacts, distribution groups, or mail-enabled public folders. An EUM (Exchange Unified Messaging) address is used by Unified Messaging servers to locate UM-enabled users within an Exchange 2010 organization. EUM addresses contain the extension number and the UM dial plan for the UM-enabled user. Click this button and use the corresponding dialog box to add an EUM address.

Custom Address Click this button and use the corresponding dialog box to add a custom address (for example, fax or X.400).

Note:

With the exception of X.400 addresses, Exchange doesn't validate custom addresses for proper formatting. You must make sure that the custom address you specify complies with the format requirements for that address type.

- **Edit** Click this button to modify the selected e-mail address.
-  Click this button to remove the selected e-mail address.
- **Set as Reply** Click this button to set your selected address as the "reply to" address. A recipient can have multiple e-mail addresses for a specific address type. This allows the recipient to receive messages that are addressed to any one of these e-mail addresses. However, a single address must be used for any messages that are sent by the recipient. If a recipient has multiple e-mail addresses, the primary address is used for any messages sent by the recipient.

  This button is available only when an address other than the primary address is selected. Primary addresses for each address type are displayed in bold type.

  If an e-mail address policy in your Exchange organization applies to this mailbox, the **Set as Reply** setting will be controlled by that policy. To change the primary address for a specific address type, you must clear the **Automatically update e-mail addresses based on e-mail address policy** check box.
- **Set as External** This button is available only for mail users and mail contacts. It's not available for user mailboxes, distribution groups, or mail-enabled public folders. Click **Set as External** to designate the selected e-mail address as the external e-mail address for the recipient.

  Note:

  This button is enabled when an address other than the external e-mail address is selected.
- **Automatically update e-mail addresses based on e-mail address policy** Select this check box to have the recipient's e-mail addresses automatically updated based on changes made to e-mail address policies in your organization. This box is selected by default.

14. Use the **Mailbox Settings** tab to configure the following settings for this mailbox.
    - **Messaging Records Management** Select this setting and then click **Properties** to open the **Messaging Records Management** dialog box. Use this dialog box to configure the following settings:

      Apply Retention Policy Select this check box and then click **Browse** to select a retention policy for the mailbox. To learn more about retention policies, see Understanding Retention Tags and Retention Policies.

Halt Retention Policy during this period Select this check box to place the mailbox on retention hold, and then use the **Start Date** and **End Date** settings to specify a timeframe for the retention hold. To learn more about retention holds, see Understanding Retention Tags and Retention Policies.
Enable Litigation Hold Select this check box to place the mailbox on litigation hold. Litigation hold preserves deleted mailbox items and records changes made to mailbox items. Deleted items and all instances of changed items are returned in a discovery search. To learn more about Litigation Hold, see Understanding Litigation Hold.
Messaging Records Management Description URL Use this box to enter the location of a Web page or document that contains more information about the litigation hold or retention hold policies in your organization. The URL is displayed in the Backstage area of Microsoft Outlook 2010. This makes it easier for users to access linked Help documents, and may reduce calls to your Help desk or Legal department by answering common questions.
Comments Use this field to type a comment that you want to be displayed to the mailbox user in the Backstage view of Microsoft Outlook 2010.

- **Sharing** Select this setting and then click **Properties** to open the **Sharing** dialog box. Use this dialog box to set the sharing policy for this mailbox. For more information, see Apply a Sharing Policy to Mailboxes.
- **Storage Quotas** Select this setting and then click **Properties** to open the **Storage Quotas** dialog box. Use this dialog box to set the storage quotas for this mailbox. For more information, see Configure Storage Quotas for a Mailbox.
- **Archive Quota** Select this setting and then click **Properties** to open the **Archive Quota** dialog box. Use this dialog box to set the archive quotas for this mailbox. If archiving isn't enabled for this mailbox, the **Properties** button will be unavailable. For more information, see Configure Archive Quotas for a Personal (On-Premises) Archive.
- **Role Assignment Policy** Select this setting and then click **Properties** to open the **Role Assignment Policy** dialog box. Use this dialog box to apply a role assignment policy for this user. Click **Browse** to view the available role assignment policies. For more information, see Change the Assignment Policy on a Mailbox.
- **Address book policy** Select this setting and then click **Properties** to open the **Address Book Policy** dialog box. Use this dialog box to apply an address book policy (ABP) for this mailbox. Click **Browse** to open the **Select Address Book Policy** dialog box. Use this dialog box to select the policy you want associated with this mailbox. To learn more, see Understanding Address Book Policies.

Use the EMC to configure resource mailbox properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Provisioning Recipient Permissions" section in the Mailbox Permissions topic.

In addition to the properties listed in the previous section, resource mailboxes have specific settings that you can configure by using the EMC. For more information about how to configure resource mailboxes by using the Shell, see Configure Custom Resource Properties for a Resource Mailbox.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the resource mailbox that you want to configure.

3. In the action pane, under the name of the resource mailbox, click **Properties**.
4. Use the **Resource General** tab to configure general settings for the resource mailbox:
   - **Resource capacity** Use this box to specify the capacity of this resource. For example, if this is a room resource, specify the maximum occupancy of the room.
   - **Resource custom properties** Use this box to specify custom resource properties that can be searched by users. In Outlook, the properties appear in the **Description** column when users select the **All Rooms** address book.
   - **Enable the Resource Booking Attendant** Select this check box to allow the Resource Booking Attendant to process resource requests and cancellations automatically.

     Note:
     If you don't select this check box, the settings that you configure on the **Resource Policy** tab, the **Resource In-Policy Requests** tab, and the **Resource Out-of-Policy Requests** tab aren't enabled.
5. Use the **Resource Policy** tab to specify under which conditions the resource mailbox automatically accepts requests:
   - **Allow conflict meeting requests** Select this check box to allow conflicting meeting requests to be scheduled by the Resource Booking Attendant.
   - **Allow repeating meetings** Select this check box to allow repeating or recurring meetings to be scheduled.
   - **Allow scheduling only during working hours** Select this check box to allow scheduling for the resource to occur during working hours. Users can set working hours either by using Outlook or Outlook Web App. Administrators can set working hours by using the **Set-MailboxCalendarConfiguration** cmdlet on the resource mailbox.
   - **Reject repeating meetings that have an end date beyond the booking window** Select this check box to allow the Resource Booking Attendant to reject recurring meeting requests that are outside of the resources booking window.
   - **Booking window (days)** Use this box to specify the number of days that the room can be booked in advance. For example, if the booking window is set for 90 days and a request is received for scheduling the resource 4 months from today's date, the Resource Booking Attendant rejects the request.
   - **Maximum duration (minutes)** Use this box to specify the maximum number of minutes that the resource can be scheduled for.
   - **Maximum conflict instances** Use this box to specify the maximum number of conflicts allowed for recurring meetings. If the number of instances for a recurring meeting in conflict exceeds this number, the recurring meeting request is declined.
   - **Conflict percentage allowed** Use this box to specify the conflict percentage threshold from recurring meetings. If the percentage of instances of a recurring meeting that conflicts with other meetings exceeds the threshold, the recurring meeting request is denied.
   - **Specify delegates of this mailbox** Click **Add** to add delegates who can control the scheduling options for the resource mailbox. Click **Remove** to remove delegates from this resource mailbox.
   - **Forward meeting requests to delegates** Select this check box to forward all meeting requests to the delegates.
6. Use the **Resource Information** tab to specify the meeting information that appears in the resource's calendar:
   - **Delete attachments** Select this check box to remove attachments from all incoming requests.
   - **Delete comments** Select this check box to remove comments from all

incoming requests.

- **Delete the subject** Select this check box to remove the subject of all incoming requests.
- **Delete non-calendar items** Select this check box to remove non-calendar items from all incoming requests.
- **Add the organizer's name to the subject** Select this check box to specify whether the resource requestor's name is added to the subject of the request.
- **Remove the private flag on an accepted meeting** Select this check box to remove the private flag for all incoming requests.
- **Send organizer information when a meeting request is declined because of conflicts** Select this check box to send the meeting organizer information regarding a denied request.
- **Customize the response message that organizers will receive** Select the **Add additional text** check box to customize the message that the requester receives when the meeting has been declined, and then type the additional information in the **Additional text** field.
- **Mark pending requests as Tentative on the calendar** Select this checkbox to specify that all pending requests are marked as Tentative in the resource's calendar. The delegate can then accept or deny the request as needed.

7. Use the **Resource In-Policy Requests** tab to specify users who are allowed to submit requests within the resource policy's configuration:
   - **Specify users who are allowed to submit in-policy meeting requests that will be automatically approved** Click **All users** or **Selected recipients**. If you click **Selected recipients**, you need to click **Add** to select the recipients. You can also remove selected recipients by clicking **Remove**.
   - **Specify who can submit in-policy meeting requests that are subject to approval by a resource mailbox delegate** Click **All users** or **Selected recipients**. If you click **Selected recipients**, you need to click **Add** to select the recipients. You can also remove selected recipients by clicking **Remove**.
8. Use the **Resource Out-of-Policy Requests** tab to specify the users who are allowed to submit out-of-policy requests. Users who have permission to submit out-of-policy requests won't have their request denied, but the requests require approval by one of the resource's delegates:
   - **All users** Click this button to allow all users to submit resource requests that don't meet the resource policy's configuration.
   - **Selected recipients** Click this button to select specific users who can submit out-of-policy requests.

Use the Shell to configure user mailbox properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Provisioning Recipient Permissions" section in the Mailbox Permissions topic.

This example shows how to forward John Peoples' e-mail messages to Jose De Oliveira's (jose@contoso.com) mailbox.

```
Set-Mailbox -Identity John -DeliverToMailboxAndForward $true -ForwardingAddress j
```

This example uses the **Get-Mailbox** command to find all the mailboxes in the Marketing organizational unit, and then uses the **Set-Mailbox** command to configure these mailboxes. The custom warning, prohibit send, and prohibit send and receive limits are set to 200 megabytes (MB), 250 MB, and 280 MB respectively, and the mailbox database's default limits are ignored. This command can be used to configure a specific set of mailboxes to have larger or smaller limits than other mailboxes in the organization.

```
Get-Mailbox -OrganizationalUnit "Marketing" | Set-Mailbox -IssueWarningQuota 2097
```

This example uses the **Get-User** command to find all users in the Customer Service department, and then uses the **Set-Mailbox** command to change the maximum message size for sending messages to 2 MB.

```
Get-User -Filter "Department -eq 'Customer Service'" | Set-Mailbox -MaxSendSize 2
```

This example sets the MailTip translation in French and Chinese.

```
Set-Mailbox JohnD@contoso.com -MailTipTranslations ("FR: C'est la langue français
```


1.8.3.24.14 Convert a Mailbox

Convert a Mailbox

Mailbox > Managing Mailbox Servers > Managing User Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic explains how to use the Exchange Management Shell to convert a mailbox to a different type of mailbox. You can convert the following:

- User mailbox to shared mailbox
- User mailbox to resource mailbox
- Shared mailbox to user mailbox
- Shared mailbox to resource mailbox
- Resource mailbox to user mailbox
- Resource mailbox to shared mailbox

You can't use this procedure to convert a user mailbox to a linked mailbox or a linked mailbox to a user mailbox. For instructions about how to convert to a linked mailbox, see Convert Linked Mailboxes.

A scenario in which you may want to convert a mailbox is if you have moved resource mailboxes from Exchange Server 2003 to Exchange Server 2010. In Exchange 2003, you use shared mailboxes to represent resources. When you move these mailboxes to Exchange 2010, they will be Exchange 2010 shared mailboxes. You must convert them from Exchange 2010 shared mailboxes to Exchange 2010 resource mailboxes so that they will have all the properties of Exchange 2010 resource mailboxes.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the Shell to convert a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

You can't use the EMC to convert a mailbox.

This example converts the shared mailbox ConfRoom1to a room mailbox.

```
Set-Mailbox ConfRoom1 -Type Room
```

You can use the following values for the *Type* parameter:

- Regular
- Room
- Equipment
- Shared

For detailed syntax and parameter information, see Set-Mailbox.

1.8.3.24.15 Convert Linked Mailboxes

Convert Linked Mailboxes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A *linked mailbox* is a mailbox that's associated with an external account. The resource forest scenario is an example of when you would want to associate a mailbox with an external account. In a resource forest scenario, user objects in the Exchange forest have mailboxes, but the user objects are disabled for logon. You must associate these mailbox objects in the Exchange forest with enabled user objects in the external accounts forest.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the Shell to convert a mailbox to a linked mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

You can't use the EMC to convert a mailbox to a linked mailbox.

1. To disconnect the mailbox object in the Exchange store from the user object in Active Directory, use this example.

```
Disable-Mailbox -Identity User1
```

2. To create a credential object, run the following command.

```
$cred = Get-Credential
```

   You will be prompted for credentials. Specify an account that has permissions to access the domain controller in the forest where the user account resides. Use the *LinkedDomainController* parameter to specify the domain controller. This domain controller obtains security information for the account to which you are linking the mailbox object.

3. To reconnect the mailbox object in the Exchange store to an external user object, use this example.

```
Connect-Mailbox -Identity User1 -Database "Mailbox Database" -LinkedDo
```

For detailed syntax and parameter information, see Disable-Mailbox or Connect-Mailbox.

Use the Shell to convert a linked mailbox to a user mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:
You can't use the EMC to convert a linked mailbox to a user mailbox.

This example converts Kweku's mailbox from a linked mailbox to a non-linked user mailbox by setting the *LinkedMasterAccount* parameter to `null`.

Important:
Performing this procedure on a linked mailbox removes all permissions on the mailbox, such as Send As, Full Access, folder permissions, and calendar delegation.

```
Set-User -Identity kweku@fabrikam.com -LinkedMasterAccount $null
```

For detailed syntax and parameter information, see Set-User.

1.8.3.24.16 Disable a Mailbox

Disable a Mailbox

Mailbox > Managing Mailbox Servers > Managing User Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) and the Exchange Management Shell to disable the mailbox of an existing Active Directory user object in Microsoft Exchange Server 2010. This task removes all the Exchange attributes from the user object in Active Directory. Based on the deleted items retention policy, the Exchange store will retain mailbox data for the user object.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the EMC to disable a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox that you want to disable.
3. In the action pane, under the name of the mailbox, click **Disable**.
4. A warning appears asking, **Are you sure you want to disable 'mailbox name'?** Click **Yes** to disable the mailbox.

Use the Shell to disable a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient provisioning permissions" section in the Mailbox

Permissions topic.

This example disables the mailbox for john@contoso.com.

```
Disable-Mailbox john@contoso.com
```

For detailed syntax and parameter information, see Disable-Mailbox.

1.8.3.24.17 Enable or Disable MAPI for a User Mailbox

Enable or Disable MAPI for a User Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) and the Exchange Management Shell to enable or disable MAPI for a user mailbox.

Looking for other management tasks related to managing user mailboxes? Check out Managing User Mailboxes.

Use the EMC to enable or disable MAPI for a user mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access user settings" entry in the Client Access Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the user mailbox for which you want to enable or disable MAPI.
3. In the action pane, under the user mailbox name, click **Properties**.
4. In **< User Mailbo > Properties**, on the **Mailbox Features** tab, click **MAPI**, and then click either **Enable** or **Disable**.
5. Click **OK**.

Use the Shell to enable or disable MAPI for a user mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access user settings" entry in the Client Access Permissions topic.

This example enables MAPI for the user John.

```
Set-CASMailbox -Identity John -MAPIEnabled $true
```

This example disables MAPI for the user John.

```
Set-CASMailbox -Identity John -MAPIEnabled $false
```

For detailed syntax and parameter information, see Set-CASMailbox.

1.8.3.24.18 Remove a Mailbox

Remove a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) and the Exchange Management Shell to remove a mailbox. When you remove a mailbox, you disconnect the mailbox from its associated user account and remove the user from Active Directory. The mailbox is retained in the mailbox database for a specified amount of time. By default, Exchange retains the disconnected mailbox for 30 days. You can reconnect the mailbox to its user account before the specified amount of time expires. For more information, see Understanding Disconnected Mailboxes.

If you want to permanently remove a mailbox, including the associated user account in Active Directory, you must use the Shell.

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the EMC to remove a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox you want to remove.
3. In the action pane, under the name of the mailbox, click **Remove**.
4. A warning appears asking, **Are you sure you want to remove 'mailbox name'?** Click **Yes** to remove the mailbox.

Use the Shell to remove a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example removes the mailbox for user John from John's user account and also deletes the user account.

```
Remove-Mailbox -Identity contoso\john
```

Use the Shell to permanently remove a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example permanently deletes the mailbox and the user account for John.

```
Remove-Mailbox -Identity contoso\john -Permanent
```

For detailed syntax and parameter information, see Remove-Mailbox.

1.8.3.24.19 Restrict the Number of Recipients per Message

Restrict the Number of Recipients per Message

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can restrict the number of recipients per message at the following levels in your Exchange organization:

- Mailbox
- Organization
- Connector (for Receive connectors only)
- Transport server

Generally, it's a best practice to configure this setting at a higher level and use the mailbox-level configuration for exceptions only. For more information about the levels at which you can configure this restriction, as well as a list of default values, see Understanding Message Size Limits.

Looking for other management tasks related to managing user mailboxes? Check out Managing User Mailboxes.

Caution:

Active Directory also has a global limit for the maximum number of recipients per message. This global limit is separate from the limits that can be managed by using the EMC or the Shell. This global limit is used in Microsoft Exchange Server 2003, but it also has an effect in Exchange Server 2010. If the global limit in Active Directory and the organization-level limit in Exchange 2010 are in conflict, the smaller of the two is used as the effective limit.
To modify the global limit in Active Directory, you must use Exchange System Manager (in Exchange 2003) or ADSI Edit.

Use the Shell to restrict the number of recipients per message for the entire Exchange organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

Note:

You can't use the EMC to perform this task.

This example restricts the number of recipients per message to 1,000 for your Exchange organization.

```
Set-TransportConfig -MaxRecipientEnvelopeLimit 1000
```

For detailed syntax and parameter information, see Set-TransportConfig.

Use the Shell to restrict the number of recipients per message on a Receive connector

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Receive connectors" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

This example restricts the number of recipients per message to 300 for messages received through the Receive connector Contoso Receive Connector.

```
Set-ReceiveConnector -Identity "Contoso Receive Connector" -MaxRecipientsPerMessa
```

For detailed syntax and parameter information, see Set-ReceiveConnector.

Use the Shell to restrict the number of recipients per message on a transport server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hub Transport server" entry in the Transport Permissions topic.

Note:
You can't use the EMC to perform this task.

This example restricts the number of recipients per message to 200 for messages processed by the Hub Transport server Server01:

```
Set-TransportServer -Identity "Server01" -PickupDirectoryMaxRecipientsPerMessage
```

For detailed syntax and parameter information, see Set-TransportServer.

Note:
This restriction applies only to messages submitted by using the Pickup directory on an Edge Transport or Hub Transport server. For more information about the Pickup directory, see Understanding the Pickup and Replay Directories.

Use the EMC to restrict the number of recipients per message for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the mailbox for which you want to restrict the number of recipients per message.
3. In the action pane, under the mailbox name, click **Properties**.
4. In **<Mailbox> Properties**, on the **Mail Flow Settings** tab, select **Delivery Options** from the list of mail flow settings, and then click **Properties**.

5. In **Delivery Options**, select the **Maximum recipients** check box, and then, in the corresponding text box, type the maximum number of recipients that can receive a message from the mailbox.
6. Click **OK** to return to the **Mail Flow Settings** tab.

Use the Shell to restrict the number of recipients per message for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example restricts the number of recipients per message to 100 for the mailbox user John Smith.

```
Set-Mailbox -Identity "John Smith" -RecipientLimits 100
```

For detailed syntax and parameter information, see Set-Mailbox.

1.8.3.24.20 Update a Recipient's Address and Phone Information

Update a Recipient's Address and Phone Information

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Exchange Management Console (EMC) and the Exchange Management Shell to update a recipient's address and phone information. The changes you make to the recipient objects also update Active Directory and the address book.

Looking for other management tasks related to managing user mailboxes? Check out Managing User Mailboxes.

Use the EMC to update a recipient's address and phone information

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the recipient you want to modify.
3. In the action pane, under the recipient's name, click **Properties**.
4. In **<Recipient> Properties**, on the **Address and Phone** tab, update the address and phone information.
5. Click **Apply**, and then click **OK**.

Use the Shell to update a recipient's address and phone information

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example configures the phone number and address for the user john@contoso.com.

```
Set-User -Identity john@contoso.com -Phone "(425) 555-0100" -StreetAddress "4567
```

For detailed syntax and parameter information, see Set-User.

1.8.3.24.21 View Logon Statistics

View Logon Statistics

Mailbox > Managing Mailbox Servers > Managing User Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The **Get-LogonStatistics** cmdlet retrieves logon information so you can view users or services currently connecting to your Microsoft Exchange Server 2010 servers. Logon statistics include information such as user name, logon time, last access time, and client version.

When you run the cmdlet from a Mailbox server, you don't have to use any parameters. In this case, the cmdlet returns the logon statistics for all mailboxes on all databases on the local server.

Note:

Users who log on to their mailboxes using Microsoft Office Outlook Web App aren't connected continuously to the Mailbox server. An Outlook Web App client connects to the server, performs tasks, and then disconnects from the server. Therefore, you may see few or no logon statistics for Outlook Web App, even if users are logged on to the client.

Because the **Get-LogonStatistics** cmdlet provides a quick snapshot of the connections to Exchange at one specific time, you may want to create a script that runs in Windows Task Scheduler to capture additional data, so you can analyze server and database usage over a specified period of time.

Note:

Running the **Get-LogonStatistics** cmdlet too often may significantly affect the CPU load on the Client Access server.

For more information, see the following topics:

- Scripting with the Exchange Management Shell
- Task Scheduler Overview

Looking for other management tasks related to user mailboxes? Check out Managing User Mailboxes.

Use the Shell to view logon statistics

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

You can't use the EMC to view logon statistics.

This example returns logon statistics for all users connected to the server MBXSVR01.

```
Get-LogonStatistics -Server MBXSVR01
```

This example returns logon statistics for a specific user with the SMTP address tony@contoso.com.

```
Get-LogonStatistics -Identity tony@contoso.com
```

This example returns logon statistics for all users who reside on the mailbox database MDB01.

```
Get-LogonStatistics -Database MDB01
```

This example returns all logon statistics for all processes and mailboxes currently logged on and groups the statistics by the session ID.

```
Get-LogonStatistics | Group SessionId
```

For detailed syntax and parameter information, see Get-LogonStatistics.

Logon Statistics Output

By default, the **Get-LogonStatistics** cmdlet returns the `UserName`, `ServerName`, `LogonTime`, and `LastAccessTime` values for each user or process that has logon statistics. The following table lists the information returned if you pipeline the output of the **Get-LogonStatistics** cmdlet to the **Format-List** cmdlet.

Logon statistics output

Value	Description
`AdapterSpeed`	This value is always blank.
`ApplicationId`	This value specifies the type of client application making the connection.
`ClientIPAddress`	If provided by the client application, this value specifies the IP address of the client computer from which the user or service is accessing Exchange.
`ClientMode`	This value is always `ExchangeServer`, because the client application connects through the Microsoft Exchange RPC Client Access service or some other Exchange service.
`ClientName`	This value specifies the name of the Exchange server initiating the connection.
`ClientVersion`	This value specifies the version of the client application accessing Exchange.
`CodePage`	This value specifies the code page that the client application is using to log on. For more information, see Code Pages.
`CurrentOpenAttachments`	This value specifies how many open attachments there were when the **Get-LogonStatistics** cmdlet was run.
`CurrentOpenFolders`	This value specifies how many open folders

	there were when the **Get-LogonStatistics** cmdlet was run.
CurrentOpenMessages	This value specifies how many open messages there were when the **Get-LogonStatistics** cmdlet was run.
DatabaseName	This value specifies the name of the mailbox database in which the mailbox resides.
FolderOperationCount	This value is always 0.
FullMailboxDirectoryName	This value specifies the full name of the mailbox directory.
FullUserDirectoryName	This value specifies the full user directory name of the account to which this mailbox belongs.
HostAddress	If provided by the client application, this value specifies the IP address of the host server from which the user or service is accessing Exchange.
Identity	This value specifies the distinguished name of the mailbox or service connecting to Exchange.
IsValid	This value specifies whether the command was valid.
LastAccessTime	This value specifies the last time an action was performed using that logon.
Latency	This value is always 0.
LocaleID	This value specifies the language locale of the mailbox.
LogonTime	This value specifies the time and date at which the user or service created the specific logon.
MACAddress	If provided by the client application, this value specifies the MAC address of the network node from which the user or service logged on to Exchange.
MapiIdentity	This value specifies the distinguished name of the mailbox or service connecting to Exchange.
MessagingOperationCount	This value is always 0.
OriginatingServer	This value specifies the fully qualified domain name (FQDN) of the server.
ProgressOperationCount	This value is always 0.
RPCCallsSucceeded	This value is always 0.
ServerName	This value specifies the name of the server

	on which the mailbox resides.
SessionID	This value specifies the unique identity of the session used to identify logons that come from the same session.
StreamOperationCount	This value is always 0.
TableOperationCount	This value is always 0.
TotalOperationCount	This value is always 0.
TransferOperationCount	This value is always 0.
UserName	This value specifies the user name of the mailbox.
Windows2000Account	This value specifies the user name of the account accessing the mailbox. For example, if the mailbox user shared a calendar with other users, this value specifies the name of the users who logged on to view the calendar.

1.8.3.24.22 Managing Disconnected Mailboxes

Managing Disconnected Mailboxes

Mailbox > Managing Mailbox Servers > Managing User Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-16*

1.8.3.24.22.1 Connect or Restore a Disabled Mailbox

Connect or Restore a Disabled Mailbox

Managing Mailbox Servers > Managing User Mailboxes > Managing Disconnected Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

A *disconnected mailbox* is a mailbox object in the Exchange store that isn't associated with an Active Directory user account.

There are two types of disconnected mailboxes:

- **Disabled mailboxes** When a mailbox is disconnected or removed by using the **Disable-Mailbox** or **Remove-Mailbox** cmdlet, Exchange retains the deleted mailbox, and the mailbox is switched to a disabled state. With disabled mailboxes, you can recover mailbox data without having to restore the entire mailbox database. Disabled mailboxes are retained in the mailbox database until the deleted mailbox retention period expires or until the mailbox is permanently deleted.
- **Soft-deleted mailboxes** When mailboxes are moved from a Microsoft Exchange Server 2010 Service Pack 1 (SP1) database to any other database, Exchange doesn't fully delete the mailbox from the source database upon completion of the move. Instead, the mailbox in the source mailbox database is switched to a *soft-deleted* state. With soft-deleted mailboxes, you can use the **MailboxRestoreRequest** cmdlet set to access mailbox data during a mailbox restore operation. Soft-deleted mailboxes are retained in the source database until either the deleted mailbox retention period expires or until the **Remove-StoreMailbox** cmdlet is used to purge the mailbox. For more information, see Restore a Soft-Deleted Mailbox.

Disabled mailboxes remain in the Exchange database for the duration specified in the deleted mailbox retention settings for the mailbox database. By default, disabled mailboxes are retained for 30 days. During this retention period, a disabled mailbox can be recovered by connecting it to a new or existing Active Directory user account.

Looking for other management tasks related to disconnected mailboxes? Check out Managing Disconnected Mailboxes.

What Do You Want to Do?

- Use the EMC to connect a disabled mailbox
- Use the Shell to connect a disabled mailbox
- Use the Shell to restore a disabled mailbox

Use the EMC to connect a disabled mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

Only disconnected mailboxes that have a disabled status are displayed in the EMC. Soft-deleted mailboxes aren't displayed.

1. In the console tree, navigate to **Recipient Configuration** > **Disconnected Mailbox**.
2. In the result pane, select the disabled mailbox that you want to reconnect.
3. In the action pane, click **Connect**.
4. On the **Introduction** page, select one of the following to specify the mailbox type for the mailbox you're connecting:

- **User Mailbox** Click this button to connect the mailbox as a mailbox owned by a user to send and receive e-mail messages. User mailboxes can't be used for resource scheduling.

  The Active Directory account associated with a user mailbox must reside in the same forest as the Exchange server. To use an account in a trusted forest, select **Linked Mailbox**.
- **Room Mailbox** or **Equipment Mailbox** Click one of these buttons to connect the mailbox as a mailbox that will be used as a location resource for scheduling meetings (room mailbox) or a shared resource (equipment mailbox) that isn't location specific. Room and equipment mailboxes can be included in meeting requests as resources and can be configured to automatically process incoming requests.

  Note:
  You can connect a room or equipment mailbox only to a disabled user account. Therefore, the **Select Recipient** dialog box that you use to select a user account on the **Mailbox Settings** page of this wizard will display only a list of disabled user accounts in the Active Directory forest.
- **Linked Mailbox** Click this button to connect the mailbox as a user mailbox that's accessed by a user in a separate, trusted forest. To store the mailbox information, you must select a user account in the forest in which the Exchange server resides.

  Linked mailboxes might be required for organizations that choose to deploy Exchange in a resource forest. Using the resource forest scenario, you can centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests.

5. On the **Mailbox Settings** page, configure the following settings:
   - **Matching User** Click this button to have Exchange locate a matching user object in Active Directory. Click **Browse** to open the **Select User** dialog box. If Exchange locates a matching user, it will appear in this dialog box. Select the user, and then click **OK**.

     If Exchange can't find a matching user, you must click **Existing User**. To locate a user account that matches the mailbox object, Exchange uses the **LegacyExchangeDN** and **DisplayName** attributes of the Exchange store mailbox object.
   - **Existing User** Click this button if you want to connect the mailbox to a user other than the matching user. Click **Browse** to see a list of users available in Active Directory. The list contains only users that don't have an associated mailbox.

     Note:
     If you're connecting a room, equipment, or linked mailbox, the **Select User** dialog box displays only users that are disabled in Active Directory. If you're connecting a user mailbox, the **Select User** dialog box displays only users that are enabled in Active Directory.
   - **Alias** Use this box to type an alias for the mailbox.
   - **Retention Policy** Select this check box to assign a retention policy to the mailbox. Click **Browse** to select a policy from a list of available retention policies. For more information, see Understanding Messaging Records Management.
   - **Exchange ActiveSync mailbox policy** Select this check box to assign a Microsoft Exchange ActiveSync policy to the mailbox. Click **Browse** to select a policy from a list of available Exchange ActiveSync policies. For more information, see Understanding Exchange ActiveSync Mailbox Policies.

6. If you're connecting a linked mailbox, use the **Master Account** page to

configure the following settings for the mailbox:

- **Trusted forest or domain** Click **Browse** to open the **Select Forest** dialog box. Select the forest that contains the master account, and then click **OK**. This enables the **Browse** button next to the **Linked domain controller** check box.
- **Use the following Window user account to access linked domain controller** Select this check box if you want to specify a different user account. To access the domain controller in the linked forest, you can use a user account other than the one you're currently logged on as. Select the **User name** and **Password** check boxes to type the credentials of the user account.
- **Linked domain controller** Click **Browse** to open the **Select Domain Controller** dialog box. Select the domain controller you want, and then click **OK**. Selecting a valid linked domain controller enables the **Browse** button next to the **Linked master account** check box.
- **Linked master account** Click **Browse** to open the **Select Master Account** dialog box. Select the user account that you want to use as the master account, and then click **OK**.

7. On the **Connect Mailbox** page, review your configuration settings. Click **Connect** to associate the disconnected mailbox with the Active Directory user that you selected on the **Mailbox Settings** page. Click **Back** to make configuration changes.

8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to connect a disabled mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example connects the mailbox for John Evans that resides on the mailbox database MBXDB02. In addition, this command bypasses the messaging records management (MRM) policy warnings for e-mail clients using versions of Microsoft Outlook earlier than Microsoft Office Outlook 2007.

```
Connect-Mailbox -Identity "John Evans" -Database "MBXDB02" -User "John Evans" -Ma
```

This example connects a linked mailbox.

```
Connect-Mailbox -Identity "John Evans" -Database "MBXDB02" -LinkedDomainControlle
```

This example connects an equipment mailbox for CAR001 that resides on the database MBXResourceDB.

```
Connect-Mailbox -Identity "CAR001" -Database "MBXResourceDB" -Equipment -User "CA
```

This example connects a room mailbox for a conference room (ConfRm212) that resides on the database MBXResourceDB.

```
Connect-Mailbox -Identity "ConfRm212" -Database "MBXResourceDB" -Room -User "Conf
```

For detailed syntax and parameter information, see Connect-Mailbox.

Use the Shell to restore a disabled mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:
You can't use the EMC to restore a disabled mailbox.

Note:
To create a restore request, you must use the `DisplayName`, `LegacyDN`, or `MailboxGUID` values to identify the disabled mailbox.

1. Use the **Get-MailboxStatistics** cmdlet to find the display name, legacy distinguished name (DN), or mailbox GUID of the disabled mailbox. This example returns the `LegacyDN`, `DisplayName`, `MailboxGUID`, and `DisconnectReason` values for all mailboxes on mailbox database MBD01 that have a disconnect reason of `Disabled`.

```
Get-MailboxStatistics -Database MBD01 | Where { $_.DisconnectReason -e
```

2. Use the **New-MailboxRestoreRequest** cmdlet to create the restore request. This example restores the disabled mailbox that has the mailbox GUID 1d20855f-fd54-4681-98e6-e249f7326ddd on mailbox database MDB01 to the target mailbox Ayla. This example assumes that the legacy DN of the target mailbox matches the legacy DN of the source mailbox.

```
New-MailboxRestoreRequest -SourceDatabase "MDB01" -SourceStoreMailbox
```

   This example restores the disabled mailbox Tony Smith to the target mailbox tony@contoso.com on the target mailbox database MDB01. The *AllowLegacyDNMismatch* parameter is used so the source mailbox can be restored to a mailbox that doesn't have the same legacy DN value.

```
New-MailboxRestoreRequst -SourceDatabase "MDB01" -SourceStoreMailbox "
```

For detailed syntax and parameter information, see the following topics:

- Get-MailboxStatistics
- New-MailboxRestoreRequest

Other Tasks

After the mailbox is connected, we recommend that you configure anti-spam features. For detailed steps, see Configure Anti-Spam Features on a Mailbox.

1.8.3.24.22.2 Restore a Soft-Deleted Mailbox

Restore a Soft-Deleted Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A disconnected mailbox is a mailbox object in the Exchange store that isn't associated with an Active Directory user account. Disconnected mailboxes remain in the Exchange database for the duration specified in the deleted mailbox retention settings for the mailbox database. By default, disconnected mailboxes are retained for 30 days. During this retention period, a mailbox can be recovered by connecting it to a new or existing Active Directory user account.

There are two types of disconnected mailboxes:

- **Soft-deleted mailboxes** When mailboxes are moved from a Microsoft Exchange Server 2010 Service Pack 1 (SP1) database to any other database, Exchange doesn't fully delete the mailbox from the source database upon completion of the move. Instead, the mailbox in the source mailbox database is switched to a *soft-deleted* state. With soft-deleted mailboxes, you can use the **MailboxRestoreRequest** cmdlet set to access mailbox data during a mailbox restore operation. Soft-deleted mailboxes are retained in the source database until either the deleted mailbox retention period expires or until the **Remove-StoreMailbox** cmdlet is used to purge the mailbox.
- **Disabled mailboxes** When a mailbox is disconnected or removed using the **Disable-Mailbox** or **Remove-Mailbox** cmdlet, Exchange retains the deleted mailbox, and the mailbox is switched to a disabled state. With disabled mailboxes, you can recover mailbox data without having to restore the entire mailbox database. Disabled mailboxes are retained in the mailbox database until the deleted mailbox retention period expires or until the mailbox is permanently deleted. For more information, see Connect or Restore a Disabled Mailbox.

Looking for other management tasks related to disconnected mailboxes? Check out Managing Disconnected Mailboxes.

Use the Shell to restore a soft-deleted mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:
You can't use the EMC to restore a soft-deleted mailbox.

Note:
To create a restore request, you must use the `DisplayName`, `LegacyDN`, or `MailboxGUID` values to identify the soft-deleted mailbox.

1. Use the **Get-MailboxStatistics** cmdlet to find the display name, legacy distinguished name (DN), or mailbox GUID of the soft-deleted mailbox. This example returns the `DisplayName`, `LegacyDN`, `MailboxGUID`, and `DisconnectReason` values for all mailboxes on mailbox database MBD01 that have a disconnect reason of `SoftDeleted`.

```
Get-MailboxStatistics -Database MBD01 | Where { $_.DisconnectReason -e
```

2. Use the **New-MailboxRestoreRequest** cmdlet to create the restore request. This example restores the source mailbox that has the display name Ayla on mailbox database MBD01 to Ayla's mailbox.

```
New-MailboxRestoreRequest -SourceDatabase "MBD01" -SourceStoreMailbox
```

For detailed syntax and parameter information, see Get-MailboxStatistics or New-MailboxRestoreRequest.

Use the Shell to restore a soft-deleted mailbox to a user's archive mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:
You can't use the EMC to restore a soft-deleted mailbox to a user's archive mailbox.

This example restores the source mailbox that has the mailbox GUID 1d20855f-fd54-4681-98e6-e249f7326ddd on mailbox database MBD01 to Tony's archive mailbox.

```
New-MailboxRestoreRequest -SourceDatabase "MBD01" -SourceStoreMailbox 1d20855f-fd
```

For detailed syntax and parameter information, see New-MailboxRestoreRequest.

Other Tasks

After you initiate the restore request, you may also want to:

- View Restore Request Properties and Statistics
- Remove a Restore Request

1.8.3.24.22.3 View Restore Request Properties and Statistics

View Restore Request Properties and Statistics

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Mailbox restore requests are used to restore disconnected mailboxes. A disconnected mailbox is a mailbox object in the Exchange store that isn't associated with an Active Directory user account. Disconnected mailboxes remain in the Exchange database for the duration specified in the deleted mailbox retention settings for the mailbox database. By default, disconnected mailboxes are retained for 30 days. During this retention period, a mailbox can be recovered by connecting it to a new or existing Active Directory user account.

You can view the properties of a mailbox restore request, or you can view the statistics. The properties provide you with basic information about the status of a mailbox restore request. The statistics provide you with detailed information that can be used for troubleshooting purposes.

The search criteria for the **Get-MailboxRestoreRequest** and **Get-MailboxRestoreRequestStatistics** cmdlets is a Boolean **And** statement. If you use multiple parameters, you can narrow your search and reduce your search results.

Looking for other management tasks related to disconnected mailboxes? Check out Managing Disconnected Mailboxes.

Use the Shell to view mailbox restore request properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Disconnected mailboxes" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to view mailbox restore request properties.

This example returns the status of the restore request Ayla\MailboxRestore using the *Identity* parameter.

```
Get-MailboxRestoreRequest -Identity "Ayla\MailboxRestore"
```

This example returns additional information about the status of the second restore request for the target mailbox with the display name Kweku by pipelining the command to the **Format-List** cmdlet.

```
Get-MailboxRestoreRequest -Identity "Kweku\MailboxRestore1" | Format-List
```

This example returns the status of restore requests being restored from the source database MBD01.

```
Get-MailboxRestoreRequest -SourceDatabase MBD01
```

This example returns all restore requests named RestoreToMBD01 that have been suspended.

```
Get-MailboxRestoreRequest -Name "RestoreToMBD01" -Suspend $true
```

For detailed syntax and parameter information, see Get-MailboxRestoreRequest.

Get-MailboxRestoreRequest Output

Be default, the **Get-MailboxRestoreRequest** cmdlet returns the name of the request, the target mailbox to which data is being restored, and the status of the request. The following table lists the information returned if you pipeline the cmdlet to the **Format-List** cmdlet.

Value	Description
SourceDatabase	Specifies the database that contains the disconnected mailbox being restored.
TargetDatabase	Specifies the database that contains the mailbox or archive to which the mailbox is being restored.
TargetMailbox	Specifies the mailbox into which data is being restored.
Name	Specifies the name of the request.
RequestGuid	Specifies the GUID of the request.
RequestQueue	Specifies the database on which the Microsoft Exchange Mailbox Replication service (MRS) stores the detailed status of the request.
Flags	Specifies flags that the cmdlet automatically

	sets when creating the request.
BatchName	Specifies a batch name. If you didn't provide a batch name, this field is blank.
Status	Specifies the status of the request.
Suspend	Specifies whether the request was created to be automatically suspended before completion.
Direction	Specifies whether the request is a push or a pull. For mailbox restore requests, this value is always Pull.
RequestStyle	Specifies whether the request is IntraOrg or CrossOrg. For Microsoft Exchange Server 2010 Service Pack 1 (SP1), this value is always IntraOrg.
OrganizationID	If the request is performed in a multi-tenant organization, this value specifies the identity of the organization on which the request is performed.
Identity	Specifies the identity of the request. This identity is a combination of the target mailbox name and the request name.
IsValid	Specifies whether the mailbox restore request is valid.

Use the Shell to view mailbox restore request statistics

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Disconnected mailboxes" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to view mailbox restore request statistics.

This example returns the default statistics for the restore request Tony\MailboxRestore1. By default, the information returned includes name, mailbox, status, and percentage complete.

```
Get-MailboxRestoreRequestStatistics -Identity Tony\MailboxRestore1
```

This example returns the statistics for Tony Smith's mailbox and exports the report to a .csv file.

```
Get-MailboxRestoreRequestStatistics -Identity Tony\MailboxRestore | Export-CSV \\
```

This example returns additional information about the restore request for Tony Smith's mailbox using the *IncludeReport* parameter and pipelining the results to the **Format-List** cmdlet.

```
Get-MailboxRestoreRequestStatistics -Identity Tony\MailboxRestore -IncludeReport
```

This example returns default statistics for a restore request being processed by the

instance of MRS running on the Client Access server CAS01. This command returns only information for restore requests currently being processed by an instance of MRS. If the Client Access server is finished processing all restore requests, no information is returned. This command is for debugging purposes and should only be performed if requested by support personnel.

```
Get-MailboxRestoreRequestStatistics -MRSInstance CAS01.contoso.com
```

This example returns additional information for all restore requests that have a status of `Failed` using the *IncludeReport* parameter, and then saves the information to the file AllRestoreReports.txt in the location where the command is being run.

```
Get-MailboxRestoreRequest -Status Failed | Get-MailboxRestoreRequestStatistics -I
```

For detailed syntax and parameter information, see Get-MailboxRestoreRequestStatistics and Get-MailboxRestoreRequest.

Get-MailboxRestoreRequestStatistics Output

By default, the Get-MailboxRestoreRequestStatistics cmdlet returns the name of the request, the status of the request, the alias of the target mailbox, and the percentage completed. The following table lists the information returned if you pipeline the cmdlet to the **Format-List** cmdlet.

Value	Description
`Name`	Specifies the name of the request.
`Status`	Specifies the status of the request.
`StatusDetail`	Specifies more details about the request status. For example, if the `Status` value returns `InProgress`, the `StatusDetail` value would return the specific stages for the `InProgress` status, such as `CreatingFolderHierarchy` and `CopyingMessages`.
`SyncStage`	Specifies how far along the request is through the restore process.
`Flags`	Specifies flags that the cmdlet automatically sets when creating the mailbox restore request.
`RequestStyle`	Specifies whether the request is `IntraOrg` or `CrossOrg`. For Exchange 2010 SP1, this value is always `IntraOrg`.
`Direction`	Specifies whether the request is a push or a pull. For mailbox restore requests, this value is always `Pull`.
`Protect`	Reserved for Microsoft internal use only.
`Suspend`	Specifies whether the restore request is suspended. This value is `true` in the following scenarios: • MRS stopped or is in the process of stopping the request due to a failure. • An administrator suspended the request.
`SourceExchangeGuid`	Specifies the GUID of the source mailbox from which data is being restored.

SourceRootFolder	Specifies the name of the root folder in the source mailbox's hierarchy from which data is being restored. If this value is blank, data is restored from the folder Top of Information Store.
SourceVersion	Specifies the version of Exchange running on the database in which the source mailbox is located.
SourceDatabase	Specifies the name of the database on which the source mailbox is located.
MailboxRestoreFlags	Specifies that the mailbox being restored is either Disabled or Soft-Deleted.
TargetAlias	Specifies the alias of the target mailbox.
TargetIsArchive	Specifies whether the mailbox is being restored into an archive.
TargetExchangeGuid	Specifies the GUID of the target mailbox or archive.
TargetRootFolder	Specifies the name of the root folder in the mailbox's or archive's hierarchy to which data is being restored. If this value is blank, data is restored to the folder Top of Information Store.
TargetVersion	Specifies the version of Exchange running on the Mailbox server on which the target database is mounted.
TargetDatabase	Specifies the name of the database on which the target mailbox is located.
TargetMailboxIdentity	Specifies the identity of the target mailbox.
IncludeFolders	Specifies the list of folders to include during the restore. If this value is blank, no folders were specified when the request was created, and all folders will be restored to the mailbox or archive (unless the *ExcludeFolders* parameter is used to exclude specific folders).
ExcludeFolders	Specifies the list of folders to exclude during the restore. If this value is blank, no folders were specified when the request was created, and all folders will be restored to the mailbox or archive (unless the *IncludeFolders* parameter is used to include specific folders).
ExcludeDumpster	Specifies whether the Recoverable Items folder was excluded when the request was created.
ConflictResolutionOption	Specifies the action for MRS to take if there are matching messages in the target and source folders.
AssociatedMessagesCopyOption	Specifies whether the associated messages are copied when the request is processed. Associated messages are special messages that contain hidden data with information about rules, views, and forms.

BatchName	Specifies a batch name. If you don't provide a batch name, this field is blank.
BadItemLimit	Specifies the number of bad items that MRS will skip if the request encounters corrupted messages.
BadItemsEncountered	Specifies the number of corrupted messages encountered by the command. If the *BadItemsEncountered* value is greater than the *BadItemLimit* value, the request fails.
QueuedTimeStamp	Specifies the date and time at which the request was initiated to MRS.
StartTimeStamp	Specifies the date and time at which the restore request started being processed by MRS.
LastUpdateTimeStamp	Specifies the date and time at which the last change was made to the request. The change may have been made by an administrator or by MRS.
SuspendTimeStamp	Specifies the date and time at which the request was suspended.
OverallDuration	Specifies the amount of time it took to complete the request. If the request is in a `Failed` state, this value specifies the amount of time between the request being initiated and the request failing. If the request isn't complete, this value specifies the amount of time between the request being initiated and the **Get-MailboxRestoreRequestStatistics** cmdlet being run.
TotalSuspendedDuration	Specifies the amount of time the request was in the `Suspended` state.
TotalFailedDuration	Specifies the amount of time the request was in the `Failed` state.
TotalQueuedDuration	Specifies the amount of time the request was in the `Queued` state.
TotalInProgressDuration	Specifies the amount of time the request was in the `In Progress` state.
TotalStalledDueToHADuration	Specifies the amount of time the request was stalled due to high availability.
MRSServerName	Specifies the name of the Client Access server that processed the request.
EstimatedTransferSize	Specifies the file size that was restored or the file size that MRS expects to restore if the request is in the `In Progress` state.
EstimatedTransferItemCount	Specifies the number of items that were restored or the number of items that MRS expects to restore if the request is in the `In Progress` state.
BytesTransferred	Specifies the total number of bytes that have been

	transferred.
BytesTransferredPerMinute	Specifies the average number of bytes that have been transferred per minute.
ItemsTransferred	Specifies the number of items that have been transferred.
PercentComplete	Specifies the percentage of the request that has been completed.
PositionInQueue	If the request hasn't started, this value specifies the request's position in the queue.
FailureCode	If there is a failure, this value specifies the failure code.
FailureType	If there is a failure, this value specifies the failure type.
FailureSide	If there is a failure, this value specifies whether the failure occurred on the target mailbox or the source mailbox.
Message	If there is a failure, this value specifies the failure message. This value can also specify the suspend comment.
FailureTimestamp	If the request failed, this value specifies the date and time at which the request failed.
FailureContext	If the request failed, this value specifies information about the action being performed at the time of failure.
IsValid	Specifies whether the request was valid.
ValidationMessage	If the request isn't valid, this value specifies the reason.
OrganizationID	If the request is performed in a multi-tenant organization, this value specifies the identity of the organization in which the request is performed.
RequestGuid	Specifies the GUID of the request.
RequestQueue	Specifies the database on which MRS stores the detailed status of the request.
Identity	Specifies the identity of the request.
Report	If you used the *IncludeReport* parameter, this value specifies information that can be used to troubleshoot the request.

1.8.3.24.22.4 Configure Restore Request Properties

Configure Restore Request Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Mailbox restore requests are used to restore disconnected mailboxes. A disconnected mailbox is a mailbox object in the Exchange store that isn't associated with an Active Directory user account. Disconnected mailboxes remain in the Exchange database for the duration specified in the deleted mailbox retention settings for the mailbox database. By default, disconnected mailboxes are retained for 30 days.

If a restore request fails, you can change the request's properties to recover from the failure.

Looking for other management tasks related to disconnected mailboxes or restore requests? Check out Managing Disconnected Mailboxes.

Use the Shell to configure restore request properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Disconnected mailboxes" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to configure restore request properties.

This example specifies that the restore request MailboxRestore1 for Ayla's mailbox skips 10 corrupted mailbox items.

```
Set-MailboxRestoreRequest -Identity "Ayla\MailboxRestore1" -BadItemLimit 10
```

This example specifies that the restore request MailboxRestore1 for Kweku's mailbox skips 100 corrupted items. Because the *BadItemLimit* value is greater than 50, the *AcceptLargeDataLoss* parameter must be specified.

```
Set-MailboxRestoreRequest -Identity "Kweku\MailboxRestore1" -BadItemLimit 100 -Ac
```

For detailed syntax and parameter information, see Set-MailboxRestoreRequest.

Other Tasks

After you configure the restore request's settings, you may also want to resume the restore request. For details, see Resume a Restore Request.

1.8.3.24.22.5 Suspend a Restore Request

Suspend a Restore Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can suspend a restore request any time after the request was created but before the request reaches the status of `Completed`. You can resume the restore request using the Resume-MailboxRestoreRequest cmdlet.

Looking for other management tasks related to restore requests or disconnected mailboxes? Check out Managing Disconnected Mailboxes.

Use the Shell to suspend a restore request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Disconnected mailboxes" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to suspend a restore request.

This example suspends the restore request MailboxRestore1 for Ayla's mailbox.

```
Suspend-MailboxRestoreRequest -Identity Ayla\MailboxRestore1
```

This example suspends all restore requests in progress by first retrieving all requests that have a status of `InProgress`, and then pipelining output to the **Suspend-MailboxRestoreRequest** cmdlet and including the suspend comment "Resume after 10:00 PM."

```
Get-MailboxRestoreRequest -Status InProgress | Suspend-MailboxRestoreRequest -Sus
```

For detailed syntax and parameter information, see Suspend-MailboxRestoreRequest and Get-MailboxRestoreRequest.

Other Tasks

After you suspend a restore request, you may also want to resume the request. For details, see Resume a Restore Request.

1.8.3.24.22.6 Resume a Restore Request

Resume a Restore Request

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Use the **Resume-MailboxRestoreRequest** cmdlet to resume a restore request that was previously suspended or failed.

Looking for other management tasks related to disconnected mailboxes? Check out Managing Disconnected Mailboxes.

Use the Shell to resume a restore request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example resumes the restore request kweku\RestoreFromDB01

```
Resume-MailboxRestoreRequest -Identity "kweku\RestoreFromDB01"
```

This example resumes any restore request that has a status of Failed.

```
Get-MailboxRestoreRequest -Status Failed | Resume-MailboxRestoreRequest
```

For detailed syntax and parameter information, see the following topics:

- Resume-MailboxRestoreRequest
- Get-MailboxRestoreRequest

Other Tasks

After you resume the restore request, you may also want to view the properties of the restore request. For details, see View Restore Request Properties and Statistics.

1.8.3.24.22.7 Remove a Restore Request

Remove a Restore Request

Managing Mailbox Servers > Managing User Mailboxes > Managing Disconnected Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Mailbox restore requests are used to restore disconnected mailboxes. A disconnected mailbox is a mailbox object in the Exchange store that isn't associated with an Active Directory user account. Disconnected mailboxes remain in the Exchange database for the duration specified in the deleted mailbox retention settings for the mailbox database. By default, disconnected mailboxes are retained for 30 days.

You can use the **Remove-MailboxRestoreRequest** cmdlet to remove a partially completed restore request. If you remove the restore request after mailbox data begins to move to the target mailbox, the mailbox data that is moved remains in the target mailbox.

Looking for other management tasks related to disconnected mailboxes? Check out Managing Disconnected Mailboxes.

Use the Shell to remove a restore request

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

You can't use the EMC to restore a mailbox.

This example removes the restore request Ayla\MailboxRestore1.

```
Remove-MailboxRestoreRequest -Identity "Ayla\MailboxRestore1"
```

This example removes all restore requests that have the status of Completed.

```
Get-MailboxRestoreRequest -Status Completed | Remove-MailboxRestoreRequest
```

This example cancels the restore request by using the *RequestGuid* parameter for a request stored on MBXDB01. The parameter set that requires the *RequestGuid* and *RequestQueue* parameters is used only for Microsoft Replication Service debugging purposes. You should use this parameter set only if instructed by Microsoft Customer Service and Support.

```
Remove-MailboxRestoreRequest -RequestQueue MBXDB01 -RequestGuid 25e0eaf2-6cc2-435
```

For detailed syntax and parameter information, see the following topics:

- Remove-MailboxRestoreRequest
- Get-MailboxRestoreRequest

1.8.3.24.22.8 Permanently Delete a Disconnected Mailbox

Permanently Delete a Disconnected Mailbox

Managing Mailbox Servers > Managing User Mailboxes > Managing Disconnected Mailboxes >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When you use the **Remove-StoreMailbox** cmdlet to purge a disconnected mailbox and all its contents from the mailbox database, the data loss is permanent. There are two types of disconnected mailboxes: soft-deleted and disabled. When running the cmdlet, you must specify one of these types. If the type you specify doesn't match the actual type of the disconnected mailbox, the command fails.

To learn more about disconnected mailboxes, see Understanding Disconnected Mailboxes.

Note:
You can run the **Remove-StoreMailbox** cmdlet only against disconnected mailboxes. If you attempt to run the cmdlet against an active mailbox, the cmdlet fails, and an error is returned. For details about how to permanently delete an active mailbox, see "Use the Shell to permanently remove a mailbox" in Remove a Mailbox.

Looking for other management tasks related to disconnected mailboxes? Check out Managing Disconnected Mailboxes.

Use the Shell to permanently delete a disconnected mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Disconnected mailboxes" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to permanently delete a disconnected mailbox.

This example permanently deletes the soft-deleted mailbox for Ayla from mailbox database MBD01.

```
Remove-StoreMailbox -Database MBD01 -Identity Ayla -MailboxState SoftDeleted
```

This example permanently deletes all soft-deleted mailboxes from mailbox database MBD01.

```
Get-MailboxStatistics -Database MBD01 | where {$_.DisconnectReason -eq "SoftDelet
```

This example permanently deletes the disabled mailbox with the GUID 2ab32ce3-fae1-4402-9489-c67e3ae173d3 from mailbox database MBD01.

```
Remove-StoreMailbox -Database MBD01 -Identity "2ab32ce3-fae1-4402-9489-c67e3ae173
```

For detailed syntax and parameter information, see Remove-StoreMailbox and Get-MailboxStatistics.

1.8.4 Securing Mailbox Servers

Securing Mailbox Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-19*

This topic summarizes the security-related options available for a computer running Microsoft Exchange Server 2010 that has the Mailbox server role installed. By default, HTTP, Microsoft Exchange ActiveSync, POP3, and IMAP4 communication between the Mailbox servers and other Exchange server roles, domain controllers, and global catalog servers is encrypted.

Make sure that your Mailbox servers aren't accessible to the Internet. Also, the Mailbox server role in Exchange 2010 includes security improvements to the Exchange store. For information about these improvements, see Understanding the Exchange 2010 Store.

1.8.5 Troubleshooting Mailbox Servers

Troubleshooting Mailbox Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-31*

After the Mailbox server role is installed on an Exchange 2010 server, you may have to test the server's functionality or solve problems related to mailbox connectivity. The following topics can help you troubleshoot common errors and test that your Mailbox server is configured correctly:

- Troubleshooting Mailbox Moves
- Autodiscover won't work with OABs in Active Directory forest that contains a single-label domain name

- "Task Mount-Database throwing terminating exception" Error Occurs When You Try to Mount a Database
- The Log Generation Number is Not Reset if You Delete the Physical Files in an Exchange Server 2010 Database
- Event IDs 1121 and 5000 Are Logged When You Try to Start the Information Store Service

1.8.5.1 Autodiscover won't work with OABs in Active Directory forest that contains a single-label domain name

Autodiscover won't work with OABs in Active Directory forest that contains a single-label domain name

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2011-11-08*

If you try to use the Autodiscover feature in Exchange Server 2007 together with offline address books (OABs) in an Active Directory forest that contains a single-label domain name, Autodiscover won't work as expected.

Single-label DNS names are DNS names that don't contain a suffix, such as .com, .corp, .net, or .org. For example, Contoso instead of Contoso.com.

This issue occurs because Outlook assumes that the default e-mail address policy would map to a publicly resolvable name. To send mail over the Internet, SMTP domains in an e-mail address policy must resolve to one of the top-level domains supported by RFCs (for example, the top-level domain names described in RFC 1591 - Domain Name System Structure and Delegation). Outlook requires that the proxy addresses defined in the e-mail address policy contain at least two levels of hierarchy in the name. Specifically, the addresses must contain at least one dotted suffix that's acceptable by Outlook. The following list includes examples of names that Outlook considers valid:

- contoso.com
- contoso.eu
- contoso.test

Note:

Although, Outlook considers contoso.test to be a valid domain name, it isn't publicly resolvable according to RFC standards because there is no top-level domain called "test" on the Internet. However, such a domain name could be used to route internal e-mail only. Recipients couldn't receive mail for that domain from outside the company.

What can I do to fix this?

To maintain your second-level domain (SLD), the proxy addresses in your default e-mail address policy must include at least two levels of hierarchy (for example, Fname.Lname@contoso.com).

Depending on your organization's structure, run one or both of the following commands:

- **Mixed Exchange 2003 and Exchange 2007 organization**
  - If the e-mail address policy (called a Recipient Policy in Exchange 2003) exists on an Exchange 2003 server, the policy won't have the OPATH filtering syntax. In this case, run Command 1 followed by Command 2.

- If the e-mail address policy exists on an Exchange 2007 server, run only Command 2.

- **Pure Exchange 2007 or Exchange 2010 organization** Run only Command 2.

Command 1

```
Set-EmailAddressPolicy "Default Policy" -IncludedRecipients AllRecipients
```

Command 2

```
Set-EmailAddressPolicy "Default Policy" -EnabledPrimarySMTPAddressTemplate "%g.%s
```

For detailed syntax and parameter information, see Set-EmailAddressPolicy.

1.8.5.2 Event IDs 1121 and 5000 Are Logged When You Try to Start the Information Store Service

Event IDs 1121 and 5000 Are Logged When You Try to Start the Information Store Service

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-10-30*

This topic provides information about how to troubleshoot an issue in which the Microsoft Exchange Information Store service does not start in Exchange Server 2010. Looking for other management tasks related to Microsoft Exchange Information Store service? Check out Managing Mailbox Servers.

When you try to start the Exchange Information Store, you receive the following error message:

> Windows could not start the Microsoft Exchange Information Store on Local Computer. For more information, review the System Event Log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 0.

When this error occurs, events that resemble the following may be recorded in the Application log in Event Viewer.

Event ID 1121

> Event Type: Error
>
> Event Source: MSExchangeIS
>
> Event Category: General
>
> Description: Error 0x8004010f connecting to the Microsoft Active Directory.

Event ID 5000

> Event Type: Error
>
> Event Source: MSExchangeIS

Event Category: General

Description: Unable to initialize the Microsoft Exchange Information Store service. - Error 0x8004010f.

This issue may occur if the **Default Policy** item was deleted from the **E-mail Address Policies** tab, and if it was replaced by a custom e-mail address policy. By default, Exchange Server 2010 is hard-coded to search for the default recipient policy when the Information Store starts.

To resolve this issue, use Active Directory Service Interfaces (ADSI) Edit to change the value of the **msExchPolicyOrder** attribute to **2147483647** for a custom e-mail address policy.

ADSI Edit can be run from a client computer or a server. The computer does not have to be a member of a domain, but the user must have the rights to view and edit the Active Directory directory service domain to which the user is connecting. For more information about how to use ADSI Edit, see ADSI Edit (adsiedit.msc).

To change one of your custom e-mail address policies to a default policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the Mailbox server configuration entry in the Mailbox Permissions topic.

1. Install ADSI Edit if it is not already installed on the computer that is running Exchange Server 2010.
2. Start ADSI Edit. To do this, click **Start**, click **Run**, type **adsiedit.msc** in the text box, and then click **OK**.
3. Expand the following container:**CN= Recipient Policies\CN=<Organization>\CN= Microsoft Exchange\CN= Services\CN= Configuration\DC=<Domain Name>\DC=com**
4. Right-click the e-mail address policy that you want to change to the default policy, and then click **Properties**.
5. In the **Attribute** column, locate the **purportedSearch** attribute, and then verify that the value in the **Value** column is **(mailNickname=*)**. If the value is incorrect, follow these steps:
   5.a.Click **purportedSearch**, and then click **Edit**.
   5.b.Click **Clear**, type **(mailNickname=*)** in the **Value** box, and then click **OK**.
6. In the **Attribute** list, click the **msExchPolicyOrder** attribute, and then click **Edit**.
7. Click **Clear**, type **2147483647** in the **Value** box, and then click **OK**.
8. Click **OK**, and then close ADSI Edit.
9. Restart the Exchange Mailbox server.

For More Information

Understanding the Exchange 2010 Store

Overview of Services Installed by Exchange Setup

1.8.5.3 Reclaim Space When the .edb File Size Grows Too Large

Reclaim Space When the .edb File Size Grows Too Large

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-10-25*

The .edb file of a database may grow too large for its volume in Microsoft Exchange Server 2010. If this occurs, you must take the following actions:

- Move mailboxes from the problem Exchange mailbox database to mailbox databases that have more space.
- Remove the problem mailbox database.

As an optional third step, you can re-create the original database, and then restore some of the mailboxes to it.

To resolve this issue, follow these steps.

Important:

Contact Microsoft Customer Service and Support for help to complete this procedure. For more information, see the Contact us website.

Prerequisites

- Verify that all copies of the database are in a healthy state. To do this, run the following command:
  - **Get-MailboxDatabaseCopyStatus (Get-MailboxDatabase | ? {$_.EdbFilePath -eq $pathToEDBdatabaseFile})**

  For more information, see Monitoring High Availability and Site Resilience.
- In Exchange Management Shell, run the following commands to determine whether mailboxes exist on the databases:
  - **Set-ADServerSettings -ViewEntireForest $True**
  - **Get-Mailbox -Database "<Database_ID>"**

  If the mailboxes do exist, see the Create a Local Move Request topic to move the mailboxes to databases that have more space.

Warning:

This process can permanently delete data. Make sure that there no mailboxes exist on the affected database before you go to the next step.

Use the shell to reclaim space when the edb file size has grown too large

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox databases" entry in the Mailbox Permissions topic.

1. Open Exchange Management Shell.
2. Note the configured properties of the affected database and database copies. See the Configure Mailbox Database Copy Properties topic for the properties that will have to be reset when the database copies are re-created.
3. Follow the instructions in the Remove a Mailbox Database Copy topic to remove all passive copies of the database.

   Note:

As mentioned in the "Remove a Mailbox Database Copy" topic, circular logging must be disabled when you remove the last passive database copy. If circular logging is enabled, run the following cmdlet to disable it for the database: **Set-MailboxDatabase "<Database_Identity>" –CircularLoggingEnabled $false**

4. Run the following cmdlet to unmount the database: **Dismount-Database "<Database_Identity>"**When you are prompted, type **a** to confirm the action.
5. Run the following cmdlet to remove the mailbox database: **Remove-MailboxDatabase "<Database_Identity>"**When you are prompted, type **a** to confirm the action.
6. Manually delete the .edb file and log files of this database from all servers that contained database copies. Also, manually delete the .edb file and log files from all servers that contain a copy of the database that you are removing.
7. Follow the instructions in the Create a Mailbox Database topic to re-create this database.
8. Run the following cmdlet to mount the empty database: **Remove-MailboxDatabase "<Database_Identity>"**.
9. Manually delete the edb and log files of this database from all servers that contained database copies.
10. Follow the instructions in the Create a Mailbox Database topic to re-create this database.
11. Run the following cmdlet to mount the empty database: **Mount-Database "<Database_Identity>" -Force**
12. Follow the instructions in the Add a Mailbox Database Copy topic to re-create all the database copies you removed in step 2. Use the properties that you noted in step 2.
13. If Circular Logging was disabled in step 3, run the following cmdlet to enable Circular Logging: **Set-MailboxDatabase "<Database_Identity>" -CircularLoggingEnabled $true**. For more information about circular logging, see the "Circular Logging" entry in the Understanding the Exchange 2010 Store topic.
14. Move some mailboxes back to this database.

Validation

To validate the database, follow these steps.

1. Run the following cmdlet to verify the health of all copies of this database: **Get-MailboxDatabaseCopyStatus "<Database_Identity>"**
2. Run the following cmdlet to verify that the database can replicate changes to all servers that contain database copies: **Test-ReplicationHealth <Each_Server_With_A_Copy_Of_The_Database>**
3. Run the following cmdlet to verify the health of all servers that contain database copies: **Test-MAPIConnectivity <Server_With_The_Mounted_Copy_Of _The_Database>**

For More Information

Managing Mailbox Databases

Managing Mailbox Database Copies

1.8.5.4 "Task

"Task Mount-Database throwing terminating exception" Error Occurs When You Try to Mount a Database

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2011-08-12*

When you try to mount a database in Microsoft Exchange Server 2010, you may receive the following error message:

Task Mount-Database throwing terminating exception when processing record of index 0. Exception: System.InvalidOperationException: The database object MB11DB1' in Active Directory has been corrupted and is in an inconsistent state: The servers of the database are null.

If this error occurs, you can use database portability to resolve the problem.

How can I fix the problem?

To resolve this problem, use database portability to move an Exchange 2010 mailbox database between Exchange 2010 Mailbox servers in the same organization. For more information about how to do this, see Move a Mailbox Database Using Database Portability.

1.8.5.5 The Log Generation Number is Not Reset if You Delete the Physical Files in an Exchange Server 2010 Database

The Log Generation Number is Not Reset if You Delete the Physical Files in an Exchange Server 2010 Database

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2011-09-09*

The current log generation does not reset in a Microsoft Exchange Server 2010 cluster database if you do the following:

- You delete the physical files in the cluster database
- You leave the objects in Active Directory directory service
- You do not delete the files in the cluster database

The system tracks the current log generation as part of the logic to maintain the loss calculation. This number is not reset by deleting the files.

To resolve this issue, an administrator must use the **Move-ActiveMailboxDatabase** cmdlet together with the *MountDialOverride* parameter to complete a lossless move of the active database to the cluster database. The value of the current log generation is determined again based on the available files. Then, the value is saved.

More information

For more information about the **Move-ActiveMailboxDatabase** cmdlet, see Move-ActiveMailboxDatabase.

1.8.5.6 Troubleshooting Mailbox Moves

Troubleshooting Mailbox Moves

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Troubleshooting content will be made available as issues arise. If there's a troubleshooting issue you'd like us to document, click **Click to Rate and Give Feedback** at the top of this topic and send us feedback. Include as much detail as you can, including any relevant error codes, error descriptions, or event IDs.

Legend

FC	Failure code
ID	Event ID source and number

General steps for troubleshooting mailbox moves

1. If the move request didn't complete, view the Move Request Statistics. For more information, see the section "Use the Shell to view the status of an in-progress move request" in View Move Request Properties.
2. If the move request completed with errors, view the move report. For more information, see the section "Use the Shell to view a completed move request report" in View Move Request Properties.
3. View the Event log on the Client Access server running the instance of the Microsoft Exchange Mailbox Replication service that's processing the failed move request.
4. Step 4 - If you still can't determine the problem, use the Exchange Management Console or the Exchange Management Shell to increase the diagnostic logging levels on the Client Access server for the **Mailbox Move** and **Service** categories of the **MSExchange Mailbox Replication** service. Then resume the failed move request. For details about how to modify the diagnostic logging level, see Manage Diagnostic Logging Levels.

Problems with cross forest\remote move requests

If you're experiencing errors when moving mailboxes across forests, it's possible that the target forest hasn't been properly prepared. For details, see Prepare Mailboxes for Cross-Forest Move Requests.

Corrupted item limit reached (FC: -2147467259 | ID: MSExchange Mailbox

Replication 1100)

Problem

The move request fails because the mailbox has more corrupted items than the move request is configured to skip.

Diagnosis

The move request fails, and the **Get-MoveRequestStatistics** cmdlet returns the following error:

Failure code	Message
-2147467259	Error: This mailbox exceeded the maximum number of corrupted items that were specified for this move request.

The following Event log entry appears on the Client Access server on which the move request was initiated:

Log Name	Application
Source	MSExchange Mailbox Replication
Date	10/26/2009 2:47:17 PM
Event ID	1100
Task Category	Mailbox Move
Level	Error
Keywords	Classic
User	N/A
Computer	CAS01.fabrikam.com
Description	Mailbox move for 'fabrikam.com/Users/TonySmith' (de278a9f-33eb-49f9-950a-070db3323715) has failed. Error code: -2147467259 This mailbox exceeded the maximum number of corrupted items that were specified for this move request.

Resolution

1. Use the Set-MoveRequest cmdlet to increase the *BadItemLimit* threshold. For details, see Configure Move Request Properties.
2. Resume the failed move request. For details, see Complete or Resume a Move Request.

Rules in source mailbox's Inbox folder are larger than 32 KB

Problem

The move request fails when you attempt to move a mailbox from Exchange 2010 to

Exchange 2003 because the size of the rules in the Exchange 2010 mailbox exceeds the size of the rules that's allowed in Exchange 2003 (32 KB).

Diagnosis

When you attempt to move the mailbox, you receive an error similar to the following:

```
Mailbox 'fabrikam.com/Users/tonysmith' could not be moved because rules in source
    + CategoryInfo          : InvalidArgument: (mbx2:MailboxOrMailUserIdParameter
```

Resolution

1. Run the Set-MoveRequest cmdlet with the *IgnoreRuleLimitErrors* parameter. For details, see Configure Move Request Properties.
2. Resume the move request. For details, see Complete or Resume a Move Request.

Note:

End users will need to re-create their rules.

The mailbox dumpster size exceeds the target quota

Problem

The recoverable items quota for the mailbox being moved has exceeded the target quota. This error occurs when you're moving mailboxes from Exchange 2003 or Exchange 2007 to Exchange 2010.

Diagnosis

When you try to move the mailbox, you receive an error similar to the following:

```
Mailbox dumpster size 713 MB (747,659,085 bytes) exceeds target quota 500 MB (524
    + CategoryInfo          : InvalidArgument: (xxxxx/xxxx/xxxx/xxxx:MailboxOrMai
```

Resolution

Move requests don't support moving an Exchange 2003 or Exchange 2007 dumpster to Exchange 2010. However, the move request will still compare the dumpster size between the two product versions. To fix this issue, perform the following steps.

1. Increase the recoverable items quota for the target mailbox database by using the Set-MailboxDatabase cmdlet with the *RecoverableItemsQuota* parameter. For details, see Configure Deleted Item Retention and Recoverable Items Quotas.
2. Resume the failed move request. For details, see Complete or Resume a Move Request.
3. When the move request is complete, return the recoverable items quota to its original size.

MapiExceptionMdbOffline error (FC: -2147467259 | ID: MSExchange Mailbox Replication 1100)

Problem

While the move was in progress, the source or target mailbox database went offline. By default, the Microsoft Exchange Mailbox Replication service (MRS) will attempt to reconnect with the offline database for 30 minutes. If the database doesn't come online within that time, the move will fail. For more information about how to change the MRS connection rate, see Understanding Move Requests.

Diagnosis

The move request fails, and when you run the Get-MoveRequestStatistics cmdlet, you

receive the following error:

Failure code	Message
-2147467259	Error: MapiExceptionMdbOffline: Unable to open entry ID. (hr=0x80004005, ec=1142)

Also, the Client Access server that was processing the move request will log an event similar to the following:

Log Name	Application
Source	MSExchange Mailbox Replication
Date	10/27/2009 10:30:02 AM
Event ID	1100
Task Category	Mailbox Move
Level	Error
Keywords	Classic
User	N/A
Computer	CAS01.fabrikam.com
Description	Mailbox move for 'fabrikam.com/Users/TonySmith' (8dfd4b3b-8147-4e1b-b86f-5d00799abbf3) has failed. Error code: -2147467259 MapiExceptionMdbOffline: Unable to open entry ID. (hr=0x80004005, ec=1142)

Resolution

1. Mount the mailbox database. For details, see Mount a Database.
2. Resume the move request. For details, see Complete or Resume a Move Request.

No available healthy database copies (FC: -2147220223 | ID: MSExchange Mailbox Replication 1100)

When the target database is a replicated database in a database availability group (DAG), MRS regularly checks the replication health of the target database. High availability infrastructure verifies the current replication health against the configured throttling behavior for high availability mailbox moves (as specified by the *DataMoveReplicationConstraint* parameter) for the target database. Depending on the results, MRS will either continue with the move or wait. If the target database isn't healthy for five minutes, MRS will fail. For details about how to change the MRS connection rate, see Understanding Move Requests.

Diagnosis

The move request fails when you run the Get-MoveRequestStatistics cmdlet and the output file returns an error similar to the following:

Failure Code	Message

-2147220223	Error: Move for mailbox '/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=MBX1' is stalled because DataMoveReplicationConstraint is not satisfied for the database 'mdb1' (agent MailboxDatabaseReplication). Failure Reason: Database 1541069d-2976-4f40-afb1-569ed323de0b does not satisfy constraint SecondCopy. There are no available healthy database copies.

Also, the Client Access server that was processing the move request will log an event similar to the following:

Log Name	Application
Source	MSExchange Mailbox Replication
Date	10/27/2009 10:30:02 AM
Event ID	1100
Task Category	Mailbox Move
Level	Error
Keywords	Classic
User	N/A
Computer	MBX01.fabrikam.com
Description	Mailbox move for 'MBX01.fabrikam.com/Users/MBX1' (214dbbab-bb93-4954-a593-515dcc200e7c) has failed. Error code: -2147220223 Move for mailbox '/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=MBX1' is stalled because DataMoveReplicationConstraint is not satisfied for the database 'mdb1' (agent MailboxDatabaseReplication). Failure Reason: Database 1541069d-2976-4f40-afb1-569ed323de0b does not satisfy constraint SecondCopy. There are no available healthy database copies.

Resolution

To resolve this issue, try the following options:

- Remove the move request and then move the mailbox to a healthy target database. For details, see Clear or Remove Move Requests.
- Resolve the issue with the target database's replication and resume the move request. For more information, see Understanding High Availability and Site Resilience.
- Update the *DataMoveReplicationConstraint* parameter on the Set-MailboxDatabase cmdlet for the target database to reflect its current state (if

the constraint that's specified is the wrong constraint). For details, see Configure Mailbox Database Properties.

Certificates are too large or too many

Problem

The user has too many certificates on the mailbox account or the certificates are too large. The maximum number of certificates should be under 1 MB.

Diagnosis

When you attempt to create a move request, you receive an error similar to the following:

```
The call to 'net.tcp:// cas01.fabrikam.com/Microsoft.Exchange.MailboxReplicationS
Error details: The maximum message size quota for incoming messages (262144) has
    + CategoryInfo          : NotSpecified: (0:Int32) [New-MoveRequest], MailboxR
```

Resolution

1. Start Active Directory Users and Computers.
2. On the **View** menu, click **Advanced Features**.
3. In the console tree, expand the domain you want, and then click **Users**.
4. In the details pane, right-click the user, and then click **Properties**.
5. In **<User Name> Properties**, on the **Published Certificates** tab, select the certificate that you want to delete, and then click **Remove**. Repeat this process until you have removed enough certificates.
6. Resume the move request. For details, see Complete or Resume a Move Request.

There aren't any available servers running the Mailbox Replication Service.

Problem

The Microsoft Exchange Mailbox Replication (MSExchangeMailboxReplication) service must be running on at least one Client Access server in the local Active Directory site.

Diagnosis

When you try to create a move request, you receive the following error:

```
There are no available servers that are running the Mailbox Replication Service.
    + CategoryInfo          : NotSpecified: (0:Int32) [New-MoveRequest], MailboxR
```

Resolution

Start the Microsoft Exchange Mailbox Replication Service on at least on Client Access server. For details about how to start the service, see Start, stop, pause, resume, or restart a service.

The Microsoft Exchange Mailbox Replication Service fails to start (ID: MSExchange Mailbox Replication 1010)

Problem

The Microsoft Exchange Mailbox Replication (MSExchangeMailboxReplication) service fails to start.

Diagnosis

The event log on the Client Access server that was processing the request logs the following event:

Provider [Name]	MSExchange Mailbox Replication
Event ID	1010
[Qualifiers]	49156
Level	4
Task	1
Keywords	0x80000000000000
TimeCreated [SystemTime]	2009-07-22T20:53:26.000Z
Channel	Application
Computer	CAS01.fabrikam.com
EventData	System.ServiceModel.CommunicationException: The TransportManager failed to listen on the supplied URI using the NetTcpPortSharing service: failed to start the service because it is disabled. An administrator can enable it by running 'sc.exe config NetTcpPortSharing start= demand'.. ---> System.InvalidOperationException: Cannot start service NetTcpPortSharing on computer '.'. ---> System.ComponentModel.Win32Exception: The service cannot be started, either because it is disabled or because it has no enabled devices associated with it --- End of inner exception stack trace --- at System.ServiceProcess.ServiceController.Start(String[] args) at System.ServiceModel.Channels.SharedConnectionListener.SharedListenerProxy.HandleServiceStart(Boolean isReconnecting) --- End of inner exception stack trace --- at System.ServiceModel.Channels.SharedConnectionListener.SharedListenerProxy.HandleServiceStart(Boolean isReconnecting) at System.ServiceModel.Channels.SharedConnectionListener.SharedListenerProxy.Open(Boolean isReconnecting) at System.ServiceModel.Channels.SharedConnectionListener.StartListen(Boolean isReconnecting) at System.ServiceModel.Channels.SharedTcpTransportManager.OnOpenInternal(Int32 queueId, Guid token) at System.ServiceModel.Channels.SharedTcpTransportManager.OnOpen() at System.ServiceModel.Channels.TransportManager.Open(TransportChannelListener channelListener) at System.ServiceModel.Channels.TransportManagerContainer.Open(SelectTransportManagersCallback selectTransportManagerCallback) at

	System.ServiceModel.Channels.ConnectionOrientedTransportChannelListener.OnOpen (TimeSpan timeout) at System.ServiceModel.Channels.TcpChannelListener`2.OnOpen(TimeSpan timeout) at System.ServiceModel.Channels.CommunicationObject.Open(TimeSpan timeout) at System.ServiceModel.Dispatcher.ChannelDispatcher.OnOpen(TimeSpan timeout) at System.ServiceModel.Channels.CommunicationObject.Open(TimeSpan timeout) at System.ServiceModel.ServiceHostBase.OnOpen(TimeSpan timeout) at System.ServiceModel.Channels.CommunicationObject.Open(TimeSpan timeout) at Microsoft.Exchange.MailboxReplicationService.MailboxReplicationServiceImpl.OnStartInternal(String[] args) in c:\E14\sources\sources\dev\mrs\src\ServiceHost\ServiceImpl.cs:line 227

Resolution

1. At the command prompt, Type the following:

```
C:\>sc.exe config NetTcpPortSharing start= auto
```

Note:
In the above command, there's a space before `auto`.

2. Start the Microsoft Exchange Mailbox Replication service on at least on Client Access server. For details about how to start the service, see Start, stop, pause, resume, or restart a service.
3. Resume the failed move request. For details, see Complete or Resume a Move Request.

MRSProxy isn't running in the source forest

Problem

When performing remote move requests, the Mailbox Replication Proxy (MRSProxy) service must be running on all Client Access servers in the source forest. By default, MRSProxy is disabled.

Diagnosis

When you attempt to create a move request, you receive an error similar to the following:

```
Service 'net.tcp://bl20102ca002.contoso.com/Microsoft.Exchange.MailboxReplication
    + CategoryInfo          : NotSpecified: (0:Int32) [New-MoveRequest], MailboxR
```

Resolution

1. Start the MRSProxy service on all Client Access servers in the source forest. For details, see Start the MRSProxy Service on a Remote Client Access Server.
2. Resume the failed move request. For details, see Complete or Resume a Move Request.

Move request can't be cleared after it's completed

Problem

The move request completes, but has the status of **Completed With Warning**. You are unable to clear the move request because the Microsoft Exchange Mailbox Replication (MSExchangeMailboxReplication) service couldn't reset the **InTransit** flag from the destination mailbox. If this flag isn't removed, end users won't be able to log on to their mailboxes.

Diagnosis

When you run the Get-MoveRequestStatistics with the *IncludeMoveHistory* parameter, the move report returns an error similar to the following:

```
Failed to reset the destination mailbox after the move.
When you run Test-MAPIConnectivity for this mailbox, it will fail with the follow
Error      : [Microsoft.Exchange.Data.Storage.MailboxInTransitException]: Cannot
```

Resolution

1. Start a new move request for the mailbox. For details, see Create a Local Move Request or Create a Remote Move Request That has Exchange 2010 in Both Forests.
2. Remove the move request as soon as it reaches the status of **In Progress**. For details, see Clear or Remove Move Requests.

1.8.6 Performance Counter Reference for Mailbox Servers

Performance Counter Reference for Mailbox Servers

Exchange Server 2010 > Mailbox >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Ensuring that servers running Microsoft Exchange Server 2010 are operating reliably is a key objective for messaging operations. An important part of Exchange 2010 operations is monitoring the Exchange components to understand the health state of servers and server roles. For more information about mailbox performance counters, see the following topics:

- Mailbox Server Counters
- Performance and Scalability Counters and Thresholds

1.8.7 Error and Event Reference for Mailbox Servers

Error and Event Reference for Mailbox Servers

Exchange Server 2010 > Mailbox >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-01*

Microsoft Exchange Server 2010 Mailbox components, features, and services generate Error events to let you effectively troubleshoot and monitor Mailbox servers.

Event Viewer is a Microsoft Management Console (MMC) snap-in that enables you to browse and manage event logs. You can also gather information about hardware and software problems, and monitor Microsoft Windows security events. Although Event Viewer isn't a Microsoft Exchange component, Event Viewer is useful when you troubleshoot problems with Exchange 2010 server roles. For more information, see Event Viewer. For more information about Exchange 2010 event logs, look for "MSExchange" event logs in the Event Viewer on your Exchange 2010 server.

Mailbox Errors and Events

The following Mailbox errors and events are grouped according to the Mailbox feature areas.

- ADAccess Errors and Events
- ApplicationLogic Errors and Events
- Common Errors and Events
- Control Panel Errors and Events
- ExchangeStoreDB Errors and Events
- MonitoringCorrelation Errors and Events
- MSExchangeAL Errors and Events
- MSExchangeFDS Errors and Events
- MSExchangeIS Errors and Events
- MSExchangeRepl Errors and Events
- MSExchangeRPC Errors and Events
- MSExchangeSA Errors and Events
- MSExchangeSetup Errors and Events
- OAB Maintenance Errors and Events
- Progress Manager Errors and Events
- Search Indexer Errors and Events

1.8.7.1 ADAccess Errors and Events

ADAccess Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-14*

Microsoft Exchange Server 2010 generates MSExchange ADAccess events in Event Viewer so that you can troubleshoot and verify the ADAccessfeatures, and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

ADAccessfeatures Errors and Events

The following table provides a list of the ADAccessfeatures errors and events.

Event ID	Category	Event type	Value or description
MSExchange	Topology	Warning	Process %1 (PID=%

ADAccess 2077			2). Exchange Active Directory Provider could not find any domain controller servers in either the local site '%3' or the following sites: %4
MSExchange ADAccess 2098	General	Warning	Process %1 (PID=%2). DSAccess performed disaster cleanup for the lock %3.
MSExchange ADAccess 2389	LDAP	Warning	Process %1 (PID=%2). A request to Directory Server %3 did not return a result within %4 seconds and is being abandoned. The search will be retried if possible. The search that failed has the following characteristics: Base DN=%5, Filter=%6, Scope=%7.
MSExchange ADAccess 2392	LDAP	Warning	Process %1 (PID=%2). DSAccess did not register an Active Directory shutdown notification with the local server, error 0x%3 (%4). To speed up the shutdown process, manually stop the Exchange services before you shut down the server.
MSExchange ADAccess 2601	General	Warning	Process %1 (PID=%2). When initializing a remote procedure call (RPC) to the Microsoft Exchange Active Directory Topology service, Exchange could not retrieve the SID for account %3 - Error code=%4. The Microsoft Exchange Active Directory Topology service will continue starting with limited permissions.
MSExchange ADAccess 2106	Topology	Warning	Process %1 (PID=%2). Exchange Active

			Directory Provider failed to obtain DNS records for forest %3. DNS Priority and Weight for the Global Catalog servers in this forest will be set to the default values %4 (priority) and %5 (weight).
MSExchange ADAccess 2124	Topology	Warning	Process %1 (PID=%2). Domain controller %3 was not found when DNS was queried for the service location (SRV) resource records for domain %4 The query was for the SRV record for %5 The following domain controllers were identified by the query:%6 Common causes of this error include the following: - The DNS SRV records required to locate a domain controller for the domain are not registered in DNS. These records are registered with a DNS server automatically when a domain controller is added to a domain. They are updated by the domain controller at set intervals. This computer is configured to use DNS servers with following IP addresses:%7 - One or more of the following zones do not include delegation to its child zone:%8 For information about correcting this problem, %9%10
MSExchange ADAccess 2114	Topology	Error	Process %1 (PID=%2). Topology discovery failed, error 0x%3 (%4). Look up the Lightweight

			Directory Access Protocol (LDAP) error code specified in the event description. To do this, use Microsoft Knowledge Base article 218185, "Microsoft LDAP Error Codes." Use the information in that article to learn more about the cause and resolution to this error. Use the Ping or PathPing command-line tools to test network connectivity to local domain controllers.
MSExchange ADAccess 2500	Site Update	Error	Process %1 (PID=%2). The site monitor API could not start - Call=%3 Error code=%4. Try to resolve this event by restarting the computer that is running Exchange. If this event reoccurs, review the Application log and System log for any corresponding Warning or Error events.
MSExchange ADAccess 2089	Configuration	Warning	Process %1 (PID=%2). The configuration domain controller specified in the registry (%3) was not found in the Sites container in the Active Directory. Exchange Active Directory Provider will select the configuration domain controller from the list of available domain controllers.
MSExchange ADAccess 2123	Topology	Warning	Process %1 (PID=%2). Exchange Active Directory Provider is unable to connect to the Domain Controller %3 although its service location (SRV)

			resource record was found in the DNS The query was for the SRV record for %4 The following domain controllers were identified by the query:%5 Common causes of this error include: - Host (A) records that map the name of the domain controller to its IP addresses are missing or contain incorrect addresses. - Domain controllers registered in DNS are not connected to the network or are not running. For information about correcting this problem, %6%7
MSExchange ADAccess 2139	Topology	Error	Process %1 (PID=%2). Active Directory topology could not be discovered in {0} seconds. Review the Application log for related Warning or Error events. Use the Ping or PathPing command-line tools to test network connectivity to local domain controllers. Run the Dcdiag command line tool to test domain controller health.
MSExchange ADAccess 2156	Validation	Error	Process %1 (PID=%2). Recipient object %3 read from %4 failed validation. A data validation exception will be given. Set event logging level for Validation category to Expert to get additional events about each failure.
MSExchange ADAccess 2060	Topology	Warning	Process %1 (PID=%2). No Global Catalog server was found in the local site %3.

			Exchange Active Directory Provider will try to find Global Catalog servers in other sites.
MSExchange ADAccess 2049	LDAP	Warning	Process %1 (PID=%2). An asynchronous LDAP call failed - Server=%3 Error code=%4 (%8). Base DN=%5, Filter=%6, Scope=%7.
MSExchange ADAccess 2118	Topology	Error	Process %1 (PID=%2). Error DNS_ERROR_RCODE_SERVER_FAILURE (0x%3) occurred when DNS was queried for the service location (SRV) resource record used to locate a domain controller for domain %4 The query was for the SRV record for %5 Common causes of this error include the following: - The DNS servers used by this computer contain incorrect root hints. This computer is configured to use DNS servers with following IP addresses:%6 - One or more of the following zones contains incorrect delegation:%7 For information about correcting this problem, %8%9
MSExchange ADAccess 2090	Configuration	Warning	Process %1 (PID=%2). The configuration domain controller specified in the registry (%3) is unreachable. Exchange Active Directory Provider will select the configuration domain controller from the list of available domain controllers.
MSExchange	Topology	Warning	Process %1 (PID=%

ADAccess 2112			2). The Exchange computer %3 does not have Audit Security Privilege on the domain controller %4. This domain controller will not be used by Exchange Active Directory Provider.
MSExchange ADAccess 2138	Configuration	Error	Process %1 (PID=%2). Exchange Active Directory Provider received a request to connection to domain controller %3 but that domain controller is not available. Use the Ping or PathPing command-line tools to test network connectivity to local domain controllers. Run the Dcdiag command line tool to test domain controller health.
MSExchange ADAccess 2053	Cache	Error	Process %1 (PID=%2). Internal error - A hash table that stores DSAccess information is damaged and cannot be used. This event may be caused because of internal memory issues. You may be able to resolve this event by restarting the Microsoft Exchange Active Directory Topology service. If the error persists, restart the Exchange server that logged this event.
MSExchange ADAccess 2137	configuration	Error	Process %1 (PID=%2). Exchange Active Directory Provider could not read attribute %3 from Root DSE of server %4. This issue must be resolved in order to allow Exchange Active

			Directory Provider to correctly operate.
MSExchange ADAccess 2066	LDAP	Warning	Process %1 (PID=%2). An LDAP Notify call failed - Server=%3 Error code=%4 (%8). Base DN=%5, Filter=%6, Scope=%7.
MSExchange ADAccess 2121	Topology	Warning	Process %1 (PID=%2). Exchange Active Directory Provider is unable to connect to any domain controller in domain %3 although DNS was successfully queried for the service location (SRV) resource record used to locate a domain controller for that domain. The query was for the SRV record for %4 The following domain controllers were identified by the query:%5 Common causes of this error include: - Host (A) records that map the name of the domain controller to its IP addresses are missing or contain incorrect addresses. - Domain controllers registered in DNS are not connected to the network or are not running. For information about correcting this problem, %6%7
MSExchange ADAccess 2159	Validation	Error	Process %1 (PID=%2). Configuration object %3 read from %4 failed validation and will be excluded from the result set. Set event logging level for Validation category to Expert to get additional events about each failure.
MSExchange	Cache	Error	Process %1 (PID=%

ADAccess 2054			2). A cache hash table that stores DSAccess information ran out of memory. This event can be caused by internal memory issues. You may be able to resolve this event by restarting the Microsoft Exchange Active Directory Topology service. If the error persists, restart the Exchange server that logged this event.
MSExchange ADAccess 2152	General	Error	Process %1 (PID=%2). An remote procedure call (RPC) request to the Microsoft Exchange Active Directory Topology service failed with error %3 (%4). Make sure that the Remote Procedure Call (RPC) service is running. In addition, make sure that the network ports that are used by RPC are not blocked by a firewall.
MSExchange ADAccess 2130	Topology	Error	Process %1 (PID=%2). Exchange Active Directory Provider could not find an available domain controller in domain %3. This event may be caused by network connectivity issues or configured incorrectly DNS server. This event may also occur if you have not configured correctly your multiple Active Directory sites.
MSExchange ADAccess 2101	topology	Warning	Process %1 (PID=%2). The configuration domain controller specified in a call to SetConfigDCName (%3) is unreachable. Exchange Active

			Directory Provider will select the configuration domain controller from the list of available domain controllers.
MSExchange ADAccess 2100	Topology	Warning	Process %1 (PID=%2). The configuration domain controller specified in a call to SetConfigDCName (%3) was not found in the Sites container in the Active Directory. Exchange Active Directory Provider will select the configuration domain controller from the list of available domain controllers.
MSExchange ADAccess 2600	General	Error	Process %1 (PID=%2). DSAccess could not initiate a remote procedure call (RPC) - Call=%3 Error code=%4.
MSExchange ADAccess 2050	General	Error	Process %1 (PID=%2). The shared memory heap could not be created. This may be caused if physical memory limits have been exceeded. It may also be caused if too many other processes are running DSAccess. You may be able to resolve this error by restarting the Exchange server that logged this event.
MSExchange ADAccess 2069	Topology	Error	Process %1 (PID=%2). Exchange Active Directory Provider couldn't find any Global Catalog servers in either the local site '%3' or the following sites: %4
MSExchange ADAccess 2502	Site Update	Error	Process %1 (PID=%2). The site monitor API could not update the msExchServerSite

			attribute in Active Directory. You must update this attribute to reflect new site name where this Exchange server is installed - Call=%3 Error code=%4.
MSExchange ADAccess 2075	Configuration	Error	Process %1 (PID=%2). DSAccess could not discover the Fully Qualified Domain Name (FQDN) of local server with Exception %3. The local name that was used to look up the server is %4. This event may be caused by an incorrectly configured DNS server. It may also occur if the local server was renamed but DNS records were not updated. To resolve this error, see "Troubleshooting DNS servers" in the Microsoft Windows Server TechCenter. In addition, if the name of the server that logged this event was changed, make sure that the computer was restarted.
MSExchange ADAccess 2091	Configuration	Warning	Process %1 (PID=%2). The domain controller specified in the registry (%3) was not found in the Sites container in Active Directory. Exchange Active Directory Provider will not use this server as a domain controller or global catalog.
MSExchange ADAccess 2104	Topology	Error	Process %1 (PID=%2). Topology discovery failed due to LDAP_SERVER_DOWN error. This event can occur if one or more domain controllers in

			local or all domains become unreachable because of network problems. Use the Ping or PathPing command line tools to test network connectivity to local domain controllers. Run the Dcdiag command line tool to test domain controller health.
MSExchange ADAccess 2086	Topology	Warning	Process %1 (PID=%2). No Domain Controller server was found in the local site %3. Exchange Active Directory Provider will try to find Domain Controller servers in other sites.
MSExchange ADAccess 2155	Validation	Error	Process %1 (PID=%2). Configuration object %3 read from %4 failed validation. DataValidationException will be thrown. Set event logging level for Validation category to Expert to get additional events about each failure.
MSExchange ADAccess 2105	Topology	Warning	Process %1 (PID=%2). Exchange Active Directory Provider failed to obtain DNS records for domain %3. DNS Priority and Weight for the Domain Controllers in this domain will be set to the default values %4 (priority) and %5 (weight).
MSExchange ADAccess 2056	Cache	Error	Process %1 (PID=%2). An internal memory cache error occurred. A record that was not valid was used with the cache hash table. This event can be caused by internal memory issues. You may be able to resolve this

			event by restarting the Microsoft Exchange Active Directory Topology service. If the error persists, restart the Exchange server that logged this event.
MSExchange ADAccess 2107	Topology	Error	Process %1 (PID=%2). Exchange Active Directory Provider failed to obtain an IP address for DS server %3, error %4 (%5). This host will not be used as a DS server by Exchange Active Directory Provider.
MSExchange ADAccess 2119	Topology	Error	Process %1 (PID=%2). Error DNS_ERROR_RCODE_NAME_ERROR (0x%3) occurred when DNS was queried for the service location (SRV) resource record used to locate a domain controller for domain %4 The query was for the SRV record for %5 Common causes of this error include the following: - The DNS SRV records required to locate a domain controller for the domain are not registered in DNS. These records are registered with a DNS server automatically when a domain controller is added to a domain. They are updated by the domain controller at set intervals. This computer is configured to use DNS servers with following IP addresses:%6 - One or more of the following zones do not include delegation to its child zone:%7 For information about correcting this

			problem, %8%9
MSExchange ADAccess 2501	Site update	Error	Process %1 (PID=%2). The site monitor API was unable to verify the site name for this Exchange computer - Call=%3 Error code=%4. Make sure that Exchange server is correctly registered on the DNS server.
MSExchange ADAccess 2076	Configuration	Error	Process %1 (PID=%2). The 'PreloadBaseDNs' and 'PreloadFilters' registry keys do not contain the same number of entries. 'PreloadBaseDNs' contains %3 strings and 'PreloadFilters' contains %4 strings. Only the first %5 preload filters will be used. Each entry in PreloadBaseDNs registry key must match an entry in PreloadFilters registry key. To resolve this error, make sure that number of entries in PreloadBaseDNs registry key equals the number of entries in PreloadFilters registry key.
MSExchange ADAccess 2122	Topology	Error	Process %1 (PID=%2). Error 0x%3 occurred when DNS was queried for the service location (SRV) resource record used to locate a domain controller for domain %4 The query was for the SRV record for %5 For information about correcting this problem, %6%7
MSExchange ADAccess 2110	LDAP	Error	Process %1 (PID=%2). Could not bind to DS server %3, error %4 (%6) at port %5.

MSExchange ADAccess 2067	General	Error	Process %1 (PID=%2). Error %3 occurred, code 0x%4. Callstack 0x%5 0x%6 0x%7 0x%8 0x%9 0x%10 0x%11 0x%12
MSExchange ADAccess 2097	General	Error	Process %1 (PID=%2). The Preload Filters registry key '%3' for the DN '%4' could not be parsed. The error is %5 (%6). This filter will not be used. To resolve this error, make sure that filter specified in PreloadFilters registry key is valid. For more information, see Microsoft Knowledge Base article 250572, "XCON: Preloading and the DSAccess Cache."
MSExchange ADAccess 2160	Validation	Warning	Process %1 (PID=%2). Recipient object %3 read from %4 failed validation and will be excluded from the result set. Set event logging level for Validation category to Expert to get additional events about each failure.
MSExchange ADAccess 2055	Cache	Error	Process %1 (PID=%2). An internal memory cache error occurred. A hash table iterator is no valid. This event can be caused by internal memory issues. You may be able to resolve this event by restarting the Microsoft Exchange Active Directory Topology service. If the error persists, restart the Exchange server that logged this event.
MSExchange ADAccess 2061	LDAP	Warning	Process %1 (PID=%2). An LDAP search call to Directory

			Server %3 failed - Error code=%4 (%8). Base DN=%5, Filter= %6, Scope=%7.
MSExchange ADAccess 2116	Topology	Warning	Process %1 (PID=% 2). The domain controller %3 is running Windows %4 %5. Exchange Active Directory Provider requires that domain controllers are running Windows Server 2003 Service Pack 1 or later versions of Windows.
MSExchange ADAccess 2190	Topology	Error	Process %1 (PID=% 2). Exchange Topology could not be discovered. Reason: %3.
MSExchange ADAccess 2051	General	Error	Process %1 (PID=% 2). The maximum allowed number of processes are using the DSAccess memory cache. No more processes can use the API. Try to resolve this event by restarting the Microsoft Exchange Active Directory Topology service. If the error persists, restart the Exchange server that logged this event.
MSExchange ADAccess 2120	Topology	Warning	Process %1 (PID=% 2). Error ERROR_TIMEOUT (0x %3) occurred when DNS was queried for the service location (SRV) resource record used to locate a domain controller for domain %4 The query was for the SRV record for %5. The DNS servers used by this computer for name resolution are not responding. This computer is configured to use DNS

			servers with the following IP addresses:%6. Verify that this computer is connected to the network, that these are the correct DNS server IP addresses, and that at least one of the DNS servers is running. For information about correcting this problem, %7%8
MSExchange ADAccess 2058	Cache	Information	Process %1 (PID=%2). The specified record key does not exist in the cache hash table.
MSExchange ADAccess 2059	Cache	Warning	Process %1 (PID=%2). The last record in the cache hash table was found.
MSExchange ADAccess 2068	General	Information	Process %1 (PID=%2). DSAccess initialized successfully.
MSExchange ADAccess 2070	Topology	Information	Process %1 (PID=%2). Exchange Active Directory Provider lost contact with domain controller %3. Error was 0x%4 (%6) (%5). Exchange Active Directory Provider will attempt to reconnect with this domain controller when it is reachable.
MSExchange ADAccess 2074	LDAP	Information	Process %1 (PID=%2). A search or read to Directory Server %3 returned object '%4' which has attribute '%5' with too many values to return in a single search. If possible, reduce the number of values in this attribute to allow normal operation.
MSExchange ADAccess 2078	General	Information	Process %1 (PID=%2). DSAccess is shutting down.

MSExchange ADAccess 2081	Topology	Information	Process %1 (PID=%2). Exchange Active Directory Provider will use the servers from the following list: Domain Controllers:%3 Global Catalogs:%4 The Configuration Domain Controller is set to %5.
MSExchange ADAccess 2082	Topology	Information	Process %1 (PID=%2). Exchange Active Directory Provider has detected that the following Domain Controller servers in the local site '%3' became reachable and is using them: %4
MSExchange ADAccess 2083	Topology	Information	Process %1 (PID=%2). Exchange Active Directory Provider has detected that the following Global Catalog servers in the local site '%3' became reachable and is using them: %4
MSExchange ADAccess 2084	Topology	Warning	Process %1 (PID=%2). No Domain Controller server is up in the local site '%3'. Exchange Active Directory Provider will use the following out of site Domain Controller servers: %4
MSExchange ADAccess 2085	Topology	Information	Process %1 (PID=%2). No Global Catalog server is up in the local site '%3'. Exchange Active Directory Provider will use the following out of site global catalog servers: %4
MSExchange ADAccess 2088	Configuration	Information	Process %1 (PID=%2). The value of %3 specified in the registry must be in the range of %4 - %5, and it was %6. Using the default

			value of %7.
MSExchange ADAccess 2092	Configuration	Information	Process %1 (PID=%2). Exchange Active Directory Provider will use Domain Controllers specified in the registry.
MSExchange ADAccess 2094	Configuration	Information	Process %1 (PID=%2). Registry key 'SYSTEM \CurrentControlSet \Services \MSExchange ADAccess\Diagnostics' is missing. Exchange Active Directory Provider cannot get a list of event log categories. Only events of level 'None' will be logged.
MSExchange ADAccess 2095	Topology	Information	Process %1 (PID=%2). The Configuration Domain Controller has been changed from %3 to %4.
MSExchange ADAccess 2096	Configuration	Information	Process %1 (PID=%2). Exchange Active Directory Provider will use the Configuration Domain Controller (%3) specified in the registry.
MSExchange ADAccess 2102	Topology	Error	Process %1 (PID=%2). All Domain Controller Servers in use are not responding: %3
MSExchange ADAccess 2103	Topology	Warning	Process %1 (PID=%2). All Global Catalog Servers in forest %3 are not responding: %4
MSExchange ADAccess 2093	Configuration	Information	Process %1 (PID=%2). Exchange Active Directory Provider will use Global Catalogs specified in the registry.
MSExchange ADAccess 2099	Topology	Information	Process %1 (PID=%2). Exchange Active Directory Provider will

			use the Configuration Domain Controller (%3) specified in a call to SetConfigDCName.
MSExchange ADAccess 2111	LDAP	Error	Process %1 (PID=%2). Received LDAP error 0x%3 (%5) from Directory Server %4 due to Kerberos ticket timeout.
MSExchange ADAccess 2113	Topology	Information	Process %1 (PID=%2). Exchange Server %3 now has Audit Security Privilege on Domain Controller %4.
MSExchange ADAccess 2115	LDAP	Error	Process %1 (PID=%2). Exchange Active Directory Provider needs to close a connection to the Domain Controller %3 due to error 0x%4 (%5).
MSExchange ADAccess 2117	General	Information	Process %1 (PID=%2). Impersonated account %3 is calling into Exchange Active Directory Provider with the following callstack: %4 %5 %6 %7 %8 %9 %10 %11
MSExchange ADAccess 2125	Cache	Warning	Process %1 (PID=%2). An attribute on object %3 is too large to be cached. Requested size was %4, maximum cacheable is %5. Performance may be degraded.
MSExchange ADAccess 2127	Topology	Information	Process %1 (PID=%2). Exchange Active Directory Provider detected that Active Directory server %3 is reachable again via port %4.
MSExchange ADAccess 2128	Configuration	Information	Process %1 (PID=%2). Object %3 was not found on the Domain Controller %4. This may indicate a

			replication or permission issue.
MSExchange ADAccess 2129	Topology	Information	Process %1 (PID=%2). Exchange Active Directory Provider needs a Domain Controller in domain %3. Found server %4.
MSExchange ADAccess 2131	LDAP	Information	Process %1 (PID=%2). Opening new connection to server %3 at port %4. Connection pool: %5.
MSExchange ADAccess 2132	LDAP	Information	Process %1 (PID=%2). Closing connection to the server %3 at port %4.
MSExchange ADAccess 2133	LDAP	Warning	Process %1 (PID=%2). An LDAP %3 operation succeeded but took %4 milliseconds - Server=%5. Base DN=%6, Filter=%7, Scope=%8.
MSExchange ADAccess 2134	LDAP	Information	Process %1 (PID=%2). Exchange Active Directory Provider received change notification for '%3'.
MSExchange ADAccess 2136	Configuration	Information	Process %1 (PID=%2). Exchange Active Directory Provider found multiple records for %3. Locate and fix the affected recipients to resume mail flow.
MSExchange ADAccess 2141	General	Information	Process %1 (PID=%2). Process preferred topology changed. Preferred Domain Controllers: %3 Preferred Global Catalog: %4 Preferred Configuration Domain Controller: %5
MSExchange ADAccess 2142	Topology	Error	Process %1 (PID=%2). Topology discovery failed, error

			0x%3.
MSExchange ADAccess 2143	Topology	Warning	Process %1 (PID=%2). Error occurred when getting server from domain Distinguished Name: %3. ADAM topology provider is not available. Please make sure Microsoft Exchange ADAM service is started.
MSExchange ADAccess 2150	Topology	Information	Process %1 (PID=%2). The following Active Directory servers are going to be used in connection pools of this process: Domain Controllers: %3 Global Catalogs: %4 Configuration Domain Controller: %5. Topology Version %6, Topology provider: %7.
MSExchange ADAccess 2151	General	Information	Process %1 (PID=%2). Microsoft.Exchange.Data.Directory.dll is loaded successfully.
MSExchange ADAccess 2154	LDAP	Information	Process %1 (PID=%2). Attribute %3 of '%4' had %5 values and required ranged read operations on Directory Server %6.
MSExchange ADAccess 2157	Validation	Warning	Process %1 (PID=%2). Configuration object %3 read from %4 failed validation. A partially valid object will be returned. Set the event logging level for Validation category to Expert to get additional events about each failure.
MSExchange ADAccess 2158	Validation	Information	Process %1 (PID=%2). Recipient object %3 read from %4 failed validation. A partially valid object will be returned. Set event logging level for

			Validation category to Expert to get additional events about each failure.
MSExchange ADAccess 2191	Exchange Topology	Information	Process %1 (PID=%2). Two servers with the same fully qualified domain name have been detected. Only %3 will be considered and %4 will be ignored.
MSExchange ADAccess 2390	LDAP	Information	Process %1 (PID=%2). DSAccess registered an Active Directory shutdown notification on the local server.
MSExchange ADAccess 2393	LDAP	Information	Process %1 (PID=%2). DSAccess failed to register an Active Directory shutdown notification with the local server because the local server does not support shutdown notifications. To expedite the shutdown process, manually shut down Exchange services before shutting down the server.
MSExchange ADAccess 2394	LDAP	Error	Process %1 (PID=%2). An LDAP search call returned a referral - Server=%3 Error code=%4 (%8). Base DN=%5, Filter=%6, Scope=%7.
MSExchange ADAccess 2402	Exchange Topology	Information	Process %1 (PID=%2). Server %3 is not assigned to any site. This can be caused by incorrect configuration of subnets or sites or by replication latency. Server will not be used.
MSExchange ADAccess 2452	General	Information	Process %1 (PID=%2). Impersonated account %3 is calling

			into Exchange Active Directory Provider and allowed.
MSExchange ADAccess 2453	General	Information	Process %1 (PID=%2). Function %3 failed indicating that the remote procedure call (RPC) server is temporarily unavailable - Error code=%4.
MSExchange ADAccess 2503	Site update	Information	Process %1 (PID=%2). Site monitor updated msExchServerSite in Active Directory. New site: %3 Old site: %4
MSExchange ADAccess 2602	General	Error	Process %1 (PID=%2). Failed to flush Kerberos ticket for local system account - Error code=%3. Microsoft Exchange Active Directory Topology service could not update token to have Exchange Servers group membership (SID: %4). This may be caused by replication latency. Wait for replication to complete and try again.
MSExchange ADAccess 2800	General	Information	Process %1 (PID=%2). The Microsoft Exchange Active Directory Topology Service has started successfully.
MSExchange ADAccess 2801	General	Information	Process %1 (PID=%2). The Microsoft Exchange Active Directory Topology Service has stopped successfully.
MSExchange ADAccess 2802	Topology	Information	Process %1 (PID=%2). %3 is a read-only domain controller. Exchange Active Directory Provider requires that domain controllers are not

			read-only.
MSExchange ADAccess 2901	General	Information	Process %1 (PID=%2). Default throttling policy for organization '%3' is missing.
MSExchange ADAccess 2902	General	Information	Process %1 (PID=%2). Multiple default throttling policies found for organization '%3'.
MSExchange ADAccess 2903	General	Information	Process %1 (PID=%2). Unable to initialize throttling performance counters. The exception was: '%3'
MSExchange ADAccess 2904	General	Information	Process %1 (PID=%2). Failed to read throttling policy with ID '%3'. The exception was: '%4'
MSExchange ADAccess 2905	General	Information	Process %1 (PID=%2). Dynamic distribution group %3 read from %4 is not valid.%5.
MSExchange ADAccess 2913	General	Information	Process %1 (PID=%2). Coudn't find a global address list for user '%3' (SID='%4')
MSExchange ADAccess 2914	General	Information	Process %1 (PID=%2). Deleted throttling policy was referenced. Id: '%3'.
MSExchange ADAccess 2920	General	Information	Process %1 (PID=%2). Component: %3. Unable to initialize resource health performance counters. Exception: '%4'
MSExchange ADAccess 2927	General	Information	Process %1 (PID=%2).The concurrency controller for resource '%3' detected that a thread stayed in the overflow queue for more than %4 milliseconds, which is a warning that the resource might be unhealthy.

MSExchange ADAccess 2929	General	Information	Process %1 (PID=%2).The concurrency controller for resource '%3' detected that the overflow queue has reached its warning limit of %4.
MSExchange ADAccess 2934	General	Information	Process %1 (PID=%2). The recipient full sync page token for tenant '%3' has been cleared from storage.
MSExchange ADAccess 2935	General	Information	Process %1 (PID=%2) Component %3. Encountered a timeout while trying to access remote performance counter '%4'. Remote server might be unresponsive.
MSExchange ADAccess 2936	General	Information	Process %1 (PID=%2) Component %3. Encountered an exception while trying to read remote performance counter '%4'. Exception: '%5'.
MSExchange ADAccess 2937	Validation	Information	Process %1 (PID=%2). Object [%3]. Property [%4] is set to value [%5], it is pointing to the Deleted Objects container in Active Directory. This property should be fixed as soon as possible.
MSExchange ADAccess 2938	General	Information	Process %1 (PID=%2).The Concurrency controller detected that Resource '%3' reached its concurrency limit and therefore the resource is set to unhealthy
MSExchange ADAccess 2939	General	Information	Process %1 (PID=%2). Unable to find UM Allowed CountryList. Id: '%3'.

1.8.7.2 ApplicationLogic Errors and Events

ApplicationLogic Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Application Logic events in Event Viewer so that you can troubleshoot and verify the MSExchangeApplicationLogic features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

MSExchangeApplicationLogic Errors and Events

The following table provides a list of the Application Logic errors and events.

Event ID	Category	Event type	Value or description
MSExchangeApplicationLogic 1002	TextMessaging	Error	Process %1 (ID %2) failed to load text messaging hosting data file %3. Failure details: %4
MSExchangeApplicationLogic 1003	TextMessaging	Information	Process %1 (ID %2) successfully loaded the text messaging hosting data files.

1.8.7.3 Common Errors and Events

Common Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Exchange Common errors and events in Event Viewer so that you can troubleshoot and verify the Common features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Common Errors and Events

The following table provides a list of the Common errors and events.

Event ID	Category	Event type	Value or description
MSExchange Common 205	General	Error	No DNS servers could be retrieved from network adapter %1. Check if the computer is connected to a network and Get-NetworkConnectionInfo returns any results.
MSExchange Common 579	General	Error	Removal of privileges from process "%1" (PID=%2, LABEL=%3) failed with error code %4.
MSExchange Common 6003	Logging	Error	%1: Failed to create the log directory: %2 because of the error: %3. Logs will not be generated until the problem is corrected.
MSExchange Common 6004	Logging	Error	%1: Failed to write logs because of the error: %2.

1.8.7.4 Control Panel Errors and Events

Control Panel Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-14*

Microsoft Exchange Server 2010 generates MSExchange Control Panel events in Event Viewer so that you can troubleshoot and verify the Exchange Control Panel features and services. Event Viewer tracks the following kinds of events in the given order based on importance:

- Error events
- Warning events
- Informational events

MSExchange Control Panel Errors and Events

The following table provides a list of the MSExchange Control Panel errors and events.

Event ID	Category	Event type	Value or description
MSExchange Control Panel 20	General	Error	The Web management interface couldn't find a mailbox for user '%

			1' and will let the user continue to site '%2'. This is expected for objects of type MailUser.
MSExchange Control Panel 30	Proxy	Error	Current User: '% 1'Client Access server "%2" tried to proxy Web management traffic to Client Access server "%3" and received the following error for "%4":%5
MSExchange Control Panel 26	Proxy	Error	Current User: '% 1'Client Access server "%2" tried to proxy Web management traffic to Client Access server "%3". This failed because the Outlook Web App registry key "AllowInternalUntrustedCerts" is set to "0", but no certificate trusted by "%2" was available for the Secure Sockets Layer (SSL) encryption of the proxy connection.
MSExchange Control Panel 28	Proxy	Error	Current User: '% 1'Client Access server "%2" tried to proxy Web management traffic to Client Access server "%3". This failed because one of the following configuration problems was encountered:1. "%3" has been set to use "http://" (not using SSL) instead of "https://" (using SSL). You can modify this by setting the InternalUrl parameter of the Web management virtual directory that this proxy traffic is going to. You can set that parameter using the Set-EcpVirtualDirectory cmdlet in the

			Exchange Management Shell.2. The destination virtual directory returned an HTTP 403 error code. This usually means it's not configured to accept SSL access. You can change this configuration by using Internet Services Manager on the Client Access server "%3".If you don't want this proxy connection to use SSL, set the registry key "AllowProxyingWithoutSSL" on this Client Access server and set the InternalUrl and SSL settings for the Web management virtual directory that this proxy traffic is going to accordingly.
MSExchange Control Panel 4	General	Warning	Current user: '%1'Request for URL '%2' failed with the following error:%3
MSExchange Control Panel 19	Redirect	Error	The Web management interface couldn't redirect user '%1' from site '%2' to site '%3' and will let the user continue to the original site. The possible causes are: There are no Client Access servers on the destination site with major version equal to '%4' or the Client Access server doesn't have an external URL.
MSExchange Control Panel 5	General	Warning	Current user: '%1'Web service call '%2' failed with the following error:%3
MSExchange Control Panel 31	General	Error	Can't determine if the current user "%1" is enabled for the RBAC role "%2". Error: "%3"

MSExchange Control Panel 27	Proxy	Error	Current User: '%1'Client Access server "%2" tried to proxy Web management traffic to Client Access server "%3". This failed because "%3" couldn't verify that the Active Directory account "%2" used to authenticate has the necessary access rights to send Web management proxy traffic. Verify in the IIS Manager that Windows Authentication is enabled in the internal 'ECP' virtual directory and that 'Get-EcpVirtualDirectory' reports 'WindowsAuthentication' as 'True' in the internal server '%3'.
MSExchange Control Panel 29	Proxy	Error	Current User: '%1'Client Access server "%2" tried to proxy Web management traffic to Client Access server "%3" but the target service wasn't available. Verify that "%2" has network connectivity with "%3", "%3" has the HTTP driver, the IIS service and IIS sites started, the "MSExchangeECPAppPool" is running, and firewall settings aren't blocking Web traffic.

1.8.7.5 ExchangeStoreDB Errors and Events

ExchangeStoreDB Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-08-10*

Microsoft Exchange Server 2010 generates ExchangeStoreDB events in Event Viewer so that you can troubleshoot and verify the ExchangeStoreDB features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

ExchangeStoreDB Errors and Events

The following table provides a list of the ExchangeStoreDB error and events.

Event ID	Category	Event type	Value or description
ExchangeStoreDB 230	Database recovery	Error	At '%8' the copy of database '%1' on this server encountered a serious I/O error that may have affected all copies of the database. The error returned by Suspend-MailboxDatabaseCopy was '%7'. Consult the event log on the server for other "ExchangeStoreDb" or "msexchangerepl" events for more specific information about the failure. All data should be immediately moved out of this database.
ExchangeStoreDB 129	Database recovery	Warning	At '%8' the Exchange store database '%1' copy on this server encountered an error. For more detail about this failure, consult the Event log on the server for other "ExchangeStoreDb" or "msexchangerepl" events. Page patching was initiated to restore the page.
ExchangeStoreDB 134	Database recovery	Error	At '%8' the Microsoft Exchange Information Store Database '%1' copy on this server encountered a serious I/O error. A

			lost write was detected. Page patching was initiated to restore the page. Consult the event log on the server for other "ExchangeStoreDb" or "msexchangerepl" events for more specific information about the failure.
ExchangeStoreDB 130	Database recovery	Warning	At '%8', the copy of database '%1' on this server encountered an error that it was able to repair. For specific information that may help identify the failure, consult the Event log on the server for other "ExchangeStoreDb" or "MSExchangeRepl" events. The Microsoft Exchange Replication service will automatically attempt to retry the operation.
ExchangeStoreDB 137	Database recovery	Error	At '%8' the copy of database '%1' on this server encountered a serious I/O error that may have affected all copies of the database. Consult the event log on the server for other "ExchangeStoreDb" or "msexchangerepl" events for more specific information about the failure. All data should be immediately moved out of this database. The passive database copy has been suspended.
ExchangeStoreDB 219	Database recovery	Warning	At '%8' database copy '%1' on this server appears to have a greater load than it can support.To help identify the

			specific issue, consult the Event log on the server for other storage and "ExchangeStoreDb" events. Service recovery was not attempted.
ExchangeStoreDB 119	Database recovery	Warning	At '%8' database copy '%1' on this server appears to have a greater load than it can support. Consult the Event log on the server for other storage and "ExchangeStoreDb" events that may identify the specific issue. Recovery was not attempted.
ExchangeStoreDB 123	Database recovery	Error	At '%8' the Microsoft Exchange Information Store Database '%1' copy on this server experienced a corrupted search catalog. Consult the event log on the server for other "ExchangeStoreDb" and "MSExchange Search Indexer" events for more specific information about the failure. Reseeding the catalog is recommended via the 'Update-MailboxDatabaseCopy' task.
ExchangeStoreDB 136	Database recovery	Error	At '%8' the copy of database '%1' on this server encountered a serious I/O error that may have affected all copies of the database. Consult the event log on the server for other "ExchangeStoreDb" or "msexchangerepl" events for more specific information about the failure. All

			data should be immediately moved out of this database.

1.8.7.6 MonitoringCorrelation Errors and Events

MonitoringCorrelation Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Monitoring Correlation events in Event Viewer so that you can troubleshoot and verify the MonitoringCorrelation features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

MonitoringCorrelation Errors and Events

The following table provides a list of the Monitoring Correlation errors and events.

Event ID	Category	Event type	Value or description
MSExchangeMonitoringCorrelation 713	General	Error	%1
MSExchangeMonitoringCorrelation 714	General	Error	%1
MSExchangeMonitoringCorrelation 715	General	Warning	%1
MSExchangeMonitoringCorrelation 717	General	Warning	%1
MSExchangeMonitoringCorrelation 718	General	Warning	%1
MSExchangeMonitoringCorrelation 719	General	Warning	%1
MSExchangeMonitoringCorrelation 716	General	Warning	%1

1.8.7.7 MSExchangeAL Errors and Events

MSExchangeAL Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Exchange Address List events in Event Viewer so that you can troubleshoot and verify the Address List Service features and services. Event Viewer tracks the following kinds of events in the given order based on importance:

- Error events
- Warning events
- Informational events

MSExchangeAL Errors and Events

The following table provides a list of the MSExchangeAL errors and events.

Event ID	Category	Event type	Value or description
MSExchangeAL 8363	Error	Error	Microsoft Exchange failed to initialize Directory Service Access (DSAccess) with error 0x%1. Proxy address calculation services will not be available on the local Exchange server. %2
MSExchangeAL 8325	Error	Error	The service can't work properly because Email Address Policy '%1' has an invalid filter rule (PurportedSearch). The error is '%2'. Use the Exchange Management Console to correct this problem. New users, contacts, and groups won't be fully provisioned until this is fixed. %3
MSExchangeAL 8326	Error	Error	The address list '%1' has an invalid filter rule (PurportedSearch). The error is '%2'. No directory entries will belong to this address list until you correct this problem in the Exchange Management

			Console. %3
MSExchangeAL 8229	Error	Error	Unsupported or unloadable policy group: '%1'. %2
MSExchangeAL 8358	Error	Error	Microsoft Exchange couldn't read the registry key '%1' under 'HKLM\%2' because the value is not a DWORD.
MSExchangeAL 8364	Error	Error	Directory Service Access (DSAccess) failed to provide a domain controller to use to read configuration with error 0x%1. Proxy address calculation services will not be available on the local Exchange server. %2
MSExchangeAL 8213	Error	Error	Couldn't find an accessible writable domain controller for domain '%1'. %2
MSExchangeAL 8142	Error	Error	The service threw an unexpected exception.
MSExchangeAL 8115	Error	Error	The Win32 API call '%1' returned an error. The service could not be initialized. Make sure that the operating system was installed properly.
MSExchangeAL 8331	Error	Error	The service threw an unexpected exception which was caught at %1(%2)
MSExchangeAL 8252	Error	Error	Could not search under entry '%1' on directory %2. Cannot access Address List information. %3
MSExchangeAL 8359	Error	Error	The Recipient Update Service is slow to start because of network issues. The service will continue to retry until it successfully restarts. Until that time, not all

			Recipient Update Service features will be available.
MSExchangeAL 8114	Error	Error	The service could not be initialized because the necessary entry point '%1' could not be found in the file %2. Make sure that the operating system was installed properly.
MSExchangeAL 8063	Error	Error	Could not read the root entry on directory '%1'. Cannot access configuration information. %2
MSExchangeAL 8357	Error	Error	The search '%1' under entry '%2' failed with error code '%3'. Microsoft Exchange cannot access schema information. %4
MSExchangeAL 8362	Error	Error	Microsoft Exchange couldn't read the forest GUID from %1. Proxy address calculation services will not be available on the local Exchange server. %2
MSExchangeAL 8260	Error	Error	Could not open LDAP session to directory '%1' using local service credentials. Cannot access Address List configuration information. Make sure the server '%1' is running. %2
MSExchangeAL 8284	Error	Error	The Recipient Update Service could not find the Address List Root which is located in the Exchange Service entry under the attribute addressBookRoots. This might have been caused by a permissions problem. %1

MSExchangeAL 8144	Error	Error	The service threw an out of memory exception.

1.8.7.8 MSExchangeFDS Errors and Events

MSExchangeFDS Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Microsoft Exchange File Distribution service events in Event Viewer so that you can troubleshoot and verify the Microsoft Exchange File Distribution features and services. Event Viewer tracks the following kinds of events in the given order based on importance:

- Error events
- Warning events
- Informational events

Microsoft Exchange File Distribution Errors and Events

The following table provides a list of the Microsoft Exchange File Distribution errors and events.

Event ID	Category	Event type	Value or description
MSExchangeFDS 1007	General	Error	Process %1 (PID=%2). Unhandled exception occurred in worker thread %3. Exception message: %4 Current synchronization task is aborted.
MSExchangeFDS 1018	General	Warning	Process %1 (PID=%2). Failed to connect to remote server %3. The remote server may be down, or its Server service may not be running.
MSExchangeFDS 1001	FileReplication	Error	Process %1 (PID=%2). Manifest file %3 for Offline Address Book file set %4 is corrupted. Quitting current file synchronization operation.

MSExchangeFDS 1012	General	Warning	Process %1 (PID=%2). Active Directory contains invalid value for PollInterval attribute of OAB Virtual Directory object. The valid value range is 0-71582. The upper range limit value is used instead.
MSExchangeFDS 1017	General	Error	Process %1 (PID=%2). %3
MSExchangeFDS 1020	General	Error	Process %1 (PID=%2). Failed to copy file %3 to directory %4, the error: %5.
MSExchangeFDS 1016	General	Error	Process %1 (PID=%2). %3
MSExchangeFDS 1014	General	Error	Process %1 (PID=%2). Failed to read from metabase. Metabase object %3 can not be found. OAB synchronization suspended.
MSExchangeFDS 1005	FileReplication	Warning	Process %1 (PID=%2). %3 operation has failed for %4. Exception message: %5 Current file synchronization operation has ended
MSExchangeFDS 1010	FileReplication	Warning	Process %1 (PID=%2). Failed to read security descriptor from Active Directory for Offline Address Book %3. Synchronization task for this object is aborted.
MSExchangeFDS 1003	General	Warning	Process %1 (PID=%2). Temporarily unable to read configuration data for object %3 (%4). Will wait for %5 seconds and retry.
MSExchangeFDS 1021	General	Information	Process %1 (PID=%2). Could not find directory %3. This is

			normal if it has never been generated. Otherwise, make sure this directory and share has read permission for "Exchange Servers" group.
MSExchangeFDS 1002	General	Warning	Process %1 (PID=%2). Manifest file %3 for dial plan %4 is corrupted. The current file synchronization operation will be aborted.
MSExchangeFDS 1011	General	Warning	Process %1 (PID=%2). Active Directory contains invalid configuration object, validation error is "%3". Will wait for %4 seconds and retry.
MSExchangeFDS 1022	General	Information	Process %1 (PID=%2). Could not find file %3. This is normal if it has never been generated. Otherwise, make sure this file has read permission for "Exchange Servers" group.
MSExchangeFDS 1015	General	Error	Process %1 (PID=%2). Failed to read property %3 from metabase object %4. OAB synchronization suspended.
MSExchangeFDS 1019	General	Error	Process %1 (PID=%2). Failed to copy file %3 to directory %4, destination directory does not exist.
MSExchangeFDS 1013	General	Error	Process %1 (PID=%2). Remote file %3 not found. Current synchronization task aborted.
MSExchangeFDS 1006	FileReplication	Warning	Process %1 (PID=%2). %3 operation has failed for %4 to %5. Exception message:

			%6 Current file synchronization operation has ended.

1.8.7.9 MSExchangeIS Errors and Events

MSExchangeIS Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-14*

Microsoft Exchange Server 2010 generates Exchange Information Store events in Event Viewer so that you can troubleshoot and verify the MSExchangeIS features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

MSExchangeIS Errors and Events

The following table provides a list of Exchange Information Store errors and events.

Event ID	Category	Event type	Value or description
MSExchangeIS 10023	Error	Error	The mailbox for %1 (GUID %2) has exceeded the maximum Recoverable Items Quota. Items cannot be deleted from this mailbox. The mailbox owner should be notified about the condition of the mailbox as soon as possible. Please remove items from Recoverable Items or increase the Recoverable Items Quota to restore functionality.
MSExchangeIS 9506	Error	Error	Out of memory
MSExchangeIS 9693	Error	Error	Failed to create a new named property for database "%1" because the number of named properties reached the quota limit for MAPI protocol (%2). User

			attempting to create the named property: "%3" Named property GUID: %4 Named property name/id: "%5"
MSExchangeIS 1088	Error	Error	The database could not be started because the distinguished name (DN) %2 of mailbox database "%3" does not match the DN of directory %1. The database may have been restored to a computer that is in an organization or site different from the original database.
MSExchangeIS 5000	Error	Error	Unable to initialize the Microsoft Exchange Information Store service. %1 - Error %2.
MSExchangeIS 9667	Error	Error	Failed to create a new named property for database "%1" because the number of named properties reached the quota limit (%2). User attempting to create the named property: "%3" Named property GUID: %4 Named property name/id: "%5"
MSExchangeIS 9643	Information	Information	Process termination function %1 was called by a function in module %2; some parameters and their values were %3. A significant section of the call stack is in the data section.
MSExchangeIS 9786	Warning	Warning	The database engine has consumed %1% of the "%2" resource (%3 used out of a maximum of %4) for database '%5'.
MSExchangeIS 9673	Error	Error	An exception with

			code %1 was thrown in module %2; some parameters and their values were %3. A significant section of the call stack is in the data section.
MSExchangeIS 9691	Error	Error	Status %1 registering RPC protocol "%2" endpoint="%3". This may be expected, depending on the machine configuration.
MSExchangeIS 1121	Error	Error	Error %1 connecting to Active Directory.
MSExchangeIS 1184	Error	Error	Cannot start the Microsoft Exchange Information Store. Error retrieving local host information. Please make sure that your server's TCP/IP networking software is properly configured.
MSExchangeIS 5003	Error	Error	Unable to initialize the Information Store service because the clocks on the client and server are skewed. This may be caused by a time change either in the client or the server, and may require a reboot of that computer. Verify that your domain is properly configured and is currently online.
MSExchangeIS 9509	Error	Error	Out of file handles
MSExchangeIS 9688	Error	Error	Exchange store '%1': The logical size of this database (the logical size equals the physical size of the .edb file minus the logical free space) is %2 GB. This database size is approaching the size limit of %3 GB. If the logical

			database size exceeds the maximum size limit, it will be dismounted on a regular basis.
MSExchangeIS 9659	Error	Error	The Microsoft Exchange Information Store encountered an unexpected exception %1 at address %2 while processing a request for user %3.
MSExchangeIS 10024	Error	Error	The mailbox for %1 (GUID %2) has exceeded the Recoverable Items Warning Quota. Please remove items from Recoverable Items or increase the Recoverable Items Warning Quota and Recoverable Items Quota. If the Recoverable Items Quota is exceeded, the user will be unable to delete items from the mailbox.
MSExchangeIS 5002	Error	Error	Unable to initialize the Microsoft Exchange Information Store service. Out of memory.

1.8.7.10 MSExchangeRepl Errors and Events

MSExchangeRepl Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Replication service errors and events in Event Viewer so that you can troubleshoot and verify the Exchange Replication service features and services. Event Viewer tracks the following kinds of events in the given order, based

on importance:

- Error events
- Warning events
- Informational events

MSExchangeRepl Errors and Events

The following table provides a list of Exchange Replication service errors and events.

Event ID	Category	Event type	Value or description
MSExchangeRepl 4038	Service	Warning	The Cluster service health check failed.%nMailbox server: %1%nError: %2
MSExchangeRepl 2120	Service	Warning	The Microsoft Exchange Replication service failed to start the HTTP listener. The error was %1
MSExchangeRepl 2017	Exchange VSS Writer	Error	The Microsoft Exchange Replication service VSS Writer initialization failed with error %1. The Exchange VSS Writer is not loaded.
MSExchangeRepl 2092	Action	Error	Database: %1%nMailbox server: %2%n%nDatabase %1 won't be mounted because the number of lost logs was greater than the amount specified by the AutoDatabaseMountDial.%n* The log file generated before the switchover or failover was: %3%n* The log file successfully replicated to this server was: %4%n* AutoDatabaseMountDial is set to: %5%n%nAttempts to copy the log files from the source server were unsuccessful. Error: %6
MSExchangeRepl 3175	Service	Warning	The Microsoft Exchange Replication service failed to start the Active Manager RPC server.

MSExchangeRepl 2069	Service	Error	The Microsoft Exchange Replication service is unable to remove log file %2 for %1 because the file is in use or because of insufficient permissions. The database copy status will be set to Failed. Error: %3
MSExchangeRepl 4040	Service	Warning	Active Manager health check failed.% nMailbox server: % 1%nMessage: %2
MSExchangeRepl 4108	Service	Warning	The Microsoft Exchange Replication service failed to clean up file '%2', which was used for an incremental reseed of database '%1'. Error: %3
MSExchangeRepl 4044	Service	Information	Database availability group members up health check failed.% nMailbox server: % 1%nMessage: %2
MSExchangeRepl 2055	Service	Error	The Microsoft Exchange Replication service failed to create a temporary log file for %1 when %2. Service recovery was not attempted.
MSExchangeRepl 4109	Service	Warning	The Microsoft Exchange Replication service failed to clean up files under '%1' for database '%2'. Error: %3
MSExchangeRepl 4051	Service	Error	Quorum group health check failed.% nMailbox server: % 1%nMessage: %2
MSExchangeRepl 2135	Service	Error	The Microsoft Exchange Replication service failed to start the Tasks RPC server. This may be due to insufficient permissions in Active Directory.

MSExchangeRepl 4046	Service	Error	Database availability group network health check failed.% nNetwork: %1% nError: %2
MSExchangeRepl 4049	Service	Warning	File share quorum health check failed.% nMailbox server: % 1%nMessage: %2
MSExchangeRepl 4053	Service	Warning	The Tasks RPC listener health check failed.%nMailbox server: %1% nMessage: %2
MSExchangeRepl 4055	Service	Warning	HttpListener health check has failed.% nMailbox Server: % 1%nSpecific Message: %2
MSExchangeRepl 2001	Service	Warning	The Microsoft Exchange Replication service has started.

1.8.7.11 MSExchangeRPC Errors and Events

MSExchangeRPC Errors and Events

Exchange Server 2010 > Mailbox > Error and Event Reference for Mailbox Servers >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Exchange RPC events in Event Viewer so that you can troubleshoot and verify the Exchange RPC features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Exchange RPC Errors and Events

The following table provides a list of MSExchangeRPC errors and events.

Event ID	Category	Event type	Value or description
MSExchangeRPC 1000	General	Information	The Microsoft Exchange RPC service

			has started successfully and is now ready to accept logons to private mailboxes.
MSExchangeRPC 1006	General	Information	Starting MSExchangeRPC service. Process ID %1. %2 %3.
MSExchangeRPC 1020	General	Information	The Microsoft Exchange RPC service has started successfully and is now ready to accept sign-ins to public folders.

1.8.7.12 MSExchangeSA Errors and Events

MSExchangeSA Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-14*

Microsoft Exchange Server 2010 generates Exchange System Attendant service events in Event Viewer so that you can troubleshoot and verify the System Attendant features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Exchange System Attendant Errors and Events

The following table provides a list of MSExchangeSA errors and events.

Event ID	Category	Event type	Value or description
MSExchangeSA 9371	Error	Error	OABGen encountered an error while generating the differential downloads of address list '%1'. The offline address book has not been updated so clients will not be able to download the current set of changes. Check other logged events

			to find the cause of this error. - %2
MSExchangeSA 9376	Error	Error	OABGen failed to create the '%1' directory. The directory name syntax is incorrect. The offline address book name cannot include certain characters ('/', '\', ':', '?', '"', '<', '>', or '|'). The offline address book won't be published. - %2
MSExchangeSA 9126	Error	Error	OABGen encountered error %1 while calculating the offline address book for address list '%2'. This offline address book won't be available for client download. - %3.
MSExchangeSA 9373	Error	Error	OABGen detected that the file '%1' is corrupted or missing. This indicates data tampering or disk problems. Restore files in this folder from the recent backup or clean up folder content and force a full OAB generation. - %2
MSExchangeSA 9385	Error	Error	Microsoft Exchange System Attendant failed to read the membership of the universal security group '%1'; the error code was '%2'. The problem might be that the Microsoft Exchange System Attendant does not have permission to read the membership of the group. If this computer is not a member of the group '%1', you should manually stop all Microsoft Exchange services, run the task 'add-

			ExchangeServerGroup Member,' and then restart all Microsoft Exchange services.
MSExchangeSA 9397	Error	Error	OALGen failed to retrieve the CMS name. OAB generation will not be performed.
MSExchangeSA 2033	Error	Error	Unable to generate a unique '%1' e-mail address type for '%2'.
MSExchangeSA 9301	Error	Error	Failed to generate offline address book %1, error '%2'
MSExchangeSA 2030	Error	Error	Unable to find the e-mail address '%1' in the directory. Error '% 2'.
MSExchangeSA 9157	Error	Error	Microsoft Exchange System Attendant does not have sufficient rights to read Exchange configuration objects in Active Directory. Wait for replication to complete and then check to make sure that the computer account is a member of the "Exchange Servers" and "Exchange Install Domain Servers" security groups.
MSExchangeSA 9152	Information	Information	Microsoft Exchange System Attendant reported an error '% 1' in its DS Monitoring thread.
MSExchangeSA 2025	Error	Error	Unable to generate the e-mail address. Address type '%1' is not valid.
MSExchangeSA 9408	Error	Error	OABGen failed to load the OAB version 4 manifest file '%1'. This may indicate data tampering or disk problems. Restore files in this folder from

			the recent backup or clean up folder content and force a full OAB generation. - %2
MSExchangeSA 9368	Error	Error	OABGen could not flush the file '%2' to the disk (error %1). The offline address book is not going to be published to the distribution point. - %3
MSExchangeSA 2027	Error	Error	Unable to generate the e-mail address. Unable to load address module '%1' for address type '%2'. Error %3.
MSExchangeSA 9370	Warning	Warning	OALGen encountered error %1 while updating the time stamp of the '%2' file. - %3
MSExchangeSA 2013	Error	Error	An error occurred adding replica of naming context '%1' to server '%2' from server '%3'. %4
MSExchangeSA 2038	Error	Error	Unable to create directory '%1'.
MSExchangeSA 9153	Information	Information	Microsoft Exchange System Attendant reported an error '%1' when setting DS notification.
MSExchangeSA 9390	Error	Error	OALGen failed to find the OAB version 4 manifest file '%1'. This is normal if it is the first time this offline address list has been published to the file system. Check other logged events to see if this is a serious error.
MSExchangeSA 9175	Error	Error	The MAPI call '%1' failed with the following error: %2
MSExchangeSA 9386	Warning	Warning	OALGen is configured to generate version 2

			or version 3 OAB files for offline address book '%1' but there is no public folder server available. OAB versions prior to version 4 require a public folder server and cannot be generated at this time. Please ensure that a public folder server with a replica of the Offline Address Book system folder is online and mounted, or disable all OAB versions other than version 4.
MSExchangeSA 9186	Warning	Warning	Microsoft Exchange System Attendant has detected that the local computer '%1' is not a member of group '%2'. System Attendant is going to add the local computer into the group. The current members of the group are '%3'.
MSExchangeSA 9384	Error	Error	OALGen only supports alphanumeric and space characters on the offline address name. The offline address list is not going to be published. - %1
MSExchangeSA 9187	Error	Error	Microsoft Exchange System Attendant failed to add the local computer as a member of the DS group object '%1'. Please stop all Exchange services, add the local computer into the group manually and restart all the services.
MSExchangeSA 9149	Information	Information	Microsoft Exchange System Attendant failed to start Exchange server '%1'.

			Error code '%2'.
MSExchangeSA 9367	Error	Error	OABGen could not copy file '%2' to '%3' (error %1). The offline address book is not going to be published to the distribution point. - %4
MSExchangeSA 2037	Error	Error	The file version of '%1' installed on the local server is not current. Unable to locate a correct version on any server in the site.
MSExchangeSA 9391	Error	Error	OALGen failed to read the OAB version 4 manifest from folder '%1'.
MSExchangeSA 9396	Error	Error	OALGen is running on an SCC cluster node which does not have the registry value '%1\%2\%3' or it is set to a non-existing path. OAB generation will not be performed.
MSExchangeSA 9392	Error	Error	OABGen is unable to read file information for file '%1'. This might indicate permission problems. - %2
MSExchangeSA 9315	Error	Error	Exchange detected that "%1" is not the correct version required to run Exchange System Manager or Exchange Server 2003. This may cause failures in Exchange System Manager, affect availability of your server, or both. For more information, see Microsoft Knowledge Base article Microsoft does not support installing Exchange Server components and Outlook on the same computer.

MSExchangeSA 1005	Error	Error	Unexpected error %1 occurred.
MSExchangeSA 9364	Warning	Warning	OABGen received error %1 while trying to delete file '%2'. This is not a fatal problem and the offline address list will be normally posted to the distribution point. - %3
MSExchangeSA 9317	Error	Error	Failed to register Service Principal Name for %1; error code was %2.
MSExchangeSA 9150	Informational	Information	Microsoft Exchange System Attendant failed to stop Exchange server '%1'. Error code '%2'.
MSExchangeSA 9393	Warning	Warning	The directory object for this computer has the serverRole attribute set to 1 (indicating a Front End server). This will be ignored.
MSExchangeSA 9369	Error	Error	OABGen encountered an error while publishing the OAB files to the distribution point '% 1'. Check other logged events to see more information about the problem. - %2
MSExchangeSA 9363	Error	Error	OALGen failed to download the files currently in offline address list '%1'. The offline address list is going to be generated without the previous differential files. - %2
MSExchangeSA 2034	Error	Error	Unable to generate an e-mail address. The '%1' address type was returned by address generation DLL '%2'.

MSExchangeSA 9340	Warning	Warning	A new parent Legacy Exchange DN container value '%1' was found during generation of the differential update file for offline address list '%2'. This will force clients using this offline address list to do a full download of the offline address list. - %3
MSExchangeSA 9154	Informational	Information	DSAccess returned an error '%1' on DS notification. Microsoft Exchange System Attendant will reset DS notification later.
MSExchangeSA 2031	Error	Error	An e-mail address of type '%1' couldn't be generated. Success was indicated, but no e-mail address was returned.
MSExchangeSA 9005	Error	Error	The OABGEN.DLL is required but cannot be loaded, error '%1'.
MSExchangeSA 9398	Error	Error	OALGen is running on a passive cluster node. OAB generation will not be performed.
MSExchangeSA 9320	Warning	Warning	OABGen could not generate full details for some entries in the offline address list for address list '%1'. To see which entries are affected, set event logging for the offline address list generator to at least medium.
MSExchangeSA 1008	Error	Error	Unable to move mailbox '%1'. Error: %2
MSExchangeSA 2035	Error	Error	The e-mail address description object in the Microsoft Exchange directory for the '%1' address type on '%2' machines is missing.

MSExchangeSA 9395	Warning	Warning	OALGen is running on CCR cluster node which does not have registry value '%1\%2\%3' or it is not set to this node name. OAB generation will not be performed.
MSExchangeSA 9394	Warning	Warning	OALGen failed to open directory '%1' as the OAB V4 publishing point. The default location under the Exchange install path will be used.
MSExchangeSA 1004	Informational	Information	%1 failed to start.
MSExchangeSA 9375	Error	Error	OABGen failed to create the '%1' directory. The directory name is invalid. The offline address book name cannot be a device name ('prn', 'aux', etc). The offline address book is not going to be published. - %2
MSExchangeSA 9321	Error	Error	OABGen could not generate full details for entry '%1' in address list '%2' because the total size of the details information is greater than 64 kilobytes. - %3
MSExchangeSA 9151	Informational	Information	Microsoft Exchange System Attendant failed while restarting its internal services: '%1'.
MSExchangeSA 1031	Error	Error	One of the System Attendant's task is blocked. Function: %1
MSExchangeSA 9300	Error	Error	Failed to generate offline address book, error '%1'
MSExchangeSA 1038	Error	Error	Microsoft Exchange System Attendant was unable to find

			the Exchange server object named '%1' in Active Directory. All known domain controllers were checked for this object.
MSExchangeSA 5017	Error	Error	An attempt was made to use the Cluster RPC interface without proper permissions.
MSExchangeSA 9387	Error	Error	OALGen failed to read the OAB version 4 property list from registry key '%1'. The registry value must be a binary value and the number of bytes must be a multiple of 4. The version 4 OAB files will not be generated until this is corrected.
MSExchangeSA 2029	Error	Error	Unable to generate e-mail addresses because no valid e-mail address types were specified.
MSExchangeSA 9130	Error	Error	OABGen could not create a message to post in the public folder for address list '%3'. MAPI component '%1' encountered error '%2'. - %4
MSExchangeSA 9389	Error	Error	The task failed to correctly generate RUS information [Proxies, Addresslists, Policies included] for this object, error '%1'.
MSExchangeSA 9001	Error	Error	The ABV DG dll is required but cannot be loaded, error '%1'.
MSExchangeSA 9360	Error	Error	OABGen encountered an error while generating the %1 file for version 2 and 3 differential downloads of address list '%2'. The offline address book has not been updated so

			clients will not be able to download the current set of changes. Check other logged events to find the cause of this error. If the cause of the problem was intentional or cannot be resolved, OABGen can be forced to post a full offline address book by creating the DWORD registry key 'HKEY_LOCAL_MACHINE\%3\%4' and setting it to 1 on this server. When OABGen next generates the offline address book, clients will perform a full OAB download. After that time, the registry key should be removed to prevent further full downloads. - %5
MSExchangeSA 9002	Error	Error	The ABV DG service failed to start, error '%1'.
MSExchangeSA 9094	Error	Error	The MAD Free Busy dll is missing or failed to start properly, error '%1'.
MSExchangeSA 1000	Informational	Information	%1 is starting. Microsoft Exchange Server System Attendant, service startup complete, version %2 (build %3).
MSExchangeSA 9006	Informational	Information	Microsoft Exchange System Attendant is loading '%1'.
MSExchangeSA 9007	Informational	Information	Microsoft Exchange System Attendant is initializing '%1'.
MSExchangeSA 9008	Informational	Information	Microsoft Exchange System Attendant is starting '%1'.
MSExchangeSA 9012	Informational	Information	Microsoft Exchange System Attendant is binding to domain

			controller '%1'.
MSExchangeSA 9013	Informational	Information	Microsoft Exchange System Attendant is being started for Exchange server '%1'.
MSExchangeSA 9014	Informational	Information	Microsoft Exchange System Attendant has been successfully started for Exchange server '%1'.

1.8.7.13 MSExchangeSetup Errors and Events

MSExchangeSetup Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-05-14*

Microsoft Exchange Server 2010 generates Exchange Setup events in Event Viewer so that you can troubleshoot and verify the MSExchangeSetup features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Exchange Setup Errors and Events

The following table provides a list of MSExchangeSetup errors and events.

Event ID	Category	Event type	Value or description
MSExchangeSetup 1002	Error	Error	Exchange Server component %1 failed. Error: %2
MSExchangeSetup 1	Informational	Information	Microsoft Exchange Setup
MSExchangeSetup 1000	Informational	Information	Exchange Setup (build %1) was started.
MSExchangeSetup 1001	Informational	Information	Exchange Setup (build %1) completed successfully.
MSExchangeSetup	Informational	Information	During installation,

1003			Exchange Setup modified the WebSvcExtRestrictionList metabase key. The WebSvcExtRestrictionList metabase key contains a list of .dll files that are either allowed or denied access to run on your server. Exchange setup has added and allowed the following .dll files and extension groups to run: %1 Parts of Microsoft Exchange require this modification to work properly.
MSExchangeSetup 1004	Informational	Information	During uninstall, Exchange Setup did not disable the following Web Service Extensions: %1

1.8.7.14 OAB Maintenance Errors and Events

OAB Maintenance Errors and Events

Exchange Server 2010 > Mailbox > Error and Event Reference for Mailbox Servers >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates OAB Maintenance events in Event Viewer so that you can troubleshoot and verify the OAB Maintenance features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

OAB Maintenance Errors and Events

The following table provides a list of OAB Maintenance errors and events.

Event ID	Category	Event type	Value or description
MSExchange OAB Maintenance 1001	General	Information	The OAB Maintenance servicelet is starting.
MSExchange OAB Maintenance 1002	General	Information	The OAB Maintenance Servicelet caught an exception of type %1:

			"%2". A Watson report will be sent, and the servicelet will be re-started.
MSExchange OAB Maintenance 1003	General	Information	The OAB Maintenance Servicelet caught an exception of type %1: "%2". The task did not complete successfully.
MSExchange OAB Maintenance 2001	Orphaned OAB Recovery	Information	The server responsible for performing the OAB recovery scan is %1.
MSExchange OAB Maintenance 2002	Orphaned OAB Recovery	Information	Because this server is not the one responsible for performing the OAB recovery scan, the task is exiting.
MSExchange OAB Maintenance 2003	Orphaned OAB Recovery	Information	Orphaned OAB recovery scan has begun.
MSExchange OAB Maintenance 2005	Orphaned OAB Recovery	Information	No orphaned offline address books were found.
MSExchange OAB Maintenance 2006	Orphaned OAB Recovery	Information	%1 orphaned offline address books were found. The OAB Maintenance Servicelet will attempt to move these offline address books to functioning servers.
MSExchange OAB Maintenance 2007	Orphaned OAB Recovery	Information	The offline address book %1 was successfully moved to server %2.
MSExchange OAB Maintenance 2008	Orphaned OAB Recovery	Information	While attempting to move the offline address book %1, the OAB Maintenance Servicelet caught an exception of type %2: "%3". The offline address book was not moved.

1.8.7.15 Progress Manager Errors and Events

Progress Manager Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates Process Manager events in Event Viewer so that you can troubleshoot and verify the Process Manager features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

Process Manager Errors and Events

The following table provides a list of Process Manager errors and events.

Event ID	Category	Event type	Value or description
MSExchange Process Manager 1032	ProcessManager	Error	Socket Access Denied. Binding: %1.
MSExchange Process Manager 1018	ProcessManager	Error	The address is already in use. Binding: %1.
MSExchange Process Manager 1019	ProcessManager	Error	Failed to start listening (Error: %1). Binding: %2.

1.8.7.16 Search Indexer Errors and Events

Search Indexer Errors and Events

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-04-24*

Microsoft Exchange Server 2010 generates MSExchange Search Indexer events in Event Viewer so that you can troubleshoot and verify the Search Indexer features and services. Event Viewer tracks the following kinds of events in the given order, based on importance:

- Error events
- Warning events
- Informational events

MSExchange Search Indexer Errors and Events

The following table provides a list of MSExchange Search Indexer errors and events.

Event ID	Category	Event type	Value or description
MSExchange Search Indexer 122	General	Information	MS Search (Exchange) reached the memory cap, and now the memory is %1 Bytes. The cap is %2 Bytes.
MSExchange Search Indexer 115	General	Warning	Exchange Search Indexer failed to retreive local server object from AD (%1).

1.9 Unified Messaging

Unified Messaging

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-16*

Unified Messaging combines voice messaging and e-mail into one Inbox, which can be accessed from the telephone and the computer. Unified Messaging integrates Exchange Server 2010 with the telephony network in your organization and brings the features found in Unified Messaging to the core of the Exchange Server product line.

The following topics are gateways to information about the Unified Messaging servers in Exchange 2010.

Understanding Unified Messaging

This topic is a collection of links to topics that provide detailed information about the Unified Messaging features in Exchange 2010. These topics will help you gain a better understanding of the Unified Messaging server role.

Planning Roadmap for New Deployments

This topic provides an overview of how to plan your Exchange 2010 deployment, including Unified Messaging features.

Deploy a New Exchange 2010 RTM UM Environment

This topic provides an overview of how to plan your Exchange 2010 Unified Messaging.

Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging

This topic describes the upgrade process from an existing Exchange Server 2007 Unified Messaging deployment to Exchange 2010 Unified Messaging.

Managing Unified Messaging

This topic is a collection of links that provide information about managing Unified Messaging features in your organization.

Securing Unified Messaging Servers

This topic is a collection of links that will help you manage the security of your Unified Messaging infrastructure.

Troubleshooting Reference for Unified Messaging Servers

This topic is a collection of links that provide troubleshooting information specific to

Unified Messaging.

Performance Counter Reference for Unified Messaging Servers

This topic is a collection of links that describe the various performance counters that are used by Unified Messaging.

Error and Event Reference for Unified Messaging Servers

This topic is a collection of links that provide explanations and suggested user actions for Unified Messaging errors and events you may encounter.

1.9.1 Understanding Unified Messaging

Understanding Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-28*

Microsoft Exchange Server 2010 Unified Messaging combines voice messaging and e-mail messaging into one store, accessible from a telephone and a computer. Unified Messaging integrates Microsoft Exchange with telephony networks and brings the UM features to the core of Microsoft Exchange. The following topics provide detailed information about the Unified Messaging features in Exchange 2010:

Overview of Unified Messaging

Understanding Unified Messaging Server Topologies

Understanding Unified Messaging Components

Understanding Unified Messaging Features

Understanding Unified Messaging and Communications Server 2007 R2

Understanding Unified Messaging Call Processing

Understanding Unified Messaging Performance and Scalability

Understanding Unified Messaging Availability

Fax Advisor for Exchange 2010

Telephony Advisor for Exchange 2010

Virtualization of the Unified Messaging Role in Exchange 2010 SP1

1.9.1.1 Overview of Unified Messaging

Overview of Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-24*

Microsoft Exchange Server 2010 Unified Messaging (UM) combines voice messaging and e-mail messaging into a single messaging infrastructure. Unified Messaging puts all e-mail and voice messages into one Exchange 2010 mailbox that can be accessed from many different devices. After Unified Messaging servers have been deployed on a network, users can access their messages using Outlook Voice Access, from any telephone, from a mobile phone, or from the computer.

Today, people in organizations frequently manage their voice messages separately from their e-mail messages. Additionally, IT administrators frequently manage the voice mail or telephony networks and the e-mail systems or data networks as separate systems. In these situations, voice mail and e-mail are located in separate inboxes that are hosted on separate servers accessed through the desktop for e-mail and through the telephone for voice mail. Unified Messaging uses the Exchange 2010 store for all messages, including e-mail and voice messages.

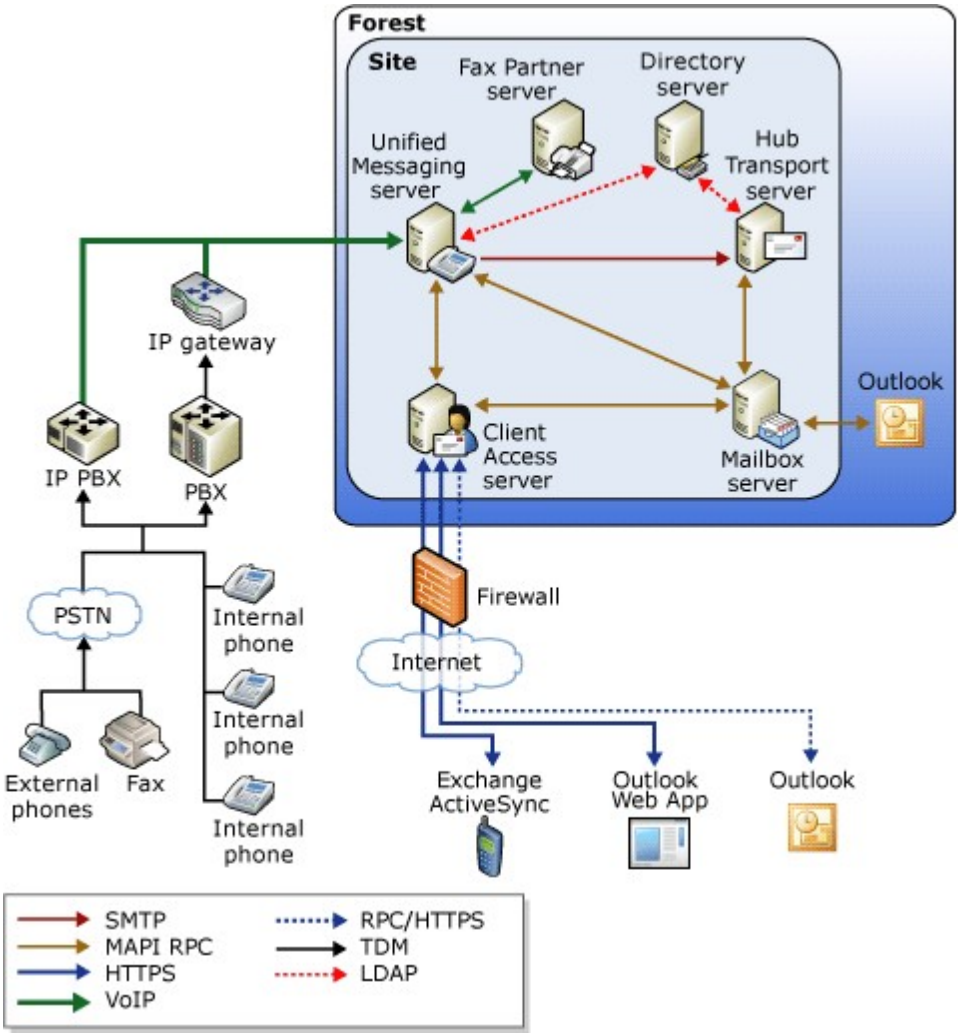
Looking for management tasks related to Unified Messaging? See Managing Unified Messaging.

Contents

Overview of Unified Messaging

In Microsoft Exchange 2010, the Unified Messaging server role is one of several server roles that you can install and then configure on a computer running Windows Server 2008. Unified Messaging is included with Exchange Server 2007 and Exchange 2010, and it brings with it new telephony concepts that may not be familiar to an Exchange administrator.

Unified Messaging combines voice messaging, fax messaging and e-mail messaging in the Exchange store. Unified Messaging integrates Microsoft Exchange with telephony networks and brings the UM features to the core of Exchange. The following figure shows the relationship between an organization's telephony network components and the UM system.



In the previous figure, the Unified Messaging solution provides access to telephony systems by using standard Voice over IP (VoIP) protocols. These protocols include Session Initiation Protocol (SIP), Realtime Transport Protocol (RTP), and the T.38 protocol. The IP gateways provide interoperability for legacy Private Branch eXchange (PBX) systems. For details, see Understanding Telephony Concepts and Components.

Note:
Installing and running the Unified Messaging server role in a virtualized environment is supported if you are running Microsoft Exchange Server 2010 Service Pack 1 (SP1) or a later version. The Unified Messaging server role is not supported in a virtualized environment that is running Exchange 2010 RTM.

Return to top

Benefits of Exchange 2010 Unified Messaging

The Exchange 2010 Unified Messaging solution offers benefits for the end user and also for the IT administrator.

User Benefits

When you deploy Exchange 2010 Unified Messaging, users can access voice mail, e-mail, and calendar information that's located in their Exchange 2010 mailbox from an e-mail client, for example, Outlook or Microsoft Office Outlook Web App, from a mobile phone with Microsoft Exchange ActiveSync set up, such as a Windows Mobile phone, or from a telephone. Additionally, users will be able to use the following features:

- **Access to Exchange information** UM-enabled users can access a full set of voice mail features from Internet-capable mobile phones, Microsoft Office Outlook 2007, Outlook 2010, and Outlook Web App. These features include many voice mail configuration options and the ability to play a voice message from either the Reading Pane, using an integrated Windows Media Player, or the message list, using computer speakers.
- **Play on Phone** The Play on Phone feature lets UM-enabled users play voice messages over a telephone. If the user works in an office cubicle, is using a public computer or a computer that isn't enabled for multimedia, or is listening to a voice message that's confidential, they might not want to or be able to listen to a voice message through computer speakers. They can play the voice message using any telephone, including a home, office, or mobile telephone.
- **Voice mail form** The Outlook 2007, Outlook Web App, and Outlook 2010 voice mail form resembles the default e-mail form. It gives users an interface for performing actions such as playing, stopping, or pausing voice messages, playing voice messages on a telephone, and adding and editing notes. The voice mail form includes the embedded Windows Media Player and an Audio notes field. The embedded Windows Media Player and notes field are displayed in either the Reading Pane when users preview a voice message or in a separate window when they open the voice message. If users aren't enabled for Unified Messaging, or if Outlook 2007 hasn't been installed on the client computer, they view voice messages as e-mail attachments, and the voice mail form isn't available.
- **User configuration** A user who's enabled for Unified Messaging can configure several voice mail options for Unified Messaging using Outlook Web App. For example, the user can configure telephone access numbers and the voice mail Play on Phone number, and can then reset a voice mail access PIN.
- **Call answering** Call answering includes answering incoming calls on behalf of users, playing their personal greetings, recording messages, and submitting them for delivery to their Inbox as an e-mail message.
- **Call Answering Rules** Call Answering Rules is a new feature in Exchange 2010. Using this feature, end users can dictate how their incoming call answering calls should be handled. The way call answering rules are applied to incoming calls is similar to the way Inbox rules are applied to incoming e-mail messages. By default, no call answering rules are configured. If an incoming call is answered by a Unified Messaging (UM) server, the caller is prompted to leave a voice message for the called party. Using call answering rules, a caller can:
  - Leave a voice message for the UM-enabled user.
  - Transfer to an alternate contact of the UM-enabled user.
  - Transfer to the alternate contact's voice mail.
  - Transfer to other phone numbers that the UM-enabled user has configured.
  - Use the Find-Me feature or locate the UM-enabled user via a supervised transfer.
- **Voice Mail Preview** In Exchange 2010, the Unified Messaging server role uses ASR on newly created voice mail messages. When users receive voice messages, the messages contain both a recording and text that's been created from the voice recording. Users see the voice message text displayed in an e-mail message from within Outlook Web App, Outlook 2007, or Outlook 2010.
- **Message Waiting Indicator** Message Waiting Indicator is a feature found in most legacy voice mail systems and can refer to any mechanism that indicates the existence of a new message. In Exchange 2007, this functionality was

provided by a third-party application, which indicated receipt of a new voice message by lighting the lamp on the desk phone. This feature has been added to Exchange 2010, and third-party software isn't needed. Enabling or disabling Message Waiting Indicator is done on the user's mailbox or on a UM mailbox policy.

- **Missed call and voice mail notifications using SMS** When users are members of a hosted or consumer dial plan, and they configure their voice mail settings with their mobile phone number and configure call forwarding, they can receive notifications about missed calls and new voice messages on their cell phones in a text message via the Short Messaging Service (SMS). However, to receive these types of notifications, the users must first configure text messaging and also enable **Notifications** on their account.
- **Protected Voice Mail** Protected Voice Mail is Unified Messaging functionality that enables users to send private mail. This mail is protected by Active Directory Rights Management Services (AD RMS), and users are restricted from forwarding, copying, or extracting the voice file from e-mail. Protected Voice Mail increases the confidentiality of Unified Messaging, and lets users rely on Unified Messaging if they want to limit the audience for voice messages. This functionality is similar to the way private e-mail messages were handled in Exchange 2007. In Exchange 2010, it also applies to voice mail messages.
- **Outlook Voice Access** There are two Unified Messaging user interfaces available to UM-enabled users: the telephone user interface (TUI) and the voice user interface (VUI). These two interfaces together are called Outlook Voice Access. Subscribers can use Outlook Voice Access when they access the Unified Messaging system from an external or internal telephone. UM-enabled users who dial in to the Unified Messaging system can access their mailbox using Outlook Voice Access. Using a telephone, a UM-enabled user can:
  - Access voice mail
  - Listen to, forward, or reply to e-mail messages
  - Listen to calendar information
  - Access or dial contacts who are stored in the global address list or a group in their Contacts
  - Accept or cancel meeting requests
  - Set a voice mail message to let callers know the called party is away
  - Set user security preferences and personal options
- **Group addressing using Outlook Voice Access** In Exchange 2007, users could use either the telephone user interface (TUI) or voice user interface (VUI) in Outlook Voice Access to send e-mail and voice messages when they logged on to their mailbox. However, users could only send a single e-mail message to a single user in their personal Contacts, to multiple recipients from the directory by adding each recipient individually, or by adding the name of a distribution list from the global address list. In Exchange 2010, when a user signs in to their mailbox using Outlook Voice Access, they can also send e-mail and voice messages to users in a group stored in their personal Contacts.

Return to top

Benefits for Administrators

Currently, most users and IT departments manage their voice mail separately from their e-mail. Voice mail and e-mail exist as separate inboxes hosted on separate servers accessed through the desktop for e-mail and through the telephone for voice mail. Unified Messaging offers an integrated store for all messages and access to content through the computer and the telephone.

Exchange administrators can manage Unified Messaging using the same interface they use to manage the rest of Exchange, using the Exchange Management Console and the Exchange Management Shell. They can:

- Manage voice mail and e-mail from a single platform
- Manage Unified Messaging using scriptable commands

- Build highly available and reliable Unified Messaging infrastructures

Exchange 2010 Unified Messaging offers administrators:

- **A complete unified messaging system** Exchange 2010 Unified Messaging offers a true unified messaging solution using a single store, transport, and directory infrastructure. The store is provided by the Exchange 2010 Mailbox server role. The transport is provided by the Exchange 2010 Hub Transport server role. All e-mail and voice mail messages can be managed from a single management point, using a single administration interface and tool set. This greatly reduces the overall cost of administration by consolidating infrastructure and training.
- **An Exchange 2010 deployment and administration model** Using the Exchange 2010 Unified Messaging solution, you can take advantage of the Exchange 2010 server design. You aren't required to purchase a new server to run the Unified Messaging server role. More important, you can reuse your Exchange knowledge, including training and troubleshooting methodology, and apply it to managing your voice mail infrastructure.
- **An Exchange 2010 security model** The Microsoft Exchange Unified Messaging service runs as an Exchange server account. This means that you don't have to create or manage a super user account for Exchange 2010 Unified Messaging.
- **Consolidation of voice mail systems** Currently, most voice messaging systems require that all the voice messaging system components be installed in every physical office location in an organization. In this kind of arrangement, the voice messaging systems in branch offices are located outside the central office and must be administered onsite. This frequently results in increased administration costs and complexity. Exchange 2010 Unified Messaging lets you manage your voice mail system from a central location. To create a centralized management system for Unified Messaging, you can place all Unified Messaging servers in a datacenter or location, and then deploy IP gateways in each of your branch offices that replace the voice messaging system for each branch office. Deploying a centralized voice messaging system in this manner can result in a significant savings in hardware and administrative costs.
- **Built-in Unified Messaging administrative roles** A set of roles for managing Unified Messaging and voice mail features has been defined within Exchange 2010. Administrative roles that included UM were available in Microsoft Exchange Server 2007. The following UM-specific administrative roles have been added for Exchange 2010:
  - UM Mailboxes
  - UM Prompts
  - Unified Messaging
- **Incoming fax support** Exchange 2007 provided built-in support for fax message creation through the Unified Messaging server role. A user with a UM-enabled mailbox could receive fax messages from calls placed to his or her phone number. There's no support in Exchange 2007 UM for inbound fax routing, or for outgoing fax.
  In Exchange 2010, direct support for fax has been removed from the Unified Messaging server role. Customers who require a fax solution that works with Exchange 2010 will have to deploy a fax partner solution. Fax partner solutions are available from several fax partners. The fax partner solutions are designed to be tightly integrated with Exchange 2010 and enable UM-enabled users to receive incoming fax messages.

Note:

If you're using the RTM version of Exchange 2010 Unified Messaging, you may have to enable inband fax tone detection for fax receiving to work correctly with some IP PBXs. You do this by changing the *EnableInbandFaxDetection* setting to True in the msexchangeum.config file. The msexchangeum.config file is located in the \Program Files\Microsoft\Exchange\V14\bin folder on an

Exchange 2010 Unified Messaging server. If you don't configure this setting, Unified Messaging servers must rely on IP gateways to perform inband fax tone detection.
Changing the *EnableInbandFaxDetection* setting to True in the msexchangeum.config file isn't required in Exchange 2010 Service Pack 1 (SP1). Enabling fax tone detection isn't necessary on a Unified Messaging server with Exchange 2010 SP1 installed because the Unified Communications Managed API v. 2.0 (UCMA) enables the Unified Messaging server to listen to both inband and out-of-band fax events.

- **Support for multiple languages** For Exchange 2010, all available language packs contain the Text-to-Speech (TTS) engine and the prerecorded prompts for a specified language and ASR support. However, only some language packs contain support for Voice Mail Preview. The US English (en-US) language pack is included on the Exchange 2010 DVD and additional UM language packs can be downloaded from the Microsoft Download Center.
- **Auto attendant** An auto attendant is a set of voice prompts that gives external and internal users access to the Exchange 2010 Unified Messaging system. The telephone keypad or speech inputs can be used to move through the auto attendant menu, place a call to a user, or locate a UM-enabled user and then place a call to them. An auto attendant gives the administrator the ability to:
  - Create a customized menu for external users.
  - Define informational greetings, business hours greetings, and non-business hours greetings.
  - Define holiday schedules.
  - Describe how to search the organization's directory.
  - Describe how to connect to a user's extension so external callers can call users by specifying their extension.
  - Describe how to search the organization's directory so external callers can search the organization's directory and call a specific user.
  - Enable external users to call the operator.

Return to top

Configuring a UM Server

During an installation of the Unified Messaging server role, a UM computer object is created in the Computers container in Active Directory. The UM computer object created in Active Directory is a representation of a physical server on which the Unified Messaging server role is installed. The UM Active Directory computer objects connect your organization's telephony infrastructure and the UM Active Directory networking environment.

Note:

For a new UM computer object to be created during installation, the UM server must be a member of a domain before the Unified Messaging server role is installed.

After the computer object is created, you can perform the procedures for deploying Unified Messaging on your network.

Server Operation

By default, the operational status of the UM server is set to Enabled after the Unified Messaging server role is installed. This lets the UM server process incoming and outgoing voice calls and route the messages to their intended recipients in your Exchange organization. A UM server won't process incoming calls unless the operational status is set to Enabled.

The operational status of the UM server can be controlled using the Enable and Disable commands in the EMC and the Shell. There are three status modes for UM servers:

- **Enabled** Process all incoming calls.
- **Disable immediately** Don't accept any new calls and drop all existing calls.
- **Disable after completing calls** Don't accept any new calls but process all existing calls.

When the UM server starts, it locates all UM IP gateways associated with the server and associated with the existing UM dial plan. To detect and determine any configuration changes on either UM dial plans or UM IP gateways, the UM server will either register a change notification or re-check the configuration every 10 minutes.

If the UM IP gateway list changes, the UM server will react accordingly and either start to use or stop using the IP gateways that are associated with the UM server's dial plan. After a UM server is working as an associated member of a UM dial plan and is communicating with an IP gateway or a PBX, you can run a set of diagnostic operations to verify that it's connected and operating correctly.

Return to top

Configuring UM Users

When you mailbox-enable a user, you're given the option to create a mailbox or to connect to an existing mailbox. After a user is connected to an existing mailbox or a mailbox is created for them, you must enable the mailbox so the user can use Unified Messaging. After the user is enabled for Unified Messaging, all e-mail and voice messages will be delivered to the user's mailbox. UM users can access their e-mail, voice messages, and calendaring information by using Outlook 2007, Outlook 2010, Outlook Web App, a mobile phone that's enabled for Exchange ActiveSync, or a regular or mobile phone.

Note:

To enable multiple UM users, use the **Enable-UMMailbox** cmdlet in the Shell.

User UM Properties

After a user is enabled for Unified Messaging, you can manage, modify, and configure the UM properties for the user.

There are two locations in which UM properties are stored for a user: the Mailbox object and the user's Active Directory object. When you enable a user for Unified Messaging, you set the UM property on the user's Mailbox object. After the Mailbox property is set to Enabled for Unified Messaging, the user can use the UM features found in Exchange 2010.

After a user is enabled for Unified Messaging, the user's UM properties, such as the user's extension number, spoken name, and other properties for the user, are stored in the user's properties in Active Directory and on the user's mailbox.

You can manage UM properties for an Active Directory user on the mailbox of the UM user by using the Shell or the EMC.

The Relationship of the UM User to a UM Mailbox Policy

When you enable a user for Unified Messaging, the user must be associated with or linked to an existing UM mailbox policy and you must provide the extension number for the user. You can associate a user with a UM mailbox policy by using the **Enable-UMMailbox** cmdlet or by selecting the UM mailbox policy when you create the user's Exchange mailbox.

A UM mailbox policy contains settings such as the dialing restrictions and PIN policies for a user. When a UM mailbox policy is created, the UM mailbox policy must be associated with only one UM dial plan. The UM dial plan is then automatically associated with at least one UM server. Any UM server that's associated with the UM dial plan can provide UM services for a UM-enabled user who uses the UM dial plan. Associating these Active Directory objects in this manner delivers the UM services by using Active Directory. After the user is enabled for Unified Messaging, the settings from a UM mailbox policy are applied to the UM-enabled user.

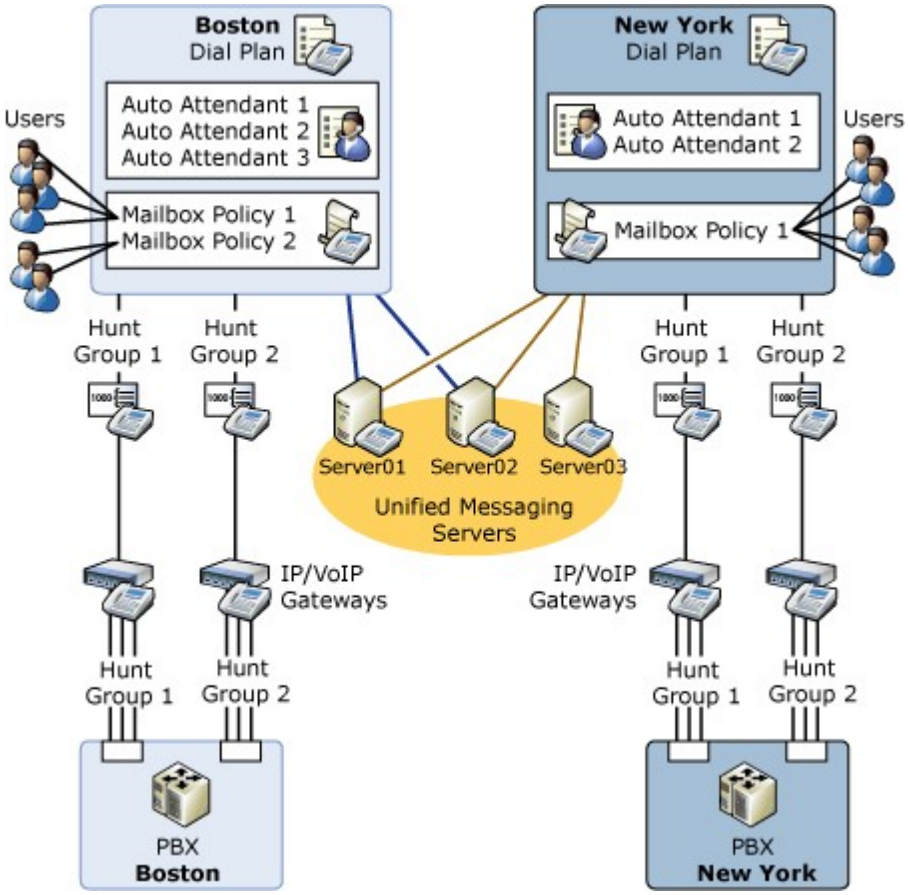
Configuring UM Components

Exchange 2010 Unified Messaging provides voice messaging services using objects that take advantage of your current Active Directory environment. UM Active Directory objects are created to support Unified Messaging. Active Directory acts as the container for all these UM objects and their configuration settings.

UM Active Directory objects make it possible for UM to interact with the telephony infrastructure. This physical infrastructure and the relationship between its components are mirrored in Active Directory. For details, see Understanding Unified Messaging Components.

Some UM Active Directory objects are created to represent each telephony hardware device, and other UM Active Directory objects are created to represent a telephony dial plan for an organization or to support a specific feature of Unified Messaging. For details, see Understanding Telephony Concepts and Components.

The following example and figure show the relationships between the UM objects found in Active Directory.



In the previous figure, the UM servers represented as Server01, Server02, and Server03 are located in the datacenter for a company. These servers are also represented as UM Server objects in Active Directory. Additionally, there are two UM dial plans, the Boston UM dial plan and the New York UM dial plan. There is a single PBX for each office. However, there are two IP gateways per PBX at each branch office to provide fault tolerance. Finally, Server01 and Server02 are members of the Boston UM dial plan, and Server01, Server02, and Server03 are all members of the New York UM dial plan.

When a call comes in to the PBX in the New York branch office and the call is forwarded to a UM server, any one of the three UM servers can answer the call and deliver the message to the user's mailbox because all the UM servers belong to the same dial plan. When a call is received in Boston for a user and the call is forwarded to a UM server, either Server01 or Server02 can answer calls for the users in the Boston dial plan.

There are several key Active Directory objects you need to create and manage. These objects are outlined in the following sections.

Return to top

UM Dial Plans

In a traditional telephony dial plan, users' extensions are configured on an IP PBX, PBX, or multiple PBXs and share a common numbering plan. This makes it possible for users to dial one another's telephone extensions without dialing a full telephone number.

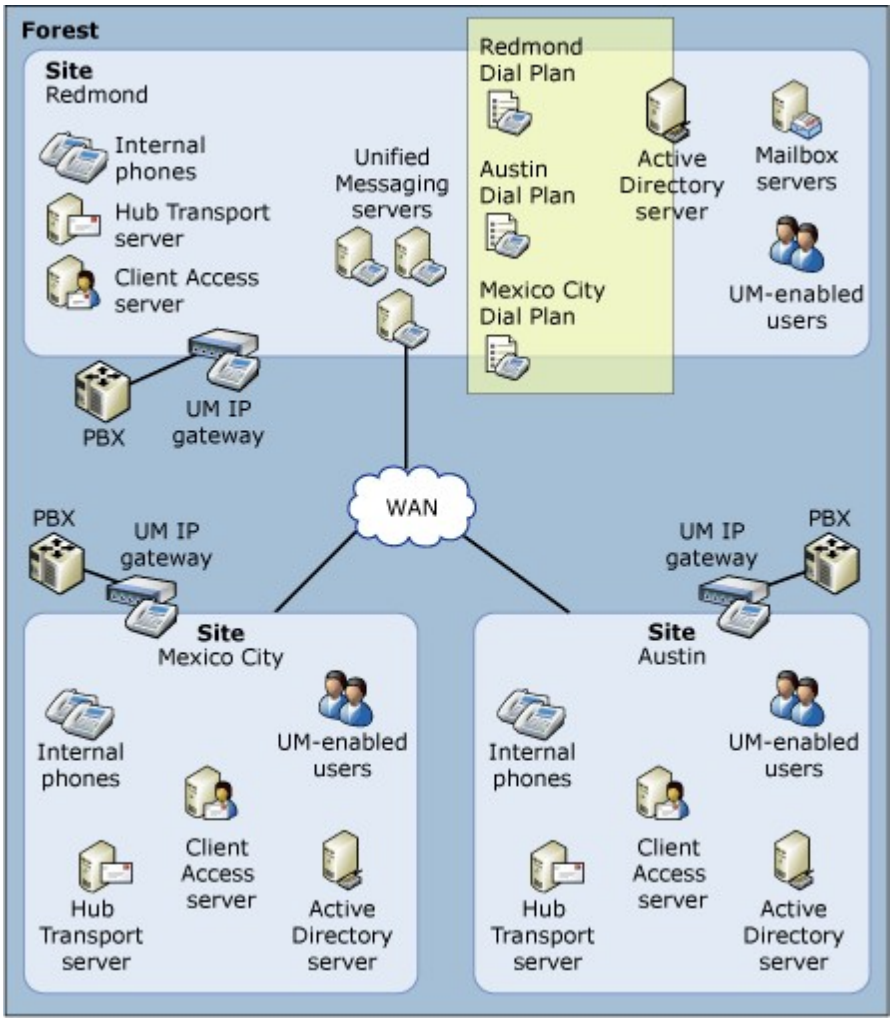
A UM dial plan mirrors a telephony dial plan. UM dial plans are required to successfully deploy Unified Messaging on your network.

A UM dial plan is an Active Directory object that represents sets or groupings of IP PBXs or

PBXs that share common user extension numbers. UM dial plans in Unified Messaging require that user telephone extension numbers be unique.

In some telephony networks, multiple PBXs and multiple dial plans exist. In these telephony networks, there can be two users who have identical telephone extensions if the two users who have the same extension number are placed in two separate UM dial plans. Putting the two users in separate dial plans makes their extension numbers unique for Unified Messaging purposes.

The following figure shows how UM dial plans can be used in an organization that has a single forest and multiple physical sites.



How Dial Plans Work

After you install the Unified Messaging server role on an Exchange 2010 computer, you must associate the UM server with at least one UM dial plan before it will answer calls. You can also associate a single UM server with multiple UM dial plans.

After the UM server is associated with a UM dial plan, you must create a UM IP gateway and associate it with the UM dial plan that was created.

Important:
Each time you create a UM dial plan by using the EMC, a UM mailbox policy will also be

created. The UM mailbox policy will be named *<DialPlanName>* Default Policy.

Creating and associating the UM dial plan and UM server objects in Active Directory enables the UM server to receive calls from the IP gateway or IP PBX and then process incoming calls for users who are associated with the UM dial plan. When a call comes in to the IP gateway or IP PBX, the IP gateway or IP PBX forwards the call to a UM server and the UM server tries to match the extension number of the user to the associated UM dial plan. The dial plan is identified from the pilot numbers that are sent by the IP gateway or IP PBX when an incoming call is received. The pilot numbers that are configured on a PBX or IP PBX may also be configured on a UM dial plan as a subscriber access number. For details, see Understanding Unified Messaging Dial Plans.

When you integrate a telephony network with Unified Messaging, there must be at least a single IP gateway or SIP-enabled IP PBX that connects your telephony network with your IP-based network. Each IP gateway or IP PBX in your organization is represented by a UM IP gateway object in Active Directory.

Return to top

UM Mailbox Policies

UM mailbox policies are required when you enable users for Unified Messaging. They're useful for applying and standardizing UM configuration settings for UM-enabled users. You create UM mailbox policies to apply a common set of policies or security settings to a collection of UM-enabled mailboxes. You use Unified Messaging mailbox policies to set UM settings for UM-enabled users, such as the following:

- PIN policies
- Dialing restrictions
- Other general UM mailbox policy properties

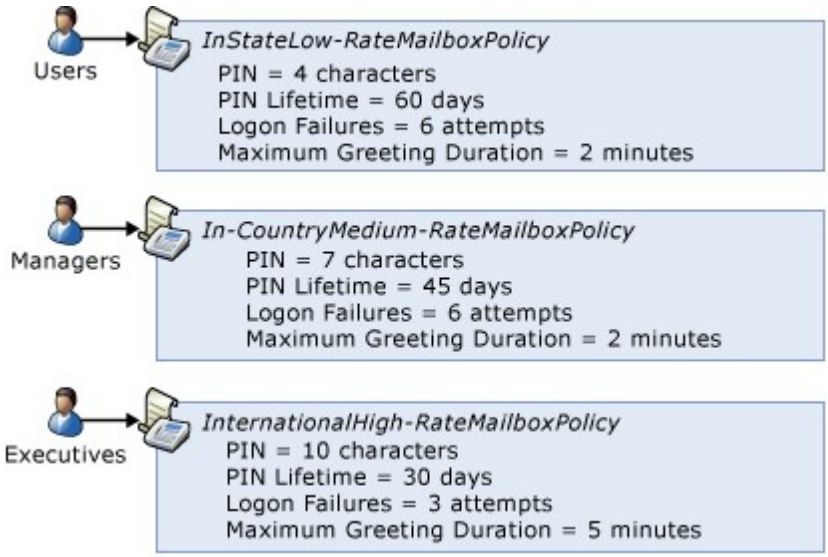
For example, you can create a UM mailbox policy to increase the level of PIN security by reducing the maximum number of logon failures before a user will be locked out for a specific group of UM-enabled users, such as executives.

UM mailbox policies are created in the **Configuration** container in Active Directory by using the Shell or the EMC. By default, a single UM mailbox policy is created every time you create a UM dial plan. The new UM mailbox policy is associated with the UM dial plan and part of the dial plan name is included in the display name of the UM mailbox policy. However, you can create additional UM mailbox policies based on the needs of your organization. Although a single UM mailbox policy is required to enable users for Unified Messaging, you can create additional UM mailbox policies and apply a common set of mailbox policy settings for other groups of users.

The mailbox of each UM-enabled user must be linked to a single UM mailbox policy when the mailbox is enabled for Unified Messaging. After you create a UM mailbox policy, you link one or more UM-enabled mailboxes to the UM mailbox policy. This lets you control PIN security settings such as the minimum number of digits in a PIN or the maximum number of logon attempts for the UM-enabled users who are associated with the UM mailbox policy. If you prefer, you can also control message text settings or dialing restrictions for the same or a different group of UM-enabled mailboxes.

Multiple UM-enabled users can be linked to a single UM mailbox policy. However, a single user can be associated with only one UM mailbox policy. After you create a new UM mailbox policy and link it to a UM dial plan, the UM mailbox policy settings that are defined are applied to the UM-enabled users. The settings that are defined on a UM dial plan and a UM mailbox policy will be applied to all users who are associated with the UM mailbox policy.

The following figure shows how UM mailbox policies can be created to control dialing restrictions and PIN security settings for three different groups.



Return to top

UM IP Gateways

A UM IP gateway is an Active Directory object that represents a physical IP gateway hardware device, an IP PBX, or another SIP server that can interoperate with Unified Messaging. Before the physical IP gateway, IP PBX, or SIP server can be used to process UM calls, it must be represented in Active Directory by an UM IP gateway object.

Although there are many types and manufacturers of PBXs, IP gateways, and IP PBXs, there are basically two types of IP gateway component configurations:

- **IP PBX** A single device
- **PBX (legacy) and an IP gateway** Two separate components

To support Unified Messaging, one or both types of IP device configurations are used when connecting a telephony network with a data network.

The UM IP gateway can be associated with one or more Active Directory UM hunt groups. The combination of the UM IP gateway object and a UM hunt group object establishes a link between an IP gateway hardware device and a UM dial plan.

Enabling and Disabling UM IP Gateways

By default, UM IP gateways are left in an enabled state after they're created. However, the UM IP gateway can be enabled or disabled. If you disable a UM IP gateway, it can be in one of two disabled modes. The first disabled mode forces all associated UM servers to drop existing calls. The second disabled mode forces the UM server associated with the UM IP gateway to stop handling any new calls presented by the IP gateway.

Note:

Before an IP gateway can be used to process calls, a UM IP gateway must be associated with at least one UM dial plan. Also, at least one UM server must be associated with at least one UM dial plan. If a UM IP gateway is deleted, the UM servers associated with the UM IP gateway will no longer be able to accept or process new call requests from the IP gateway or IP PBX.

Return to top

UM Hunt Groups

In a telephony network, a hunt group is defined as a set of extension numbers that are

grouped as a single unit. When an incoming call is received, the PBX or IP PBX uses the hunt group to "hunt" for an available or open line, extension, or channel that can be used to receive the call.

Hunt groups are used to efficiently distribute calls into or out of a specific unit. For example, a PBX or IP PBX might be configured to have 10 extension numbers for a sales department. The 10 sales extension numbers would be configured as one hunt group.

Multiple algorithms or methods have been created for use by a PBX or IP PBX to define how the open line, extension, or channel will be located. These include the following:

- Round robin
- Most idle
- Start with lowest number

Creating and defining a hunt group in a PBX or IP PBX reduces the possibility that a caller who places an incoming call will receive a busy signal when the call is received.

Understanding UM Hunt Groups

UM hunt groups are used to define the PBX or IP PBX hunt group from which incoming calls will be received and are very important to the operation of the UM system. The UM hunt group represents an existing PBX or IP PBX hunt group. UM hunt groups act as a connection or link between the UM IP gateway and the UM dial plan. A single UM hunt group is associated with at least one UM IP gateway and one UM dial plan.

The pilot number defined for a hunt group in the physical PBX or IP PBX must also be defined for the UM hunt group. A pilot number is a telephone number that points to a hunt group and is the phone number for calls that are routed to Unified Messaging servers. The pilot number is used to match the information presented with incoming calls using the SIP header on the message. The pilot number enables the UM server to interpret the call together with the correct dial plan so that the voice message can be routed correctly. It's very important to configure UM hunt groups correctly, because incoming calls that don't correctly match the pilot number defined on the UM hunt group won't be answered and incoming call routing will fail.

When you create a UM hunt group, you're enabling all UM servers specified within the UM dial plan to communicate with an IP gateway. If you delete the UM hunt group, the associated IP gateway will no longer service calls by using the specified pilot number. If the IP gateway is left without remaining UM hunt groups, the IP gateway won't be able to handle incoming calls.

UM Auto Attendants

Unified Messaging enables you to create one or more UM auto attendants, depending on the needs of your organization. UM auto attendants can be used to create a voice menu system for an organization that lets external and internal callers move through the UM auto attendant menu system to locate and place or transfer calls to company users or departments in an organization.

When anonymous or unauthenticated users call an external business telephone number, or when internal callers call a defined extension number, they're presented with a series of voice prompts that help them place a call to a user or locate a user in the organization and then place a call to that user. The UM auto attendant is a series of voice prompts or .wav files callers hear instead of a human operator when they call an organization that has Unified Messaging. The UM auto attendant lets callers move through the menu system, place calls, or locate users by using DTMF or voice inputs. However, for automatic speech recognition (ASR) or voice inputs to be used, you must enable ASR on the UM auto attendant.

Important:

In some companies (especially in East Asia), office telephones may not have letters on

the keys of the telephone. This makes the spell-the-name feature that uses the DTMF interface almost impossible without a working knowledge of the key mappings. By default, Unified Messaging uses the E.161 key mapping. For example, 2=ABC, 3=DEF, 4=GHI, 5=JKL, 6=MNO, 7=PQRS, 8=TUV, and 9=WXYZ. When a combination of letters and numbers is inputted, for example "Mike1092", the numeric digits are mapped to themselves. For an e-mail alias of "Mike1092" to be entered correctly, the user must press the numbers 64531092. Also, there won't be a telephone key equivalent for characters other than A-Z and 0-9. Therefore, these characters shouldn't be entered. For example, the e-mail alias "mike.wilson" would be entered as 6453945766. Even though there are 11 characters to be input, only 10 digits are entered by the user because the period (.) doesn't have a digit equivalent.

The UM auto attendant:

- Provides corporate or informational greetings.
- Provides custom corporate menus so that you can link a menu option to another auto attendant to have more than one level.
- Provides a directory search function that enables a caller to search an organization's directory for a name.
- Enables a caller to connect to the telephone of, or leave a message for, members of the organization.

In Active Directory, each UM auto attendant created is represented as an object. There is no limit to the number of UM auto attendants you can create in Active Directory. Each auto attendant can support an unlimited number of extensions. A UM auto attendant is associated with one, and only one, UM dial plan. However, UM auto attendants can reference or link to other UM auto attendants.

An incoming call that is received from an external telephone number or an internal telephone extension is processed by a UM server and then sent to a UM auto attendant that has been created. The UM auto attendant is configured by the system administrator to use prerecorded voice (.wav) files that are then played over the telephone to the caller and that enable the caller to move through the UM menu system. When you configure a UM auto attendant, you can customize all the .wav files that are used to meet the needs of your organization. For more information about custom prompts in Unified Messaging, see Understanding Unified Messaging Audio Prompts.

For more information about message flow with UM auto attendants, see Unified Messaging Auto Attendant Call Processing.

Return to top

Auto Attendant with Multiple Languages

There are situations in which you may have to provide callers with auto attendants that have different languages. The language setting that's available on a UM auto attendant lets you configure the default prompt language on the auto attendant. When you're using the default system prompts for the auto attendant, the default prompt language is the language that the caller will hear when the auto attendant answers the incoming call. This language setting will affect only the default system prompts that are provided when the Unified Messaging server role is installed. This setting won't affect custom prompts that have been configured on an auto attendant. The language selected as the default for the auto attendant is based on the version of Exchange 2010 installed.

When you install the U.S.-English version of Exchange 2010, there will be only one language available to configure on UM auto attendants: U.S. English. However, if you install a localized version of Exchange 2010, for example, Japanese, you'll be able to configure the auto attendant you create to use Japanese or U.S. English as the default language. Additional UM language packs can be installed on a UM server to let you use other default language options on an auto attendant.

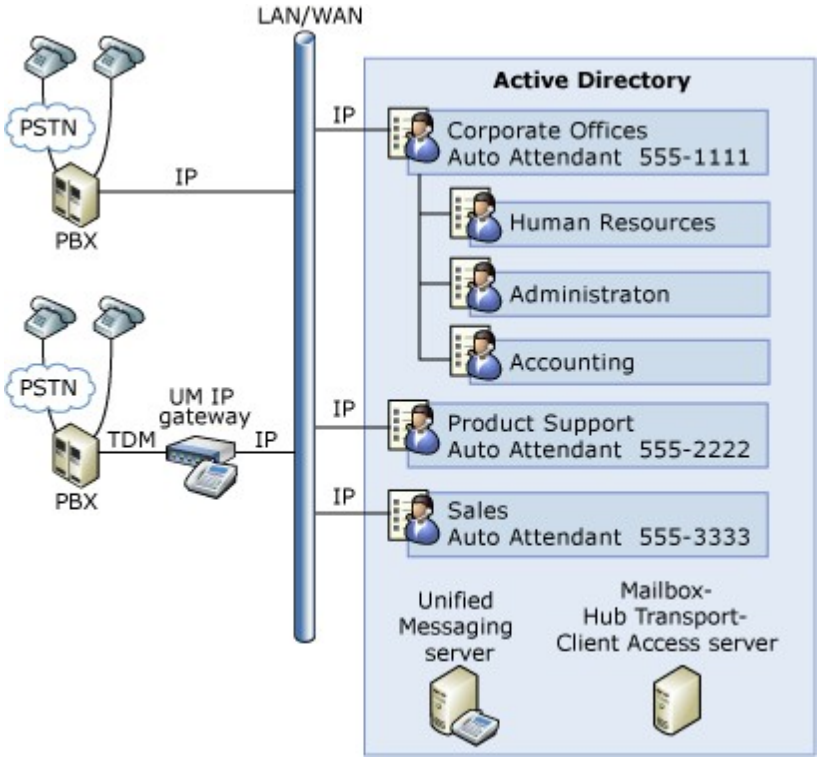
Caution:
You can't install UM language packs using the .msi file for the language.

For example, if you have a business that's based in the United States but requires a menu system that gives callers the options of moving through the system in U.S. English, Spanish, and French, you have to first install the UM language packs that you need. In this case, if you've installed the U.S.-English version of Exchange 2010, you'd install the UM language packs for Spanish and French. However, because a UM auto attendant can have only one language configured at a time, you'd create four auto attendants: a main auto attendant configured to use U.S. English and then one auto attendant for each language: U.S. English, Spanish, and French. You'd then configure the main auto attendant to have the appropriate key mappings to access the other auto attendants you've created for each language. In this example, the main auto attendant would answer the incoming call and the caller would hear, "Welcome to Contoso, Ltd. For English, press or say 1. For Spanish, press or say 2. For French, press or say 3."

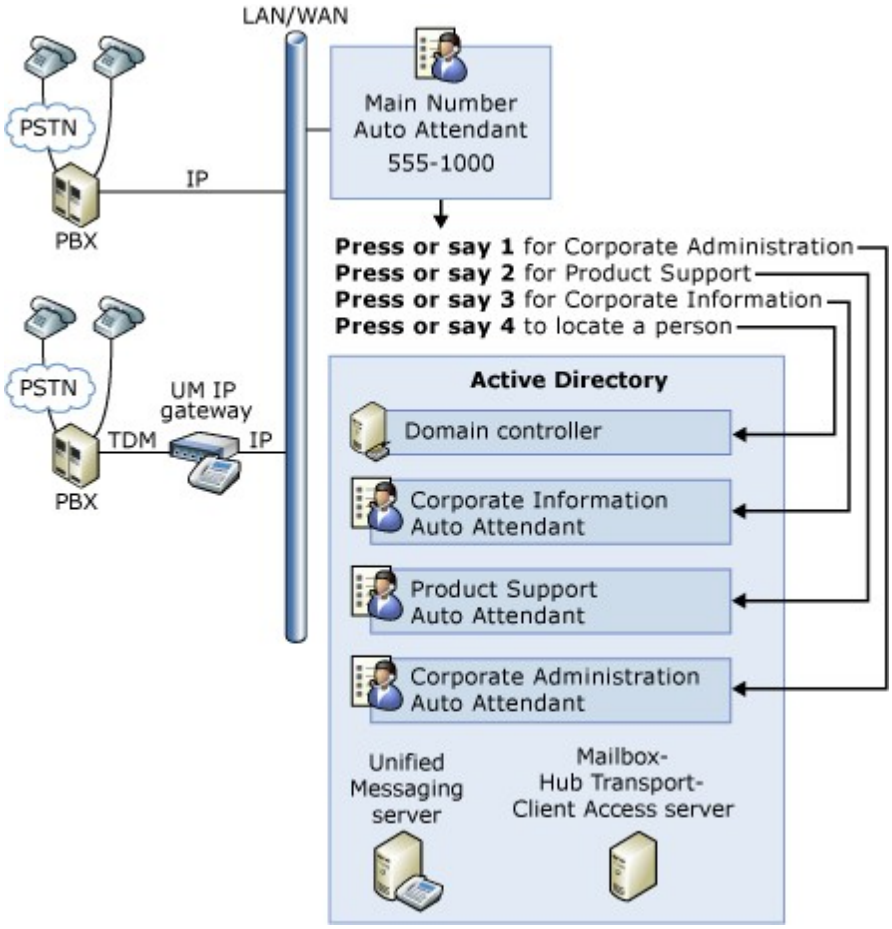
Auto Attendant Examples

The following examples demonstrate how you can use UM auto attendants together with Unified Messaging:

- **Example 1** At a company called Contoso, Ltd., external customers can use three external telephone numbers: 425-555-1111 (Corporate Offices), 425-555-2222 (Product Support), and 425-555-3333 (Sales). The Human Resources, Administration, and Accounting departments have internal telephone extensions and must be accessed from the Corporate Offices UM auto attendant.
  To create a UM auto attendant structure that supports this scenario, create and configure three UM auto attendants that have the appropriate external telephone numbers. Create three other UM auto attendants for each department in the Corporate Offices. Then you configure each UM auto attendant based on your requirements, such as the greeting type or other navigational information.
  The following figure is a graphical representation of how UM auto attendants can be used in Example 1.



- **Example 2** At a company called Contoso, Ltd., external customers call one main number for the business, 425-555-1000. When an external caller calls the main number, the UM auto attendant answers and prompts the caller by saying, "Welcome to Contoso, Ltd. Please press or say 'One' to be transferred to corporate administration. Please press or say 'Two' to be transferred to product support. Please press or say 'Three' to be transferred to corporate information. Please press or say 'Zero' to be transferred to the operator." To create a UM auto attendant structure that supports this scenario, you create a UM auto attendant that has customized extensions that route the call to the appropriate extension number.
  The following figure is a graphical representation of how UM auto attendants can be used in Example 2.



Return to top

UM Call Answering

This section describes how Unified Messaging handles message flow in different incoming call scenarios.

Unified Messaging handles the following types of incoming calls:

- Voice
- Outlook Voice Access
- Play on Phone
- Auto attendant

Unified Messaging depends on Active Directory to route incoming calls. For call answering to function correctly, each UM-enabled recipient must have a telephone extension number listed in Active Directory. The extension number for the recipient is listed in Active Directory and is mapped to the extension number that is configured on the user's UM-enabled Exchange mailbox. When a UM server answers a call, an Active Directory lookup is performed to locate the appropriate UM-enabled recipient, and then the message is routed to the recipient's mailbox.

Message Flow

Message flow in Unified Messaging is the process by which a message that's received by a UM server is routed in an Exchange 2010 organization.

Note:
In earlier versions of Microsoft Exchange, routing groups were used to route messages between bridgehead servers. In Exchange 2007 and Exchange 2010, bridgehead servers are known as Hub Transport servers. There are no routing groups in Exchange 2007 or Exchange 2010.

For example, in an incoming call scenario that includes incoming voice messages, a UM server uses the SMTP transport to submit the voice message to the Exchange 2010 server that has the Hub Transport server role installed. In a routing scenario that includes multiple Hub Transport servers, the incoming voice mail message is first submitted to the closest Hub Transport server and is then routed to the appropriate Mailbox server that contains the UM-enabled mailbox.

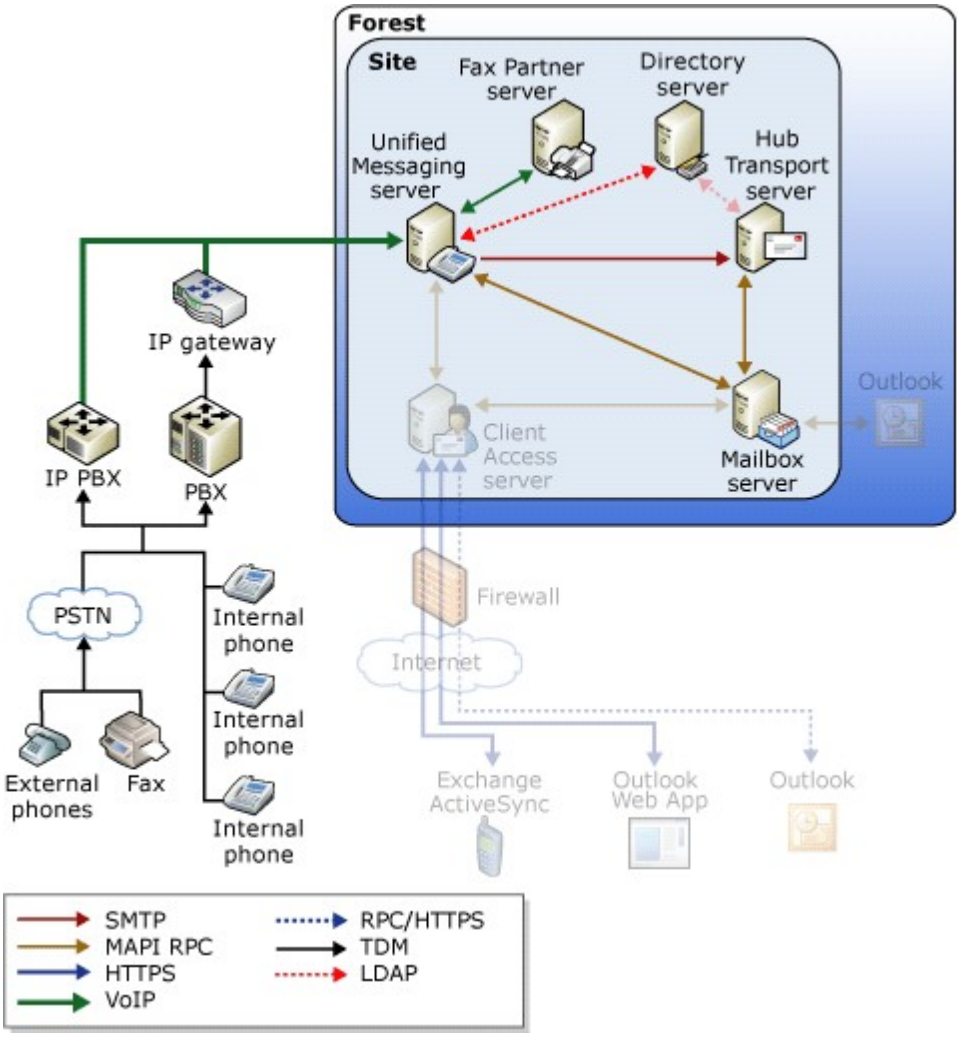
Note:
To make sure all incoming messages are transmitted and delivered to UM-enabled recipients, the UM servers use a spooling or retry algorithm. The UM servers try to connect to a Hub Transport server every 30 seconds to submit all messages that are stored on the UM server.

Return to top

Voice Call Processing

Voice calls that come in to an Exchange 2010 organization can be placed by callers who are inside or outside the organization. When a caller places a call to a UM-enabled user's telephone extension and the user isn't available to answer the call, the PBX forwards or routes the incoming call to an IP gateway and then to the UM server. In a UM system that uses an IP PBX, the IP PBX forwards the incoming message to the UM server. The IP gateway or the IP PBX translates or converts the incoming audio stream into RTP for incoming voice messages. The stream of IP data is then passed to the UM server. After the UM server receives the call, the UM server processes the message and determines how to route the message.

The following figure shows how incoming voice messages flow in an Exchange 2010 organization.



In this example, a call arrives at the PBX and is then forwarded to the UM pilot number. The pilot number is mapped to the hunt group that goes to the IP gateway. The IP gateway presents the call to the UM server. The UM server then receives SIP invitation header information such as who the call is for, who the caller is, and why the call was redirected. The UM server then looks up the number that was called and identifies which user was called and which dial plan the user belongs to. From there, the UM server looks in Active Directory to see whether the user is enabled for Unified Messaging. If the user is enabled for Unified Messaging, the caller receives a greeting for the user. Users' greetings are securely stored in their mailbox. This lets them manage their greetings. After callers reach the user's voice mail greeting, they can leave a voice message that will be sent to the user's mailbox. The UM server then records the message, locates a Hub Transport server, and submits the voice message to the Mailbox server that contains the UM-enabled user's mailbox.

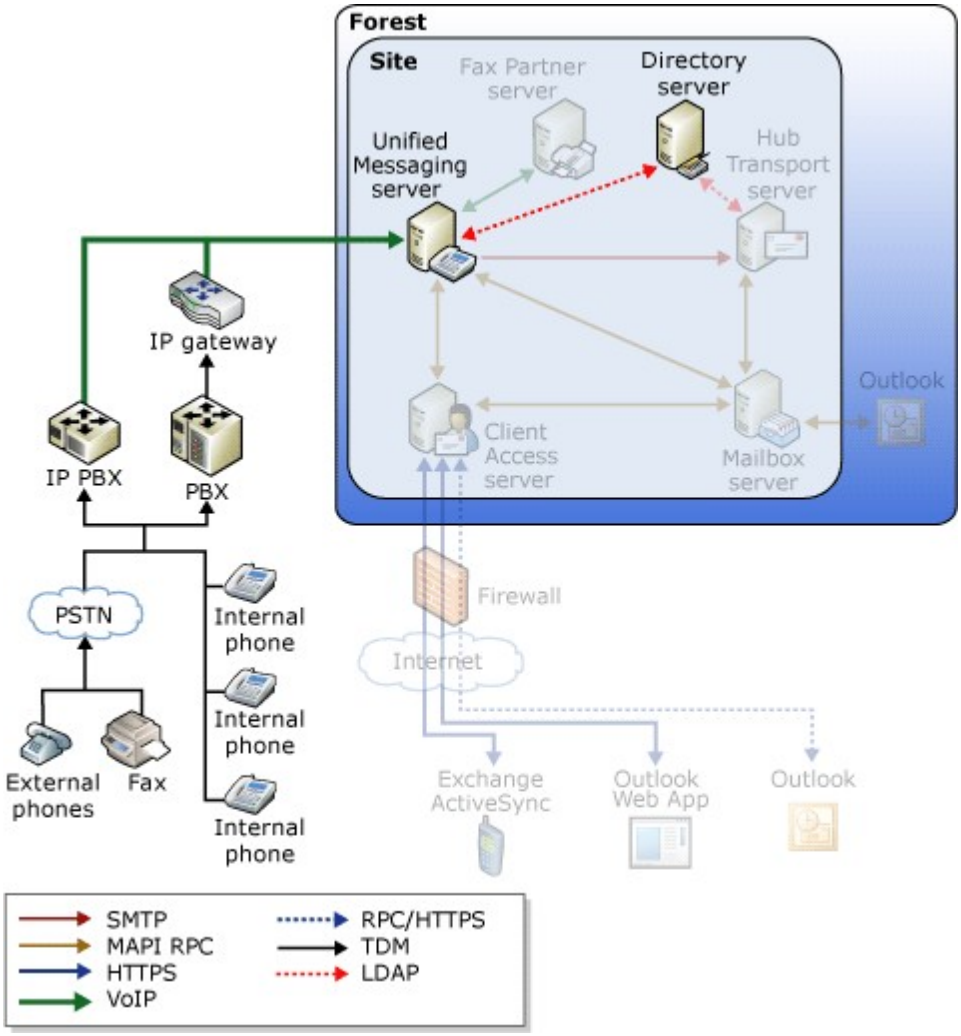
UM Auto Attendant Message Processing

When external or anonymous callers place a call by using an external business telephone number, or internal anonymous callers place a call to an internal extension number, they're presented with voice prompts to help them move through the UM menu system. The UM auto attendant is a set of voice prompts or .wav files that are played to callers instead of a human operator or receptionist when they call in to an organization that has Unified Messaging. Unified Messaging lets you create one or more auto attendants, depending on the needs of your organization.

Auto Attendant Message Flow

When a call is received by a UM server, the UM server performs a Lightweight Directory Access Protocol (LDAP) query to an Active Directory domain controller to determine how to handle the incoming call.

The following figure shows the message flow when UM auto attendants are used in an Exchange 2010 organization.



After you've created and enabled the auto attendant for your organization and associated it with a UM dial plan, the auto attendant can start to process calls. When a call for an auto attendant is received, it's first processed by the IP gateway and mapped to the appropriate hunt group. The call is then sent to the UM server. The UM server looks up the auto attendant object in Active Directory and then provides the correct auto attendant to handle the call.

Return to top

UM Outlook Voice Access Call Processing

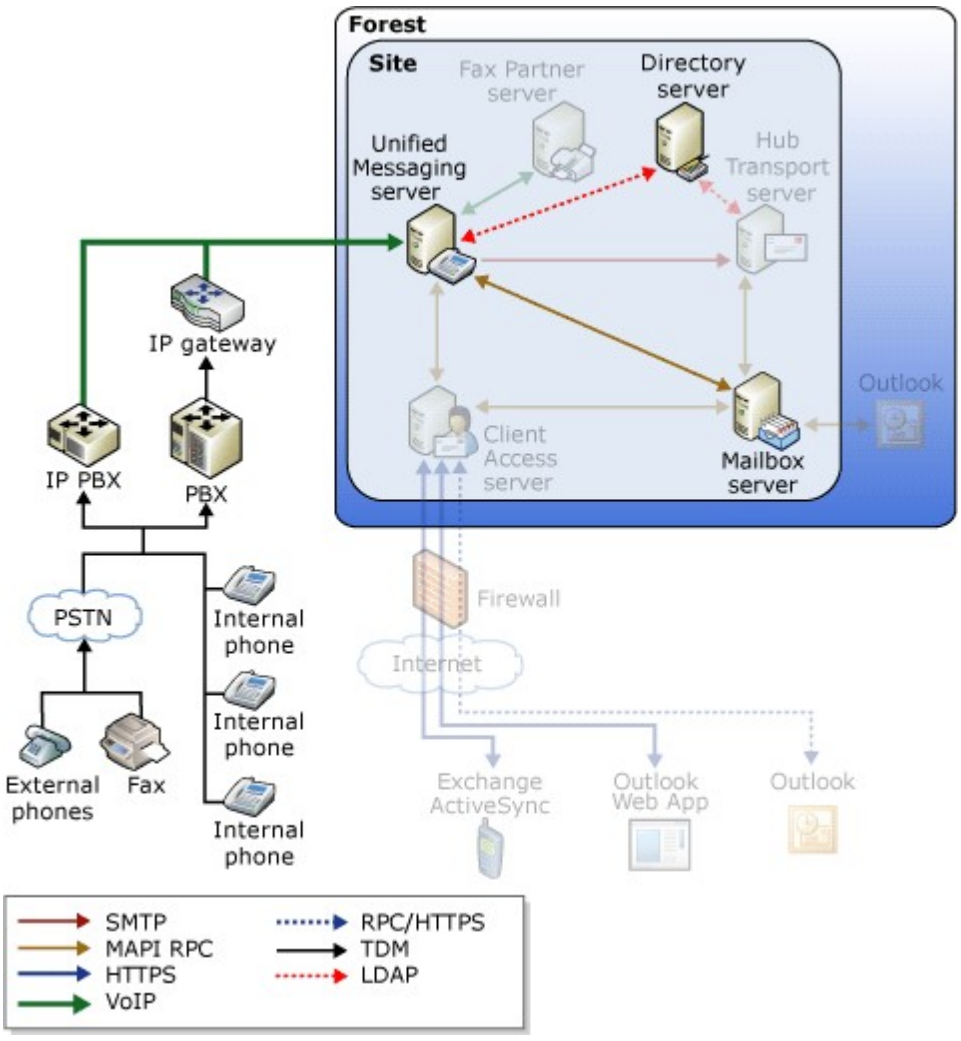
With Unified Messaging, UM-enabled users can access their e-mail, voice mail, contacts, and calendaring information using a standard analog, digital, or mobile telephone. Using Outlook Voice Access, a UM-enabled user can:

- Listen to new and saved e-mail and voice mail messages.
- Forward, reply to, save, and delete e-mail and voice mail messages.
- Interact with their calendar.
- Locate a person in the global address list or their personal Contacts.
- Send a voice message to a person.
- Change their PIN, spoken name, or greetings.

Outlook Voice Access Message Flow

Incoming calls that are received by a UM server from an Outlook Voice Access user are only routed to a Mailbox server to enable users to access their mailbox. However, if a message is submitted by using Outlook Voice Access, for example, a change in the schedule of a meeting, the message is first submitted to a Hub Transport server within the same Active Directory site as the UM server before it's routed to the recipient's mailbox.

The following figure shows how incoming calls and messages placed by subscribers or UM-enabled users flow in an Exchange 2010 organization.



When a user calls in to Outlook Voice Access, the PBX receives the call for the UM number and the IP gateway presents the call to the UM server. The UM server then looks up the user account information in Active Directory and collects information about the user. This

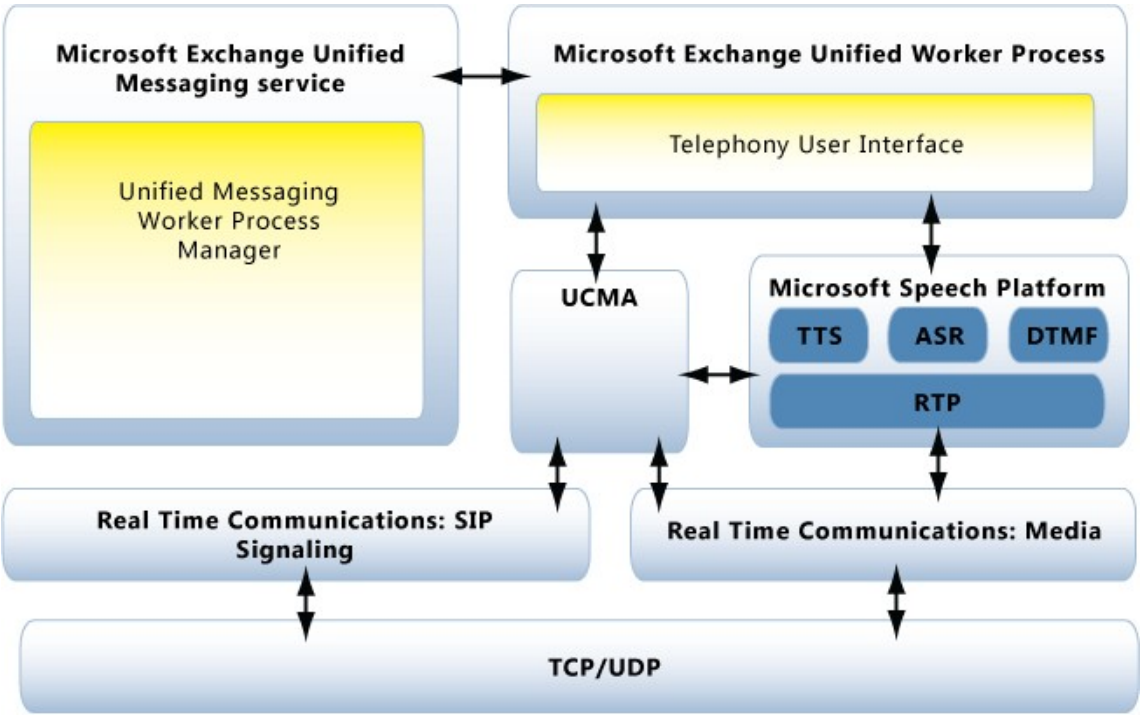
information includes dial plan information. If users place the call from their own extension, they're prompted for their PIN. The UM server contacts the Mailbox server and authenticates the user. From there, the UM server and the Mailbox server communicate information back to the user, as requested.

Overview of Unified Messaging Services and Components

When you install the Unified Messaging (UM) server role on a computer running Exchange 2010, several UM-specific components and services are installed. The Unified Messaging services and components installed by Setup enable a Unified Messaging server to answer and process incoming voice calls and enable users to interact with the Unified Messaging system by using Outlook Voice Access or by hearing a UM auto attendant when they call in to the Unified Messaging system.

Beginning with Exchange 2010 SP1, the UM server relies on Unified Communications Managed API v. 2.0 (UCMA) for its underlying SIP signaling and media, and speech processing. This dependency requires that the UCMA platform and prerequisites be installed on the UM server before Exchange 2010 UM SP1 installation or upgrade.

The following figure illustrates the relationships between Unified Messaging components.



Unified Messaging Services

The Microsoft Exchange Unified Messaging service is one of the two services that provide Unified Messaging services for your network. The Microsoft Exchange Unified Messaging service performs the following functions:

- Retrieves the dial plan configuration from Active Directory
- Loads the configuration information for monitoring UM worker processes from the Msexchangeum.config file

- Initializes the UM Worker Process Manager and the startup of a UM worker process
- Registers SIP endpoints

The Microsoft Exchange Unified Messaging service first accepts all incoming connections, and then reroutes those requests to a UM worker process that handles the incoming request. In addition, the Microsoft Exchange Unified Messaging service monitors any UM worker process that's created and ensures that the UM worker process is functioning correctly. If a UM worker process becomes unresponsive, the Microsoft Exchange Unified Messaging service stops the UM worker process and then creates a new UM worker process to replace it.

Note:

By default, each UM worker process will be recycled every seven days or 604,800 seconds. The setting can be found in the V14\bin\Msexchangeum.config file.

The Microsoft Exchange Unified Messaging service works with the Microsoft Exchange Speech Engine service to implement all the telephony features offered by Unified Messaging. The Microsoft Exchange Unified Messaging service handles call control and interacts with the Unified Communications Managed API 2.0 to handle the incoming media streams that are negotiated in the SIP signaling information between the Microsoft Exchange Unified Messaging service and a SIP-enabled telephony device such as an IP gateway or IP PBX. The following events happen when an incoming call is initiated by the Microsoft Exchange Unified Messaging service:

1. A call session is initiated by the Microsoft Exchange Unified Messaging service.
2. The Microsoft Exchange Unified Messaging service redirects the call to a UM worker process.
3. The UM worker process requests that a media session be established with Unified Communications Managed API 2.0, and then the UM worker process relays the media information back to the caller.
4. Unified Communications Managed API 2.0 provides a UDP port for the RTP stream.
5. The UM worker process uses the SIP signaling information to inform Unified Communications Managed API to end the call session when the RTP media stream is no longer needed.

UM Worker Process

A UM worker process is a process that's created during the startup of the Microsoft Exchange Unified Messaging service. UM worker processes interact with all incoming and outgoing requests received by the Microsoft Exchange Unified Messaging service.

The UM Worker Process Manager is also a component of the Microsoft Exchange Unified Messaging service. The UM Worker Process Manager handles the creation and monitoring of all the UM worker processes that are created. The UM Worker Process Manager creates new instances of a UM worker process based on the configuration settings located in the Msexchangeum.config file and also monitors the health of these processes. As a new incoming call arrives, the UM Worker Process Manager determines the appropriate instance of a UM worker process to redirect the call to. The UM worker process then interacts with the Unified Communications Managed API 2.0 components to correctly process incoming and outgoing requests. The UM worker process is responsible for the following startup tasks:

- Allocation of the runtime management objects
- Loading of the Unified Messaging configuration from Msexchangeum.config
- Registration of the process with Unified Communications Managed API 2.0
- Initialization of Simple Mail Transfer Protocol (SMTP) message submission

Unified Communications Managed API 2.0

Starting with Exchange 2010 SP1, the Unified Messaging server role relies on the Microsoft Unified Communications Managed API v. 2.0 (UCMA). UCMA simplifies the architecture of Unified Messaging and doesn't include any dependencies of other Windows-based or Exchange-based services. UCMA can be broken down into the following areas:

- **SIP Signaling** SIP signaling in UCMA v. 2.0 is very similar to SIP signaling in UCMA v. 1.0.
- **RTP Media** UCMA provides access to RTP media streams.
- **Collaboration** provides presence and conferencing support.

UCMA v. 2.0 is a managed-code platform that enables developers to build applications that provide access to and control over Enhanced Presence information, instant messaging, telephone and video calls, voice messaging, and audio/video conferencing. It enables both text-based and voice-based (speech technology-enabled) conversations and collaboration. UCMA v. 2.0 is intended to support the development of server side, middle-tier applications targeting Microsoft Office Communicator 2007 R2, Office Communications Server 2007 R2, or Microsoft Lync Server 2010 (the next generation of Office Communications Server) and Exchange 2010. It contains a SIP stack, a media stack, powerful speech engines for both Automatic Speech Recognition (ASR), as well as speech synthesis that's generated by Text-to-Speech (TTS).

UCMA v. 2.0 can be used to add communications capabilities to your business software and processes. It can also be used to create outbound applications such as alerts, notifications, or surveys, as well as inbound speech technology-enabled interactive voice response applications and automated agents. UCMA v.2.0 provides access to the presence information available in Communications Server 2007 R2 and can be used to build role agents that use Microsoft Enhanced Presence information to streamline communications between people.

UCMA v.2 makes more advanced developer scenarios possible, for applications such as automated call distributors, which perform skill-based routing; for conferencing services, such as conference access control; for custom client gateways that can interface with, for example, other communications networks, other Interactive Voice Response platforms, and with speech servers that are using the Microsoft ASR and TTS engines.

The UCMA platform replaces the Microsoft Exchange Speech Engine service and the Speech Engine service worker process (SESWorker.exe) and controls the following:

- The DTMF (touchtone) interface.
- ASR, which is used with the voice user interface (VUI) in Outlook Voice Access.
- The TTS engine that reads e-mail, voice mail, and calendar items and plays the menu prompts for callers.

UCMA v. 2.0 also supports the following features in Unified Messaging:

- ASR input recognition.
- DTMF (touchtone) input recognition.
- The TTS conversion process.
- Recording e-mail and voice mail messages.
- Playing e-mail and voice mail messages for users.

As a result of the integration of UCMA and Unified Messaging, you receive the following benefits when you integrate UM and Microsoft Lync Server 2010:

- Unified Messaging reports Quality of Experience (QoE) data to Lync Server 2010 Quality of Experience Monitoring or QMS servers. This is available in both on-premises and cross-premises integrated environments.
- UM doesn't drop the first incoming call if the first call to the UM server is being made from an Enterprise Voice user who's connected the Internet.

In earlier versions of Office Communications Server, the A/V Edge resources that were associated with the Office Communications Server pool didn't communicate with a specific UM server for a specific call. This led to less-than-optimal media quality in some scenarios.

With Exchange 2010 SP1, you can set, on a per UM-server basis, the Office Communications Server pool and associated A/V Edge server resources that should be used for all calls to and from that specific UM server.

Prerequisites for UCMA

The Unified Messaging server role in Exchange 2010 SP1 relies on the following, and requires that they be installed prior to installing SP1:

- Windows Server 2008 or Windows Server 2008 R2 - Installing Windows Server 2008 R2
- Microsoft .NET Framework 3.5 Service Pack 1 (SP1) - Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64 updates - Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64

Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu) - Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0)

- Microsoft Speech Platform - Server Runtime (Version 10.1) - (SpeechPlatformRuntime.msi).
- Unified Communications Managed API 2.0, Core Runtime (64-bit) (UcmaRuntimeWebDownloadX64.msi).

Note:

If you've already installed a version of the Unified Communications Managed API 2.0 on a Client Access server in your Exchange organization, you must also install a hotfix. For information about how to install the required hotfix, see OCS 2007 R2 Web Service Provider Hotfix KB 981256.

For more information about UCMA, see UCMA 2.0 Core Architecture.

For more information about the grammar files used in Unified Messaging, see Understanding Automatic Speech Recognition Directory Lookups.

Service Ports

The Microsoft Exchange Unified Messaging service and the UM worker process use multiple Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) service ports to communicate with IP gateways. The Microsoft Exchange Unified Messaging service and the UM worker process use Session Initiation Protocol (SIP) over TCP. By default, the Microsoft Exchange Unified Messaging service listens on both TCP port 5060 in Unsecured mode and TCP port 5061 when mutual Transport Layer Security (mutual TLS) is used. Each UM worker process that's created listens on port 5065 and 5067 (unsecured) and 5066 and 5068 (secured). But when an IP gateway or IP PBX sends Realtime Transport Protocol (RTP) traffic to the Speech Engine service worker process, the IP gateway or IP PBX will use a valid UDP port that ranges from 1024 through 65535.

A TCP control port is also used on a Unified Messaging server. When a UM worker process is created, the Microsoft Exchange Unified Messaging service passes the appropriate configuration options to the UM worker process. The configuration options sent include the parameters for the TCP control port number that's used for communication between the Microsoft Exchange Unified Messaging service and the UM worker process. The TCP control port that's chosen will be between TCP ports 16,000 to 17,000.

Return to top

1.9.1.2 Understanding Unified Messaging Components

Understanding Unified Messaging Components

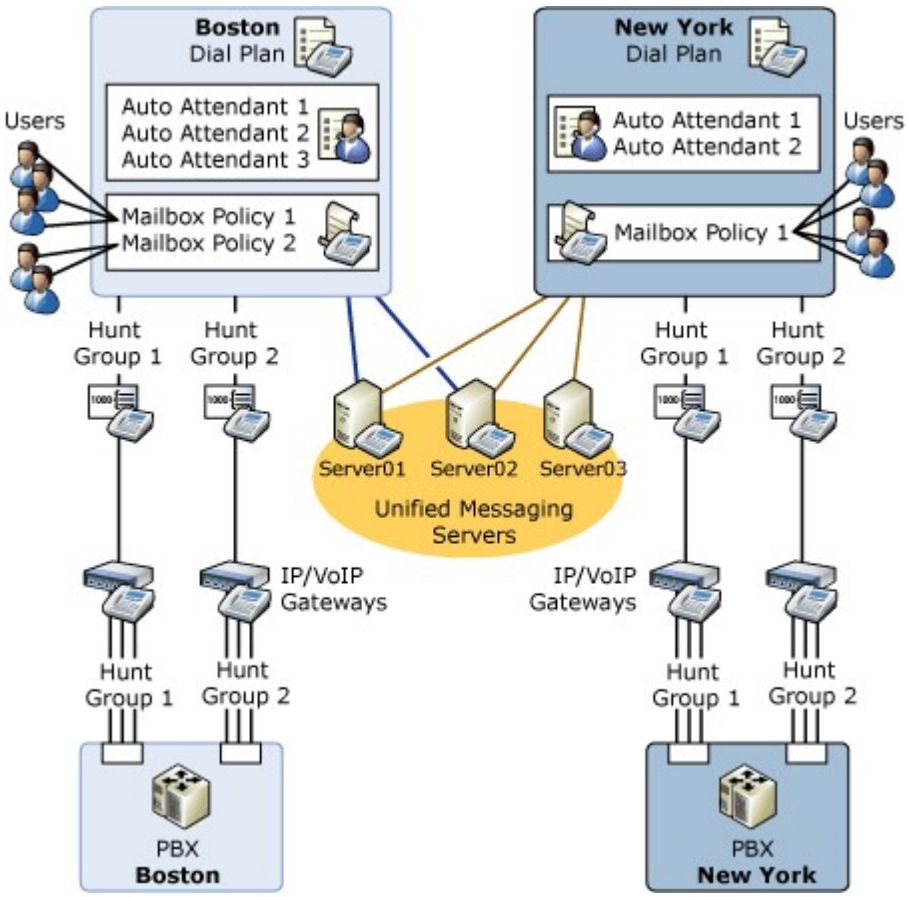
Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-03*

Active Directory objects are required for the deployment and operation of Microsoft Exchange Server 2010 Unified Messaging (UM). The UM Active Directory objects connect the telephony infrastructure and the Exchange 2010 UM Active Directory environment.

UM Active Directory Objects

The UM Active Directory objects enable the integration of Unified Messaging into Active Directory and the existing telephony infrastructure. Active Directory acts as a container for all the UM objects that are created and their configuration settings. Each UM object within Exchange 2010 is necessary to support Unified Messaging in an Active Directory environment. Some UM Active Directory objects are created to logically represent a telephony hardware device but others are created to represent a telephony dial plan for an organization or to support a specific feature of Unified Messaging. The following figure shows the relationships between the UM objects found in Active Directory.



There's a tightly integrated and interconnected relationship between the UM Active Directory objects and the features available in Unified Messaging. To successfully plan and deploy Unified Messaging in your organization, you need to fully understand this logical

relationship between each of the UM objects.

For more information about the UM Active Directory objects, see:

- Understanding Unified Messaging Dial Plans
- Understanding Unified Messaging Mailbox Policies
- Understanding Unified Messaging IP Gateways
- Understanding Unified Messaging Hunt Groups
- Understanding Unified Messaging Auto Attendants
- Understanding Unified Messaging Servers
- Understanding Unified Messaging Users

1.9.1.2.1 Understanding Unified Messaging Dial Plans

Understanding Unified Messaging Dial Plans

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-10*

Unified Messaging (UM) dial plans are integral to the operation of Microsoft Exchange Server 2010 Unified Messaging and are required to successfully deploy Unified Messaging on your network. The following sections discuss UM dial plans and how UM dial plans are used when you deploy Exchange 2010 Unified Messaging on your network.

Overview of UM Dial Plans

Although Unified Messaging has many Active Directory objects that must be created and configured during deployment, UM dial plan objects are the central component of the Unified Messaging system. A UM dial plan object is an Exchange 2010 organization-wide object created in Active Directory. It represents sets or groupings of Private Branch eXchanges (PBXs) or IP PBXs that share common user extension numbers. In practical terms, all users' extensions hosted on PBXs or IP PBXs within a dial plan contain the same number of digits. Users can dial one another’s telephone extensions without appending a special number to the extension or dialing a full telephone number.

A UM dial plan mirrors a telephony dial plan. A telephony dial plan is configured on PBXs or IP PBXs.

For more information about telephony components, see Understanding Telephony Concepts and Components.

In Unified Messaging, the following UM dial plan topologies can exist:

- A single dial plan that represents a subset of extensions or all extensions for an organization with one PBX or IP PBX.
- A single dial plan that represents a subset of extensions or all extensions for an organization with multiple networked PBXs or IP PBXs.
- Multiple dial plans that represent a subset of extensions or all extensions for an organization with one PBX or IP PBX.
- Multiple dial plans that represent a subset of extensions or all extensions for an organization with multiple PBXs or IP PBXs.

Users who belong to the same dial plan have these characteristics:

- An extension number that uniquely identifies the user mailbox in the dial plan.
- The ability to call or send voice messages to other members in the dial plan using only the extension number.

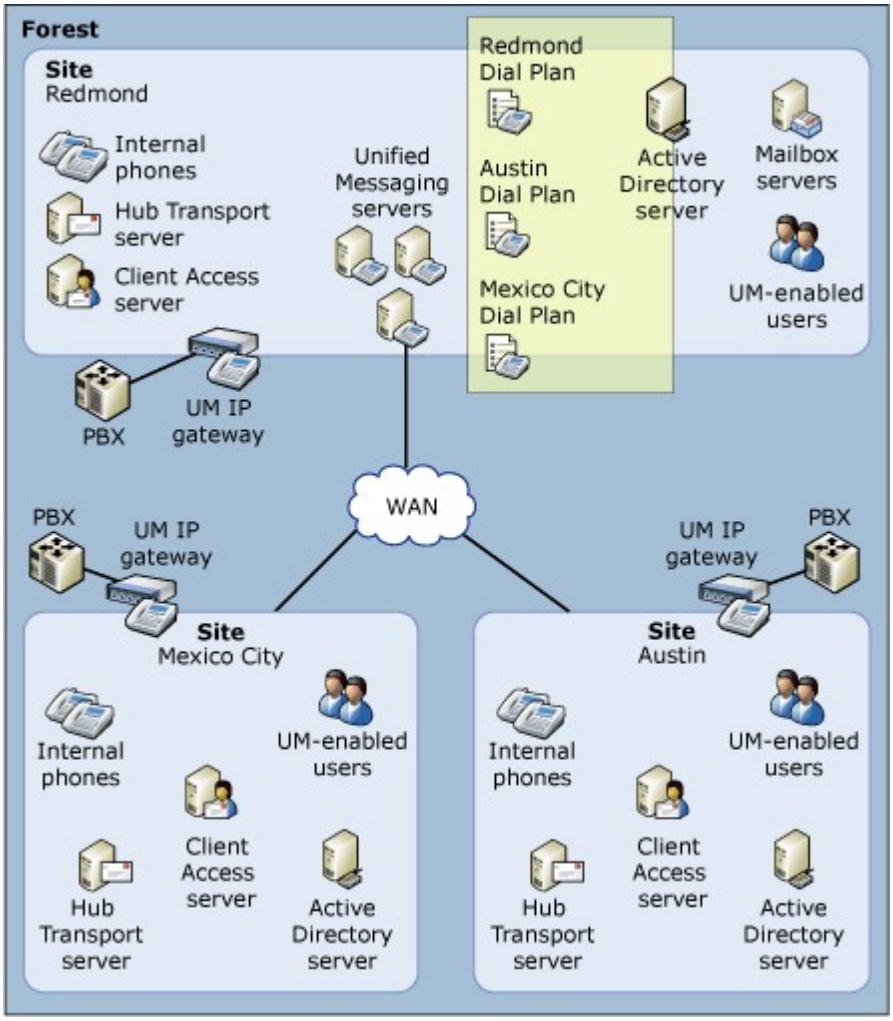
For more information about how to enable a user for Unified Messaging, see Enable a User for Unified Messaging.

UM dial plans are implemented in Exchange 2010 Unified Messaging to make sure that user telephone extensions are unique. In some telephony networks, multiple PBXs or IP PBXs can exist. In these telephony networks, there could be two users in Active Directory who have the same telephone extension number. UM dial plans resolve this situation. You can put the two users into two separate UM dial plans. This makes their extensions unique.

Note:

A user can be a member of only one UM dial plan. You can also use a UM dial plan to establish a common set of policies for a group of users. For example, you can enable different languages for different UM dial plans, or you can enable different features for different UM dial plans.

The following figure illustrates how UM dial plans can be used in an organization that has a single forest and multiple physical sites.



How Dial Plans Work

When you integrate a telephony network with Exchange 2010 Unified Messaging, there must be a hardware device called an IP gateway that connects your telephony network to your IP-based network. IP gateways convert circuit-switched protocols found in a telephony network to a data-switched protocol such as IP. Each IP gateway in your organization is represented by a UM IP gateway object in Active Directory. For more information about UM IP gateways, see Understanding Unified Messaging IP Gateways.

Exchange 2010 Unified Messaging requires that you create at least one UM dial plan and that the UM dial plan has a Unified Messaging server and a UM IP gateway associated with it. After you install the Unified Messaging server role on an Exchange 2010 computer, you must associate the Unified Messaging server with at least one UM dial plan before it will answer calls. You can also associate a single Unified Messaging server with multiple UM dial plans. After the Unified Messaging server is associated with a UM dial plan, you must create a UM IP gateway and associate it with the UM dial plan that was created.

Important:

Each time you create a UM dial plan, a UM mailbox policy will also be created. The UM mailbox policy will be named *<Dial Plan Name>* Default Policy.

When you create the first UM IP gateway and specify a UM dial plan at the time you create it, a default UM hunt group is also created. Creating and associating these objects

in Active Directory enables the Unified Messaging server to receive calls from the IP gateway and then process incoming calls for users who are associated with the UM dial plan. When a call comes in to the IP gateway, it forwards the call to a Unified Messaging server, and the Unified Messaging server tries to match the extension number of the user to the associated UM dial plan.

For more information about how to add a Unified Messaging server to a UM dial plan, see Add a UM Server to a Dial Plan.

Types of Dial Plans

A Uniform Resource Identifier (URI) is a string of characters that's used to identify or name a resource. In Unified Messaging, the main purpose of a URI is to enable Voice over IP (VoIP) devices to communicate with other devices using specific protocols. A URI defines the naming and numbering format or scheme used for the calling and called party information contained within a Session Initiation Protocol (SIP) header for an incoming or outgoing call.

The types of UM dial plans you create in Exchange 2010 Unified Messaging will depend on the URI types supported by the IP gateways, PBXs, or IP PBXs in your organization. When you create a dial plan, you should know the specific URI types supported by your PBXs or IP PBXs. There are three formats or URI types that can be configured on UM dial plans:

- Telephone Extension
- SIP URI
- E.164

In Unified Messaging, each time you create a dial plan, the dial plan will, by default, be created to use the telephone extension URI format type. However, you can configure the URI type when you create a dial plan using the New Dial Plan wizard or the **New-UMDialPlan** cmdlet. After you create a dial plan, you will be unable to change the URI type.

Telephone Extension

The Telephone Extension URI type is the most common type of UM dial plan and is used with PBXs and IP gateways. When you configure a telephone extension (TelExtn) dial plan, the IP gateways and IP PBXs must support the telephone extension (TelExtn) URI type. When the IP gateway or IP PBX communicates with a Unified Messaging server associated with a dial plan, the dial plan must then be configured to support the TelExtn URI type. Generally, most PBXs today support the telephone extension URI type. However, the IP gateway and the UM dial plan must also support the telephone extension URI type.

When a call is received by the PBX or IP PBX and the UM-enabled user isn't available to answer the call, the PBX or IP PBX will forward the call to the IP gateway. In the header for the SIP packet received by the Unified Messaging server from the IP gateway, the calling and called party information will be listed in one of the following formats:

- Tel:512345
- 512345@<*IP address*>

The telephone extension (TelExtn) format used is based on the configuration of the IP gateway or IP PBX.

SIP URI

Session Initiation Protocol (SIP) is a standard protocol for initiating interactive user sessions that involve multimedia elements such as video, voice, chat, and gaming. SIP is a request-to-response based protocol that answers requests from clients and responses from servers. Clients are identified by SIP URLs. Requests can be sent through any transport protocol, such as UDP or TCP. SIP determines the endpoint to be used for the

session by selecting the communication media and media parameters.

When you create a new dial plan, you have the option of creating a SIP URI dial plan that can be used in an environment that has Microsoft Office Communications Server 2007 deployed or in organizations that have IP PBXs. However, in organizations that have IP PBXs, the IP PBXs must also support SIP URIs and SIP routing.

A SIP URI is the SIP addressing scheme used to call another person using SIP. In other words, a SIP URI is a user's SIP phone number. The SIP URI resembles an e-mail address and is written in the following format: sip*:<user name>@<domain or IP address>*:*Port*. When a SIP-enabled IP PBX or an IP gateway is used to send the call to a Unified Messaging server, the device will send only the SIP URI for the calling and called party in the SIP header and will not include extension numbers.

E.164

E.164 is a standard numbering format that defines the international public telecommunication numbering plan used in the Public Switched Telephone Network (PSTN) and some data networks. E.164 defines the format of telephone numbers. E.164 numbers can have a maximum of 15 digits and are usually written with a plus sign (+) before the digits of the telephone number. To dial an E.164-formatted telephone number from a telephone, the appropriate international call prefix must be included in the number dialed. In an E.164 numbering plan for public telephone systems, each assigned number contains a country code (CC), a national destination code (NDC), and a subscriber number (SN).

When you create a new dial plan, you have the option to create an E.164 dial plan. However, if you create and configure an E.164 dial plan, the PBXs and IP PBXs must support E.164 routing. The SIP header received by the Unified Messaging server from an IP gateway associated with an E.164 dial plan will include the E.164-formatted telephone number for the calling and called party information and will be listed in the following format: Tel:+14255550123.

VoIP Security

Unified Messaging servers that have Exchange 2010 installed can communicate with IP gateways, IP PBXs, and other Exchange 2010 computers in either Unsecured, SIP secured, or secured mode, depending on how the UM dial plan is configured. A Unified Messaging server can operate in any mode configured on a dial plan because the Unified Messaging server is configured to listen on TCP port 5060 for unsecured requests and TCP port 5061 for secured requests at the same time. A Unified Messaging server can be associated with a single or multiple UM dial plans and can be associated with dial plans that have different VoIP security settings. A single Unified Messaging server can be associated with dial plans configured to use a combination of unsecured, SIP secured, and secured modes.

By default, when you create a UM dial plan, it will communicate in unsecured mode, and the Unified Messaging servers associated with the UM dial plan will send and receive data from IP gateways, IP PBXs, and other Exchange 2010 computers without using encryption. In unsecured mode, neither the Realtime Transport Protocol (RTP) media channel nor the SIP signaling information will be encrypted. You can use the **Get-UMDialPlan** cmdlet in the Exchange Management Shell to determine the security setting for a specific UM dial plan.

You can configure a Unified Messaging server to use mutual Transport Layer Security (TLS) to encrypt the SIP and RTP traffic sent and received from other devices and servers. When you add a Unified Messaging server to a UM dial plan and configure the dial plan to use SIP secured, only the SIP signaling traffic will be encrypted, and the RTP media channels will still use TCP, which is not encrypted. However, if you add a Unified Messaging server to a UM dial plan and configure the dial plan to use Secured mode, both the SIP signaling traffic and the RTP media channels are encrypted. An encrypted signaling media channel

that uses Secure Realtime Transport Protocol (SRTP) also uses mutual TLS to encrypt the VoIP data.

You can configure the VoIP security mode either when you're creating a new dial plan or after you create a dial plan using the EMC or the **Set-UMDialPlan** cmdlet in the Shell. When you configure the UM dial plan to use SIP secured or Secured mode, the Unified Messaging servers associated with the UM dial plan will encrypt the SIP signaling traffic or the RTP media channels or both. However, to be able to send encrypted data to and from a Unified Messaging server, you must correctly configure the UM dial plan, and devices such as IP gateways or IP PBXs must support mutual TLS.

For more information about VoIP security and UM dial plans, see Understanding Unified Messaging VoIP Security.

Outlook Voice Access

There are two types of callers who access the Unified Messaging system using the subscriber access number configured on a UM dial plan: unauthenticated callers and authenticated callers. When callers dial the subscriber access number configured on a dial plan, they are considered anonymous or unauthenticated until they input information including their voice mail extension and a PIN. However, the only option available to anonymous or unauthenticated callers is the directory search feature. After callers input their voice mail extension and their PIN, they will be authenticated and given access to their mailbox. After they gain access to the system, they are using the Outlook Voice Access feature. Outlook Voice Access is a series of voice prompts that give the caller access to e-mail, voice mail, calendar, and other information. Outlook Voice Access lets authenticated callers navigate their personal information in their mailbox, place calls, or locate users using dual tone multi-frequency (DTMF), also known as touchtone, inputs or voice inputs.

Important:

In some companies (especially in East Asia), office telephones may not have letters on the keys of the telephone. This makes the spell-the-name feature using the touchtone inputs almost impossible to use, without a working knowledge of the key mappings. By default, Exchange 2010 Unified Messaging uses the E.161 key mapping. For example, 2=ABC, 3=DEF, 4=GHI, 5=JKL, 6=MNO, 7=PQRS, 8=TUV, 9=WXYZ.
When inputting the combination of letters and numbers, for example, Jim1092, the numeric digits are mapped to themselves. For an e-mail alias of Jim1092 to be entered correctly, the user must press the numbers 5461092. Also, for characters other than A-Z and 0-9, there won't be a telephone key equivalent. Therefore, these characters shouldn't be entered. For example, the e-mail alias jim.wilson would be entered as 546945766. Even though there are 10 characters to be input, only 9 digits are entered by the user because the period (.) doesn't have a digit equivalent.

Subscriber Access Numbers

After you've created a UM dial plan, you need to add at least one subscriber access number. Subscriber access numbers are also called pilot numbers. This number is used by Outlook Voice Access users to access their mailboxes and lets them search the directory.

By default, when you create a UM dial plan, no subscriber access number is configured. To enable subscriber access, you must configure at least one telephone or extension number. The number of alphanumeric characters in the subscriber access number can't exceed 20. After you configure this number on the dial plan, this number will be displayed in the Microsoft Office Outlook 2007, Outlook 2010, and Outlook Web App voice mail options.

You can use the **Enter the telephone number to associate** field on the UM dial plan to add a telephone number or extension that a user will call to access the Unified Messaging system using Outlook Voice Access. In most cases, you'll enter an extension number or an

external telephone number. However, because this field accepts alphanumeric characters, a SIP URI can be used if you're using an IP PBX.

Depending on the needs of your organization, you may need one or more subscriber access numbers. You can have a single subscriber access number configured on a single UM dial plan or you can have multiple subscriber access number in a single UM dial plan, but you can't have a single subscriber access number that spans multiple UM dial plans.

1.9.1.2.2 Understanding Unified Messaging Mailbox Policies

Understanding Unified Messaging Mailbox Policies

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Components >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Unified Messaging (UM) Active Directory mailbox policies are required when you enable users for Exchange 2010 Unified Messaging. You create UM mailbox policies to apply a common set of policies or security settings to a collection of UM-enabled mailboxes. UM mailbox policies are used to set Unified Messaging settings for UM-enabled users, such as the following:

- PIN policies.
- Dialing restrictions.
- Other general UM mailbox policy properties.

For example, you can create a UM mailbox policy to increase the level of PIN security by reducing the maximum number of sign-in failures for a specific group of UM-enabled users, such as executives.

Looking for management tasks related to Unified Messaging mailbox policies? See Managing UM Mailbox Policies.

UM Mailbox Policies

UM mailbox policies are created in the Configuration container in the Active Directory directory service using the Exchange Management Shell or the Exchange Management Console. By default, a single UM mailbox policy is created every time you create a UM dial plan. The new UM mailbox policy is associated with the UM dial plan and part of the dial plan name is included in the display name of the UM mailbox policy. However, you can create additional UM mailbox policies based on the needs of your organization. Although a single UM mailbox policy is required to enable users for Unified Messaging, you can create additional UM mailbox policies and apply a common set of mailbox policy settings for other groups of users.

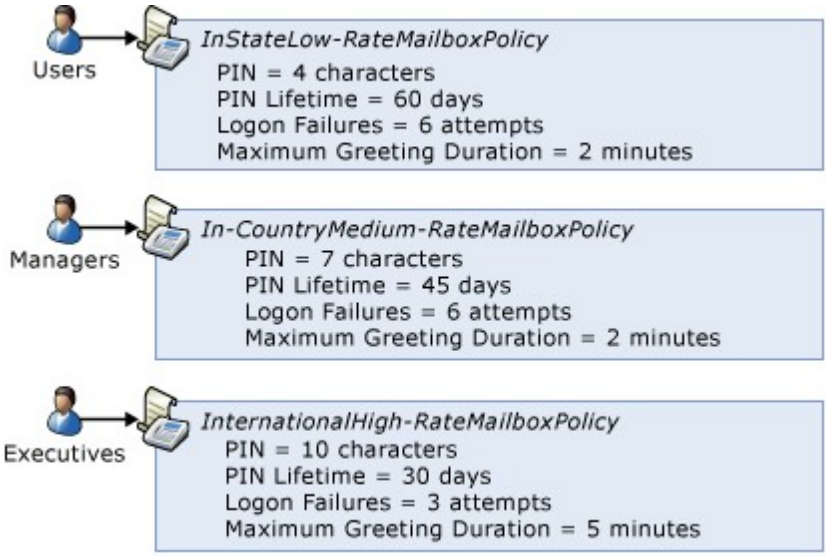
Each UM-enabled user's mailbox must be linked to a single UM mailbox policy. After you create a UM mailbox policy, you link one or more UM-enabled mailboxes to the UM mailbox policy. This lets you control PIN security settings such as the minimum number of digits in a PIN or the maximum number of logon attempts for the UM-enabled users who are associated with the UM mailbox policy. If you prefer, you can also control message text settings or dialing restrictions for the same or a different group of UM-enabled mailboxes.

Multiple UM-enabled users can be linked to a single UM mailbox policy. However, a single user can be associated with only one UM mailbox policy. When a user is enabled for

Unified Messaging, you must specify an existing UM mailbox policy to be linked to the UM-enabled user's mailbox. After you create a new UM mailbox policy and link it to a UM dial plan, the UM mailbox policy settings defined are then applied to the UM-enabled users. The settings defined on a UM mailbox policy apply only to UM-enabled users to which the UM dial plan is linked and the UM mailbox policy is associated.

Unified Messaging Policy Examples

The following figure illustrates how UM mailbox policies can be created to control dialing restrictions and PIN security settings for three different groups.



1.9.1.2.3 Understanding Unified Messaging IP Gateways

Understanding Unified Messaging IP Gateways

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Components >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-06-18*

The Unified Messaging (UM) IP gateway is a container object that logically represents a physical IP gateway hardware device. Before the IP gateway can be used to process Unified Messaging calls, the IP gateway must be represented by an object in the Active Directory directory service.

Contents

Overview of IP Gateways

Traditionally, *gateway* is a term that describes a physical device that connects two incompatible networks. With Microsoft Exchange Server 2010 Unified Messaging and other Unified Messaging solutions, the IP gateway is used to translate between the Public Switched Telephone Network (PSTN)/Time Division Multiplex (TDM) or circuit-switched based telephony network and an IP or packet-switched data network.

Note:

A packet-switched network is a network in which packets (messages or fragments of messages) are individually routed between nodes that may be shared by many other nodes. This contrasts with a circuit-switched network that sets up a dedicated connection between the two nodes for their exclusive use for the duration of the communication.

Exchange 2010 Unified Messaging relies on the ability of the IP gateway to translate TDM or telephony circuit-switched based protocols, such as Integrated Services Digital Network (ISDN) or QSIG, from a Private Branch eXchange (PBX) to protocols based on Voice over IP (VoIP) or IP, such as Session Initiation Protocol (SIP), Realtime Transport Protocol (RTP), or T.38 for real-time facsimile transport.

Types of IP Gateways

Although there are many types and manufacturers of PBXs, IP gateways, and IP PBXs, there are basically two types of IP gateway component configurations:

- **IP PBX** A single device
- **PBX (legacy) and an IP gateway** Two separate components

To support Exchange 2010 Unified Messaging, one or both types of IP/VoIP device configurations are used when connecting a telephony network infrastructure to a data network infrastructure.

IP Gateway Objects

The UM IP gateway is an Active Directory container object that contains one or more Active Directory UM hunt groups and other UM IP gateway configuration settings. UM IP gateways are created within Active Directory to logically represent a physical hardware device called an IP gateway. The UM IP gateway can represent either an IP gateway or an IP PBX. The combination of the UM IP Gateway object and a UM Hunt Group object establishes a logical link between an IP gateway hardware device and a UM dial plan.

After the UM IP gateway is created, the IP gateway can be linked to or associated with a single or multiple UM hunt groups and UM dial plans. The UM hunt group provides a link between the UM IP gateway and a UM dial plan. By creating multiple UM hunt groups, you can associate a single UM IP gateway with multiple UM dial plans.

After you create a UM IP Gateway object, the Unified Messaging server associated with the UM IP gateway will send a SIP OPTIONS request to the IP gateway to ensure that the IP gateway is responsive. If the IP gateway doesn't respond to the SIP OPTIONS request from the Unified Messaging server, the Unified Messaging server will log an event with ID 1400 stating that the request failed. To resolve this issue, ensure that the IP/VoIP is available and online and that the Unified Messaging configuration is correct.

A Unified Messaging server communicates only with IP gateways or IP PBXs listed as a trusted SIP peer. In some cases, if two IP gateways are configured to use the same IP address, an event with ID 1175 will be logged. Unified Messaging protects against unauthorized requests by retrieving the internal URL of the Unified Messaging Web services virtual directory located on the server that has the Client Access server role installed, and then uses the URL to build the list of FQDNs for the trusted SIP peers. When two FQDNs are resolved to the same IP address, this event will be logged.

Note:
Before an IP gateway can be used to process calls, a UM IP gateway must be associated with at least one UM dial plan. Also, at least one Unified Messaging server must be associated with at least one UM dial plan.

Enabling and Disabling UM IP Gateways

By default, IP gateways are left in an enabled state after they're created. However, the UM IP gateway can be enabled or disabled. If you disable a UM IP gateway, it can be in one of two disabled modes. The first disabled mode forces all associated Unified Messaging servers to drop existing calls. The second disabled mode forces the Unified Messaging server associated with the UM IP gateway to stop handling any new calls presented by the IP gateway.

Note:
If a UM IP gateway is deleted, the Unified Messaging servers associated with the IP gateway will no longer be able to accept or process new call requests from the IP gateway.

1.9.1.2.4 Understanding Unified Messaging Hunt Groups

Understanding Unified Messaging Hunt Groups

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-03*

This topic discusses Microsoft Exchange Server 2010 Unified Messaging (UM) hunt groups and how UM hunt groups must be implemented in your Exchange 2010 organization to support Unified Messaging.

Looking for management tasks related to Unified Messaging hunt groups? See Managing UM Hunt Groups.

Contents

What Is a Hunt Group?

Hunt group is a term used to describe a group of Private Branch eXchange (PBX) or IP PBX resources or extension numbers that are shared by users. Hunt groups are used to efficiently distribute calls into or out of a specific business unit. For example, a PBX or IP PBX might be configured to have 10 extension numbers for the sales department. The 10 sales extension numbers would be configured as one hunt group. In a PBX or IP PBX, hunt groups are used to efficiently locate an open line, extension, or channel when an incoming call is received.

In a telephony network, a hunt group is defined as a set of extension numbers grouped as a single logical unit. When an incoming call is received, the PBX or IP PBX uses the hunt group or group of extensions that are defined to *hunt* for an available or open line, extension, or channel that can be used to receive the call.

There are multiple algorithms or methods that have been created to be used by a PBX or IP PBX to define how the open line, extension, or channel will be located. These include:

- Round robin
- Most idle
- Start with lowest number

Creating and defining a hunt group in a PBX or IP PBX minimizes the chance that a caller who places an incoming call will receive a busy signal when the call is received.

Pilot Number

In a telephony network, a PBX or IP PBX can be configured to have a single hunt group or multiple hunt groups. Each hunt group created on a PBX or IP PBX must have an associated pilot number. The PBX or IP PBX uses the pilot number to locate the hunt group and in turn to locate the telephone extension number on which the incoming call was received. Without a defined pilot number, the PBX or IP PBX can't locate where the incoming call was received.

A pilot number is the address or location of the hunt group inside the PBX or IP PBX. A pilot number is generally defined as a blank extension number or one extension number from a hunt group of extension numbers that doesn't have a person or telephone associated with it. For example, you configure a hunt group on a PBX or IP PBX to contain extension numbers 4100, 4101, 4102, 4103, 4104, and 4105. The pilot number for the hunt group is configured as extension 4100. When a call is received on the extension number 4100, the PBX or IP PBX looks for the next available extension number to determine where to deliver the call. In this case, the PBX or IP PBX looks at the extension numbers 4101, 4102, 4103, 4104, and 4105.

Using a pilot number helps eliminate busy signals and helps route incoming calls to the circuits that are available. The PBX or IP PBX pilot number, when used with Exchange 2010 Unified Messaging, is used as the target. When an incoming call is unanswered or the line is busy, the call is correctly routed to an Exchange 2010 Unified Messaging server.

For more information about telephony concepts, see Understanding Telephony Concepts and Components.

Return to top

UM Hunt Groups

Unified Messaging hunt groups are critical to the operation of the Unified Messaging system. The UM hunt group is a logical representation of an existing PBX or IP PBX hunt group. UM hunt groups act as a connection or link between the UM IP gateway and the UM dial plan. Therefore, a single UM hunt group must be associated with at least one UM IP gateway and one UM dial plan.

Unified Messaging hunt groups are used to locate the PBX or IP PBX hunt group from which the incoming call was received. A pilot number defined for a hunt group in the PBX or IP PBX must also be defined within the UM hunt group. The pilot number is used to match the information presented for incoming calls through the Session Initiation Protocol (SIP) signaling message information on the message. The pilot number enables the Unified Messaging server to interpret the call together with the correct dial plan so that

the call can be routed correctly. The absence of a hunt group prevents the Unified Messaging server from knowing the origin or location of the incoming call. It is very important to configure the UM hunt groups correctly, because incoming calls that don't correctly match the pilot number defined on the UM hunt group will not be answered, and incoming call routing will fail.

When you create a Unified Messaging hunt group, you are enabling all Unified Messaging servers that are specified within the UM dial plan to communicate with an IP gateway. If you delete the UM hunt group, the associated IP gateway will no longer service calls with the specified pilot number. If the IP gateway is left without remaining UM hunt groups, the IP gateway will be unable to handle incoming calls.

For more information about IP gateways, see Understanding Unified Messaging IP Gateways.

Return to top

1.9.1.2.5 Understanding Unified Messaging Auto Attendants

Understanding Unified Messaging Auto Attendants

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Components >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Microsoft Exchange Server 2010 Unified Messaging (UM) enables you to create a single or multiple UM auto attendants, depending on the needs of your organization. Unlike other Unified Messaging objects, such as UM dial plans and UM IP gateways, you aren't required to create UM auto attendants. However, auto attendants help internal and external callers locate users or departments that exist in an organization and transfer calls to them. This topic discusses the UM auto attendant feature found in Exchange 2010 Unified Messaging.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Contents

Auto Attendants

In telephony or Unified Messaging environments, an automated attendant or auto attendant menu system transfers callers to the extension of a user or department without the intervention of a receptionist or an operator. In many auto attendant systems, a receptionist or operator can be reached by pressing or saying zero. The automated attendant is a feature in most modern Private Branch eXchange (PBX) and Unified Messaging solutions.

Some auto attendant systems use message-only information menus and voice menus so an organization can provide business hours, directions to the premises, information about job opportunities, and answers to other frequently asked questions. After the message plays, callers are forwarded to the receptionist or operator, or they can return to the main menu.

In more complex auto attendant systems, the menu system can be used to search for other auto attendant menus, locate a user in the system, or transfer to another outside telephone line. The menu system can also be used to let the caller interact with the system in certain situations, such as when a student enrolls for a college class or checks a grade, or when you activate a credit card over the telephone.

Although auto attendants can be very useful, if they aren't designed and configured correctly, they can confuse and frustrate callers. For example, specifically in large organizations, when auto attendants aren't designed correctly, callers can be led through a lengthy series of questions and menu prompts before they are finally transferred to a person to answer their questions.

UM Auto Attendants

Exchange 2010 Unified Messaging enables you to create one or more UM auto attendants depending on the needs of your organization. UM auto attendants can be used to create a voice menu system for an organization that lets external and internal callers move through the UM auto attendant menu system to locate and place or transfer calls to company users or departments in an organization.

When anonymous or unauthenticated users call an external business telephone number, or when internal callers call a defined extension number, they are presented with a series of voice prompts that help them place a call to a user or locate a user in the organization and then place a call to that user. The UM auto attendant is a series of voice prompts or .wav files that callers hear instead of a human operator when they call an organization that has Exchange 2010 Unified Messaging. The UM auto attendant lets callers move through the menu system, place calls, or locate users by using dual tone multi-frequency (DTMF) or voice inputs. However, for Automatic Speech Recognition (ASR) or voice inputs to be used, you must enable ASR on the UM auto attendant.

Important:

In some companies (especially in East Asia), office telephones may not have letters on the keys of the telephone. This makes the spell-the-name feature that uses the DTMF interface almost impossible to use, without a working knowledge of the key mappings. By default, Exchange 2010 Unified Messaging uses the E.161 key mapping. For example, 2=ABC, 3=DEF, 4=GHI, 5=JKL, 6=MNO, 7=PQRS, 8=TUV, 9=WXYZ.
When inputting the combination of letters and numbers, for example Mike1092, the numeric digits are mapped to themselves. For an e-mail alias of Mike1092 to be entered correctly, the user must press the numbers 64531092. Also for characters other than A-Z and 0-9, there won't be a telephone key equivalent. Therefore, these characters shouldn't be entered. For example, the e-mail alias mike.wilson would be entered as 6453945766. Even though there are 11 characters to be input, only 10 digits are entered by the user because the period (.) doesn't have a digit equivalent.

A UM auto attendant has the following features:

- It provides corporate or informational greetings.

- It provides custom corporate menus. You can customize these menus to have more than one level.
- It provides a directory search function that enables a caller to search the organization's directory for a name.
- It enables a caller to connect to the telephone of, or leave a message for, members of the organization.

In the Active Directory directory service, each UM auto attendant created is represented as an object. There is no limit to the number of UM auto attendants you can create in Active Directory. Each Exchange 2010 Unified Messaging auto attendant can support an unlimited number of extensions. A UM auto attendant can reference one, and only one, UM dial plan. However, UM auto attendants can reference or link to other UM auto attendants.

An incoming call received from an external telephone number or an internal telephone extension is processed by a Unified Messaging server and then sent to a UM auto attendant that has been created. The UM auto attendant is configured by the system administrator to use prerecorded voice (.wav) files that are then played over the telephone to the caller and that enable the caller to move through the Unified Messaging menu system. You can customize all the .wav files used when you configure a UM auto attendant to meet the needs of your organization.

For more information about message flow with UM auto attendants, see Unified Messaging Auto Attendant Call Processing.

Return to top

Auto Attendant with Multiple Languages

There are situations in which you may have to provide callers with auto attendants that have different languages. The language setting available on a UM auto attendant enables you to configure the default prompt language on the auto attendant. When you are using the default system prompts for the auto attendant, this is the language that the caller will hear when the auto attendant answers the incoming call. This language setting affects only the default system prompts provided after the Unified Messaging server role is installed. This language setting doesn't affect custom prompts configured on an auto attendant. The language selected as the default for the auto attendant is based on the version of Exchange 2010 installed.

When you install the U.S. English version of Exchange 2010, U.S. English is the only language available to configure on UM auto attendants. If you install a localized version of Exchange 2010, for example, Japanese, you can configure the auto attendant that you create to use Japanese or U.S. English for the default language. Additional UM language packs can be installed on a Unified Messaging server to enable you to use other default languages on an auto attendant.

Caution:

You cannot install UM language packs using the .msi file for the language.

For example, if you have a business that's based in the United States but requires a menu system that gives callers the options of U.S. English, Spanish, and French, you must first install the UM language packs that you need. In this case, if you have installed the U.S. English version of Exchange 2010, you would install the UM language packs for Spanish and French. However, because a Unified Messaging auto attendant can have only one language configured at a time, you would create four auto attendants: a main auto attendant configured to use U.S. English and then one auto attendant for each language: U.S. English, Spanish, and French. You would then configure the main auto attendant to have the appropriate key mappings to access the other auto attendants that you created for each language. In this example, the main auto attendant would answer the incoming

call and the caller would hear, "Welcome to Contoso, Ltd. For English, press or say 1. For Spanish, press or say 2. For French, press or say 3."

Return to top

Non-Business and Business Hours Custom Greetings

After you create a UM auto attendant, a default system prompt will be used for the non-business hours main menu prompt greeting heard by callers after the non-business hours welcome greeting is played. Although the system prompts mustn't be replaced or changed, you probably want to customize the greetings and menu prompts used with UM auto attendants. Frequently, in addition to configuring a customized non-business hours welcome greeting, you also want to create and configure a custom non-business hours main menu prompt greeting. After you configure a custom non-business hours main menu prompt greeting, you must enable key mappings on the UM auto attendant for non-business hours.

A custom non-business hours main menu prompt greeting is a list of options callers hear during non-business hours. To let callers hear a non-business hours main menu prompt greeting, you first must configure the business and non-business hours schedule by using the **Times** tab available on the Properties for a UM auto attendant. For example, "You have reached Trey Research after normal business hours. If you are experiencing a medical emergency, please hang up and dial 911. To leave a message for one of our doctors, press 1. To leave a message for one of our physical therapists, press 2. To leave a general message for one of our front office coordinators, press 3. To be connected with an after hours operator, press 0."

By default, when you create a UM auto attendant, the business and non-business hours greetings or prompts aren't configured and no key mappings are defined for business or non-business hours main menu prompts. To correctly configure customized non-business hours main menu greetings and prompts, you must:

1. Configure business and non-business hours on the **Times** tab.
2. Create the greeting file that will be used for the non-business hours welcome greeting.
3. Configure the non-business hours welcome greeting on the **Greetings** tab.
4. Create the greeting file that will be used for the non-business hours main menu prompt greeting.
5. Configure the non-business hours main menu prompt greeting on the **Greetings** tab.
6. Enable and configure the non-business hours key mappings on the **Key Mapping** tab.

Return to top

Key Mappings

If you use the default main menu prompt greeting and define a key mapping or multiple key mappings, the UM Text-to-Speech (TTS) engine will synthesize a main menu prompt. However, the TTS engine will only synthesize a main menu prompt if the default greeting is configured and at least one key mapping has been defined. The TTS engine will not synthesize a main menu prompt if you're using a custom main menu prompt. For example, "For the sales department, press 1. For the support department, press 2." To create this main menu prompt, you must create two key mappings: one named "Sales Department" and another named "Support Department", and then configure the key mapping entry to play an audio file, transfer to an extension number, or send the caller to another auto

attendant.

When you configure key mappings, you define the options and the operations that will be performed if a caller speaks a phrase while they're using a speech-enabled auto attendant or the caller presses the key on the keypad of the telephone while they're using an auto attendant that isn't speech-enabled. To configure key mappings, you must add key mapping entries. When you configure the key mapping entries for an auto attendant, you must:

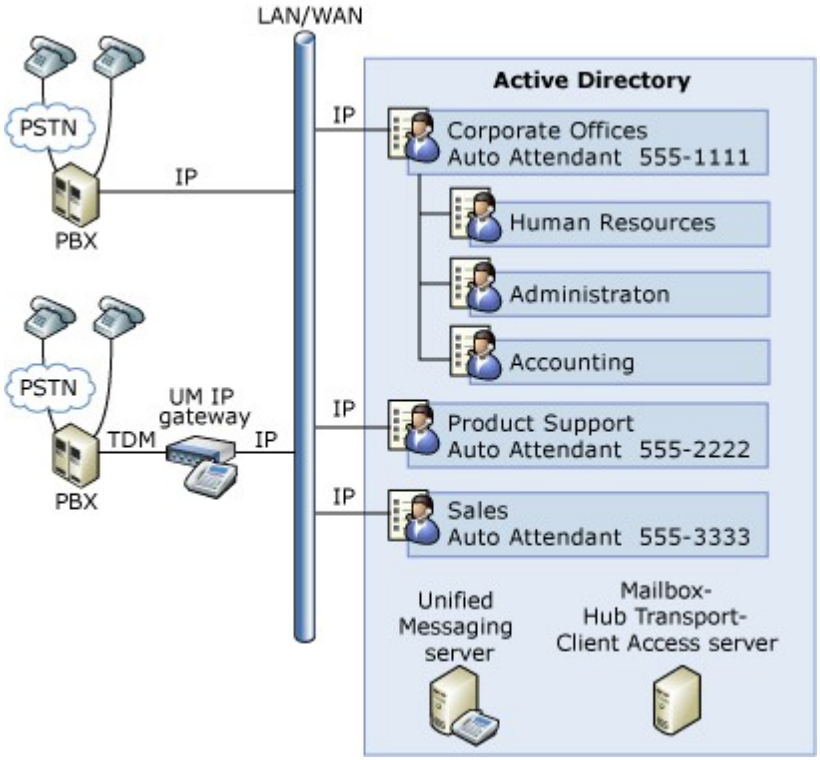
- Enable business hours key mapping.
- Add a key mapping entry.
- Type the name of the key mapping entry.
- Select **Presses this key** or **Presses no key (Time-out)** or type the phrase that the caller will say in the **Or the user says this phrase** field.
- Configure the action you want performed:
  - Play an audio file
  - Transfer to an extension number
  - Run an auto attendant

Return to top

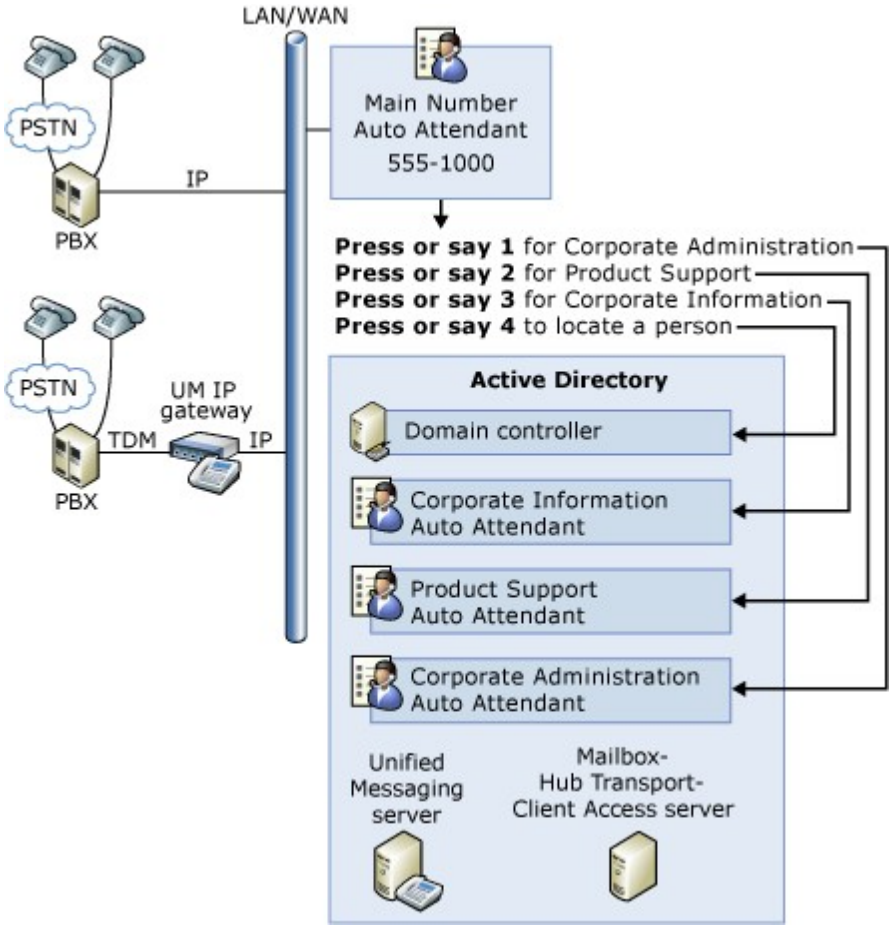
Auto Attendant Examples

The following examples demonstrate how you can use UM auto attendants with Exchange 2010 Unified Messaging:

- **Example 1** At a company called Contoso, Ltd., external customers can use three external telephone numbers: 425-555-0111 (Corporate Offices), 425-555-0122 (Product Support), and 425-555-0133 (Sales). The Human Resources, Administration, and Accounting departments have internal telephone extensions and must be accessed from the Corporate Offices UM auto attendant.
  To create a UM auto attendant structure that supports this scenario, create and configure three UM auto attendants that have the appropriate external telephone numbers. Create three other UM auto attendants for each department in the Corporate Offices. You then configure each UM auto attendant based on your requirements, such as the greeting type or other navigational information.
  The following figure is a graphical representation of how UM auto attendants can be used in Example 1.



- **Example 2** At a company called Contoso, Ltd., external customers call one main number for the business, 425-555-0100. When an external caller calls the external number, the UM auto attendant answers and prompts the caller by saying, "Welcome to Contoso, Ltd. Please press or say 'One' to be transferred to corporate administration. Please press or say 'Two' to be transferred to product support. Please press or say 'Three' to be transferred to corporate information. Please press or say 'Zero' to be transferred to the operator." To create a UM auto attendant structure that supports this scenario, you create a UM auto attendant that has customized extensions that route the call to the appropriate extension number.
  The following figure is a graphical representation of how Unified Messaging auto attendants can be used in Example 2.



Return to top

1.9.1.2.6 Understanding Unified Messaging Servers

Understanding Unified Messaging Servers

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Components >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-10*

When you install the Unified Messaging (UM) server role on a computer running Microsoft Exchange Server 2010, a computer object is created in the Active Directory directory service. This topic discusses Unified Messaging server objects and Unified Messaging server operations that are included in Exchange 2010 Unified Messaging.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Computer Objects

Unified Messaging Active Directory computer objects are created in the Computers

container during the installation of the Unified Messaging server role. The Unified Messaging objects connect the telephony infrastructure of your organization and the Exchange 2010 Unified Messaging Active Directory networking environment and are a basic part of the Unified Messaging system. The Unified Messaging computer object created in Active Directory is a logical representation of a physical server on which the Unified Messaging server role is installed.

Important:

The Unified Messaging server must be a member of a domain before the Unified Messaging server role is installed so that a new Unified Messaging computer object can be created during the installation.

After the computer objects have been created, you can perform the procedures that are required to successfully deploy Unified Messaging on your network.

Note:

You can also apply Group Policy settings to the computer after the computer running Exchange 2010 is added to the domain.

Server Operation

A Unified Messaging server won't process incoming calls unless the operational state is set to enabled. By default, however, the operational status of the Unified Messaging server is set to enabled after installation. When its operational status is set to enabled, the Unified Messaging server can process incoming and outgoing voice calls and route the messages to the intended recipients in your Exchange organization.

Although the operational status of the Unified Messaging server is set to enabled after installation, the Unified Messaging server also maintains a status parameter that's used to control the operational status of the server. The status parameter lets you stop call processing so that the Unified Messaging server can be taken offline in a controlled way.

The operational status of the Unified Messaging server can be controlled by the enable and disable commands in the Exchange Management Console and the Exchange Management Shell. The following are the status modes for Unified Messaging servers:

- **Enable** Process all incoming calls.
- **Disable Immediately** Don't accept any new calls and drop all existing calls.
- **Disable After Completing Calls** Don't accept any new calls but process all existing calls.

For more information about how to enable and disable a Unified Messaging server, see Enable Unified Messaging on Exchange 2010 and Disable Unified Messaging on Exchange 2010.

Even though the operational status of the Unified Messaging server is set to enabled after the Unified Messaging server role is installed, the server can't correctly process and route incoming calls to UM-enabled users until it's associated with at least one UM dial plan, and the UM dial plan is associated with at least one UM IP gateway. For more information about how to add a Unified Messaging server to a UM dial plan, see Add a UM Server to a Dial Plan.

For more information about UM IP gateways, see Understanding Unified Messaging IP Gateways.

After the Unified Messaging server is started, it locates all IP gateways that are associated with the UM dial plans and with the Unified Messaging server. To detect and identify any configuration changes on either UM dial plans or UM IP gateways, the Unified Messaging server will either register a change notification or check the configuration every 10 minutes.

If the UM IP gateway identifies any changes to the configuration, the Unified Messaging server reacts accordingly, and either starts using or stops using the appropriate IP gateways. After a Unified Messaging server is associated with a UM dial plan and is communicating with an IP gateway or IP Private Branch eXchange (PBX), you can run a set of diagnostic operations to verify the correct operation and connectivity.

1.9.1.2.7 Understanding Unified Messaging Users

Understanding Unified Messaging Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

With Microsoft Exchange Server 2010 Unified Messaging (UM), users in an Exchange 2010 organization can receive all their e-mail and voice messages in one mailbox. The Unified Messaging functionality found in Exchange 2010 greatly increases user productivity and enables more flexible messaging throughout an organization.

When you're creating an Exchange 2010 recipient, you're given the option of creating a mailbox or connecting to an existing mailbox. After the mailbox is created for the user or the user is connected to an existing mailbox, you must enable the mailbox so that the user can use the Unified Messaging capabilities found in Exchange 2010. After the user is enabled for Unified Messaging, all e-mail and voice messages will be delivered to the user's Inbox. By using Microsoft Office Outlook 2007, Outlook Web App, a mobile phone enabled for Microsoft Exchange ActiveSync, or a regular or mobile telephone, users can access their e-mail, voice messages, and calendaring information.

Contents

UM User Properties

By default, a user who has an Exchange 2010 mailbox isn't enabled for Unified Messaging. You must create a mailbox for the Exchange 2010 user before they can be enabled for Unified Messaging. After the user is enabled for Unified Messaging, you can manage, modify, and configure the UM properties for them.

Note:

To enable multiple UM users, use the **Enable-UMMailbox** cmdlet in the Exchange Management Shell.

There are two locations in which UM properties are stored for a user: the Mailbox object and the user's Active Directory object. When you enable a user for Unified Messaging, you set the UM property on the user's Mailbox object. After the Mailbox property is set to

enabled for Unified Messaging, the user can use the Unified Messaging features found in Exchange 2010.

After a user is enabled for Unified Messaging, their UM properties are stored in their properties and their mailbox. The user's UM properties, including their extension number, spoken name, and other properties, are stored in their properties in the Active Directory directory service.

You can manage UM properties for a UM-enabled user on the mailbox of the Exchange 2010 Unified Messaging user by using the Shell or the Exchange Management Console.

Relationship Between the UM User and Other Active Directory Objects

When you enable a user for Unified Messaging, the user must be associated with or linked to an existing UM mailbox policy, and you must provide their extension number. You can associate a user with a UM mailbox policy by using the **Enable-UMMailbox** cmdlet or by selecting the UM mailbox policy when you create the user's Exchange mailbox.

A UM mailbox policy contains settings such as the dialing restrictions and PIN policies for a user. When a UM mailbox policy is created, the UM mailbox policy must be associated with only one UM dial plan. The UM dial plan is then associated with at least one Unified Messaging server. Any Unified Messaging server associated with the UM dial plan can provide Unified Messaging services for a UM-enabled user who uses the UM dial plan. Associating these Active Directory objects in this manner delivers the Unified Messaging services by using Active Directory. After the user is enabled for Unified Messaging, the settings from a UM mailbox policy object are applied to the UM-enabled user.

Note:
In a circuit-switched telephony environment, the user's telephone must be programmed in the Private Branch eXchange (PBX) to forward busy or unanswered calls to a UM IP gateway associated with the user's dial plan.

Extension Numbers and SIP Addresses

When you enable a user for Unified Messaging, you must define at least one extension number that Unified Messaging will use when voice mail is submitted to the user's Exchange 2010 mailbox. After you enable the user for Unified Messaging, you can add extension numbers to the user's mailbox, or modify or remove them by configuring the Exchange Unified Messaging proxy address (EUM proxy address) on the user's mailbox.

Note:
There's no limit to the number of secondary extension numbers that you can add for a UM-enabled user.

The mailbox of a UM-enabled user can be associated with only one UM dial plan. However, the mailbox of a UM-enabled user can be assigned the following:

- A single extension number, Session Initiation Protocol (SIP) address, or E.164 address on a single dial plan.
- Multiple extension numbers, SIP addresses, or E.164 addresses on a single dial plan.
- Multiple extension numbers, SIP addresses, or E.164 addresses on two separate dial plans.

Note:
Each extension number must be unique within a dial plan.

For example, a UM-enabled user travels frequently from New York to Tokyo. The user's mailbox is associated with the New York dial plan and a single extension number is configured on the user's mailbox. A second extension number is configured on the user's mailbox for the Tokyo dial plan. When callers dial either extension number and leave a voice message for the user, the voice message will be delivered to the same UM-enabled mailbox.

Return to top

Disabling UM for a User

When you disable Unified Messaging for a user, the user's account may still be listed when a caller performs a directory search using a UM auto attendant menu or using Outlook Voice Access. Callers may be able to locate a user in the directory, but when they try to contact the user, they're taken back to the main menu in Unified Messaging. This may cause callers to become frustrated with the system. You can prevent callers from using a directory search to contact a user who's been disabled for Unified Messaging by connecting the user to another voice mail system, removing the user from the UM auto attendant directory search, or removing the user's account from Active Directory.

After a UM-enabled user account is disabled for Unified Messaging, the user may still have access to the individual UM-enabled mailbox using Outlook Voice Access or Microsoft Outlook. This can occur when all domain controllers in Active Directory haven't fully replicated all changes to objects to the Active Directory database. To lessen the risk of a user gaining access to the mailbox even though the account has been disabled for Unified Messaging, you can manually force Active Directory replication to occur or remove all Unified Messaging information from the user's mailbox when the user is disabled for Unified Messaging.

1.9.1.3 Understanding Unified Messaging Features

Understanding Unified Messaging Features

Exchange Server 2010 > Unified Messaging > Understanding Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Microsoft Exchange Server 2010 Unified Messaging (UM) introduces new concepts in Exchange messaging. Exchange 2010 Unified Messaging provides a single storage location for e-mail and voice mail messages.

This overview of the new components, features, and concepts in Unified Messaging includes the following:

- Active Directory UM objects
- Auto attendants
- Subscriber access using Outlook Voice Access

Contents

Additional Components

Active Directory UM Objects

After you install and configure the Unified Messaging server, you can create Active Directory objects that enable the UM functionality found in Exchange 2010. You must create the following objects after you successfully install the Unified Messaging server role:

- Dial Plan objects
- IP Gateway objects
- Hunt Group objects
- Mailbox Policy objects
- Auto Attendant objects
- UM Server objects

The Active Directory UM objects provide the configuration information required to integrate Unified Messaging, Active Directory, and the existing telephony infrastructure. Each type of object created in Active Directory controls a feature set in Unified Messaging.

For example, when you create a UM Auto Attendant object, the settings on the Auto Attendant object control the features and settings for that auto attendant. When you configure or modify an Auto Attendant object, you control such settings as business hours, non-business hours, informational greetings, and whether to use dual tone multi-frequency (DTMF) inputs or enable speech recognition for the auto attendant.

For more information about UM objects, see Understanding Unified Messaging Components.

Auto Attendants

When internal or external callers call in to the UM system, a series of voice prompts helps them move through the menu system called an auto attendant. The auto attendant lets the caller connect to a person in an organization or locate a user in the organization so they can place a call without assistance from a human operator. Callers hear voice prompts instead of a human operator, such as, "Press 1 for technical support."

You can create multiple auto attendants in Unified Messaging. Within Active Directory, each auto attendant is represented as an object. Configuration settings for an auto attendant are made on the Active Directory object and can include language settings, customized menus, and other menu navigational settings. You can also configure each UM auto attendant so that when an external caller or an internal caller places a call, and it's answered by a UM auto attendant, the caller can use either DTMF inputs or voice inputs to move through the UM menu system.

Note:

When a caller uses the keypad on a telephone to move through the menu system, it is called DTMF input. If this is the case, the telephone user interface is used.

For more information about auto attendants, see Understanding Unified Messaging Auto Attendants.

Subscriber Access

Unified Messaging gives subscribers access to the UM system. A subscriber is an internal

business user or network user who has been enabled for Unified Messaging and has an Exchange 2010 mailbox. Subscriber access is used by the internal users to access their individual mailboxes to retrieve e-mail, voice messages, and contact and calendar information. Each Dial Plan object that's created contains at least one subscriber access number or extension number. Subscribers use this telephone or extension number to access their individual mailboxes.

For more information about subscriber access, see Understanding Unified Messaging Subscriber Access.

There are two Unified Messaging user interfaces available to UM-enabled subscribers: the telephone user interface and the voice user interface. In Exchange 2010, these two interfaces together are called Outlook Voice Access. Subscribers can use Outlook Voice Access when they access the UM system from an external or internal telephone. They can use Outlook Voice Access to access their Exchange 2010 mailbox, including their personal e-mail, voice messages, and calendar information.

Note:

For a copy of the Unified Messaging Outlook Voice Access Quick Reference Guide, see the Quick Start Guide for Outlook Voice Access 2010.

Return to top

Additional Components

For more information about the many components and features in Unified Messaging, see the following topics:

- Understanding Unified Messaging Incoming Calls
- Understanding Unified Messaging Audio Prompts
- Understanding Unified Messaging Audio Codecs
- Understanding Unified Messaging Languages
- Understanding Automatic Speech Recognition Directory Lookups
- Understanding the DTMF Interface
- Understanding Storage Quotas and Voice Mail
- Understanding Unified Messaging VoIP Security
- Understanding Operator Transfers in Unified Messaging
- Understanding Outdialing
- Understanding Dial Codes, Number Prefixes, and Number Formats

Return to top

1.9.1.3.1 Understanding Unified Messaging Incoming Calls

Understanding Unified Messaging Incoming Calls

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

This topic provides an overview of the call handling features included with Microsoft Exchange Server 2010 Unified Messaging (UM). Each section in this topic gives you the information required to understand one or more of the call handling features included in Exchange 2010 Unified Messaging.

Contents

Overview

Call handling is a term that describes how incoming calls are answered and handled by a computer running Exchange 2010 Unified Messaging. The types of incoming calls handled by Exchange 2010 Unified Messaging include the following:

- Voice calls
- Outlook Voice Access
- Play on Phone feature
- UM auto attendants

For more information about Unified Messaging message flow and routing, see Understanding Unified Messaging Call Processing.

Voice Calls

Voice call handling is used when an internal or external user leaves a voice message for a subscriber on the Exchange 2010 Unified Messaging system. Incoming voice calls are created as MIME messages and then submitted using SMTP from the Exchange 2010 computer that has the Unified Messaging server role installed to an Exchange 2010 computer that has the Hub Transport server role installed. The two server roles must be installed in the same Active Directory site. The SMTP message transport for incoming voice calls is not only site aware, but all voice messages are submitted to the Hub Transport server using SMTP, even if the mailbox resides on the same computer that has the Mailbox server role installed.

For more information about voice calls and message routing, see Unified Messaging Voice Call Processing.

Outlook Voice Access

Unified Messaging servers also process and route incoming calls that are received by Outlook Voice Access users. When UM-enabled users or subscribers dial a subscriber access number that's set on a UM dial plan to access their Exchange 2010 mailbox, they are presented with a welcome message and a series of Telephone User Interface (TUI) voice prompts. The voice menu system presented to the user is called Outlook Voice Access. These voice prompts help the user navigate and interact with the Unified Messaging system using touchtone or speech inputs.

Note:

When an Outlook Voice Access caller uses touchtone inputs on a telephone keypad, the TUI is used. When the same caller uses speech inputs over the telephone, the Voice User Interface (VUI) is used.

For more information about the voice prompts found in Exchange 2010 Unified Messaging,

see Understanding Unified Messaging Audio Prompts.

Outlook Voice Access is the feature that enables UM-enabled users to access their Exchange 2010 mailbox using an analog, digital, or mobile telephone. By accessing their Exchange 2010 mailbox, they can perform the following tasks:

- Listen to new and saved e-mail and voice mail messages.
- Forward, reply, save, and delete e-mail and voice messages.
- Interact with their calendar, including:
  - Listening to daily calendar appointments and meeting details.
  - Accepting or declining e-mail and meeting requests.
  - Sending an "I'll be late" message to meeting participants.
  - Replying to a meeting request using voice inputs to send a message to meeting participants.
  - Declining or canceling meetings.
- Interact with global address list and personal contacts. These interactions may include:
  - Locating a person in the global address list or personal contacts.
  - Inputting a telephone extension number to leave a message for a person.
  - Sending a voice message to a person.
- Change their PIN, spoken name, or greetings.

For more information about how to navigate the Outlook Voice Access menus, see the Microsoft Exchange 2010 Unified Messaging Outlook Voice Access Quick Start Guide. For a copy of the Microsoft Exchange 2010 Unified Messaging Outlook Voice Access Quick Start Guide, see the Microsoft Download Center.

For more information about Outlook Voice Access message routing, see Unified Messaging Outlook Voice Access Call Processing.

Return to top

Play on Phone Feature

To enable the Play on Phone feature for UM-enabled users, the Unified Messaging server must first answer and then correctly route a call when it's placed by a user who is using Microsoft Office Outlook Web App or Office Outlook 2007. If UM-enabled users are in a location that's not private or the voice message is confidential, they will likely not want to play their voice message over their computer speakers. The Exchange 2010 Unified Messaging Play on Phone feature lets UM-enabled users listen to a voice message using a telephone instead of playing it over their computer speakers or headphones.

For more information about Play on Phone message flow, see Unified Messaging Play on Phone Call Processing.

UM Auto Attendants

To enable the UM auto attendant feature found in Exchange 2010 Unified Messaging, Unified Messaging servers must correctly answer and then route the incoming calls received from internal and external anonymous or unauthenticated users.

To enable a UM auto attendant to answer incoming calls, you must first create and configure a UM auto attendant. Creating and configuring UM auto attendants is an optional feature in Exchange 2010 Unified Messaging. However, auto attendants help internal and external callers locate and place calls to company users or departments that are in an organization.

A UM auto attendant is a set of voice prompts that callers hear instead of a human operator when they place a call to an organization that has Exchange 2010 Unified Messaging. A UM auto attendant helps callers navigate the organization's menu system using dual tone multi-frequency (DTMF) (also known as touchtone) inputs or voice-activated inputs that use Automatic Speech Recognition (ASR) so that they can locate a user or department in an organization and then place a call to that user or department.

- For more information about UM auto attendant message routing, see Unified Messaging Auto Attendant Call Processing.
- For more information about UM auto attendants, see Understanding Unified Messaging Auto Attendants.

Return to top

1.9.1.3.2 Understanding Unified Messaging Audio Prompts

Understanding Unified Messaging Audio Prompts

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-10*

When you install the Unified Messaging (UM) server role on a computer running Microsoft Exchange Server 2010, a common set of default audio files used for the Unified Messaging system and menu prompts, greetings, and informational announcements is copied to the Unified Messaging server. Although you can have a fully functional UM auto attendant or a dial plan that uses only the default audio prompts included in Exchange 2010, the audio files installed for greetings, informational announcements, and system and menu prompts are too generic to serve as an acceptable public interface for many companies. This topic discusses the system and menu prompts, greetings, and informational announcements used by UM dial plans and auto attendants and how they're used when callers access the Unified Messaging system.

Contents

Overview of Audio Prompts and Greetings

After the Unified Messaging server role is installed, audio files for UM dial plans and auto attendants are copied to the Unified Messaging server. By default, the installation program copies the audio files to the Program Files\Microsoft\Exchange Server\V14\Unified Messaging\Prompts\<*language*> folder. If you've installed the U.S. English version of Exchange 2010, a folder named \en is created during installation to hold the U.S. English versions of the system prompts. The UM server plays these system prompts to callers so

they can hear greetings, menu prompts, and informational announcements and so they can navigate the Unified Messaging menus.

These system audio files or prompts copied to the UM server should never be changed. However, Unified Messaging does enable you to customize UM dial plan and auto attendant welcome greetings, main menu prompts, and informational announcements.

The following table summarizes the prompts and greetings used with UM dial plans.

Audio prompts for UM dial plans

Prompts and greetings	Description
System prompts	Must not be modified.
Welcome greeting	The default welcome greeting is a system prompt that is played by default. However, you can use a customized greeting file that you create.
Informational announcement	By default, informational announcements are disabled. If you enable an informational announcement, you must specify a customized greeting file.

The following table summarizes the prompts and greetings used with UM auto attendants.

Audio prompts for UM auto attendants

Prompts and greetings	Description
System prompts	Must not be modified.
Business hours menu prompts	By default, business hours menu prompts are enabled and a system prompt is played. However, you can use a customized greeting file that you create.
Non-business hours menu prompts	By default, non-business hours prompts are enabled and a system prompt is played. However, you can use a customized greeting file that you create.
Business hours greeting	By default, a business hours greeting is enabled and a system prompt is played. However, you can use a customized greeting file that you create. This is also known as a welcome greeting.
Non-business hours greeting	By default, a non-business hours greeting is enabled and a system prompt is played. However, you can use a customized greeting file that you create. This is also known as a welcome greeting.
Informational announcement	By default, informational announcements are disabled. If you enable an informational announcement, you must specify a customized greeting file.

Caution:

Modifying the installed system prompts isn't supported.

Return to top

System Prompts

Unified Messaging is installed with a set of default audio prompts for use with Outlook Voice Access, dial plans, and auto attendants. Hundreds of system prompts for each language are installed on the Unified Messaging server. The UM server plays the audio files for these system prompts to callers when they access the Unified Messaging system. The following are some examples of these system prompts:

- "Please enter your PIN."
- "To access your mailbox, enter your extension."
- "To contact someone, press the # key."
- "Spell the name of the person you are calling, last name first."
- "To reach a specific person, just tell me the name."

Caution:

Modifying the installed system prompts isn't supported.

Note:

When the Unified Messaging service starts on the Unified Messaging server, it will verify that all the system prompts are available. If a system prompt can't be found, Unified Messaging will return an error. To fix the error that is returned, locate the event using Event Viewer and copy the file listed in the **Event Properties** window from the Exchange 2010 installation DVD into the appropriate folder on the UM server.

UM Dial Plan Greetings and Announcements

After you install the Unified Messaging server role and create a UM dial plan, you've the option to use the audio files for the default system prompts that are copied to the UM server during installation or to create customized audio files that can be used with UM dial plans.

UM dial plans have a welcome greeting and an optional informational announcement you can modify. The welcome greeting is used when Outlook Voice Access users or another caller calls the subscriber access number. The callers hear a default welcome greeting that says, "Welcome, you are connected to Microsoft Exchange." This audio file is the default greeting for a UM dial plan. However, you might want to change this greeting and provide an alternative welcome greeting specific to your company, for example, "Welcome to Outlook Voice Access for Woodgrove Bank." If you customize this greeting, you can record the customized greeting and save it as a .wav file, and then you can configure the dial plan to use this customized greeting.

Unified Messaging allows for an informational announcement to follow the welcome greeting. By default, there is no informational announcement configured. However, you may want to provide one for callers. You can use the informational announcement for general announcements that change more often than the welcome greeting or for announcements required by corporate compliance policies. When it's important that the whole informational announcement is heard, you can configure it to be uninterruptible. This prevents a caller from pressing a key or speaking a command to interrupt and stop the informational announcement.

The following table describes the UM dial plan greetings and informational

announcements.

UM dial plan greetings and informational announcements

Greeting	Default example	Customized example
Welcome greeting	"Welcome, you are connected to Microsoft Exchange."	"Welcome to Outlook Voice Access for Woodgrove Bank."
Informational announcement	By default, an informational announcement isn't configured.	"By using this system you agree to adhere to all corporate policies when you are accessing this system."

When you are customizing and configuring greetings and announcements, make sure the language setting configured on the UM dial plan is the same as the language of the custom prompts you create. If not, a caller may hear a message or greeting in one language and another message or greeting in a different language.

Return to top

UM Auto Attendant Greetings, Announcements, and Menu Prompts

As with UM dial plans, UM auto attendants have a welcome greeting, an optional informational announcement, and an optional custom menu prompt. There are different versions of the welcome greeting and menu prompt that you can configure for business hours and non-business hours. You can modify all of them.

The welcome greeting is the first thing a caller hears when a UM auto attendant answers the call. By default, this says, "Welcome to the Microsoft Exchange auto attendant." The audio file that is played for the call is the default system prompt for the UM auto attendant. However, you may want to provide an alternative greeting specific to your company, for example, "Thank you for calling Woodgrove Bank." To customize this welcome greeting, record the customized greeting and save it as a .wav file, and then configure the auto attendant to use this customized greeting. As with the welcome greetings, you can also customize the menu prompts.

Unified Messaging also allows for an informational announcement to follow a business hours greeting or a non-business hour greeting. By default, no informational announcement is configured, but you may want to provide one to callers. The informational announcement can announce your company's business hours, for example, "Our business hours are 8:00 A.M. to 5:00 P.M., Monday through Friday, and 8:30 A.M. to 1:00 P.M. on Saturday." The informational announcement can also provide information required for compliance with corporate policies, for example, "Calls may be monitored for training purposes." When it's important that the whole informational announcement is heard, you can configure it to be uninterruptible. This prevents the caller from pressing a key or speaking a command to interrupt and stop the informational announcement.

The following table describes the UM auto attendant greetings and informational announcements.

UM auto attendant greetings, informational announcement, and menu prompts

Greeting	Default example	Customized example

Business hours greeting	"Welcome to the Exchange auto attendant."	"Thank you for calling Woodgrove Bank."
Non-business hours greeting	No default non-business hours greeting is played until you configure the business hours for the auto attendant. However, the business hours greeting is played for callers during all times of the day.	"You have reached Woodgrove Bank after business hours. Our business hours are from 8:00 A.M. until 5:00 P.M., Monday through Friday."
Informational announcement	By default, informational announcements aren't configured.	"Calls may be monitored for training purposes."
Business hours main menu prompt	No default business hours main menu prompt will be played until you configure key mappings on the auto attendant.	"For technical support, press or say 1. For corporate offices and administration, press or say 2. For sales, press or say 3."
Non-business hours main menu prompt	No default non-business hours main menu prompt will be played until you configure key mappings and the business hours schedule on the auto attendant.	"Your call is very important to us. However, you have reached Woodgrove Bank after business hours. If you want to leave a message, please press or say 1, and we will return your call as soon as possible."

As with UM dial plans, make sure the language setting configured on the UM auto attendant is the same as the language of the custom greetings you create and is set to the same language as the UM dial plan. If not, a caller may hear a message or greeting in one language and another message or greeting in a different language.

Return to top

Customizing Greetings, Announcements, and Menu Prompts

Although the system prompts mustn't be replaced or changed, you'll probably want to customize the greetings, informational announcements, and menu prompts used with UM dial plans and auto attendants. After the Unified Messaging server role is installed, you can configure the UM dial plans and auto attendants to use these custom audio files (.wav). You must follow these steps before you can enable custom voice prompts for callers:

- Record the custom greeting and save it as a .wav file. The Linear PCM (16 bit/sample), 8 kilohertz (kHz) audio codec must be used to encode the .wav file. If you don't use this specific format for the .wav file, an error will be generated stating that the source file is in an unsupported format. Although an error is generated, the error won't appear in Event Viewer.
- Configure the UM dial plan or auto attendant to use the customized greeting. After you create a UM auto attendant, a default system prompt will be used for the non-business hours main menu prompt greeting heard by callers after the non-business hours welcome greeting is played. Although the system prompts mustn't be replaced or changed, you probably want to customize the greetings and menu prompts used with UM auto attendants. Frequently, in addition to configuring a customized non-business hours welcome greeting,

you also want to create and configure a custom non-business hours main menu prompt greeting. After you configure a custom non-business hours main menu prompt greeting, you must enable key mappings on the UM auto attendant for non-business hours.
A custom non-business hours main menu prompt greeting is a list of options callers hear during non-business hours. To let callers hear a non-business hours main menu prompt greeting, you first must configure the business and non-business hours schedule by using the **Times** tab available on the Properties for a UM auto attendant. For example, "You have reached Trey Research after normal business hours. If you are experiencing a medical emergency, please hang up and dial 911. To leave a message for one of our doctors, press 1. To leave a message for one of our physical therapists, press 2. To leave a general message for one of our front office coordinators, press 3. To be connected with an after hours operator, press 0."
By default, when you create a UM auto attendant, the business and non-business hours greetings or prompts aren't configured and no key mappings are defined for business or non-business hours main menu prompts. To correctly configure customized non-business hours main menu greetings and prompts, you must:

- Configure business and non-business hours on the **Times** tab.
- Create the greeting file that will be used for the non-business hours welcome greeting.
- Configure the non-business hours welcome greeting on the **Greetings** tab.
- Create the greeting file that will be used for the non-business hours main menu prompt greeting.
- Configure the non-business hours main menu prompt greeting on the **Greetings** tab.
- Enable and configure the non-business hours key mappings on the **Key Mapping** tab.

Return to top

1.9.1.3.3 Understanding Unified Messaging Audio Codecs

Understanding Unified Messaging Audio Codecs

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-26*

In Microsoft Exchange Server 2010 Unified Messaging (UM), a codec is used to store voice mail messages. Another codec is used between an IP gateway or IP Private Branch eXchange (PBX) and the Unified Messaging server. Exchange 2010 Unified Messaging can use any of the following four audio codecs to create and store voice messages:

- MP3 (default)
- Windows Media Audio (WMA)
- Group System Mobile (GSM) 06.10
- G.711 Pulse Code Modulation (PCM) Linear

However, the G.711 (PCMA and PCMU) and the G.723.1 codecs are VoIP codecs used between an IP gateway and the Unified Messaging server.

Part of planning your Unified Messaging system involves selecting the correct audio codec based on the needs and requirements of your organization. This topic discusses the audio

codecs that Unified Messaging can use and will help you plan your UM deployment.

Codecs

Two types of codecs are used in Unified Messaging: the codec used between IP gateways and the Unified Messaging server or between a PBX and IP gateway, depending on the type of PBX, and the codec used to encode and store voice messages for users.

The term *codec* is a combination of the words "coding" and "decoding" and is used with digital audio data. A codec is a software program that transforms digital data into an audio file format or audio streaming format. Codecs are used to convert an analog voice signal to a digital version of the voice signal. Codecs can vary in their sound quality, the bandwidth required to use them, and the system requirements needed to do the encoding.

When you use an ordinary telephone over the Public Switched Telephone Network (PSTN) your voice is transported in an analog format over the telephone line. But with Voice over IP (VoIP), your voice must be converted into digital signals. This conversion process is known as encoding. Encoding is performed by a codec. After the digitized voice has reached its destination, it must then be decoded back to its original analog format so the person on the other end of the call can hear and understand the caller.

VoIP Codec

In Unified Messaging, three types of codecs can be used between IP gateways or IP PBXs and the Unified Messaging server. Unified Messaging servers can accept the following VoIP codecs from an IP gateway or IP PBX:

- G.711 µ-law
- G.711 A-law
- G.723.1

G.711 is a standard that was developed for use with audio codecs. There are two main algorithms defined in the standard for G.711: the µ-law algorithm that is used in North America and Japan and the A-law algorithm that is used in Europe and other countries. The G.723.1 audio codec is mostly used in VoIP applications and requires a license to be used. G.723.1 is a high quality, high compression type of codec.

Both a Unified Messaging server and a supported IP gateway or IP PBX can offer both the G.711 and G.723.1 codec. By default, the first codec to be used is G.723.1. If you want to use a different codec other than G.723.1 between the Unified Messaging server and the IP gateway or IP PBX, we recommend that you change the configuration on the IP gateway or IP PBX. The following table summarizes some common VoIP codecs.

VoIP codecs

VoIP codec	Bandwidth (Kbps)	Description
G.711	64	This codec requires very low processing. It needs a minimum of 128 kilobits per second (Kbps) for two-way communication.
G.723.1	5.3/6.3	This codec offers high compression with high quality audio. It requires more processing than the G.711 codec. The G.723.1 codec uses reduced bandwidth but offers poorer quality audio.

UM Voice Message Storage Codec

Unified Messaging dial plans are integral to the operation of Unified Messaging. By default, when you create a UM dial plan, the UM dial plan uses the WMA audio codec. However, after you create the UM dial plan, you can configure the UM dial plan to use GSM 06.10 or G.711 PCM Linear audio codecs.

Each audio codec has advantages and disadvantages. The WMA audio codec was selected as the default audio codec because of its sound quality and compression properties. GSM 06.10 and G.711 PCM Linear audio codecs were included as available options because of their ability to support other types of messaging systems.

When you plan for Unified Messaging, you must balance the size and the relative quality of the audio file that will be created for voice messages. Generally, the higher the bit rate for an audio file, the higher the quality. You must also consider whether the audio file is compressed. The sample bit rate (bit/sec) and compression properties for each audio codec used in Unified Messaging are as follows:

Default UM voice message storage codecs

Voice message storage codec	Bits	Compressed file?
MP3	16 bit	Yes
WMA	16 bit	Yes
G.711 PCM	16 bit	No
GSM 06.10	8-bit	Yes

In Unified Messaging, the MP3, WMA, G.711 PCM Linear, and GSM 06.10 audio codecs are used to create .mp3, .wma and .wav audio files for voice messages. However, the file type created depends on the audio codec that is used to create the voice message audio file. In Unified Messaging, the .mp3 audio codec creates .mp3 audio files, the .wma audio codec creates .wma audio files and the GSM 06.10 and G.711 PCM Linear audio codecs produce .wav audio files. Both kinds of audio files are sent together with the e-mail message to the recipient of the voice message.

Frequently, but not always, coding and decoding the digital data also involves compression or decompression. Audio compression is a form of data compression that reduces the size of audio data files. The audio compression algorithm used by the audio codec compresses the .wma or .wav audio files. In Unified Messaging, the type of audio compression algorithm that is used is based on the type of audio codec selected in the UM dial plan properties. After the audio file is created and compressed, it's attached to the voice message.

Sometimes information from the digital data is lost during compression and decompression. The higher the compression that is used to compress the audio file, the greater the loss of information during the conversion. However, less disk space is used because the size of the audio file is reduced. Conversely, the lower the compression, the lower the loss of the information. However, more disk space must be used because of the increased size of each audio file.

RTAudio wideband or high fidelity audio for recording voice messages is also available as an audio codec. However, high fidelity audio using RTAudio is available only after you have successfully integrated Exchange 2007 Unified Messaging with Office Communications Server 2007 R2 or Microsoft Lync Server 2010 (the next generation of Office Communications Server). To enable RTAudio, the UM dial plan must be configured as a Session Initiation Protocol (SIP) URI-type dial plan and you must set the call answering codec on the dial plan to WMA.

Important:
RTAudio is not available in environments where Office Communications Server 2007 or R2 or Lync Server 2010 is not deployed. This is because, in these environments, the dial plan is set to Telephone Extension and not SIP URI.

There are two media streams for each incoming call: inbound to a Unified Messaging server and outbound from a Unified Messaging server. When the dial plan type is set to SIP URI and the call-answering codec on the dial plan is set to WMA, a Unified Messaging server tries to select the RTAudio VoIP codec for the inbound media stream. If negotiation is successful, the RTAudio codec for the inbound stream will be used for call answering calls or calls that originate from Office Communicator 2007.

Note:
Calls placed by using the Play on Phone feature will not use the RTAudio codec. The inbound stream for calls placed by using Play on Phone will use the G.711 or G.723.1 codec.

When the RTAudio codec is used, the voice message that is recorded will be recorded in high fidelity and will be stored as an audio file that has a .wma extension. When the voice message is played back to the user in Office Outlook 2007 or Outlook Web Access, they will hear the voice message in high fidelity audio. If negotiation is unsuccessful, either the G.711 or G.723.1 codec will be used. Both the G.711 and the G.723.1 codecs are narrowband codecs. When they're used as the VoIP codec, the voice message is recorded and stored as a narrowband audio file that has a .wma extension.

The outbound media stream will always be negotiated by using either the G.711 or G.723.1 codec. This means that callers will always hear narrowband audio over the telephone. This also applies to situations when a call is placed by using Office Communicator.

The audio format and codec that Unified Messaging servers use to store the audio in voice messages depends not only on the audio codec that's configured on the dial plan but also on the bit rate of the audio that UM negotiates with a SIP peer. If your environment includes Office Communications Server 2007 R2, Lync Server 2010, or the SIP endpoints, a Unified Messaging server will also negotiate the audio codec to use with a SIP peer. For example, when wideband RTAudio is negotiated as the wire codec, a Unified Messaging server will then use either the 32 Kbps MP3 or WMA 9.2 format when creating voice messages, depending on the dial plan setting. The following table shows the relationship between the voice message storage audio codec and the VoIP or wire audio codec that's used.

Relationship between the storage audio codec and the VoIP or wire audio codec

Audio codec configured on a UM dial plan	VoIP or wire codec (narrowband) - G.723, G.711, or RTAudio (8KHz)	VoIP or wire codec (wideband) - RTAudio (16KHz)
G.711	G.711	Not applicable. A UM server doesn't negotiate wideband audio if the dial plan is set to G.711.
WMA	WMA 9 Voice	WMA 9.2
GSM	GSM 6.10	Not applicable. A UM server doesn't negotiate wideband audio if the dial plan is set to G.711.

MP3	MP3 (16 Kbps)	MP3 (32 Kbps)

Return to top

UM Message Sizing

You can configure Unified Messaging to use one of the four following audio codecs for creating voice messages: MP3, WMA, GSM 06.10, and G.711 PCM Linear. By default, the MP3 format is selected. The MP3 format is a common audio file format that's used to greatly reduce the size of the audio file and is most commonly used by personal audio devices or MP3 players. MP3 is a cross-platform type of audio codec and is used for compatibility with many mobile phones and devices and different computer operating systems.

The WMA audio codec is always stored in the Windows Media format, and the attachment is a file that has a .wma file name extension. Audio files encoded using the GSM or G.711 PCM Linear audio codecs are always stored in RIFF/WAV format, and the attachment is a file that has a .wav file name extension.

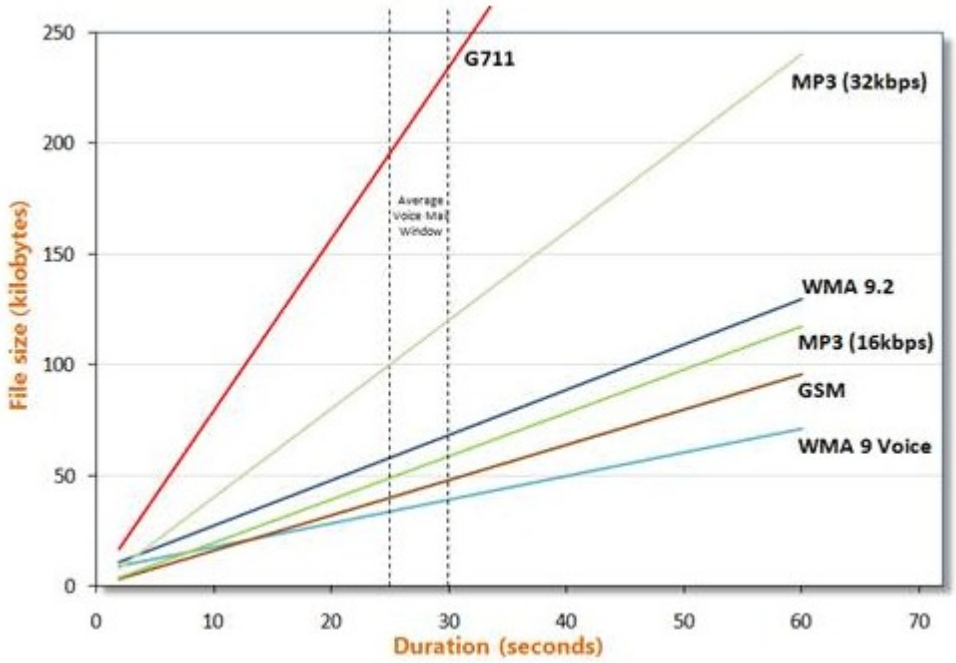
The size of Unified Messaging voice messages depends on the size of the attachment that holds the voice data. In turn, the size of the attachment depends on the following factors:

- The duration of the voice mail recording
- The audio codec that is used
- The audio file storage format

The following figure shows how the size of the audio file depends on the duration of the voice mail recording for the three audio codecs that you can use in UM.

Note:

In this figure, the average length of a call-answered voice message is approximately 30 seconds.



MP3

By default, the MP3 format is selected and is the default audio file format for voice mail messages. The MP3 format is a common audio file format that's used to greatly reduce the size of the audio file and is most commonly used by personal audio devices or MP3 players. MP3 is a cross-platform type of audio codec and is used for compatibility with many mobile phones and devices and different computer operating systems.

WMA

WMA is the most highly compressed audio codec of the three kinds of codecs. The compression is approximately 11,000 bytes for each 10 seconds of audio. However, the .wma file format has a much larger header section than the .wav file format. The .wma file header section is approximately 7 kilobytes (KB), whereas the header section for the .wav file is less than 100 bytes. Although WMA audio recordings are recorded for longer than 15 seconds, they become smaller than GSM audio recordings. Therefore, for the smallest but highest quality audio files, use the WMA audio codec.

G.711 PCM Linear

The G.711 PCM Linear audio codec creates .wav audio files that are not compressed. Therefore, G.711 PCM Linear .wav audio files occupy the most space for any given duration when they're compared to the GSM and WMA audio codecs. G.711 PCM Linear .wav audio files occupy just over 160,000 bytes for each 10 seconds of audio. G.711 PCM Linear .wav audio files have the highest audio quality of the three audio codecs used by Unified Messaging. However, the quality of comparable audio files created using the WMA and GSM audio codecs are acceptable to most users who listen to voice messages.

GSM

The GSM audio codec creates .wav audio files that are compressed. GSM .wav audio files are just over 16,000 bytes for each 10 seconds of audio. However, GSM creates an audio file larger than the audio file created by the WMA audio codec. Therefore, when you are balancing the quality of the voice message and the size, this may not be the best choice.

Return to top

1.9.1.3.4 Understanding Unified Messaging Languages

Understanding Unified Messaging Languages

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-30*

You can install and configure language packs to support multiple languages in Microsoft Exchange Server 2010 Unified Messaging (UM) environments.

Exchange 2010 UM language packs let callers and Outlook Voice Access users interact with the Unified Messaging system in multiple languages. After you install an additional language on a Unified Messaging server, callers and Outlook Voice Access users can hear e-mail messages and interact with the Unified Messaging system in that language.

Several key components rely on UM language packs to enable users and callers to interact effectively with Exchange 2010 Unified Messaging in multiple languages. Each UM language pack includes a Text-to-Speech (TTS) engine, the pre-recorded prompts and support for Automatic Speech Recognition (ASR) and Voice Mail Preview for a specific language. This topic discusses UM language packs, the UM components that use the UM language packs, and how UM language packs, after they're installed, can be used to configure UM dial plans and UM auto attendants to use other languages.

Exchange Unified Messaging language packs are version-specific and platform-specific. Since Exchange Server 2007, there have been separate releases for UM language packs, including the RTM version of Exchange 2007, Exchange 2007 SP1, SP2, and SP3, the RTM version of Exchange Server 2010, and Exchange 2010 SP1 and SP2. For some of these versions, both 32-bit and 64-bit downloads are available, but for other releases only 64-bit downloads are available.

It's very important that you install the correct version and platform of the UM language packs on a UM server. Don't install UM language packs on a Unified Messaging server that's running an earlier version of Exchange or that's designed for a 32-bit platform.

Contents

Overview of UM Language Packs

Unified Messaging language packs allow an Exchange 2010 UM server to speak additional languages to callers and recognize other languages when callers use ASR or when voice messages are transcribed. UM language packs contain:

- Pre-recorded prompts in the language of the UM language pack. For example, "After the tone, please record your message. When you've finished recording, hang up, or press the # key for more options."
- Grammar files in the language of the UM language pack that are used by a UM server to look up the names of given users in the directory.
- Text-to-Speech (TTS) translation so that content (e-mail, calendar, contact information, etc.) can be read to callers in the language of the UM language pack.
- Support for Automatic Speech Recognition (ASR), which allows callers to interact with UM using the voice user interface (VUI) in the language of the UM language pack.
- Support for Voice Mail Preview, which allows users to read the transcript of voice mail messages in a specific language from within a supported e-mail client such as Outlook or Outlook Web App.

The UM language packs that are included with Exchange 2010 contain pre-recorded prompts, TTS conversion support for a specific language, and in some cases, support for ASR. In multiple-language environments, you may have to install additional UM language packs because some callers prefer to be prompted in a different language, or because they receive e-mail in more than one language. You must install multiple UM language packs to support the ability for the Unified Messaging server to read an e-mail message that contains more than one language, because the TTS conversion system must be instructed which language to select based on the text of the message that will be read. If the Unified Messaging language pack hasn't been installed, the e-mail message will be illogical and incoherent when it's read back to the user. Installing the appropriate language pack enables the TTS engine to read e-mail and calendar items to the Outlook Voice Access user by using the correct language and also provides the language-specific pre-recorded prompts for Unified Messaging. In some cases, they may also provide support for ASR.

Note:

The TTS engine converts text to speech but doesn't convert from speech to text. UM-

enabled users can send an e-mail message that has a voice file attached to another user. However, they can't create and send a text-based e-mail message to another user.

When you install a language pack, the installation program does the following:

1. Copies the language prompts that will be used to configure UM dial plans and auto attendants.
2. Allows the TTS engine to read messages when Outlook Voice Access users access their Inbox.
3. Enables ASR for speech-enabled UM dial plans and auto attendants for the language installed.
4. Enables Voice Mail Preview for clients in other languages.

You can add UM language packs using the **Setup.com** command or run the *<UMLanguagePack>*.exe installation program after you've downloaded the UM language pack from Exchange Server 2010 SP2 UM Language Packs. However, you can remove a UM language pack only by using the Setup.com command. There's no Exchange Management Shell cmdlet that you can use to add or remove languages from a Unified Messaging server. For more information about how to install a UM language pack, see Install a Unified Messaging Language Pack on a UM Server. For more information about how to remove a UM language pack, see Remove a Unified Messaging Language Pack from a UM Server.

Note:
By default, when you install Exchange 2010, the U.S. English language (en-US) will be installed and can't be removed unless you remove the Unified Messaging server role from the computer.

Return to top

The following table lists the Unified Messaging language packs that are currently available. It also lists the installation file name for each UM language pack and the culture ID for the UM language.

UM language pack installation file names and culture IDs

Language	Country/Region	Culture ID	Installation file name	Availability
Catalan	Spain	ca-ES	UMLanguagePack. ca-ES	Download available
Chinese (Hong Kong)	China	zh-HK	UMLanguagePack. zh-HK	Download available
Chinese (Simplified)	China	zh-CHS	UMLanguagePack.zh-CN	Download available
Chinese (Traditional)	Taiwan	zh-TW	UMLanguagePack.zh-TW	Download available
Danish	Denmark	da-DK	UMLanguagePack.da-DK	Download available
Dutch	Netherlands	nl-NL	UMLanguagePack.nl-NL	Download available
English	Australia	en-AU	UMLanguagePack.en-AU	Download available
English	Canada	en-CA	UMLanguagePack. en-CA	Download available

English	India	en-IN	UMLanguagePack. en-IN	Download available **Caution:** Deploying the Exchange 2010 SP1 English (India) (en-IN) Unified Messaging language pack in organizations that include Exchange Server 2007 servers running on Windows Server 2003 will cause the Exchange 2007 servers to fail. Further details are contained in this Microsoft Knowledge Base article.
English	United Kingdom	en-GB	UMLanguagePack.en-GB	Download available
English	United States	en-US	Included with installation of the Unified Messaging server role	Download available
Finnish	Finland	fi-Fl	UMLanguagePack.fi-Fl	Download available
French	Canada	fr-CA	UMLanguagePack.fr-CA	Download available
French	France	fr-FR	UMLanguagePack.fr-FR	Download available
German	Germany	de-DE	UMLanguagePack.de-DE	Download available
Italian	Italy	it-IT	UMLanguagePack.it-IT	Download available
Japanese	Japan	ja-JP	UMLanguagePack.ja-JP	Download available
Korean	Korean	ko-KR	UMLanguagePack.ko-KR	Download available
Norwegian (Bokmal)	Norway	nb-NO	UMLanguagePack.nb-NO	Download available
Polish	Poland	pl-PL	UMLanguagePack.pl-PL	Download available
Portuguese	Brazil	pt-BR	UMLanguagePack.pt-BR	Download available

Portuguese	Portugal	pt-PT	UMLanguagePack.pt-PT	Download available
Russian	Russia	ru-RU	UMLanguagePack. ru-RU	Download available
Spanish	Spain	es-ES	UMLanguagePack.es-ES	Download available
Spanish	Mexico	es-MX	UMLanguagePack.es-MX	Download available
Swedish	Sweden	sv-SE	UMLanguagePack.sv-SE	Download available

Return to top

UM Language Components and Features

There are several key components and features in Exchange 2010 Unified Messaging that enable users and callers to interact with a multiple-language Unified Messaging system. For these components and features to work correctly and enable callers to interact with the system in multiple languages, the UM language packs must be installed correctly on a Unified Messaging server.

Pre-recorded Prompts

The Exchange 2010 Unified Messaging server role is installed with a set of default audio prompt files. These audio files contain the recordings for Outlook Voice Access menus, voice mail greetings, and numbers that are used by Exchange Unified Messaging. The audio files are played by a Unified Messaging server to incoming callers, both internal and external. Many of the audio files are default prompts that provide the users of the Telephone User Interface (TUI) and Outlook Voice Access the information that they need to move through the TUI and the Voice User Interface (VUI). The prompts are located in *<Program Files>*\Microsoft\Exchange Server\V14\UnifiedMessaging\Prompts\<language>. The prompts used by the Unified Messaging server to help callers move through the menus shouldn't be replaced or changed.

When an additional UM language pack is installed, the pre-recorded prompts for that language will also be installed. After a UM language pack is installed, the pre-recorded prompts for that language can be used by UM dial plans and auto attendants.

TTS Languages

Unified Messaging relies on the Text-to-Speech (TTS) engine. TTS functionality is provided by the Microsoft Speech Server service. The TTS engine reads and converts written text into audible output that can be heard by a caller. The TTS engine reads and converts the following items in a user's mailbox:

- E-mail and voice mail message bodies, subjects, and names
- Calendar item bodies, subjects, locations, and names
- Personal contact names
- Users' default voice mail greetings

Note:

After a user has recorded personalized voice mail greetings, the TTS version of the voice greetings are no longer used.

Automatic Speech Recognition

In addition to TTS, Automatic Speech Recognition (ASR) support is included in Exchange 2010 Unified Messaging. ASR functionality is provided by the Microsoft Speech Server service. ASR enables callers to use voice commands to interact with the Unified Messaging

system. Using ASR, callers can move through menus and interact with items from their individual mailboxes, including messages, personal contacts, and calendar. ASR support is included with each language pack.

Return to top

Voice Mail Preview

In addition, UM language packs provide support for Voice Mail Preview, which allows users to quickly triage their voice messages by reading their transcripts from within a supported e-mail client such as Outlook or Outlook Web App.

When a caller leaves a voice message for a UM-enabled user, the voice message file and a transcript of the voice message are placed in the body of the voice mail message that's sent to the user's mailbox.

All UM language packs are single files that can be downloaded. These language packs include the pre-recorded prompts, grammar files, Text-to-Speech (TTS) translation, and ASR. However, not all the UM language packs contain support for Voice Mail Preview.

The following UM language packs contain support for all the components and features, including Voice Mail Preview:

1. English (US) - (en-US)
2. English (Canada) (en-CA)
3. French (France) - (fr-FR)
4. Italian - (it-IT)
5. Polish (pl-PL)
6. Portuguese (Portugal) (pt-PT)
7. Spanish (Spain) (es-ES)

For more information about Voice Mail Preview, see Voice Mail Preview for End Users.

By default, when you install the Exchange 2010 Unified Messaging server role, the server will send voice mail previews to UM-enabled users if a supported UM language pack is installed.

There are Exchange 2010 Unified Messaging Voice Mail Preview partners that offer enhanced transcription support for the Voice Mail Preview feature. These partners employ people to correct voice mail transcriptions that were created using Automatic Speech Recognition (ASR). Each Voice Mail Preview partner must meet a set of requirements to be certified to interoperate with Exchange 2010 Unified Messaging.

If you determine that the voice mail previews sent to your users aren't accurate enough, you can contact one of the certified Voice Mail Preview partners listed on the Microsoft PinPoint web page and sign up with them at an additional cost. For more information, see Voice Mail Preview Advisor for Exchange 2010.

You can download the Exchange 2010 UM language packs for SP1 from the Microsoft Download Center. For details, see Install a Unified Messaging Language Pack on a UM Server.

Unified Messaging Languages

To enable callers to use the multiple language features found in Exchange 2010 Unified Messaging, you must first install a UM language pack, as described below. Then you have the option to configure other UM components.

- Install the UM language pack on the Unified Messaging server.
- If required, configure the default language for a UM dial plan. This lets Outlook

Voice Access users associated with the UM dial plan use the new language when they access their mailbox. However, users can still configure their language setting in the options that are available in Outlook Web App.

- If required, configure the language setting on a UM auto attendant. By default, a UM auto attendant uses the UM dial plan language. However, you can change this setting and enable unauthenticated callers to connect to your organization and move through the auto attendant menus in the language that you've specified on the UM auto attendant.

Unified Messaging Server Languages

You install a UM language pack on the Unified Messaging server using Setup.com. After you install the new language pack on the Unified Messaging server, the language associated with the language pack will be added to the list of available languages that you can use. You can view the languages that have been installed using the **UM Settings** tab in the Unified Messaging server properties in the Exchange Management Console or using the Get-UMServer cmdlet in the Exchange Management Shell.

When you install the UM language pack, the files that are used by the TTS engine and the pre-recorded prompts for the chosen language are copied and made available for users who connect to the Unified Messaging system.

UM Dial Plan Languages

Each UM dial plan that's created contains a default language setting. The UM dial plan language setting is needed because Unified Messaging may have to use TTS conversion or play a standard audio prompt for Outlook Voice Access users when they access their Exchange 2010 mailbox. You don't have to select a default dial plan language.

When you first install Exchange 2010, U.S. English will be the default language, and the only available language option for your dial plan. After you install a UM language pack on a Unified Messaging server, the language associated with the language pack will be listed as an available option when you configure the default language for the dial plan.

The default language is important to callers. When an Outlook Voice Access user calls in to the Unified Messaging system, the language setting chosen is based on the language setting configured in Outlook Web App that was set when the user first signed in to the mailbox using Outlook Web App. Unified Messaging then compares the language set in Outlook Web App to the list of available languages on the dial plan with which the user is associated. If there is no suitable match for the language, the default UM dial plan language will be used. Sometimes, you may have to set this language as the default language. For example, if you have a dial plan that contains only users from France, you may want to change the default language setting on the dial plan to French. For more information about how to change the default language for a UM dial plan, see Configure the Default Language on a UM Dial Plan.

UM Auto Attendant Languages

By default, because UM auto attendants are associated with a UM dial plan when they are created, they use the default language setting of the associated UM dial plan. However, this setting can be changed after the UM auto attendant is created.

The UM auto attendant language setting is needed because Unified Messaging may have to use TTS conversion or play a standard audio prompt to a caller. Unified Messaging doesn't check whether the language of custom prompts for the auto attendant matches the language setting on the auto attendant. However, as a best practice, make sure that the language setting of the auto attendant matches the language of the custom prompts. Otherwise, the caller may hear the system shift from one language to another.

Being able to change the UM auto attendant language setting is also useful if you need several different language-specific auto attendants for callers. For more information about how to configure language settings on a UM auto attendant, see Configure the Language Setting on a UM Auto Attendant.

Important:
To ensure that all Unified Messaging features are available in the UM language packs you install, you must install the Exchange 2010 Client and Server Language Pack on each UM server in the dial plan. If you don't install the Client and Server Language Pack, some features may not work as expected. Some features, like Voice Mail Preview, will work in the language that is configured on the dial plan but when only the UM language pack is installed. However, features like Outlook Voice Access and user interface text won't work in the language by the user without having both the UM language pack and the Client and Server Language Pack installed. To download and install additional client and server language packs on servers in your organization, see the Microsoft Exchange Server 2010 SP1 Language Pack Bundle.

Return to top

1.9.1.3.5 Understanding Storage Quotas and Voice Mail

Understanding Storage Quotas and Voice Mail

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

When a caller leaves a voice message for a Unified Messaging (UM)-enabled user, the storage quotas or limits configured on the user's mailbox may prevent voice messages from being delivered correctly. This topic discusses the relationship between the configuration of the Microsoft Exchange Server 2010 Unified Messaging server and the storage quotas that could potentially prevent a caller from recording a voice message.

Looking for management tasks related to storage groups? See Managing Mailbox Servers.

Contents

UM Dial Plans

Although there are many Active Directory objects that must be created and configured when Exchange 2010 Unified Messaging is deployed, UM dial plan objects are the central component of the Unified Messaging system. A UM dial plan object is an Exchange 2010 organization-wide object created in the Active Directory directory service.

After you install the Unified Messaging server role, you must associate the Unified Messaging server with at least one UM dial plan. You can also associate a single Unified Messaging server with multiple UM dial plans. For more information about how to create a new UM dial plan, see Create a UM Dial Plan.

There are many configuration settings that you can change after you create a UM dial plan to meet the needs of your organization. After you create a UM dial plan, you can configure

subscriber access numbers, greetings, message properties, and other UM dial plan features. Although there are many settings that can be changed to control your Unified Messaging environment, one of the more important mailbox settings is storage quotas. If you don't set the storage quotas for users correctly, you might unintentionally prevent voice messages from being recorded for Exchange users in your organization.

Because Windows Media Audio (.wma) and .wav files are attached to each voice message, voice messages may be larger than e-mail messages. This may cause problems for users by filling their mailbox more quickly than e-mail messages that don't include attachments. When you plan your storage quotas for users, you should consider the maximum length of a voice message that a caller will leave. Very long voice messages create large files. However, you can control the size of the voice files by reducing the length of time that callers have to leave a voice message.

The **Maximum recording duration (minutes)** setting controls the maximum length for the recorded messages from callers. This setting can range from 5 through 100 minutes, but the default setting is 20 minutes. You can change this setting using the Exchange Management Console or using the **Set-UMDialPlan** cmdlet in the Exchange Management Shell. For more information about how to configure settings on a UM dial plan, see View or Configure the Properties of a UM Dial Plan.

In some Exchange environments, the default setting of 20 minutes may be too high or too low. If the storage quota is set too high, you may risk using too much storage space on your Exchange servers or users may exceed their storage quotas too quickly. If the storage quota is set too low, it may frustrate callers by not giving them enough time to leave a whole message. Callers may then have to call back to leave another voice message for the user.

Storage Quotas

Users may store too many e-mail and voice messages in their mailbox, in addition to attached files. If users in your organization store numerous e-mail messages, voice messages, and attached files, you may have to limit the storage space allocated to each user's mailbox to reduce the storage demands on your computers running Exchange 2010. Frequently, large mailbox stores lead to long backup and restore times. Large mailbox stores may also affect the availability and reliability of your Exchange environment. Therefore, we recommend that you control the size of users' mailboxes to avoid running out of storage space on your Exchange servers. When users don't have a storage quota configured or they have a large storage quota configured, they could possibly fill the disk drives on an Exchange server. To prevent this, enable and configure storage quotas on users' mailboxes. By default, and starting with the first installation, each new mailbox database includes the following default limits:

- **Warning** 1991680 kilobytes (KB)
- **Prohibit Send** 2097152 KB
- **Prohibit Send/Receive** 2411520 KB

After you configure storage quotas, if a storage limit is exceeded, the mailbox-enabled user is warned or prohibited from sending or receiving e-mail. You can use the default storage limits, or you can set your own storage limits to control the amount of data that can be stored in a user's mailbox. For more information about how to manage recipient storage quotas, see Managing User Mailboxes.

Because storage quotas are implemented in most Exchange environments, there may be times when a caller can't leave a voice message for a user. Make sure that you understand the effect that setting storage quotas can have on your Unified Messaging environment and correctly plan your storage quotas for users so that voice messages are recorded correctly.

Return to top

Voice Mail Delivery

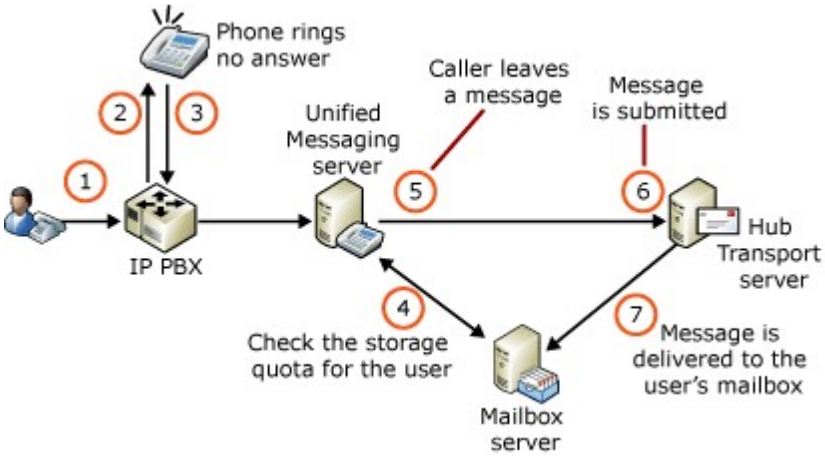
The following three scenarios describe what can occur when a voice message is delivered to a user's mailbox in different circumstances:

- The voice message fits into the user's mailbox.
- The voice message can't fit into the user's mailbox, and it fills the remaining storage space in the user's mailbox.
- The user's mailbox has already reached its storage capacity.

In the first scenario, the telephone rings and there's no answer. The call is transferred to the Private Branch eXchange (PBX) and then to the Unified Messaging server. The Unified Messaging server checks the user's mailbox storage quota. If the user's mailbox hasn't reached its storage limit and a voice message is created by the Unified Messaging server for the caller, the voice message is submitted to a computer that has the Hub Transport server role installed. The Hub Transport server then routes and submits the voice message to the appropriate Mailbox server. Because the voice message doesn't exceed the storage quota set for the user's mailbox and the storage quota hasn't already been reached, the voice message is delivered to the mailbox of the intended recipient.

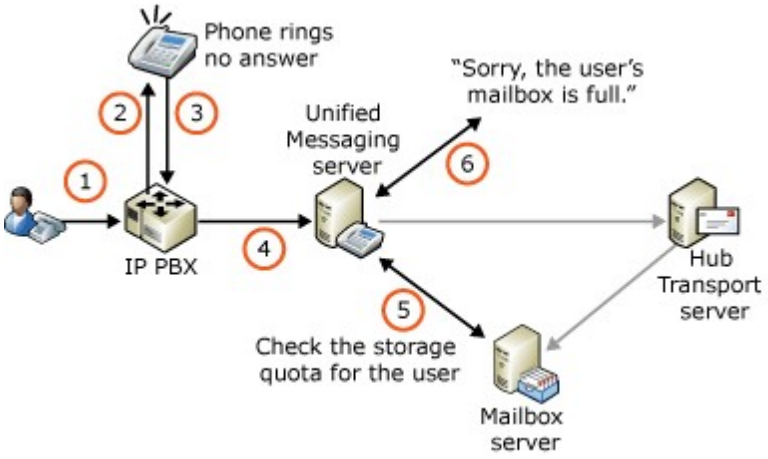
In the second scenario, the Unified Messaging server checks the user's mailbox storage quota. If the user's mailbox hasn't reached the storage limit, the voice mail message is submitted to a Hub Transport server. The Hub Transport server routes the voice mail message to the appropriate Mailbox server. The voice message is submitted to the Mailbox server, but the voice message fills the remaining storage space and exceeds the set storage quota for the user. When this occurs, the voice message is still delivered. Even though the storage quota is exceeded when the voice message is delivered, the voice message is still delivered the same way a non-delivery report (NDR) is delivered to a user even though the mailbox has reached its capacity.

The following figure illustrates how a voice message is submitted when the user's storage quota hasn't been reached and how a message is submitted when a voice message causes the storage quota to be reached for the user's mailbox.



In the third scenario, the Unified Messaging server checks the user's mailbox storage quota. Because the user's mailbox has already reached its storage capacity, the Unified Messaging server won't record a voice message and informs the caller that the recipient's mailbox is full. The user must delete or archive messages to reduce the size of the mailbox to be lower than the storage quota to be able to receive voice messages again.

The following figure illustrates how a call is handled when a user's mailbox storage quota has been reached.



Return to top

1.9.1.3.6 Understanding Unified Messaging VoIP Security

Understanding Unified Messaging VoIP Security

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-16*

An important aspect of your network security is the ability to protect your Unified Messaging (UM) infrastructure. There are components within your Unified Messaging environment that you must correctly configure to help protect the data sent and received from Unified Messaging servers on your network. These include components such as Unified Messaging servers and dial plans. This topic discusses how you can increase protection for the Unified Messaging network data and servers in your organization. You must follow these steps to help secure your Unified Messaging environment and enable Voice over IP (VoIP) security:

1. Install the Unified Messaging server role.
2. Create a new self signed or public certificate that you can use for mutual TLS.
3. Associate a certificate with the UM server.
4. Configure the UM dial plan as SIP Secured or Secured.
5. Configure the startup mode on the UM server.
6. Associate the Unified Messaging servers with the UM dial plan.
7. Configure the UM IP gateways used to have a fully qualified domain name (FQDN) and to use TCP port 5061.
8. Export and import the required certificates to enable the Unified Messaging servers, IP gateways, IP Private Branch eXchanges (IP PBXs), and other servers running Microsoft Exchange Server 2010 to use mutual Transport Layer Security (mutual TLS).

Contents

Types of Certificates

Configuring Mutual TLS

IPsec

UM Dial Plans and VoIP Security

How Unified Messaging Determines Security Mode and Selects Certificates

Protecting Unified Messaging

There are several security methods that can help you protect your Unified Messaging servers and the network traffic sent between your IP gateways and Unified Messaging servers and between your Unified Messaging servers and other Exchange 2010 servers in your organization. The following table lists some possible threats to your Unified Messaging infrastructure and the security methods that can be implemented to help protect it.

Protecting Unified Messaging

What am I protecting against?	How can I protect it?
Monitoring voice traffic	• Use Internet Protocol security (IPsec). The IP gateway or IP PBX must support IPsec. • Use Secure Realtime Transport Protocol (SRTP).
An attack against an IP gateway or IP PBX	• Use strong authentication methods. • Use strong administrative passwords. • Use Secure Sockets Layer (SSL) to protect administrative credentials. The IP gateway or IP PBX must support SSL. • Use Secure Shell (SSH) instead of Telnet.
Unauthorized long distance calls	• Use UM dial plan rules and dialing restrictions. These can be configured on the UM dial plan and UM mailbox policies. • Optionally, you may be able to enforce other dialing restrictions by configuring your PBX.
A denial of service attack	• The Unified Messaging server communicates only with UM IP gateways or IP PBXs included in the list of trusted VoIP devices or servers. This list of trusted VoIP devices or servers is created when a UM IP gateway is created in the Active Directory directory service. • Use mutual TLS.
A Session Initiation Protocol (SIP) proxy impersonation	• Use mutual TLS. • Use IPsec. The IP gateway or IP PBX must support IPsec. • Configure trusted LANs, such as virtual LANs (VLANs), dedicated WAN circuits,

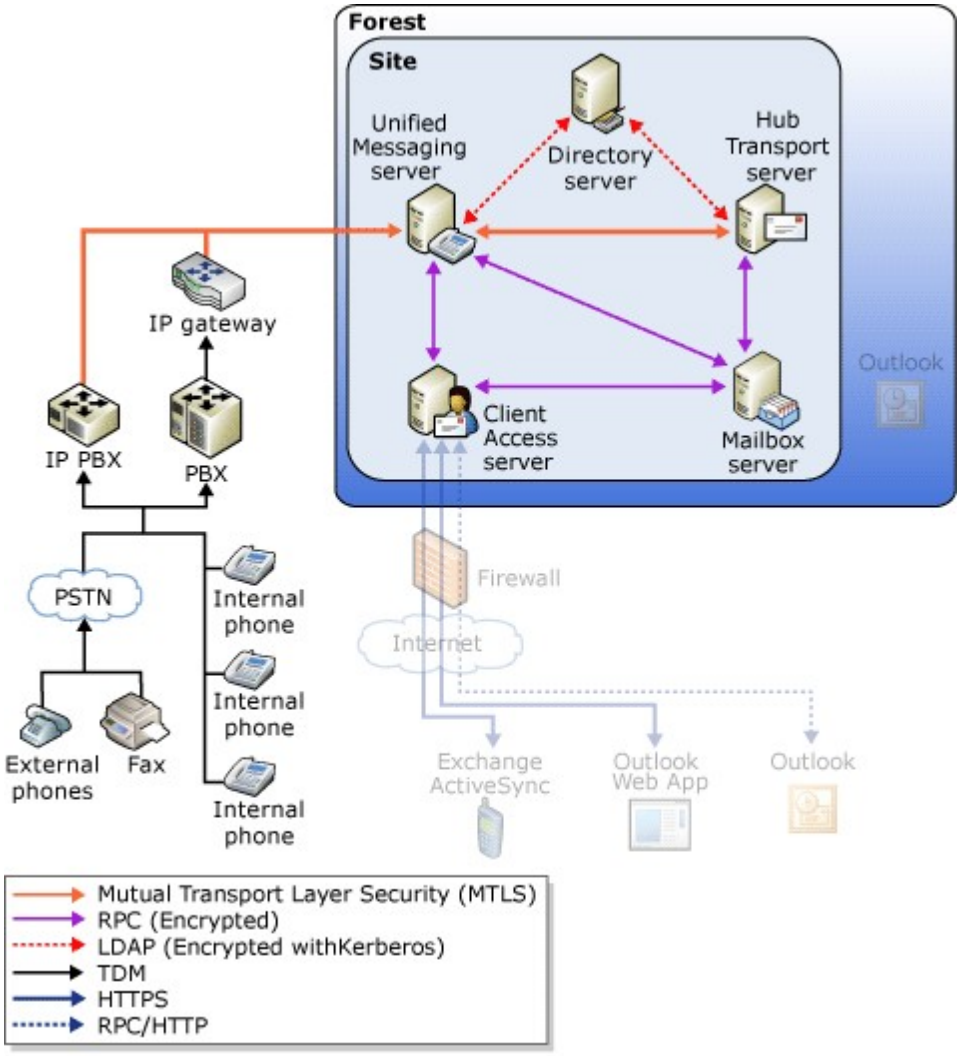
	or virtual private networks (VPNs).
Eavesdropping and session hijacking	• Use mutual TLS to reduce signal eavesdropping. • Use IPsec. The IP gateway or IP PBX must support IPsec. • Configure trusted LANs, such as VLANs, dedicated WAN circuits, or VPNs.

There are several security methods listed in the previous table that you can use to protect your Unified Messaging environment. One of the most important mechanisms for protecting your Unified Messaging infrastructure and the network traffic generated by Unified Messaging is mutual TLS.

You can use mutual TLS to encrypt Voice over IP (VoIP) traffic passed between IP gateways, IP PBXs, and other Exchange 2010 servers and the Unified Messaging servers on your network. The best choice for protecting this data is to use mutual TLS to encrypt the VoIP data.

However, depending on the security threat, you can also configure IPsec policies to enable data encryption between IP gateways or IP PBXs and a Unified Messaging server or between a Unified Messaging server and other Exchange 2010 servers on your network. In some environments, you might be unable to use IPsec because IPsec may be unavailable or may not be supported on the IP gateways or IP PBXs. Additionally, IPsec puts an additional processing load on system resources on Unified Messaging servers. Considering these two factors, mutual TLS is a better choice for protecting the VoIP network traffic in your Unified Messaging environment.

After you correctly implement and configure mutual TLS, the VoIP traffic between the IP gateways, IP PBXs, and from other Exchange servers to the Unified Messaging servers is encrypted. However, when mutual TLS cannot be used to help secure the traffic sent or received from a Unified Messaging server, such as when a Unified Messaging server communicates with another server on your network, such as an Active Directory domain controller or an Exchange 2010 Mailbox server, other types of encryption are used to protect the data. The following figure shows the methods of encryption that you can use to protect Unified Messaging.



Return to top

Types of Certificates

Digital certificates are electronic files that work like an online passport to verify the identity of a user or computer and are used to create an encrypted channel to protect data. A certificate is basically a digital statement issued by a certification authority (CA) that vouches for the identity of the certificate holder and enables the parties to communicate in a secure manner using encryption. They can be issued by a trusted third-party CA, such as Certificate Services, or be self-signed. Each type of certificate has its advantages and disadvantages. However, certificates are always tamperproof and cannot be forged. Certificates can be issued for a variety of functions, such as Web user authentication, Web server authentication, S/MIME, IPsec, TLS, and code signing.

A certificate binds a public key to the identity of the person, computer, or service that holds the corresponding private key. The public and private keys are used by both the client and the server to encrypt the data before it's transmitted across the wire. Certificates are used by a variety of public key security services and applications that provide authentication, data integrity, and secure communications across networks such as the Internet. For Windows-based users, computers, and services, trust in a CA is

established when there's a copy of the root certificate in the trusted root store and the certificate contains a valid certification path. This means that no certificates in the certification path have been revoked or have had the validity period expire.

Digital certificates do the following:

- They authenticate that their holders—people, Web sites, and even network resources such as routers—are truly who or what they claim to be.
- They protect data exchanged online from theft or tampering.

There are traditionally three options or kinds of certificates that Unified Messaging and IP gateways or IP PBXs can use. In all three approaches or options, the public key of the certificate owner is part of the certificate so that the server, user, Web site, or other resource on the other end can decrypt the messages. The private key is known only to the signer of the certificate. Each certificate has an **EnhancedKeyUsage** attribute set on it to dictate the specific usage for the certificate. For example, usage could be specified only for server authentication or for use with the encrypting file system. Unified Messaging uses the certificate for server authentication and data encryption.

Self-Signed Certificates

A self-signed certificate is a certificate signed by its own creator. The subject and the name of the certificate match. On self-signed certificates, the issuer and subject are defined on the certificate. Self-signed certificates don't require the presence of a CA from your organization or from a third party. You must configure these certificates explicitly and copy them to the trusted root certificate store on each IP gateway, IP PBX, other Unified Messaging servers, and other Exchange 2010 computers if they're to be trusted by the Unified Messaging server that has issued the certificate.

If a public key infrastructure (PKI)-based or third-party certificate is unavailable, the Unified Messaging server will search for a self-signed certificate in the local certificate store. If it cannot find a PKI or third-party certificate, it will generate a self-signed certificate for mutual TLS. However, because it's a self-signed certificate, it won't be trusted by the IP gateways, IP PBXs on the network, or other servers on the network. To make sure that the self-signed certificate is trusted by IP gateways, IP PBXs, or other servers, you must import the self-signed certificate into the local trusted root certificate store for the devices and servers. After you do this, when the Unified Messaging server presents this self-signed certificate to the IP gateway, IP PBX, or server, it will be able to verify that the certificate was issued by a trusted authority because the issuer will equal the subject defined on the self-signed certificate.

If you're using only self-signed certificates, you must import a single self-signed certificate for each IP gateway, IP PBX, or server. In large network environments that have multiple devices or computers, this may not be the best choice for implementing mutual TLS. Using self-signed certificates in a large enterprise network doesn't scale well because of the additional administrative overhead. However, administrative overhead isn't a problem if you have multiple devices and you're using a PKI or commercial third-party certificate. This is because each device has a certificate that has been issued by the same trusted root authority. Having a certificate from the same trusted root authority guarantees that all IP gateways, IP PBXs, and other servers trust the Unified Messaging server.

For mutual TLS to work using self-signed certificates:

1. Take the Unified Messaging server's self-signed certificate and import it into the trusted root certificate store on each IP gateway and IP PBX and on other servers that the Unified Messaging server will communicate with using mutual TLS.
2. Take the self-signed certificate from each IP gateway, IP PBX, and other server and import it into the Unified Messing server's trusted root certificate store. If you're using a PKI or third-party certificate, you will import the certification authority's certificate into the trusted root certificate store on all devices and servers.

Self-signed certificates are frequently not the best certificate option when you deploy mutual TLS or certificate-based authentication. However, smaller organizations with a limited number of devices or computers may decide to use the self-signed certificate method because it's the most easy to configure and the least expensive method to use when you implement mutual TLS. Frequently, smaller organizations decide not to use a third-party certificate or to install their own PKI to issue their own certificates because of the expense, because their administrators lack the experience and knowledge to create their own certificate hierarchy, or for both reasons. The cost is minimal and the setup is simple when you're using self-signed certificates. However, establishing an infrastructure for certificate life-cycle management, renewal, trust management, and revocation is much more difficult with self-signed certificates. For more information about how to create a certificate for TLS, see Understanding TLS Certificates.

Return to top

Public Key Infrastructure

A PKI is a system of digital certificates, CAs, and registration authorities (RAs) that verify and authenticate the validity of each party involved in an electronic transaction using public key cryptography. When you implement a CA in an organization that uses Active Directory, you provide an infrastructure for certificate life-cycle management, renewal, trust management, and revocation. These qualities provide a solid infrastructure for all the certificates in your organization. However, there's some cost involved in deploying additional servers and infrastructure to create and manage these types of certificates.

You can install Certificate Services on any server in the domain. If you obtain certificates from a domain Windows-based CA, you can use the CA to request or sign certificates to issue to your own servers or computers on your network. This enables you to use a PKI that resembles using a third-party certificate vendor but is less expensive. Although these PKIs cannot be deployed publicly, as other types of certificates can be, when a PKI is used, a CA signs the requestor's certificate using the private key, and the requestor is verified. The public key of this CA is included with the certificate issued by the CA. Anyone who has this CAs certificate as a root certificate can use that public key to decrypt the requestor's certificate and authenticate the requestor.

When you use a PKI certificate to implement mutual TLS, you must copy the required certificates to the IP gateways or IP PBXs. Then you must copy the certificates on the IP gateways or IP PBXs to the Unified Messaging servers associated with the UM dial plan that has been configured in secured mode.

The setup and configuration for using PKI certificates and third-party certificates resemble the procedures that you perform when importing and exporting the self-signed certificates. However, you mustn't only install the computer certificate into the trusted root certificate store. You must also import or copy the trusted root certificate for the PKI into the trusted root certificate store on the Unified Messaging servers and the IP gateways and IP PBXs on your network.

To deploy mutual TLS when you've already deployed a PKI infrastructure, follow these steps:

1. Generate a certificate request on each IP gateway or PBX.
2. Copy the certificate request to use when requesting the certificate from a certification authority.
3. Request a certificate from the certification authority using the certificate request. Save the certificate.
4. Import the certificate that you saved onto each device or computer.
5. Download the trusted root certificate for your PKI.
6. Import the trusted root certificate from your PKI on each device. If you're importing the trusted root certificate on an Exchange 2010 computer running the Unified Messaging server role, you can also use Group Policy to import the trusted root certificate into the trusted root certificate store on the

Unified Messaging server or other Exchange 2010 servers. However, this process is also used when you're configuring a server running the Unified Messaging server role.

Note:
You will use the same steps if you're using a commercial third-party certificate to implement mutual TLS.

For more information about certificates and PKIs, see the following topics:

- For more information about certificates, see Public Key Infrastructure for Windows Server 2003.
- For more information about best practices for implementing a Windows Server 2003 public key infrastructure, see Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure.
- For more information about how to deploy a Windows Server 2008-based PKI, see the Step-By-Step Example Deployment of the PKI Certificates Required for Configuration Manager Native Mode: Windows Server 2008 Certification Authority.
- For more information about Windows Server 2008 Certificate Services for a Windows Server 2008-based PKI, see Active Directory Certificate Services Overview.

Third-Party Certification Authorities

Third-party or commercial certificates are certificates generated by a third-party or commercial CA and then purchased for you to use on your network servers. One problem with self-signed and PKI-based certificates is that, because the certificate isn't trusted, you must make sure that you import the certificate into the trusted root certificate store on client computers, servers, and other devices. Third-party or commercial certificates don't have this problem. Most commercial CA certificates are already trusted because the certificate already resides in the trusted root certificate store. Because the issuer is trusted, the certificate is also trusted. Using third-party certificates greatly simplifies deployment.

For larger organizations or organizations that must publicly deploy certificates, it's best to use a third-party or commercial certificate, even though there's a cost associated with the certificate. Commercial certificates may not be the best solution for smaller and medium-size organizations, and you might decide to use one of the other certificate options available.

Depending on the configuration of the IP gateway or IP PBX, you might still have to import the third-party or commercial certificate into the trusted certificate store on the IP gateways and IP PBXs to be able to use the third-party certificate for mutual TLS. However, in some cases, the third-party certificate will be included in the trusted root certificate store on your Unified Messaging server and other Exchange 2010 computers in your organization.

The procedures that you perform to use a commercial third-party certificate for enabling mutual TLS are the same procedures that you perform when you use a PKI certificate. The only difference is that you won't have to generate a PKI certificate because you've purchased a certificate from a commercial third-party certificate vendor that will be imported into the trusted root certificate store on the servers and devices on your network.

Return to top

Configuring Mutual TLS

By default, when an incoming call is received from an IP gateway, the VoIP traffic isn't encrypted and doesn't use mutual TLS. However, the security setting for a Unified

Messaging server is configured on the UM dial plan associated with the Unified Messaging server. To enable the Unified Messaging server to communicate securely with IP gateways, IP PBXs, and other Exchange 2010 servers, you must use the **Set-UMDialPlan** cmdlet to configure VoIP security on the UM dial plan, and then enable mutual TLS for the Unified Messaging servers associated with the UM dial plan.

After you've enabled VoIP security on the UM dial plan, all Unified Messaging servers associated with the UM dial plan can communicate in a secure manner. However, depending on the type of certificate that you use for enabling mutual TLS, you must first import and export the required certificates both on the Unified Messaging servers and the IP gateways and PBXs. After the required certificate or certificates have been imported on the Unified Messaging server, you must restart the Microsoft Exchange Unified Messaging service to be able to use the certificate that was imported to establish an encrypted connection with the IP gateways or IP PBXs. For more information about how to import and export certificates, see Import and Export Certificates.

After you successfully import and export the required trusted certificates, the IP gateway will request a certificate from the Unified Messaging server, and then it will request a certificate from the IP gateway. Exchanging the trusted certificates between the IP gateway and the Unified Messaging server enables the IP gateway and Unified Messaging server to communicate over an encrypted connection using mutual TLS. When an incoming call is received by an IP gateway or IP PBX, it will initiate a certificate exchange and negotiate security using mutual TLS with the Unified Messaging server. The Microsoft Exchange Unified Messaging service isn't involved in the certificate exchange process or in determining whether the certificate is valid. However, if a trusted certificate cannot be located on a Unified Messaging server, a trusted certificate is found but isn't valid, or a call is rejected because of a mutual TLS negotiation failure, the Unified Messaging server will receive a notification from the Microsoft Exchange Unified Messaging service.

Although the Microsoft Exchange Unified Messaging service doesn't participate in the certificate exchange between the Unified Messaging server and the IP gateways, the Microsoft Exchange Unified Messaging service does the following:

- Provides a list of FQDNs to the Microsoft Exchange Speech service so that calls from only the IP gateways or IP PBXs included on the list are accepted.
- Passes the **issuerName** and **SerialNumber** attributes of a certificate to the Microsoft Exchange Speech service. These attributes uniquely identify the certificate that the Unified Messaging server will use when an IP gateway or IP PBX requests a certificate.

After the Unified Messaging server and the IP gateways or IP PBXs have performed the key exchange to establish an encrypted connection using mutual TLS, the Unified Messaging servers will communicate with the IP gateways and IP PBXs using an encrypted connection. The Unified Messaging servers will also communicate with other Exchange 2010 servers, such as Client Access servers and Hub Transport servers, using an encrypted connection that uses mutual TLS. However, mutual TLS will only be used to encrypt the traffic or messages submitted from the Unified Messaging server to a Hub Transport server.

Important:

To be able to enable mutual TLS between a UM IP gateway and a dial plan operating in secured mode, you must first configure the UM IP gateway with an FQDN and configure the UM IP gateway to listen on port 5061. To configure a UM IP gateway, run the following command: `Set-UMIPGateway -Identity MyUMIPGateway -Port 5061`.

Return to top

IPsec

IPsec also uses certificates to encrypt data. It provides a key line of defense against private network and Internet attacks.

IPsec has the following goals:

- To protect the contents of IP packets.
- To defend against network attacks through packet filtering and the enforcement of trusted communication.

IPsec is a framework of open standards that helps ensure private, secure communications over IP networks using cryptographic security services.

IPsec uses cryptography-based protection services, security protocols, and dynamic key management. It provides the strength and flexibility to protect communications between private network computers, domains, sites, remote sites, extranets, and dial-up clients. It can even be used to block receipt or transmission of specific types of traffic.

IPsec is based on an end-to-end security model that establishes trust and security from a source IP address to a destination IP address. The IP address itself doesn't have to be considered an identity. Instead, the system behind the IP address has an identity validated through an authentication process. The only computers that must know about the traffic being secured are the sending and receiving computers. Each computer handles security at its respective end and operates under the assumption that the medium over which the communication occurs isn't secure. Computers that route data only from source to destination aren't required to support IPsec unless firewall-type packet filtering or network address translation is being done between the two computers. This enables IPsec to be deployed successfully for the following organizational scenarios:

- **LAN** Client-to-server, server-to-server, and server-to-VoIP device
- **WAN** Router-to-router and gateway-to-gateway
- **Remote access** Dial-up clients and Internet access from private networks

Typically, both sides require IPsec configuration to set options and security settings that allow two systems to agree on how to help secure traffic between them. This is known as an IPsec policy. The Microsoft Windows 2000 Server, Windows XP, Windows Server 2003, and the Windows Server 2008 operating system implementations of IPsec are based on industry standards that were developed by the Internet Engineering Task Force (IETF) IPsec working group. Parts of IPsec-related services were jointly developed by Microsoft and Cisco Systems, Inc. For more information about how to configure IPsec policies, see Creating, modifying, and assigning IPSec policies.

For more information about IPsec, see IPSec Concepts.

Caution:

If you currently have IPsec policies implemented on your network, you must exclude the IP gateways and IP PBXs from the IPsec policy. If you don't, for every 3 seconds of a voice mail, there will be a 1 second drop of the voice transmission. This is a known issue and there's a hotfix for Windows Server 2003. For more information about this hotfix, see How to simplify the creation and maintenance of Internet Protocol (IPsec) security filters in Windows Server 2003 and Windows XP.

UM Dial Plans and VoIP Security

Unified Messaging servers can communicate with IP gateways, IP PBXs, and other Exchange 2010 computers in either unsecured, SIP secured, or secured mode depending on how the UM dial plan is configured. A Unified Messaging server can operate in any mode configured on a dial plan because the Unified Messaging server is configured to listen on TCP port 5060 for unsecured requests and TCP port 5061 for secured requests at the same time. A Unified Messaging server can be associated with a single or multiple UM dial plans and can be associated with dial plans that have different VoIP security settings. A single Unified Messaging server can be associated with dial plans configured to

use a combination of unsecured, SIP secured, or secured mode.

By default, when you create a UM dial plan, it will communicate in an unsecured mode, and the Unified Messaging servers associated with the UM dial plan will send and receive data from IP gateways, IP PBXs, and other Exchange 2010 computers using no encryption. In unsecured mode, both the Realtime Transport Protocol (RTP) media channel and SIP signaling information won't be encrypted.

You can configure a Unified Messaging server to use mutual TLS to encrypt the SIP and RTP traffic sent and received from other devices and servers. When you add a Unified Messaging server to a UM dial plan and configure the dial plan to use SIP secured mode, only the SIP signaling traffic will be encrypted, and the RTP media channels will still use TCP. TCP isn't encrypted. However, if you add a Unified Messaging server to a UM dial plan and configure the dial plan to use secured mode, both the SIP signaling traffic and the RTP media channels are encrypted. A secure signaling media channel that uses Secure Realtime Transport Protocol (SRTP) also uses mutual TLS to encrypt the VoIP data.

You can configure the VoIP security mode either when you're creating a new dial plan or after you create a dial plan using the Exchange Management Console or the **Set-UMDialPlan** cmdlet. When you configure the UM dial plan to use SIP secured or secured mode, the Unified Messaging servers associated with the UM dial plan will encrypt the SIP signaling traffic or the RTP media channels, or both. However, to be able to send encrypted data to and from a Unified Messaging server, you must correctly configure the UM dial plan, and devices such as IP gateways or IP PBXs must support mutual TLS.

You can use the **Get-UMDialPlan** cmdlet in the Exchange Management Shell to determine the security setting for a specific UM dial plan. If the VoIP security parameter has been enabled, you can verify that the Microsoft Exchange Unified Messaging service has started in secured mode by checking the application event log to see whether information events numbered 1114 and 1112 have been logged.

Important:

If you're configuring mutual TLS to encrypt data exchanged between a Dialogic model 2000 or 4000 IP gateway, you must use the Computer V3 certificate template that supports both server and client authentication. The Web Server certificate template that supports server authentication will only work correctly with Dialogic 1000 and 3000 IP gateways, AudioCodes IP gateways, and Microsoft Office Communications Server 2007.

Return to top

How Unified Messaging Determines Security Mode and Selects Certificates

When the Microsoft Exchange Unified Messaging service starts, it checks the associated UM dial plan and the *VoipSecurity* parameter setting and identifies whether it should start in a secured or an unsecured mode. If it determines that it must start in a secured mode, it then determines whether it has access to the required certificates. If the Unified Messaging server isn't associated with any UM dial plans, it determines which mode to start in by looking at the *StartSecured* parameter in the Msexchangeum.config file. This parameter can be set with a value of 0 or 1. A value of 1 starts the Unified Messaging server using encryption to protect the VoIP traffic. A value of 0 starts the server, but encryption won't be used to protect the VoIP traffic. If you want to change the startup behavior of the Unified Messaging server from secured to unsecured or from unsecured to secured, you can associate the server with the appropriate UM dial plans and then restart the Unified Messaging server. You can also change the configuration setting in the Msexchangeum.config configuration file and the restart the Microsoft Exchange Unified Messaging service.

If the Microsoft Exchange Unified Messaging service is started in unsecured mode, it will start correctly. However, make sure that you verify that the IP gateways and IP PBXs are also running in unsecured mode. Also, if you're testing the Unified Messaging server's connectivity in unsecured mode, use the **Test-UMConnectivity** cmdlet with the -*Secured:false* parameter.

If the Microsoft Exchange Unified Messaging service is started in secured mode, it queries the local certificate store to find a valid certificate to use for mutual TLS to enable encryption. The service first looks for a valid PKI or commercial certificate and then, if an appropriate certificate isn't found, it looks for a self-signed certificate to use. If no PKI, commercial, or self-signed certificate is found, the Microsoft Exchange Unified Messaging service creates a self-signed certificate to use to start in secured mode. If the Unified Messaging server is starting in unsecured mode, a certificate isn't needed.

All the details of the certificate used to start in secured mode will be logged whenever a certificate is used or if the certificate has changed. Some details logged include the following:

- Issuer Name
- Serial Number
- Thumbprint

The thumbprint is the Secure Hash Algorithm (SHA1) hash and can be used to uniquely identify the certificate used. You can then export the certificate used by the Microsoft Exchange Unified Messaging service to start in secured mode from the local certificate store and then import this certificate on the IP gateways and IP PBXs on your network into the trusted certificate store.

After an appropriate certificate has been found and is used, and no additional changes have occurred, the Microsoft Exchange Unified Messaging service will log an event one month before the certificate being used expires. If you don't make any changes to the certificate during this time, the Microsoft Exchange Unified Messaging service will log an event each day until the certificate expires and each day after the certificate has expired.

When the Unified Messaging server is looking for a certificate to use for mutual TLS to establish an encrypted channel, it will look in the trusted root certificate store. If there are multiple certificates that are valid and are from different issuers, the Unified Messaging server will choose the valid certificate that has the longest time before the certificate will expire. If multiple certificates exist, the Unified Messaging server will choose the certificates based on the issuer and the date that the certificate will expire. The Unified Messaging server will look for a valid certificate in this order:

1. PKI or commercial certificate with the longest expiration period.
2. PKI or commercial certificate with the shortest expiration period.
3. Self-signed certificate with the longest expiration period.
4. Self-signed certificate with the shortest expiration period. A valid commercial, PKI, or self-signed certificate is required. If a valid certificate isn't found, the Unified Messaging server will generate a self-signed certificate. The Unified Messaging server needs a valid certificate to encrypt the VoIP traffic when it's operating in SIP secured or secured mode.

Important:

When a new certificate is installed on a Client Access server used to encrypt Play on Phone data between the Client Access server and a Unified Messaging server, you must run the **IISreset** command from a command prompt to load the correct certificate.

Return to top

Understanding Operator Transfers in Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-14*

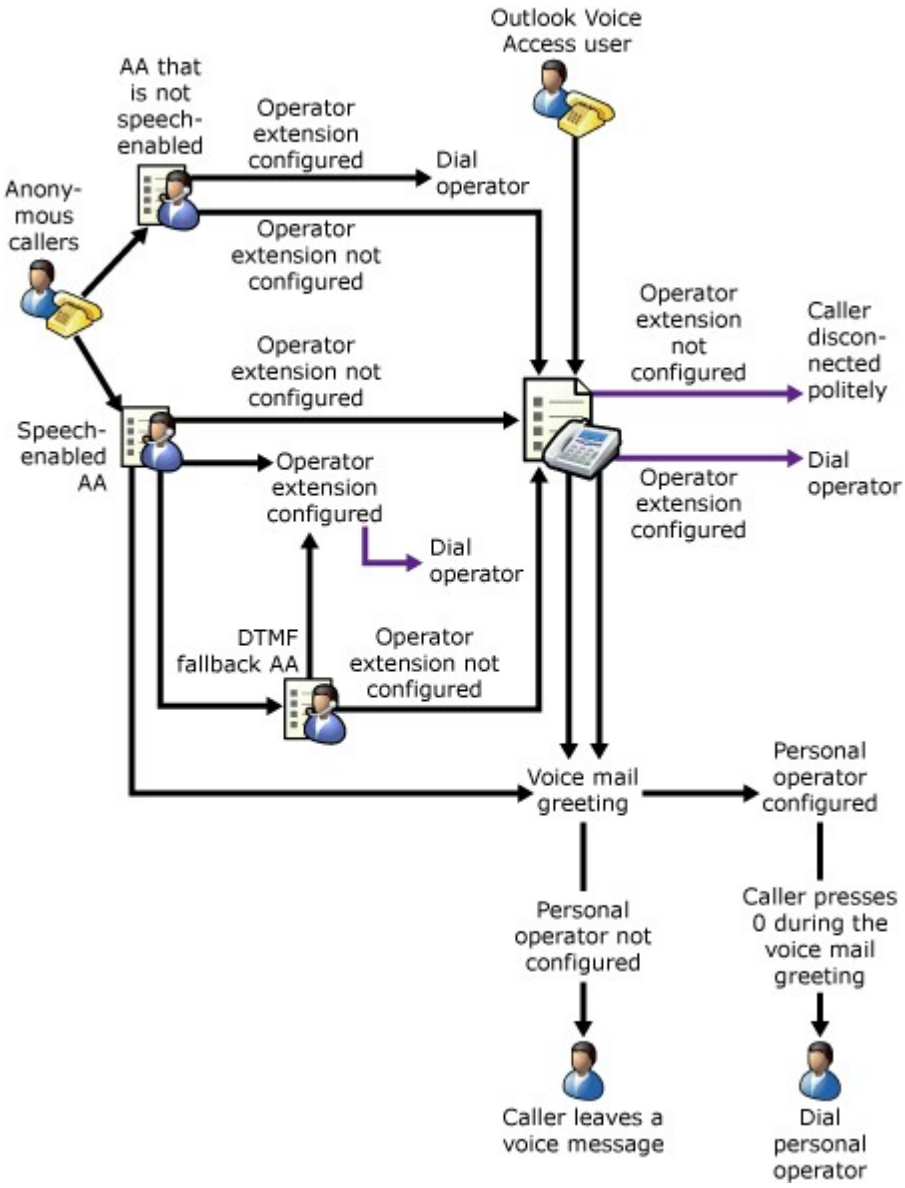
Microsoft Exchange Server 2010 Unified Messaging (UM) includes functionality that enables callers to be transferred to an operator if the caller isn't able to correctly navigate the system or must speak to a human operator. There are several types of operators that you can configure. These operators allow callers to be forwarded to the extension number of a receptionist, administrative assistant, operator, or in some cases, to another auto attendant. This topic discusses the different types of operators that you can configure in Exchange 2010 Unified Messaging and how incoming calls can be transferred to each type of operator, depending on how the caller dials in to the Unified Messaging system.

Overview of Operators in Unified Messaging

In Exchange 2010 Unified Messaging, you can configure one or all of the following types of operators:

- Dial plan
- Auto attendant
- Personal

The following figure illustrates the different types of operators found in Exchange 2010 Unified Messaging.



With Exchange 2010 Unified Messaging, you have the option to configure an operator extension on UM dial plans, UM auto attendants, and on UM-enabled users' mailboxes. If you configure an operator extension number on a UM dial plan or on a UM auto attendant that's not speech-enabled, the caller will hear a voice prompt that says, "To reach an operator, press 0." When a caller calls in to a speech-enabled UM auto attendant and an operator extension number is configured, the caller will have the option to press 0 or say "operator" or "reception" and be transferred to an operator extension number.

When you configure an operator extension number for a UM dial plan, auto attendant, or to another UM-enabled user (called a *personal operator*), you can configure the extension number using one of the following:

- **An internal telephone extension number** This can be an extension number for a specific person within the organization such as a receptionist, administrative assistant, or another person who's available to answer the call. Generally, this is an extension number where a person is always available to answer an incoming call.
- **The extension number for a UM auto attendant** This can be used when you

want to allow callers additional menu options before they're transferred to a human operator or when your organization doesn't have a human operator. In this case, you can configure an extension number that transfers the incoming call to the extension number associated with a UM auto attendant. The auto attendant can be either speech-enabled or not speech-enabled.

- **An external telephone number** This can be used when a vendor or external answering service is used to answer incoming calls for your organization. If you choose to configure an operator extension number with a telephone number external to your organization, you must verify that you've correctly configured your outdialing rules on the UM dial plans and Private Branch eXchanges (PBXs) so that the calls are transferred successfully.

At a minimum, we recommend that you configure either the UM dial plan or a UM auto attendant associated with the dial plan to have an operator extension number to help callers find the person they're trying to reach or to navigate the menu system. For more information about how to configure an operator extension on a UM auto attendant, see Configure an Operator Extension on a UM Auto Attendant. For more information about how to configure an operator extension number on a UM dial plan, see Configure an Operator Extension on a UM Dial Plan.

Dial Plan Operators

Although Exchange 2010 Unified Messaging has many Active Directory objects that must be created and configured during deployment, a UM dial plan is a central component of the Unified Messaging system. A UM dial plan is an Exchange 2010 organization-wide object created in the Active Directory directory service.

The UM dial plan is an Active Directory object that represents sets or groupings of PBXs that share common user extension numbers. In practical terms, user extensions hosted on PBXs share a common extension numbering format. Users in the same dial plan can dial one another's telephone extensions without appending a special number to the extension or dialing a full telephone number. Therefore, a UM dial plan is a representation of a telephony dial plan created on a PBX or IP PBX.

There are two types of callers who access the Unified Messaging system using the subscriber access number configured on a UM dial plan: unauthenticated callers and authenticated callers. When callers dial the subscriber access number configured on a dial plan, they're considered anonymous (unauthenticated) until they input information. This information includes their voice mail extension and a PIN. The only option available to anonymous (unauthenticated) callers is the directory search feature. However, if an operator extension number is configured on the dial plan, unauthenticated users can use the directory search feature and can also press 0 to be transferred to the operator extension number configured on the dial plan.

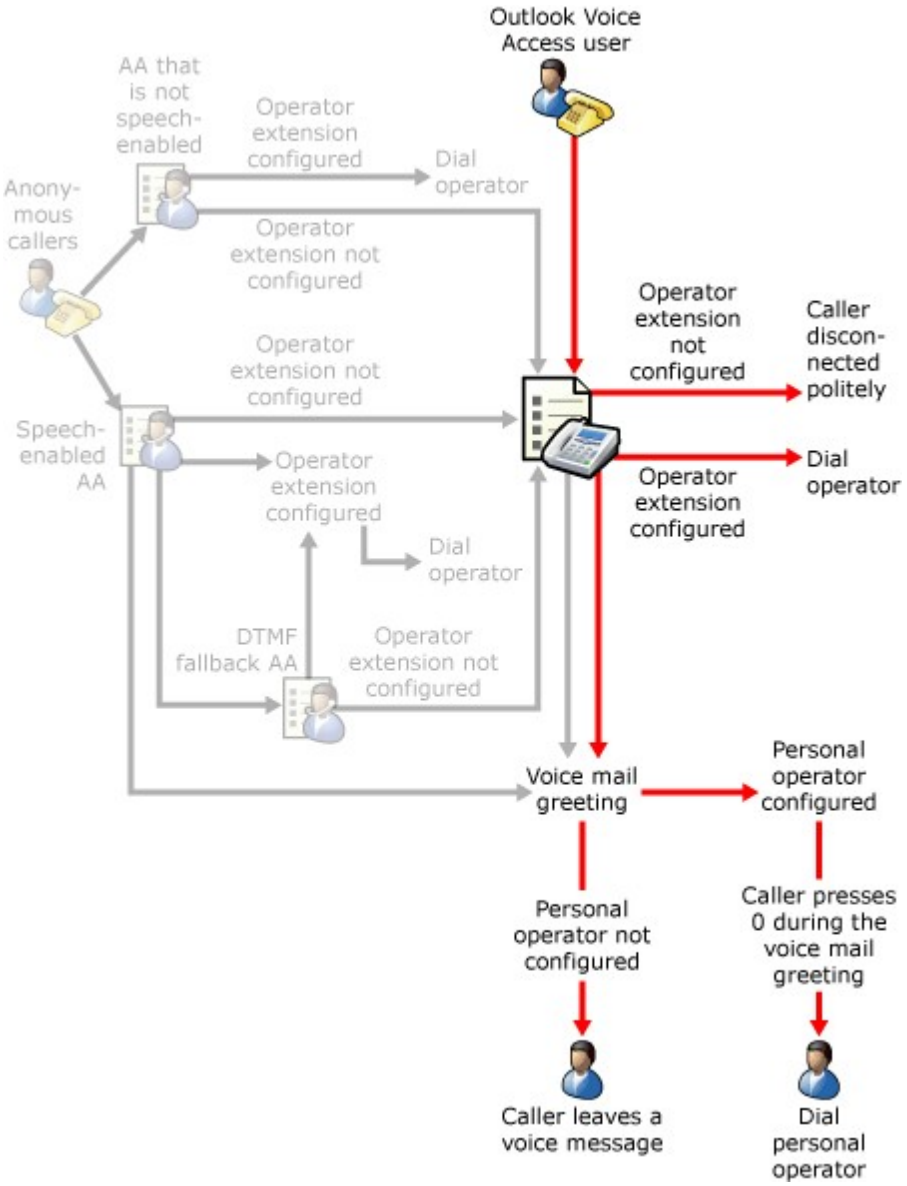
After callers input their extension number and their PIN, they're authenticated and given access to their Exchange 2010 mailbox. After they gain access to their mailbox, they use Outlook Voice Access. Outlook Voice Access is a series of voice prompts that allows authenticated callers to access their e-mail, voice mail, calendar, and contact information using a standard analog, digital, or mobile phone. Outlook Voice Access also enables authenticated callers to navigate their personal information in their mailbox, place calls, locate users, and navigate the system prompts and menus using dual tone multi-frequency (DTMF), also known as touchtone, inputs or voice inputs.

When UM-enabled users use Outlook Voice Access, they can perform the following tasks:

- Listen to new and saved e-mail and voice mail messages.
- Forward, reply, save, and delete e-mail and voice mail messages.
- Interact with their calendar.
- Locate a person in the global address list or personal contacts.
- Send a voice message to a person.

- Change their PIN, spoken name, or greetings.

When an Outlook Voice Access user dials the subscriber access number configured on a UM dial plan, and an operator extension has been configured on the dial plan, and the user presses the 0 key or says "operator" or "reception," the user will be transferred to the telephone number that you configured on the UM dial plan. If no telephone number has been configured for an operator extension on the dial plan, users won't be given the option to reach an operator and will be politely disconnected from the Unified Messaging system. The following figure illustrates the operator transfer options available to Outlook Voice Access users when they dial in to a subscriber access number.



For more information about subscriber access in Exchange 2010 Unified Messaging, see Understanding Unified Messaging Subscriber Access.

For a printable copy of the menus and options available with Outlook Voice Access, see the Microsoft Download Center for a copy of the Outlook Voice Access Quick Start Guide.

Auto Attendant Operators

In Exchange 2010 Unified Messaging, many Active Directory objects must be created and configured during and after deployment. UM auto attendants aren't required objects; they're optional. UM auto attendant objects are Exchange 2010 organization-wide objects created in Active Directory.

Exchange 2010 Unified Messaging enables you to create one or more UM auto attendants, depending on the needs of your organization. UM auto attendants can be used to create a voice menu system for an organization. This voice menu system lets external and internal callers locate users in an organization and place or transfer calls to users, departments, or to an operator extension number configured on the UM auto attendant.

There are three types of UM auto attendants that you can configure to use an operator extension number:

- Auto attendants that aren't speech-enabled
- Speech-enabled auto attendants that don't have a DTMF fallback auto attendant
- Speech-enabled auto attendant that have a DTMF fallback auto attendant

You can configure the operator extension number on a UM auto attendant to be the extension number of a human operator, another auto attendant, a UM-enabled mailbox, or a telephone number external to an organization. The internal or external telephone number you enter for the operator's extension number can be from 1 through 20 digits.

You can configure an operator extension number on UM auto attendants that are speech-enabled and on auto attendants that aren't speech-enabled. Configuring an operator extension number on a UM auto attendant allows callers to press 0 or say "operator" or "receptionist" to transfer to a human operator or another auto attendant if they can't navigate the auto attendant menu.

If you use an external telephone number, you must verify that you've correctly configured the appropriate outdialing rule groups and entries to enable this functionality. For more information about how to configure outdialing entries, see Create a Dialing Rule Entry on a UM Dial Plan.

If you create a speech-enabled auto attendant and configure an operator extension on the speech-enabled auto attendant, when the caller says "operator," the auto attendant will forward the call to the number configured on the speech-enabled auto attendant. If the speech-enabled auto attendant is configured to have a DTMF fallback auto attendant but not to have an operator extension number, and the DTMF auto attendant is configured to have an operator extension number, the operator extension number on the DTMF fallback auto attendant will be dialed. If no extension number is configured on the speech-enabled auto attendant or the DTMF fallback auto attendant, and the caller says "operator," the system will call the operator extension configured on the dial plan associated with the auto attendant. If neither of the auto attendants or the dial plan is configured to have an operator extension, the system will respond by saying "Sorry. Neither the operator or the touchtone service are available."

Note:

At a minimum, we recommend that you configure either the auto attendant or the dial plan associated with the auto attendant to have an operator extension number to help callers.

Operator Transfers for Business and Non-business Hours

For UM auto attendants, you can configure business hours operator transfers on the properties for the UM auto attendant. By default, business hours transfers are enabled. You can also configure non-business hours operator transfers on the UM auto attendant.

However, by default, the business hours for a UM auto attendant are 24 hours a day, so non-business hours or after hours operator transfers aren't available. To configure operator transfers after business hours, you must first configure the business hours schedule on the UM auto attendant properties and then enable or disable operator transfers during business or non-business hours.

By default, operator transfers are disabled for non-business hours. However, you can enable operator transfers for non-business hours to allow callers to be transferred to an operator. Operator transfers for non-business hours happen according to the business hours you've defined on the **Times** tab on the properties of the UM auto attendant.

- For more information about how to configure business and non-business hours for your organization, see Configure Business Hours for a UM Auto Attendant.
- For more information about how to configure the business hours for a UM auto attendant, see Configure Business Hours for a UM Auto Attendant
- For more information about how to enable or disable operator transfers during business hours, see Enable or Disable Operator Transfers During Business Hours on a UM Auto Attendant.

When you configure an operator extension number on a UM auto attendant and enable non-business hours operator transfers, a caller can connect to the auto attendant operator by doing one of the following:

- Pressing the zero (0) key
- Saying "Reception"
- Saying "Operator"

Note:

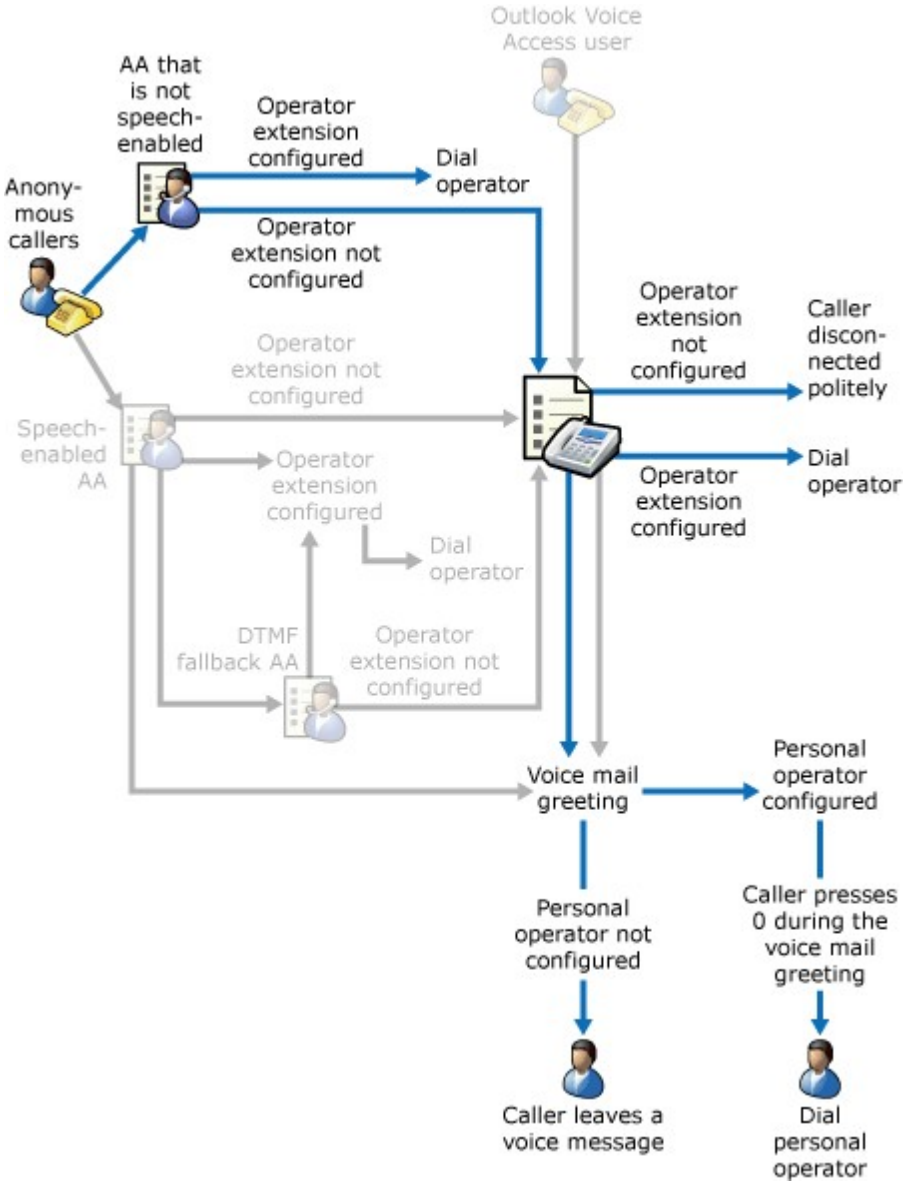
If callers exceed the maximum number of touchtone or voice input retries, they're also transferred to the operator extension number, if you've defined an operator extension number and enabled non-business hours operator transfers.

If no operator extension number is configured on a speech-enabled auto attendant, an auto attendant that isn't speech-enabled, or a DTMF fallback auto attendant, and the caller says "Operator" or "Reception" or presses the zero (0) key, the system will call the operator extension that's configured on the dial plan associated with the auto attendant. If neither of the auto attendants or the dial plan is configured to have an operator extension, the system will respond by saying, "Sorry. Neither the operator or the touchtone service are available." The caller will be politely disconnected. By default, an operator extension number isn't configured on a dial plan.

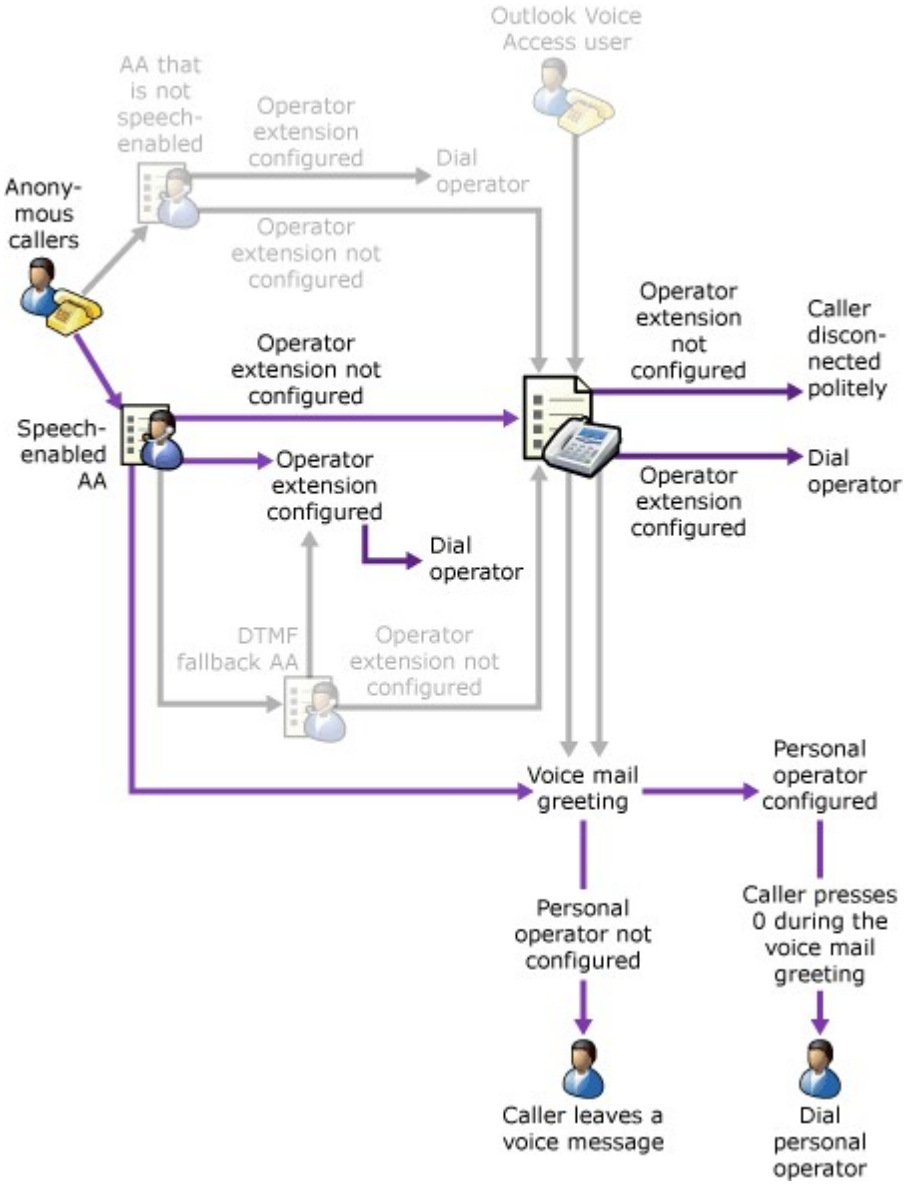
- At a minimum, we recommend that you configure either the UM auto attendant or the UM dial plan associated with the auto attendant to have an operator extension number. This will help callers find the user they're trying to reach or navigate the menu system.
- For more information about how to configure an operator extension on a UM auto attendant, see Configure an Operator Extension on a UM Auto Attendant.
- For more information about how to enable or disable operator transfers after business hours, see Enable or Disable Operator Transfers After Business Hours on a UM Auto Attendant.

Auto Attendant Operator Transfers

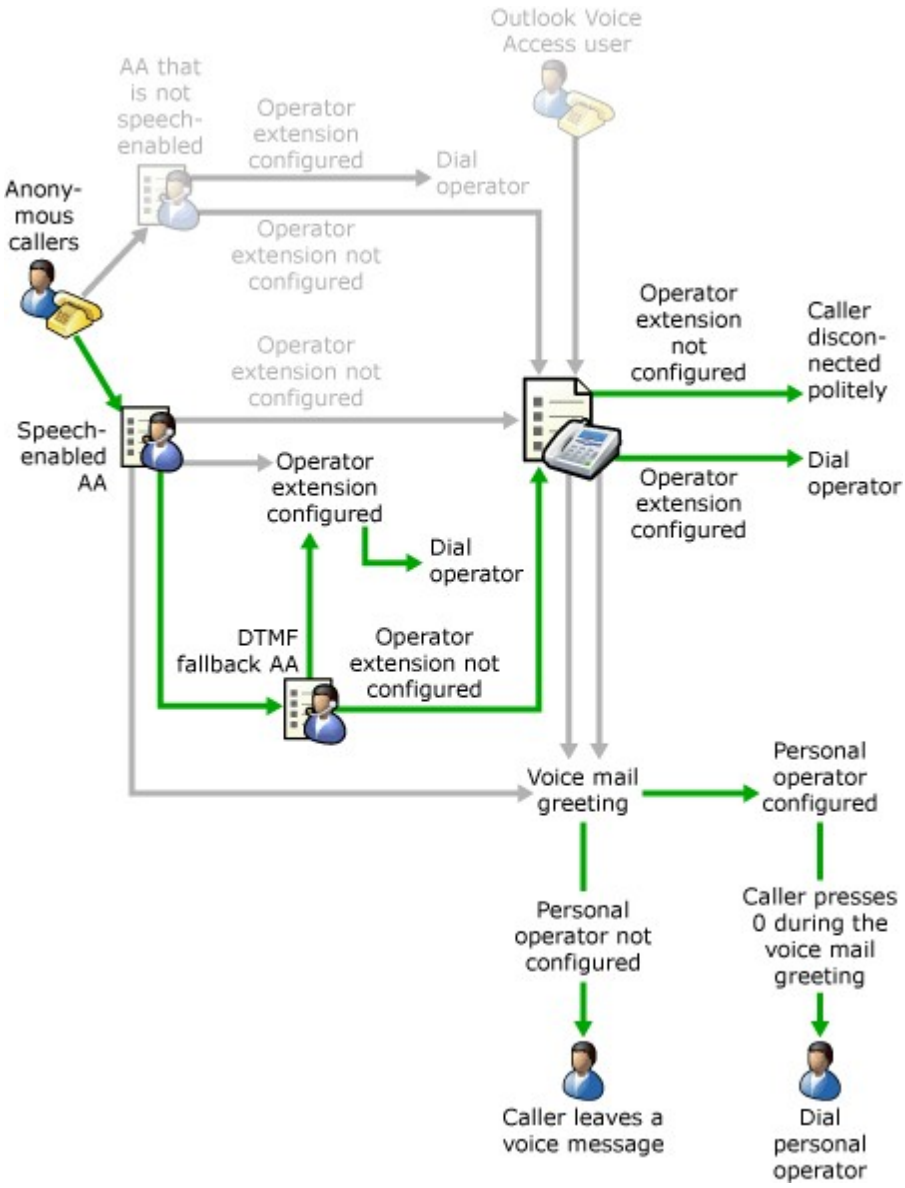
- The following figure illustrates the operator transfer options available to callers when they dial in to a UM auto attendant that's not speech-enabled. For more information about how to create a UM auto attendant, see Create a UM Auto Attendant.



The following figure illustrates the operator transfer options available to callers when they dial in to a UM auto attendant that's speech-enabled but doesn't have a DTMF fallback auto attendant configured. For more information about how to speech-enable a UM auto attendant, see Enable or Disable Automatic Speech Recognition on a UM Auto Attendant.



The following figure illustrates the operator transfer options available to callers when they dial in to a UM auto attendant that's speech-enabled and also has a DTMF fallback auto attendant configured. For more information about how to configure a UM auto attendant that has a DTMF fallback auto attendant, see Configure a UM Auto Attendant with a DTMF Fallback Auto Attendant.



Although UM auto attendants are an optional feature that can be created and configured when you're deploying Unified Messaging, we recommend that if you make the choice to create and configure a single UM auto attendant or multiple auto attendants, you take the time to plan them carefully. One of the most important factors when planning for auto attendants is to make sure that callers can contact a human operator or another auto attendant to correctly direct their calls. If you don't plan and implement the auto attendants for your organization correctly, the system could frustrate callers so that they won't call in to the system again.

Personal Operators

Exchange 2010 Unified Messaging enables you, as the administrator, to configure a personal operator extension number on a user's UM-enabled mailbox. However, the UM-enabled user won't be able to configure this setting. If UM-enabled users were able to configure this setting, they could potentially forward all their calls to another UM-enabled user or to an internal extension number that isn't valid. This could be very frustrating for

both the user to whom the calls were being forwarded and the callers. A caller wouldn't be able to leave a voice message for the person they were trying to contact and could lose their place in the menu system, and might eventually give up without reaching the person they were trying to contact.

The personal operator extension setting on a UM-enabled user's mailbox can be used when an administrative assistant or personal assistant answers incoming calls for a specific user instead of voice mail being generated for the user. By default, a personal operator extension number isn't defined.

For a caller to be transferred to a personal operator, the caller must press zero (0) on the telephone keypad when the user's custom voice mail message greeting is being played. Therefore, we recommend that, if users are going to use a personal operator, they include information in their custom voice mail greeting to give the caller instructions about how to access their personal operator.

However, if the user hasn't configured a customized voice mail greeting, the default system greeting will be used and the system will add the operator prompt automatically. For example, "Please leave a message for Tony Smith. To speak to an administrative assistant and leave a message, press 0." If the caller doesn't press 0 during the voice mail greeting, the caller will be able to leave a voice message for the user.

If you haven't configured a personal operator extension for a UM-enabled user's mailbox, the Unified Messaging server uses the operator extension number configured on the UM auto attendant or UM dial plan, depending on which number the caller has called. If callers have called an auto attendant telephone extension number, they're forwarded to the operator, if one has been configured on the UM auto attendant. If they've called the subscriber access number configured on a UM dial plan, they're forwarded to the operator extension number configured on the UM dial plan. If an operator extension hasn't been configured, callers are politely disconnected from the system. For more information about how to configure a personal operator, see Enable or Disable a Personal Operator for a UM-Enabled User.

In most cases, an internal extension number for an administrative assistant, receptionist, or operator will be configured as a personal operator. A personal operator extension number can be configured as an internal or external telephone number that ranges from 1 through 20 digits. However, if you use an external telephone number, you must verify that you've correctly configured the appropriate outdialing rule groups and entries to enable this functionality. For more information about how to configure outdialing entries, see Create a Dialing Rule Entry on a UM Dial Plan.

1.9.1.3.8 Understanding Outdialing

Understanding Outdialing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-03*

There are many outdialing settings used on a Microsoft Exchange Server 2010 Unified Messaging (UM) server to dial internal and external calls for users. To configure outdialing, you must configure dialing rule groups, dialing rule entries, and dialing restrictions on UM dial plans and UM mailbox policies. Additionally, you can also configure UM dial plans to have dialing or access codes, a national number prefix, and in-country/region or international number formats that enable you to control outdialing in your organization.

This topic discusses dialing rule groups, dialing rule entries, and dialing restrictions and how they are used to control outdialing for your organization.

Contents

Overview

Outdialing is the process used by users when they call in to a UM dial plan or UM auto attendant and place or transfer a call to an internal or external telephone number. When a user calls in to a UM dial plan or a UM auto attendant and places a call, a Unified Messaging server will use the settings configured on the dial plan, auto attendant, and if appropriate, the UM mailbox policy to place the call. The outdialing process happens when:

- A Unified Messaging server places a call to an external telephone number for a caller.
- A Unified Messaging server transfers a call to an auto attendant.
- A Unified Messaging server transfers a call to a user in your organization who is UM-enabled or not UM-enabled.
- A UM-enabled user uses the Play on Phone feature found in Microsoft Office Outlook 2007 or Outlook Web App in Exchange 2010.

For outdialing to work correctly, the following settings must be configured correctly:

- **Dialing group rules** Dialing group rules determine the types of calls users within a dial group can make.
- **Dialing rule entries** Dialing rule entries define the number that is dialed by the UM-enabled user and the actual number that will be dialed by the Private Branch eXchange (PBX) or IP PBX.
- **Dialing restrictions** Dialing restrictions determine the restrictions that will be applied to prevent users from incurring unnecessary telephone charges or from dialing long distance calls.

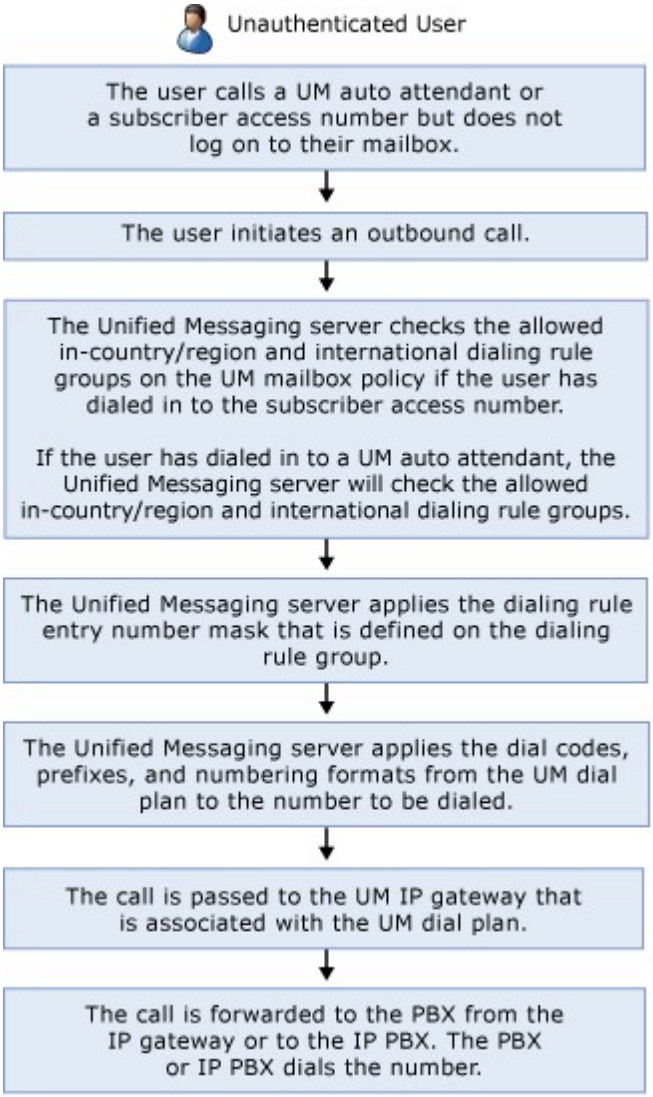
To enable outdialing for users who call into a dial plan or auto attendant, you must:

- Make sure the UM IP gateway or IP gateways associated with the dial plan will allow outgoing calls.
- Create dialing rule groups by creating dialing rule entries on the UM dial plan.
- Create dialing restrictions on the UM dial plan or auto attendant associated with the same dial plan as the UM IP gateway.

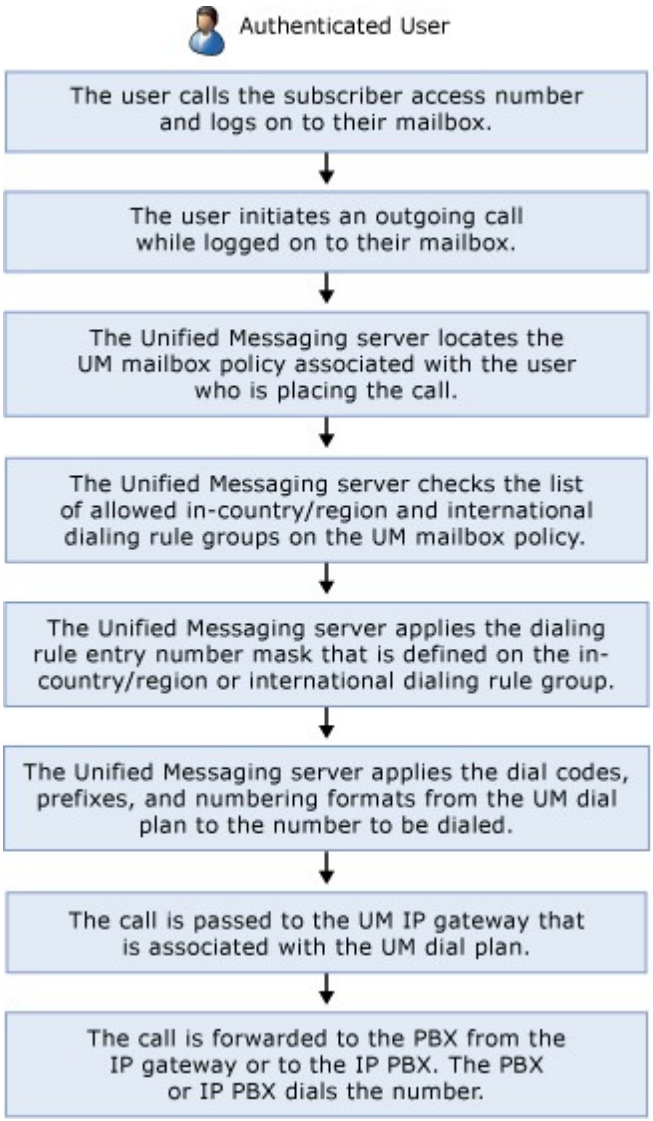
UM-Enabled Users

There are two types of users who can use the outdialing feature in Unified Messaging: authenticated and unauthenticated. The users who call in to a subscriber access number configured on a UM dial plan are unauthenticated at first. All users who call in to a UM

auto attendant are unauthenticated. When users call in to a subscriber access number, they are considered unauthenticated because they haven't provided their extension number and PIN and signed in on to their Exchange 2010 mailbox. The following figure illustrates the outdialing process for an unauthenticated user.



Users are authenticated after they provide their extension number and PIN and successfully sign in to their Exchange 2010 mailbox. The following figure illustrates the outdialing process for a user who has been authenticated.



When users call in to a subscriber access number configured on a UM dial plan and try to place or transfer a call without signing in to their Exchange 2010 mailbox, only the UM dial plan outdialing settings will apply to the call. Users are unauthenticated because they didn't sign in to their mailbox. However, when anonymous or unauthenticated users call in to a UM auto attendant, both the outdialing settings configured on the auto attendant and the outdialing settings configured on the dial plan associated with the auto attendant are applied to the call.

When users call in to the subscriber access number configured on a dial plan and successfully sign in to their Exchange 2010 mailbox, they become authenticated users. The configuration settings from the UM dial plan and the UM mailbox policy associated with the authenticated user are both applied to any outdialing calls the user makes.

Return to top

Outdialing Settings

There are several settings that you must configure to apply outdialing rules for your organization. To control outdialing, you must configure the UM dial plans, UM auto

attendants, and UM mailbox policies that you have created. The following outdialing settings are configured on dial plans, auto attendants, and UM mailbox policies:

- Outside line, country/region, and international access codes
- National number prefixes
- In-country/region and international number formats
- Configured in-country/region and international dialing rule groups
- Allowed in-country/region and international dialing rule groups
- Dialing rule entries
- Dialing restrictions

For you to successfully configure outdialing for your Exchange 2010 organization, you must first understand how each component can be used with outdialing and how the component must be configured. The following table introduces each component that must be configured on UM dial plans, UM auto attendants, and UM mailbox policies to enable outdialing to function correctly.

Outdialing components

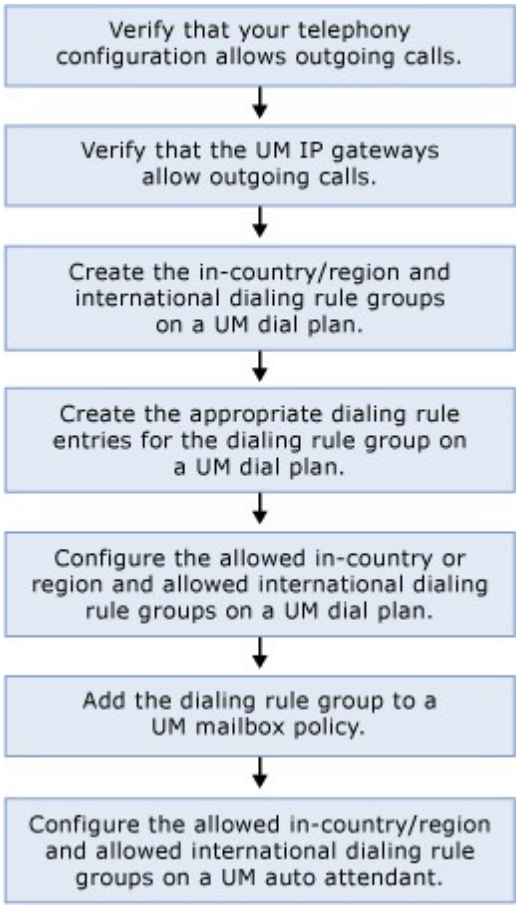
Component	Description
Dial codes, number prefixes, and number formats	Dial codes, number prefixes, and number formats are used by a Unified Messaging server to determine the correct number to dial when placing an outgoing call. You can configure dial codes, number prefixes, and number formats to restrict outgoing calls for users who dial in to a UM auto attendant associated with a UM dial plan or for users who dial in to the subscriber access number configured on the dial plan. For more information about dial codes, number prefixes, and number formats, see Understanding Dial Codes, Number Prefixes, and Number Formats.
Dialing rule groups	Dialing rule groups are created to enable telephone numbers to be modified before they are sent to the Private Branch eXchange (PBX) for outgoing calls. Dialing rule groups remove numbers from or add numbers to telephone numbers being placed by a Unified Messaging server. For example, you can create a dialing rule group that automatically adds a 9 as a prefix to a 7-digit telephone number to provide access to an outside line. In this example, users who place outgoing calls don't have to dial the 9 before the telephone number to reach someone external to the organization. Each dialing rule group contains dialing rule entries that determine the types of in-country/region and international calls that users within a dialing rule group can make. Dialing rule groups apply to the users who are associated with a UM dial plan or UM auto attendants and UM mailbox policies associated with the UM dial plan. Each dialing rule group must contain at least one dialing rule entry.

Dialing rule entries	A dialing rule entry is used to determine the types of calls that users within a dialing rule group can make. When you create a dialing rule group, you configure one or more dialing rule entries. When you configure each dialing rule entry, you must enter the name, number mask, and dialed number. You can also enter a comment. Comments can be used to describe how the dialing rule entry will be used or to describe a group of users to whom the dialing rule entry will apply. When you add a number mask and the dialed number to a dialing rule entry, you can substitute the letter x to replace a digit in a telephone number, for example, 91425xxxxxxx. You can also use an asterisk (*) symbol as a wildcard character, for example, 91425*.
Dialing restrictions	A dialing restriction uses dialing rule groups to apply dialing restrictions for users who are associated with a specific UM mailbox policy. They can also be used when you want to let users place calls to in-country/region or international telephone numbers. After you create a dialing rule group on a UM dial plan, you add the dialing rule group to a UM mailbox policy. After the dialing rule group is added to a UM mailbox policy, all settings or rules defined will apply to UM-enabled users who are associated with the UM mailbox policy.

Return to top

We recommend that you follow the steps in the following figure when you configure outdialing on your dial plans, auto attendants, and UM mailbox policies, to ensure that outdialing functions correctly.

Configuring outdialing



Configuring Outdialing

A dialing rule group is a collection of one or more dialing rule entries configured on a UM dial plan. There are two types of dialing rule groups that can be configured on a UM dial plan: in-country/region and international. In-country/region dialing rule groups apply to telephone numbers dialed within the same country or region. International dialing rule groups apply to international telephone numbers dialed from one country or region to another country or region.

Each UM dial plan can contain one or more dialing rule groups. However, to apply a dialing rule group to a set of users, after you create the dialing rule group, you must add the configured dialing rule group to the list of allowed dialing rule groups on the UM dial plan and on the UM auto attendants and UM mailbox policies associated with the UM dial plan.

Dialing rule groups enable you to specify dialing rule entries that you want to apply to a group of UM-enabled users who fall into a specific category. For example, you can use dialing rule groups to specify which group of users can place international calls and which group can only make in-state or local calls. You can create a dialing rule group using the Exchange Management Console or the **Set-UMDialPlan** cmdlet in the Exchange Management Shell. When you create a dialing rule group, you must define at least one dialing rule entry for the dialing rule group.

When a number is dialed by a user, the Unified Messaging server takes the telephone number and looks for a match in the dialing rule entries. If a match is found, the dialing rule entry configured on the dialing rule group is applied. The Unified Messaging server looks at the dialing rule entry to determine the number to dial by looking at the telephone number or digits listed in the DialedNumber section of the dialing rule entry. The number

listed in the DialedNumber section of the dialing rule entry will be dialed by the Unified Messaging server.

The following table shows an example of dialing rule groups and dialing rule entries. In this example, Local-Calls-Only and Low-Rate are the dialing rule groups that have been created. The dialing rule group Local-Calls-Only has two dialing rule entries: 91425* and 91206*, and the dialing rule group Low-Rate also has two dialing rule entries: 91509* and 91360*.

Dialing rule groups and dialing rule entries

Name	NumberMask	DialedNumber	Comment
Local-Calls-Only	91425*	91*	Local calls
Local-Calls-Only	91206*	91*	Local calls
Low-Rate	91509*	9*	In-state calls
Low-Rate	91360*	9*	In-state calls

For example, when a user dials 9-1-425-555-1234, the telephone number that the Unified Messaging server dials is 4255551234. The Unified Messaging server will remove any nonnumeric characters (in this example, the hyphens) and apply the number mask from the dialing rule entry. In this example, the Unified Messaging server will apply the number mask 91*. This tells the Unified Messaging server not to dial the 9 or the 1, but to dial all the other numbers in the telephone number that appear to the right of the number 1. This includes all the numbers represented by the asterisk (*).

You can use the EMC or the Shell to create and configure single or multiple in-country/region and international dialing rule groups and dialing rule entries. However, if you're creating many or complex dialing rule groups and dialing rule entries, you can use a comma-separated value (.csv) file in the Exchange Management Shell. You can import or export a list of dialing rule groups and dialing rule entries.

To import a list of dialing rule groups and dialing rule entries that you've defined in a .csv file, run the **Set-UMDialPlan** cmdlet, as follows.

```
Set-UMDialPlan "MyUMDialPlan" -ConfiguredInCountryOrRegionGroups $(IMPORT-CSV c:\
```

To retrieve a list of the dialing rule groups configured on a UM dial plan, run the **Get-UMDialPlan** cmdlet, as follows.

```
(Get-UMDialPlan -id "MyUMDialPlan").ConfiguredInCountryOrRegionGroups | EXPORT-CS
```

The .csv file must be created and saved in the correct format for the file to be used. Each line in the .csv file represents one dialing rule entry. However, each dialing rule entry is configured on the same dialing rule group. Each entry in the file will have four sections separated by commas. These sections are name, number mask, dialed number, and comment. Each section is required, and you must enter the correct information in each section except for the comment section. There should be no spaces between the text entry and the comma for the next section, nor should there be any blank lines in between entries or at the end. The following is an example of a .csv file that can be used to create in-country/region dialing rule groups and dialing rule entries.

Name,NumberMask,DialedNumber,Comment

Low-rate,91425xxxxxxx,9xxxxxxx,Local call

Low-rate,9425xxxxxxx,9xxxxxxx,Local call

Low-rate,9xxxxxxx,9xxxxxxx,Local call

Any,91*,91*,Open access to in-country/region numbers

Long-distance,91408*,91408*,long distance

The following is an example of a .csv file that can be used to create international dialing rule groups and dialing rule entries.

Name,NumberMask,DialedNumber,Comment

International, 901144*, 901144*, international call

International, 901133*, 901133*, international call

Return to top

Applying Configured Dialing Rule Groups

Dialing rule groups are created on a UM dial plan. You can create in-country/region or international dialing rule groups using the EMC or the **Set-UMDialPlan** cmdlet in the Shell. After you create the appropriate dialing rule groups on a UM dial plan and define the dialing rule entries, you can apply the dialing rule groups that you created to a UM dial plan, a UM auto attendant, or to users who are associated with a UM mailbox policy, depending on how the user accesses the Unified Messaging system.

You can apply the dialing rule groups that you created on a UM dial plan to the following:

- **Same dial plan** The settings will apply to all users who call in to the subscriber access number but don't sign in to their Exchange 2010 mailbox. To apply an in-country/region dialing rule group named MyAllowedDialRuleGroup to the same dial plan, use the Exchange Management Shell **Set-UMDialPlan** cmdlet, as follows.

```
Set-UMDialPlan -Identity MyUMDialPlan -AllowedInCountryOrRegionGroups M
```

- **Single or multiple UM mailbox policies** The settings configured on a UM mailbox policy will apply to all users who are associated with a specific UM mailbox policy. The settings configured on a UM mailbox policy apply to users who call in to a subscriber access number and sign in to their Exchange 2010 mailbox. To apply an in-country/region dialing rule group named MyAllowedDialRuleGroup to a single UM mailbox policy, use the **Dialing Restrictions** tab in the EMC or use the **Set-UMMailboxPolicy** cmdlet in the Shell, as follows.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowedInCountryOrRegi
```

- **Single or multiple auto attendants associated with the UM dial plan** This will apply to all users who call in to a UM auto attendant. To apply the in-country/region dialing rule group named MyAllowedDialRuleGroup to a single UM auto attendant, use the Exchange Management Shell **Set-UMAutoAttendant** cmdlet, as follows.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AllowedInCountryOrRegi
```

Return to top

The following table summarizes the way that dialing rule groups are applied in Unified

Messaging.

Applying outdialing rules

Caller type	Scope	Outdialing settings applied
Subscriber access or Outlook Voice Access	User calls a dial plan subscriber access number and signs in to the mailbox	UM mailbox policy
Anonymous caller	User calls a dial plan subscriber access number	UM dial plan
Anonymous caller	User calls an auto attendant pilot number	UM auto attendant
Caller from inside the organization	User calls the Play on Phone number	UM mailbox policy

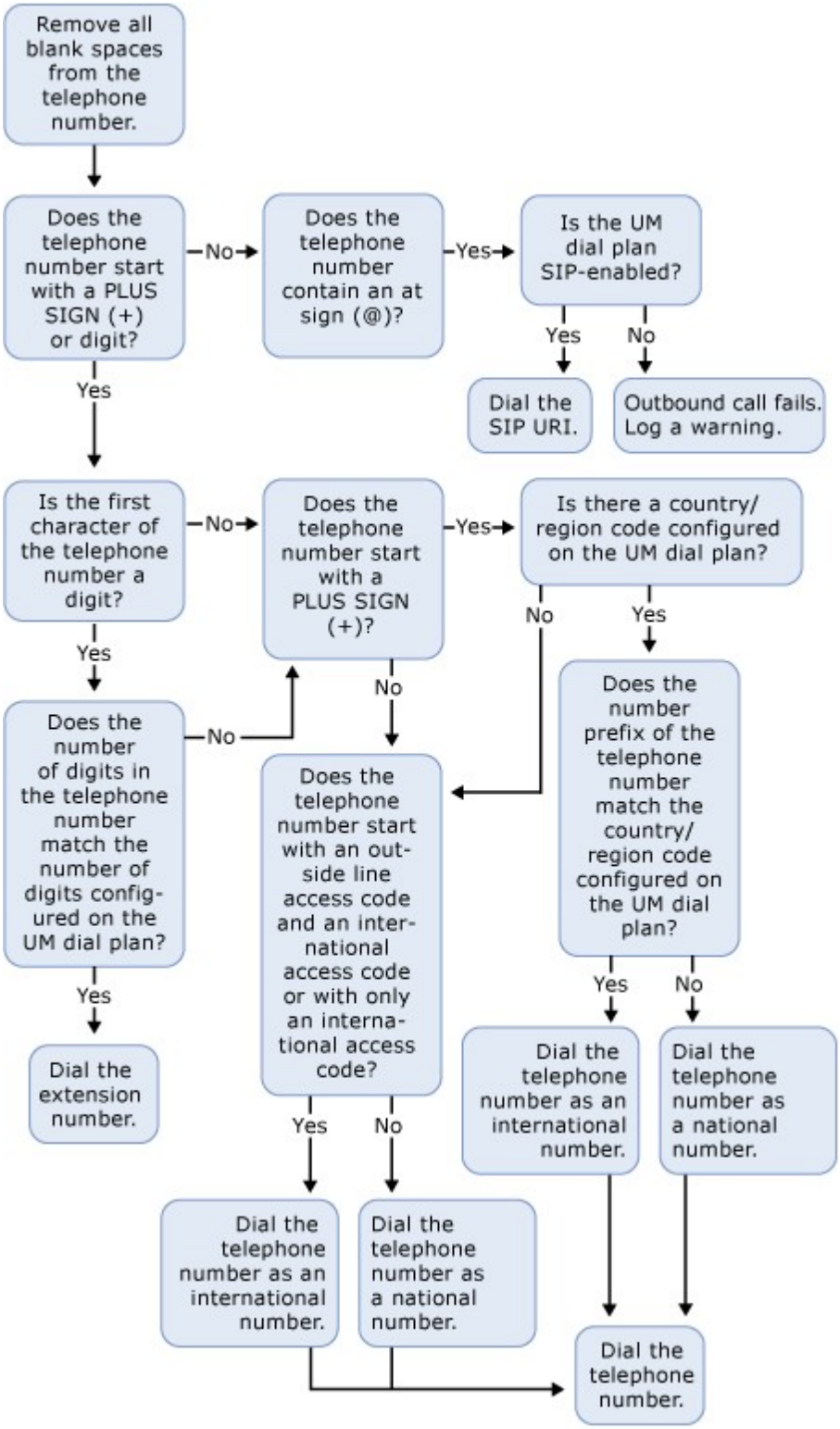
Applying Dialing Rules

The outdialing process happens when:

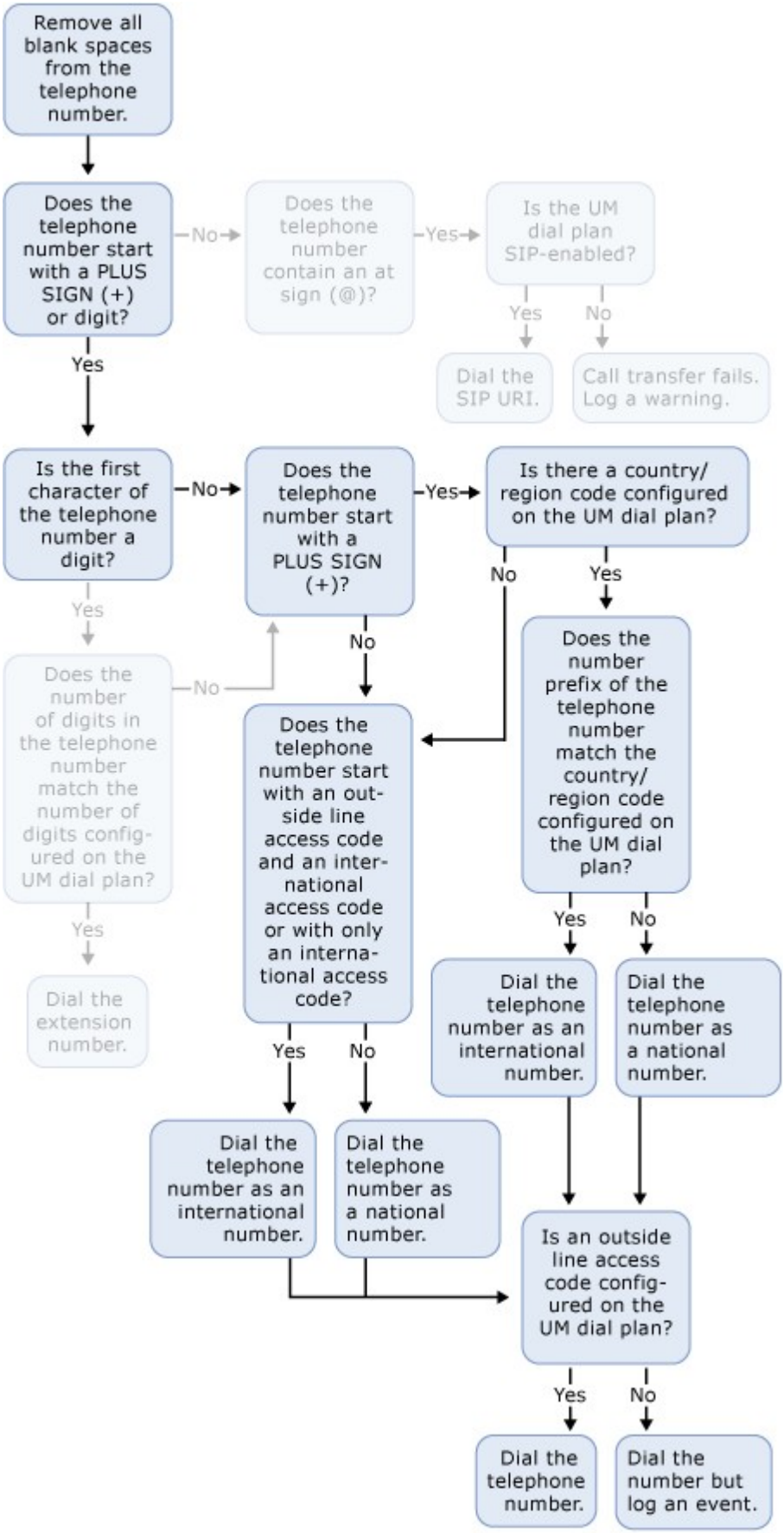
- A Unified Messaging server places a call to an external telephone number for a caller.
- A Unified Messaging server transfers a call to an auto attendant.
- A Unified Messaging server transfers a call to a user in your organization who is UM-enabled or not UM-enabled.
- A UM-enabled user uses the Play on Phone feature found in Outlook 2007 or Outlook Web App in Exchange 2010.

In each outdialing scenario, a Unified Messaging server will apply the outdialing rules that have been configured, and then place the call for the user. However, depending on the scenario and how the call is initiated by the user, a Unified Messaging server may apply only some of the outdialing rules to the telephone number being dialed. In other outdialing scenarios, the Unified Messaging server may apply all the outdialing rules configured to the telephone number being dialed. The outdialing rules applied are based on how the call was initiated and are illustrated in the following figures.

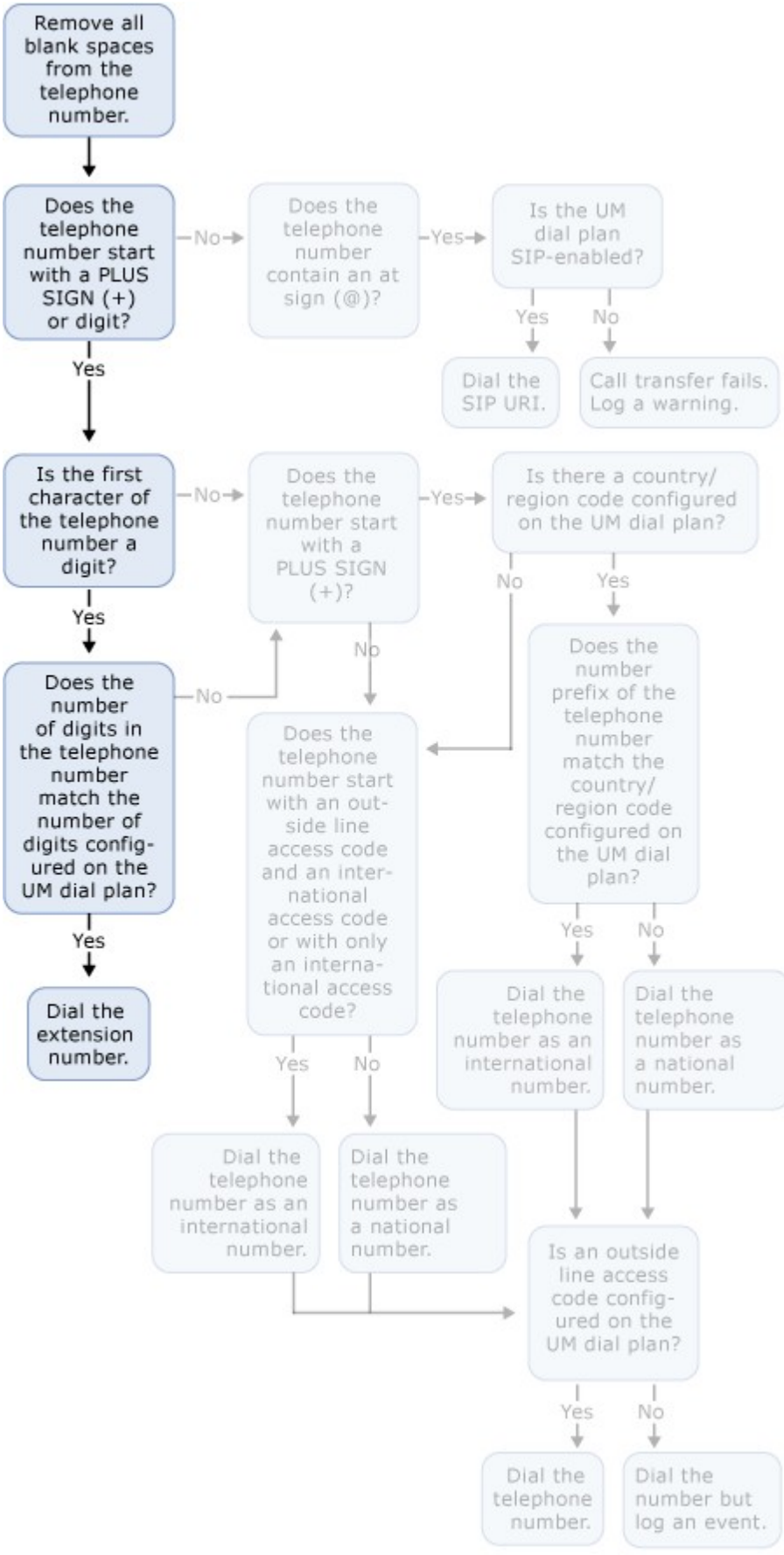
The following figure illustrates how outdialing rules are applied when a user uses the Play on Phone feature to place a call.



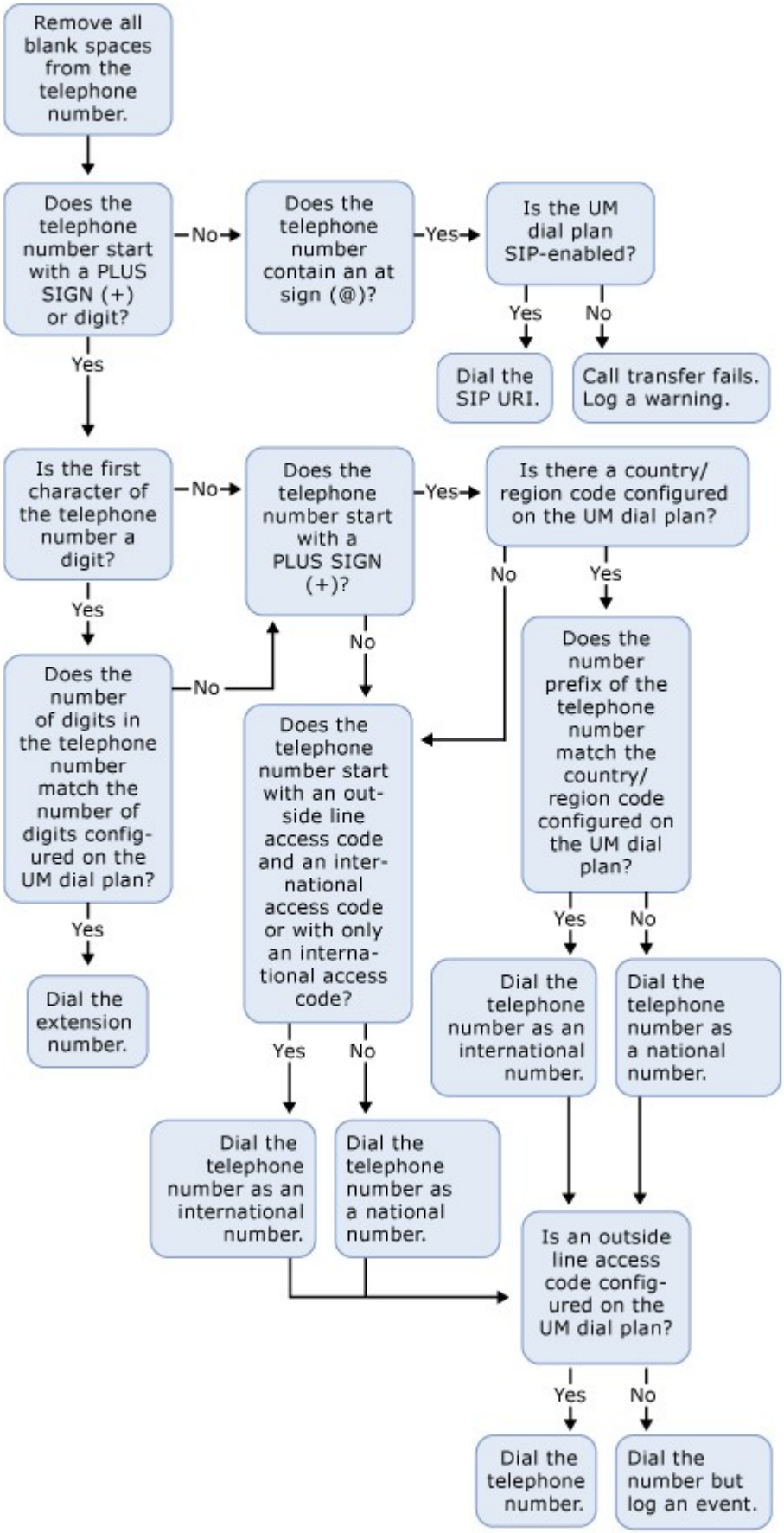
The following figure illustrates how outdialing rules are applied when a user places a call to a personal contact.


Remove all blank spaces from the telephone number.
Does the telephone number start with a PLUS SIGN (+) or digit?
No
Does the telephone number contain an at sign (@)?
Yes
Is the UM dial plan SIP-enabled?
Yes
No
Dial the SIP URI.
Call transfer fails. Log a warning.
Yes
Is the first character of the telephone number a digit?
No
Does the telephone number start with a PLUS SIGN (+)?
Yes
Is there a country/ region code configured on the UM dial plan?
No
Yes
Yes
Does the number of digits in the telephone number match the number of digits config-ured on the UM dial plan?
No
No
Does the telephone number start with an out-side line access code and an inter-national access code or with only an interna-tional access code?
Does the number prefix of the telephone number match the country/ region code configured on the UM dial plan?
Yes
Dial the extension number.
Yes
No
Dial the telephone number as an international number.
Dial the telephone number as a national number.
Yes
No
Dial the telephone number as an international number.
Dial the telephone number as a national number.
Is an outside line access code config-ured on the UM dial plan?
Yes
No
Dial the telephone number.
Dial the number but log an event.

The following figure illustrates how outdialing rules are applied when a user who is UM-enabled places a call to another UM-enabled user.


Remove all blank spaces from the telephone number.
Does the telephone number start with a PLUS SIGN (+) or digit?
No
Does the telephone number contain an at sign (@)?
Yes
Is the UM dial plan SIP-enabled?
Yes
No
Dial the SIP URI.
Call transfer fails. Log a warning.
Yes
Is the first character of the telephone number a digit?
No
Does the telephone number start with a PLUS SIGN (+)?
Yes
Is there a country/ region code configured on the UM dial plan?
No
Yes
Yes
No
Does the number of digits in the telephone number match the number of digits config-ured on the UM dial plan?
No
Does the telephone number start with an out-side line access code and an inter-national access code or with only an interna-tional access code?
Does the number prefix of the telephone number match the country/ region code configured on the UM dial plan?
Yes
No
Yes
No
Dial the extension number.
Dial the telephone number as an international number.
Dial the telephone number as a national number.
Yes
No
Dial the telephone number as an international number.
Dial the telephone number as a national number.
Is an outside line access code config-ured on the UM dial plan?
Yes
No
Dial the telephone number.
Dial the number but log an event.

The following figure illustrates how outdialing rules are applied when a user who is UM-enabled places a call to a user who isn't UM-enabled.


Remove all blank spaces from the telephone number.
Does the telephone number start with a PLUS SIGN (+) or digit?
No
Does the telephone number contain an at sign (@)?
Yes
Is the UM dial plan SIP-enabled?
Yes
No
Dial the SIP URI.
Call transfer fails. Log a warning.
Yes
Is the first character of the telephone number a digit?
No
Does the telephone number start with a PLUS SIGN (+)?
Yes
Is there a country/ region code configured on the UM dial plan?
No
Yes
Yes
Does the number of digits in the telephone number match the number of digits config-ured on the UM dial plan?
No
No
Does the telephone number start with an out-side line access code and an inter-national access code or with only an interna-tional access code?
Does the number prefix of the telephone number match the country/ region code configured on the UM dial plan?
Yes
Dial the extension number.
Yes
No
Yes
No
Dial the telephone number as an international number.
Dial the telephone number as a national number.
Dial the telephone number as an international number.
Dial the telephone number as a national number.
Is an outside line access code config-ured on the UM dial plan?
Yes
No
Dial the telephone number.
Dial the number but log an event.

Return to top

1.9.1.3.9 Understanding Dial Codes, Number Prefixes, and Number Formats

Understanding Dial Codes, Number Prefixes, and Number Formats

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-10*

You can configure several dialing codes used by a Unified Messaging (UM) server to dial internal and external calls for UM-enabled users. Frequently, you want to configure a dial plan together with the dialing or access codes, a national number prefix, or the in-country/region or international number formats so that you can control outdialing for users in your organization. This topic discusses dial codes, number prefixes, and number formats and how you can use them to control outdialing for your organization.

Contents

Overview

Outdialing is the process used by users when they call in to a UM dial plan or UM auto attendant and then place a call to an internal or external telephone number. When a user calls in to a UM dial plan or a UM auto attendant and then places a call, a Unified Messaging server uses the settings configured on the dial plan, auto attendant, and UM mailbox policies to place the call. A Unified Messaging server places an outgoing call in the following situations:

- When it places a call to an external telephone number for a caller.
- When it transfers a call to an auto attendant.
- When it transfers a call to a user (either UM-enabled or not) in your organization.
- When a UM-enabled user uses the Play on Phone feature in Microsoft Office Outlook 2007 or the version of Outlook Web App that released with Microsoft Exchange Server 2010.

There are two types of users who use outdialing: authenticated and unauthenticated. Unauthenticated users call in to a subscriber access number configured on a UM dial plan but don't sign in to their mailbox. Unauthenticated users also call in to a number

configured on a UM auto attendant. Authenticated users call in to a subscriber access number and successfully sign in to their Exchange 2010 mailbox. When users call in to a subscriber access number, they are considered unauthenticated because they haven't provided their extension number and PIN and logged on to their mailbox. They are authenticated after they provide their extension number and PIN and successfully sign in to their Exchange 2010 mailbox.

When an unauthenticated user calls in to a UM auto attendant and places a call using outdialing, the outdialing settings configured on the UM dial plan and the auto attendant are used. When an unauthenticated user calls in to a subscriber access number configured on a dial plan, the settings configured on the dial plan are the only settings that are used. However, when users have successfully signed in to their Exchange 2010 mailbox, configuration settings from the dial plan and the UM mailbox policy associated with the authenticated users are applied to the authenticated users.

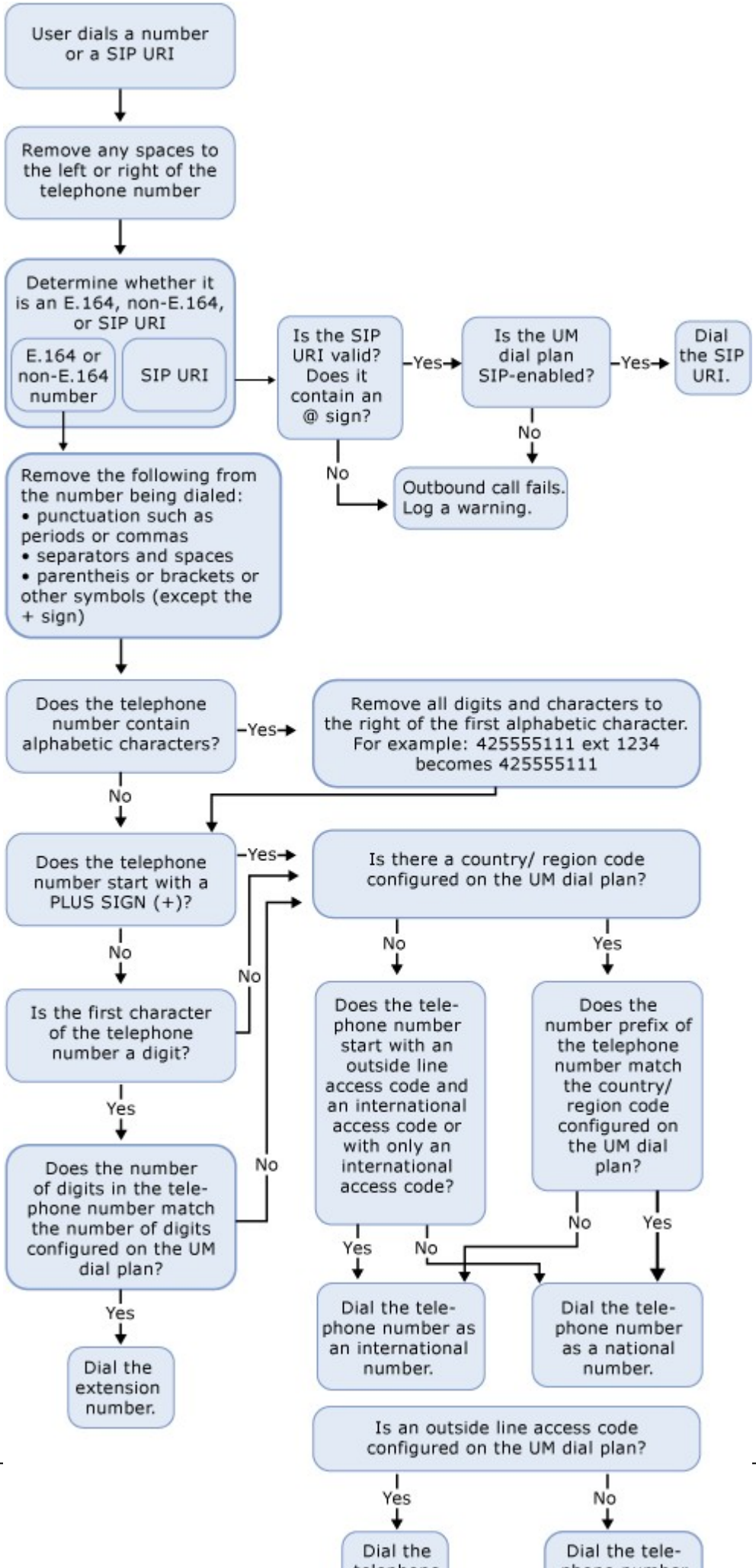
There are several settings that you must configure to control outdialing for your organization. To control outdialing, you must configure the UM dial plans, auto attendants, and UM mailbox policies in Exchange 2010 Unified Messaging. The following settings can be configured on UM dial plans, auto attendants, and UM mailbox policies to control outdialing:

- Outside line, country/region, and international access codes
- National number prefixes
- In-country/region and international number formats
- In-country/region and international dialing rule groups
- Allowed in-country/region and international dialing rule groups
- Dialing rule entries

You configure access codes, number prefixes, and number formats on a UM dial plan on the **Dial Codes** tab in the Exchange Management Console. You can also configure the settings using the **Set-UMDialPlan** cmdlet. You can choose to configure all the settings, none of the settings, or only some of the settings. However, each setting controls a specific part of the outdialing process.

Access codes, number prefixes, and number formats are used by a Unified Messaging server to determine the correct number to dial and can be configured to restrict outgoing calls for users who dial in to a UM auto attendant associated with a UM dial plan or when users dial in to the subscriber access number configured on the dial plan. The following figure illustrates the outdialing process and how access codes can be used to control outdialing.

Outdialing overview


User dials a number or a SIP URI
Remove any spaces to the left or right of the telephone number
Determine whether it is an E.164, non-E.164, or SIP URI
E.164 or non-E.164 number
SIP URI
Is the SIP URI valid? Does it contain an @ sign?
Yes
Is the UM dial plan SIP-enabled?
Yes
Dial the SIP URI.
No
Outbound call fails. Log a warning.
No
Remove the following from the number being dialed:
• punctuation such as periods or commas
• separators and spaces
• parentheis or brackets or other symbols (except the + sign)
Does the telephone number contain alphabetic characters?
Yes
Remove all digits and characters to the right of the first alphabetic character. For example: 425555111 ext 1234 becomes 425555111
No
Does the telephone number start with a PLUS SIGN (+)?
Yes
Is there a country/ region code configured on the UM dial plan?
No
Yes
No
Is the first character of the telephone number a digit?
Yes
No
Does the tele-phone number start with an outside line access code and an international access code or with only an international access code?
Does the number prefix of the telephone number match the country/ region code configured on the UM dial plan?
Yes
No
Yes
No
Does the number of digits in the tele-phone number match the number of digits configured on the UM dial plan?
No
Yes
Dial the tele-phone number as an international number.
Dial the tele-phone number as a national number.
Dial the extension number.
Is an outside line access code configured on the UM dial plan?
Yes
No
Dial the
Dial the tele-

For more information about outdialing in Unified Messaging, see Understanding Outdialing.

Return to top

Outside Line Access Code

An outside line access code should be configured on each dial plan that you create. However, this depends on the type of telephony network that you have and how it's configured. You can configure an outside line access code, also known as a *trunk access code*, on each dial plan that you create. This is the number used to gain access to an outside telephone line. This number is also configured on the Private Branch eXchanges (PBXs) or IP PBXs in your organization. In most telephony networks, users dial the number 9 to gain access to an outside line and place a call to an external telephone number.

If you don't configure the outgoing dial codes on a dial plan, when a Unified Messaging server associated with the dial plan dials an outgoing call, the PBX or IP PBX may not be able to recognize the number string that's sent. If this happens, the PBX or IP PBX can't complete the outgoing call for the user. For example, as stated earlier, in many organizations, the access code that users dial to gain access to an outside line is 9, and this is configured on a PBX or IP PBX. The Unified Messaging server must add the outside line access code (9) before the telephone number string for the PBX or IP PBX to correctly dial the outgoing number. If you configure the dialing code so that the Unified Messaging server will add the outside line access code, the Unified Messaging server will be able to use the outside line access code to access an outside line before it dials the external telephone number string. The dialing code that you configure will apply to all users who are associated with a UM mailbox policy associated with the UM dial plan.

National Number Prefix

The national number prefix and the country/region code can also be configured on a UM dial plan. The number you enter is used by the Unified Messaging server to dial the correct national number prefix or country/region code when a user dials an outgoing call destined within the same country/region or an international call. For example, when a user from North America places an outgoing international call to Europe, the Unified Messaging server will add the national number prefix before the number string that it sends to the PBX to place the outgoing call. The Unified Messaging server will add the number 0 for Europe to the telephone number string. The number 1 is used as the national number prefix for North America.

Country/Region Access Code

A country/region access code can be configured on a UM dial plan. The country/region access code consists of the digits associated with a specific country or region. The country/region access code is used by the Unified Messaging server to dial the correct telephone number when a call is placed to a telephone number from inside the same country or region. The Unified Messaging server will add this number before the number string that it sends to the PBX or IP PBX when it places the outgoing call. For example, the Unified Messaging server will add the number 1 to a call placed from the United States and destined for the United States. For the United Kingdom, the country/region code is 44.

International Access Code

An international access code can be configured on a UM dial plan. The international access code consists of the digits used to access international telephone numbers. The international access code is used by the Unified Messaging server to dial the correct international access code when a call is placed from a telephone number within a country/region but the number being dialed is located in another country/region. The Unified Messaging server will add this number before the number string that it sends to the PBX or IP PBX when it places the outgoing call. For example, the Unified Messaging server will use 011 as the international access code for the United States. For Europe, the international access code is 00.

Return to top

In-Country/Region and International Number Formats

You can configure the incoming call configuration for in-country/region and international number formats on a UM dial plan. After you configure these settings, the Unified Messaging server will be able to recognize incoming calls from inside a country/region and internationally from other UM dial plans within the same Exchange 2010 organization. Configuring these options also enables your organization to save money by preventing outgoing calls that shouldn't be made by users from inside your organization and helps prevent toll fraud. The Unified Messaging server will use the information that you configure to match the number format of the incoming call and verify that the number pattern matches before it accepts the call. For example, you may have multiple dial plans inside an organization that exist within the same Active Directory forest. If you have one dial plan for the United States and another for the United Kingdom, you may want to let users in the United States dial plan have Unified Messaging servers place calls to users who are located in the United Kingdom dial plan but not let the users in the United States dial plan place calls directly to other country/regions or internationally.

1.9.1.3.10 Understanding Name Lookups from a Caller ID

Understanding Name Lookups from a Caller ID

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-24*

Unified Messaging (UM) uses information about the calling and called parties to perform a name lookup. This lookup enables a caller's name to be included in the following situations:

- In a missed call notification
- When a caller leaves a voice message for a UM-enabled user if the calling party's name is located in Active Directory or in the called party's personal contacts

Contents

Equivalent Dial Plan Groups

Caller ID

Caller ID is a service that's provided by telephone companies. It can tell a person who's receiving a call the telephone number, and sometimes the name, of the person who's calling and other information about the call. This information is sent over a serial cable by using call signaling. When a call is received by a PBX or IP PBX from a telephone company, the call includes calling identification information such as the following:

- The calling party's number
- The called party's number
- Status codes that indicate such things as the following:
  - Ring-no-answer (The phone rang, but the called party didn't answer.)
  - The state or condition of the telephone line
  - Line busy (The call connected, but the line is busy.)
  - Call forward always (The incoming call is always forwarded to another number.)
- The line or port number that's being used for the call

Name Lookup Process

Unified Messaging uses two data sources to receive information about the calling party and to map it to the name of the caller: Active Directory and personal Contacts. When the name lookup process is successful, the name of the calling party will be inserted into voice mail messages and missed call notifications if they've been enabled for the called party. When an incoming call is received, the calling party information is passed to a Unified Messaging server. The caller can be calling from inside or outside your organization.

In Microsoft Exchange Server 2007 Unified Messaging, a call that was diverted to a Unified Messaging server because of a ring-no-answer or busy condition is answered and a voice message is taken. After the call is answered, Exchange 2007 Unified Messaging tries to resolve the caller ID. It does this so that it can insert a name, rather than a number, into the sender information.

In Exchange 2007, name lookups for voice mail messages are done by using information about a caller who's in the same dial plan as the user being called in one of the following ways:

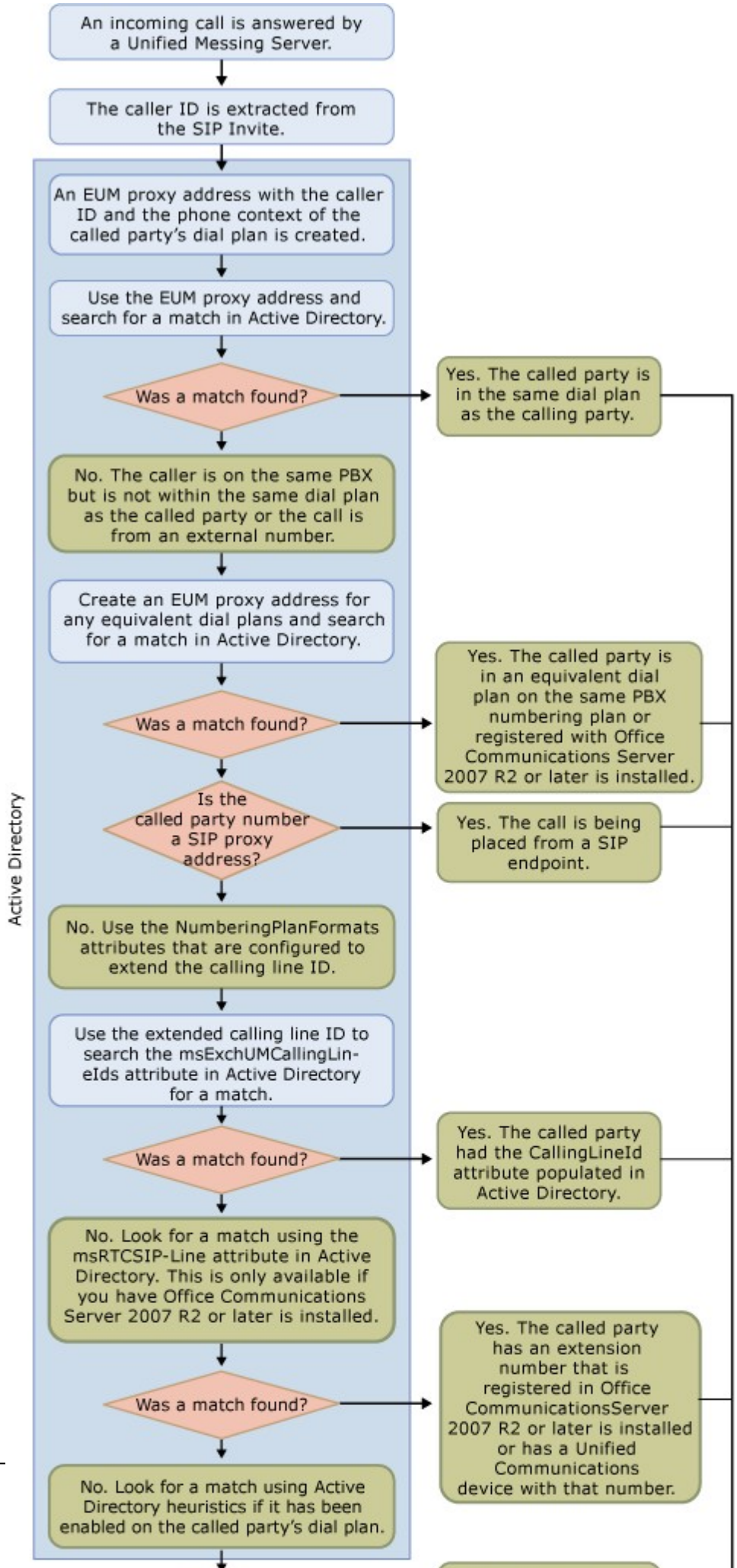
- Using an EUM proxy address.
- From the personal Contacts of the user receiving the call.
- Using the **msRTCSIP-Line** attribute in Active Directory if Service Pack 1 (SP1) for Exchange 2007 was installed and Exchange 2007 was integrated with Microsoft Office Communications Server 2007 or Office Communications Server 2007 R2.

In Microsoft Exchange Server 2010, the name lookup methods differ from those used in Exchange 2007. The following steps are used in Exchange 2010 to look up a name from the calling party's information:

1. The caller's name is used if the caller signed in to their mailbox from Outlook Voice Access or if they use a Microsoft Unified Communications client such as Microsoft Office Communicator 2007 or Communicator Phone Edition to place the call. The caller's identity is known because they've been authenticated when they use Outlook Voice Access, Office Communicator 2007, or Communicator Phone Edition.
2. The EUM proxy address or addresses in Active Directory are used. If the proxy address contains an '@' sign, it's considered a SIP URI. If the proxy address begins with a '+' character, it's considered to be an E.164 number. If neither of these characters is present, the proxy address is considered an

extension within the same dial plan as the called party or an equivalent dial plan.
3. If the caller ID is a valid SIP URI, Active Directory is used to resolve the SIP URI using the EUM proxy address or addresses.
4. If the caller ID is a valid E.164 number, Active Directory is used to resolve the number to the calling party's name. For this to work correctly, you must have manually configured the *UMCallingLineIds* parameter on the UM-enabled mailbox for the called party. This configuration is useful when you don't want to publish a telephone number, such as a personal mobile phone number, in Active Directory, but still want to resolve the calling party's name by using this phone number.
5. Active Directory heuristic matching is used, if it's enabled, to resolve the number to the calling party's name. Active Directory heuristic matching must be enabled on the dial plan, and the user's account in Active Directory must be populated with one or more of the fields, such as telephone number, home, or mobile, for this to work correctly.
6. The personal Contacts of the called party are used to resolve the number to the calling party's name.

The following figure shows the steps that are performed by a Unified Messaging server when it tries to perform a name lookup from the calling party information that's provided.


An incoming call is answered by a Unified Messing Server.
The caller ID is extracted from the SIP Invite.
Active Directory
An EUM proxy address with the caller ID and the phone context of the called party's dial plan is created.
Use the EUM proxy address and search for a match in Active Directory.
Was a match found?
Yes. The called party is in the same dial plan as the calling party.
No. The caller is on the same PBX but is not within the same dial plan as the called party or the call is from an external number.
Create an EUM proxy address for any equivalent dial plans and search for a match in Active Directory.
Was a match found?
Yes. The called party is in an equivalent dial plan on the same PBX numbering plan or registered with Office Communications Server 2007 R2 or later is installed.
Is the called party number a SIP proxy address?
Yes. The call is being placed from a SIP endpoint.
No. Use the NumberingPlanFormats attributes that are configured to extend the calling line ID.
Use the extended calling line ID to search the msExchUMCallingLin-eIds attribute in Active Directory for a match.
Was a match found?
Yes. The called party had the CallingLineId attribute populated in Active Directory.
No. Look for a match using the msRTCSIP-Line attribute in Active Directory. This is only available if you have Office Communications Server 2007 R2 or later is installed.
Was a match found?
Yes. The called party has an extension number that is registered in Office CommunicationsServer 2007 R2 or later is installed or has a Unified Communications device with that number.
No. Look for a match using Active Directory heuristics if it has been enabled on the called party's dial plan.

Return to top

Improved E.164 Number Resolution

In Exchange 2010 Unified Messaging, four new methods are used to improve resolution of the caller ID to the calling party's name. The four methods are:

- Calling line IDs
- Numbering plan formats
- Active Directory heuristics
- Dial plan equivalency groups

Calling Line IDs

In Exchange 2007, E.164 number resolution was limited and, in some cases, couldn't return the name of the caller in a missed call notification or in the voice message that the called party received in their mailbox. What was needed was the ability to apply an E.164 number or set of numbers for an UM-enabled user and to use these numbers to help resolve an incoming number from another user or a caller from outside the organization.

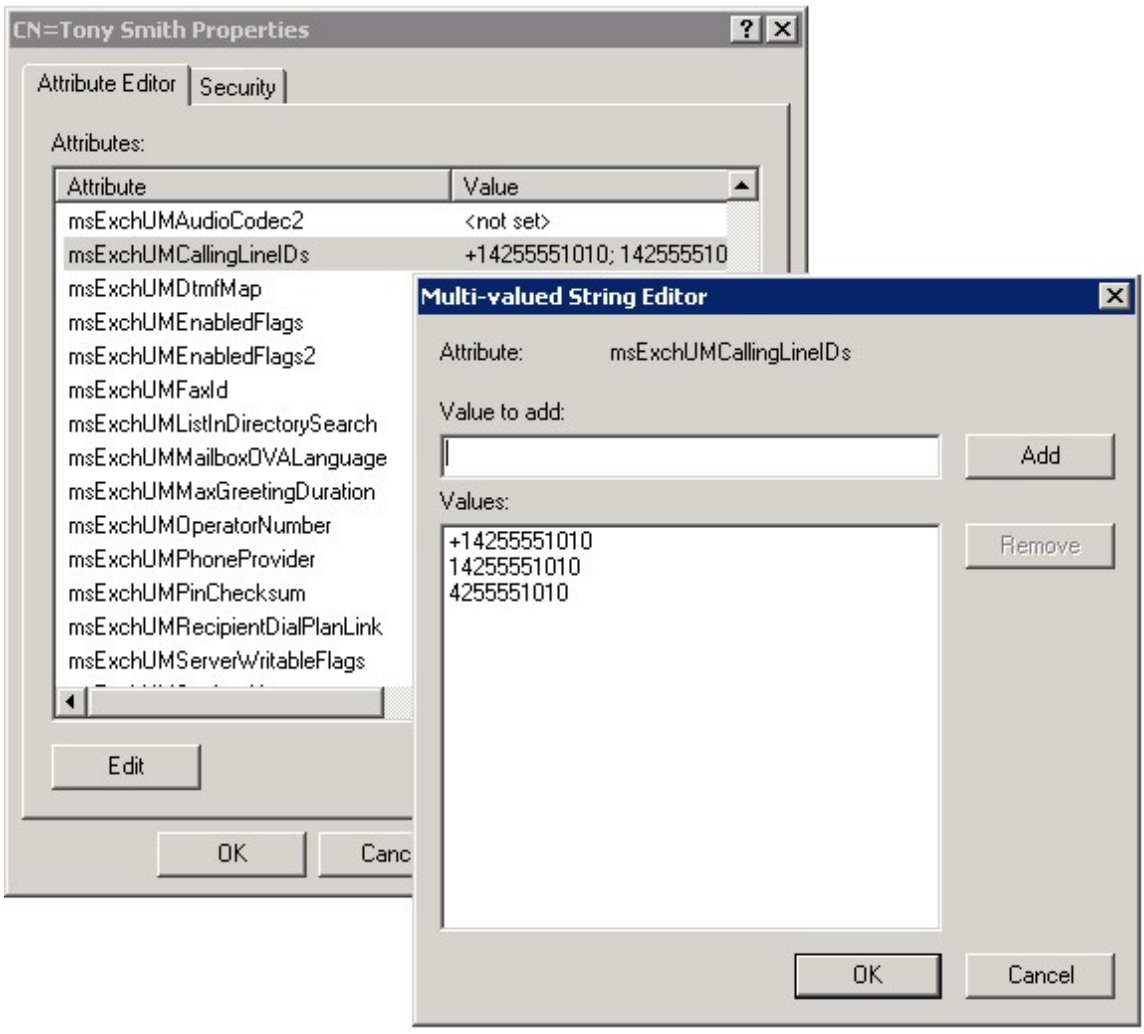
The UM server would take the E.164 number from the caller ID, convert it into an E.164 number, and then just do a lookup for the name of the caller in Active Directory or in the UM-enabled user's personal Contacts. However, without Exchange Unified Messaging being integrated with Communications Server 2007 R2 or Microsoft Lync Server 2010, an E.164 couldn't be used.

In Exchange 2010, a multivalued attribute named **msExchUMCallingLineIDs** was added to the Active Directory schema. This attribute enables a UM server to take an E.164 number or set of numbers, convert the number or numbers, and then perform a name lookup. This attribute can contain a list of numbers that are mapped to a specific user and can be configured on the user's Active Directory object. For example, you could add the numbers, 4255551010, 14255551010, and +14255551010 to the **msExchUMCallingLineIDs** attribute for a specific user. Although the last number in this list is an E.164 number, a correctly formatted E.164 number isn't required. You can add any phone number that looks like a valid phone number that contains digits, and those digits can, optionally, begin with a plus (+) sign.

Note:

The **msExchUMCallingLineIDs** attribute isn't limited to UM-enabled users and can be configured for all users in Active Directory.

The following figure shows where multiple phone numbers are located for a user on the **msExchUMCallingLineIDs** attribute.



msRTCSIP-Line is a Communications Server 2007 R2 or Microsoft Lync Server 2010 schema attribute that exists on an Active Directory recipient object when Communications Server 2007 R2 or Lync Server 2010 is installed. The **msExchUMCallingLineIDs** attribute for Unified Messaging is used for caller ID to name resolution in very much the same way the **msRTCSIP-Line** attribute is used in Communications Server 2007 R2 or Lync Server 2010. A Unified Messaging server will use the **msRTCSIP-Line** attribute to resolve a caller ID to a name, but Exchange Unified Messaging doesn't grant administrators the ability to change or edit this attribute using any method, including Unified Messaging cmdlets.

Communications Server 2007 R2 or Lync Server 2010 specifies the format and validation of the **msRTCSIP-Line** attribute. There are two reasons Unified Messaging administrators aren't allowed to make changes to the attribute.

- Communications Server 2007 or R2 Lync Server 2010 depends on the correct administration of this attribute to correctly route calls to the intended Unified Communications device. If Unified Messaging were allowed to configure this attribute, both Unified Messaging and Communications Server 2007 R2 or Lync Server 2010 would have to share in the validation and administration.
- The **msRTCSIP-Line** isn't very flexible because it's single valued. As an Exchange Unified Messaging administrator, you'd most likely want to provision more than one phone number for a user by including an E.164 formatted number for them.

For these reasons, the Exchange 2010 recipient schema includes the

msExchUMCallingLineIDs attribute as a multivalued and indexed property. When you want to add, remove, or change the phone numbers for a specific user, you'll add or remove numbers by using the *UMCallingLineIds* parameter for the **Set-User** cmdlet. After you add, remove, or change the numbers on the **msExchUMCallingLineIDs** attribute, no further action is needed.

The following table shows the cmdlets, type, description, and the default setting for the *UMCallingLineIds* parameter.

UMCallingLineIds parameter description

Cmdlets	Type	Description	Default
Set-User **Get-User**	Microsoft.Exchange.Data.MultiValuedProperty	The *UMCallingLineIds* parameter specifies telephone numbers or extensions that can be mapped to a UM-enabled user. You can specify more than one telephone number for each user, separated by a comma. This parameter accepts digits less than 128 characters and may include an optional plus sign (+) preceding the numbers. Each UM-enabled user must have a unique *UMCallingLineIds* parameter value.	empty

The **Get-User** and **Set-User** cmdlets will read and write to the **msExchUMCallingLineIDs** attribute. If a caller ID isn't correctly resolved using the **msExchUMCallingLineIDs** attribute, UM will then look at the phone number that's configured on **msRTCSIP-Line** attribute for a user.

Return to top

Number Plan Formats for Dial Plans

In addition to the *UMCallingLineIds* parameter that was added to help resolve a caller ID to the name of the caller, the UM server must also have the ability to take numbers from the *UMCallingLineId*, such as 51010, 555-1010, and 4255551010 and extend them into a correctly formatted E.164 phone number. The *NumberingPlanFormats* parameter on the **Set-UMDialPlan** cmdlet is used to do this.

The syntax for adding numbering plan formats to a UM dial plan is:

```
Set-UMDialplan -identity MyUMDialPlan -NumberingPlanFormats "425567xxxx","425678x
```

There are two requirements if you want to resolve caller ID to calling party name this way:

- Each user must be correctly provisioned with E.164 numbers. However, configuring each recipient in Active Directory make take some time.
- Rules that a UM server can use to map incoming caller IDs and convert them into correctly formatted E.164 phone numbers must be configured. An example of such a rule is extension length IDs.

An Exchange 2010 Unified Messaging server can change non-canonical numbers, such as an extension number of 5 digits, into more canonical forms like the E.164 format by using number masking.

A number mask is used to define the telephone number format that a Unified Messaging server uses to determine what outgoing telephone number it will dial for a user or the phone number that's used in the diversion header of an incoming call. Number masking is done for both incoming calls and outgoing dialing rules. An example of a valid number mask is 91xxxxxxxxx. For example, when an outgoing call is made to a number like 4255551010, the 91xxxxxxxxxx number mask on the dialing rule entry the Unified Messaging server replaces the right-most digits that are matched to the dialed number. In this example, there are 10 digits in the phone number that is dialed and 10 digits (represented by 'x'). Since these digits match, the UM server will dial 914255551010. This field can contain only numbers and the character x. The same process is used for incoming calls.

The *NumberingPlanFormats* parameter is a multivalued property and is used when a caller ID number is received by a UM server that's associated with a UM dial plan that can then be expanded into a correctly formatted E.164 number.

The following table shows the cmdlets, type, description, and default setting for the *NumberingPlanFormats* parameter.

NumberPlanFormats parameter description

Cmdlets	Type	Description	Default
Set- DialPlan **Get-DialPlan**	Microsoft.Exchange.Data.MultiValuedProperty	The *NumberingPlanFormats* parameter specifies one or more phone number masks that can be used for resolving caller ID to names of users in Active Directory.	empty

In Exchange 2007 Unified Messaging, the International number format on a dial plan was used to enhance caller ID resolution by creating an E.164 phone number. The E.164 phone number would then be used when the UM server searched for the phone number for the caller using the **msRTCSIPLine** attribute.

In Exchange 2010 Unified Messaging, equivalent dial plan groups have been added to enhance caller ID resolution to widen the scope of the search. This is done by configuring the numbering plan format on each dial plan, which will help to convert the caller ID into the E.164 format. For details about equivalent dial plans, see Equivalent Dial Plan Groups later in this topic.

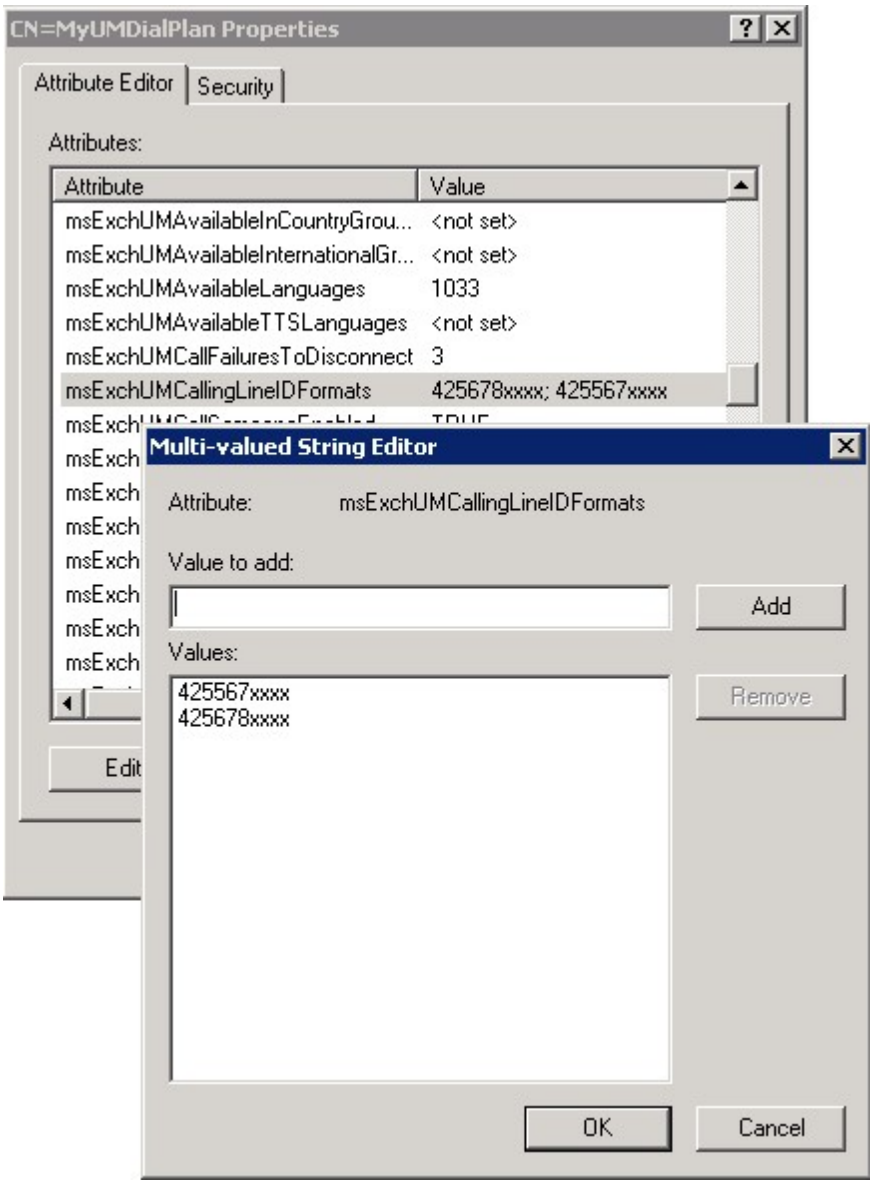
For example, consider a company that has 20,000 employees. This company would need 20,000 unique Direct Inward Dial (DID) telephone numbers for its employees. However, the company couldn't get numbers within consecutive DID ranges, for example, 425-555-xxxx to 425-556-xxxx. Instead, the first group of 10,000 employees had the number prefix 425-567-xxxx, and the second group of 10,000 employees had the number prefix 425-678-xxxx.

Say the administrator creates a single UM dial plan for these 20,000 employees and uses a 5-digit extension for each user. When a call is received by the PBX, the PBX will send the 5-digit caller ID. However, when the company migrates from a legacy PBX to an IP PBX, the users will be on two separate PBXs, each with its own 5-digit UM dial plan. After the users are migrated to the IP PBX, the caller ID name resolution will start to fail, and only

the 5-digit extension will appear in the voice message, instead of the caller's name.

This happens because only a single International number format is configured on the UM dial plan that's shared by these two prefixes. Therefore, only half the UM-enabled users will have correctly formatted E.164 numbers created. Also, the users are on different PBX dial plans. So even if an equivalent dial plan is enabled on the UM dial plan, the caller isn't UM enabled, and the caller's extension number won't resolve to a name.

The *NumberingPlanFormats* parameter can be used to resolve this issue. For each UM dial plan, there's an **msExchangeUMCallingLineIDFormats** attribute that can be configured using the *NumberPlanFormats* parameter to specify one or more phone number masks that can resolve caller IDs to names in Active Directory. The following figure shows this attribute and the numbering plan formats.



When a UM server answers an incoming call, it reads the caller ID. The UM server will parse the list of configured number plan formats from the top down until a match is not found or there's a conflict in the digits where x in the number mask is treated as a wild-

card. When this happens, the UM server will try to back fill the caller ID for the incoming call into each number mask. In the case of the employees whose number prefixes are 425-567-xxxx, and 425-678-xxxx, the digits "7" and "8" are the keys by which a correct mask will be selected for the calling ID number. After the UM server successfully back fills a numbering plan format pattern, it takes the E.164 number that's generated and performs a lookup against the **msExchUMCallingLineIDs** attribute. If that lookup fails, the UM server performs a lookup against the **msRTCSip-Line** attribute.

Unified Messaging administrators must check for ambiguous and nonsensical numbering plan format rules and reconfigure them. Ambiguous numbering plan format rules are two or more rules in which the right-most characters are identical and equal the number of digits configured on the dial plan. A nonsensical numbering plan format rule is one that has a wildcard character in any position other than one of the right-most digits that equals the number of digits in the extension numbers that are configured on the dial plan.

Return to top

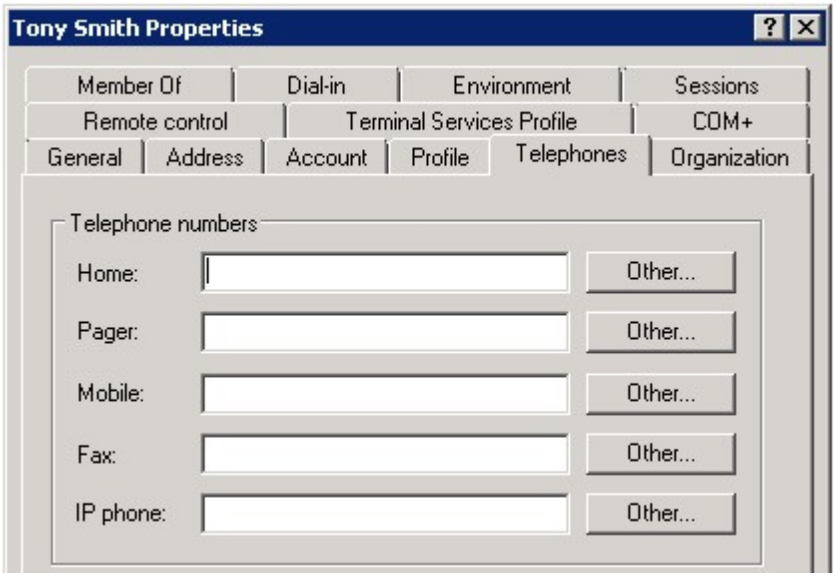
Active Directory Heuristics

In addition to UM calling line IDs and numbering plan formats, Exchange 2010 Unified Messaging enables Active Directory heuristics.

In Exchange 2007, caller ID resolution doesn't include telephone fields on the user's object in Active Directory when trying to resolve the caller ID on an incoming call to a name. This is because:

- The fields located on the **Telephones** tab and **Telephone number** field aren't indexed and searchable.
- The fields located on the **Telephones** tab and in the **Telephone number** field may not be in a standardized format.

The following figure shows these fields in Exchange 2010.



There's a major problem with the **Telephone number** field on the **Telephones** tab on a user's object in Active Directory. The field contains no validation or limits for formatting the numbers that are inserted. This means that there's no standardized format for these numbers. Here are the potential issues that prevent resolution of a caller ID to a name:

- The administrator didn't enter a number in the **Telephone number** field.
- The administrator doesn't use the **Telephones** tab at all for phone numbers.
- E.164 numbers are entered without any parentheses, hyphens, or the correct

spaces.

- The numbers aren't in the correct E.164 format. Examples of the correct format include the following:
  - (425) 555-1010
  - (425) 555-1234 x51010
  - (425) 555-1234 ext. 51010
  - 425-555-1010
  - 425.555.1010
  - 425/555-1010
  - 1425-555-1010
- Both extensions and international numbers are used. Examples that show both extensions and international numbers used together include the following:
  - +7890
  - +441234567890
  - +44(1)234567890
  - +44 (0)1 2345 6789

An Exchange 2010 Unified Messaging server will query Active Directory to examine up to 8 Active Directory attributes, together with the EUM proxy addresses and the **msExchUMCallingLineIDs** and **msRTCSIP-Line** attributes, when it tries to resolve a caller ID. There is an **msExchAllowHeuristicADCallingLineIDResolution** attribute on each dial plan. By default, the **msExchAllowHeuristicADCallingLineIDResolution** attribute is set to true when you create a UM dial plan.

You can use the **Set-UMDialPlan** cmdlet to enable or disable Active Directory heuristics. The following table shows the UM dial plan cmdlets, type, description, and default setting for the *AllowHeuristicADCallingLineIdResolution* parameter.

AllowHeuristicADCallingLineIdResolution parameter description

Cmdlets	Type	Description	Default
Set-UMDialPlan **Get-UMDialPlan**	System.Boolean	The AllowHeuristicADCallingLineIdResolution parameter specifies whether to allow calling line ID resolution using telephone number fields that may be configured in Active Directory. When this parameter is set to $true, the telephone numbers, such as those defined on the **Telephones** tab and the telephone number for a user in Active Directory, are used. Setting this parameter to $true allows resolution of calling IDs for both UM-enabled and non-UM-enabled users. You may want to set this parameter to	Enabled

		$false if the telephone numbers for users aren't in a standard format. If the telephone numbers aren't in a standard format, the Unified Messaging server may be unable to correctly resolve the caller ID to the name of a user consistently.	

After you enable Active Directory heuristics, UM will use the phone number fields, such as telephone number, home, or mobile, that are configured for a user who's in Active Directory. However, there's no way to select which of the phone fields to include. The following telephone attributes for a user in Active Directory will be used to resolve a caller ID to a name:

- **telephoneNumber**
- **homePhone**
- **mobile**
- **facsimileTelephoneNumber**
- **otherTelephone**
- **otherHomePhone**
- **otherMobile**
- **otherFacsimileTelephoneNumber**

If you use the **Set-User** cmdlet to populate one or more of the telephone attributes for a user, you must run **GalGrammarGenerator.exe –u** to update the DTMF map for each user. If you populate the phone fields or update phone numbers before you install the Unified Messaging server role or use a program other than the Exchange Management Shell, you'll also have to run **Galgrammargenerator.exe –u** before the telephone number fields will be indexed. For more information about how to run GalGrammarGenerator.exe, see one of the following topics:

- Update the Speech Grammar Files on a UM Server
- Understanding Automatic Speech Recognition Directory Lookups

Return to top

Equivalent Dial Plan Groups

Sometimes the number of UM dial plans can become unwieldy, either because the number of forests has increased or because the number of UM dial plans in a single forest has been increased. To provide a more scalable solution, a new Active Directory object has been added in Exchange 2010 Unified Messaging: equivalent dial plan group. An equivalent dial plan group is a container object in Active Directory that will contain equivalent dial plans that are from separate Active Directory forests.

Two Active Directory attributes are used with equivalent dial plan groups:

- **msExchangeUMEquivalenceDialPlan**
- **msExchangeUMEquivalentDialPlanPhoneContexts**

The concept of an equivalent dial plan has been added in Exchange 2010 Unified Messaging to allow UM administrators to connect two dial plans that are in the same PBX numbering plan but are broken into two dial plans. Two dial plans might be contained in a single PBX numbering plan, for example, when users in the two separate dial plans sit next to each other and can dial each other using an extension number but exist in different dial plans for reasons unrelated to the telephony infrastructure.

Note:
Extension numbers must be unique within a dial plan, but they must also be unique within an equivalent dial plan group.

For every dial plan, there can be an equivalent dial plan phone context for two or more dial plans that should be one dial plan but have been separate. You can add names for other dial plans and link to other dial plans. The dial plans you enter names for or link to can be in the same Active Directory forest or in different forests. When you add an equivalent dial plan, the dial plan's phone context will be automatically added to the equivalent dial plan group.

After you have added multiple dial plans with different phone contexts, when a call comes in the Unified Messaging server, instead of only looking for EUM proxy addresses that have the same phone context, it will look at EUM proxy addresses that have the phone context listed on an equivalent dial plan. As long as the dial plan is listed as an equivalent dial plan, and only the caller ID is being sent, then all Unified Messaging users' numbers from both dial plans will be resolved correctly to a name.

The following table shows the cmdlets, type, description, and default setting for the *EquivalentDialPlanPhoneContexts* parameter.

EquivalentDialPlanPhoneContexts parameter description

Cmdlets	Type	Description	Default
Set- DialPlan **Get-DialPlan**	Microsoft.Exchange.Data.MultiValuedProperty	The *EquivalentDialPlanPhoneContexts* parameter specifies the name of an equivalency dial plan. This parameter can be used when two UM dial plans exist but are in different forests or when a Private Branch eXchange (PBX) numbering plan spans two UM dial plans. Adding the name of the equivalency dial plan enables name lookups using a caller ID to search in the user's dial plan but then also search for a name for the calling line ID in any equivalent dial plans that are configured.	empty

For example, by having equivalent dial plan phone contexts on a dial plan, you could run the following command to add two UM dial plans to a single equivalent dial plan group.

```
Set-UMDialPlan  -identity MyUMDialPlan1 -EquivalentDialPlanPhoneContexts "dialpla
```

If the extension of a caller matches any UM-enabled user on any of the three dial plans specified in the command, the extension number will be resolved to a name of the caller.

Return to top

1.9.1.3.11 Understanding the DTMF Interface

Understanding the DTMF Interface

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-10*

In Microsoft Exchange Server 2010 Unified Messaging (UM), callers can use dual tone multi-frequency (DTMF), also referred to as touchtone, and voice inputs to interact with the system. The method callers can use depends on how the UM dial plans and auto attendants are configured.

The DTMF interface enables callers to use the telephone keypad to locate users and navigate the Unified Messaging menu system when they call a subscriber access number configured on a dial plan or when they call a telephone number configured on an auto attendant. This topic discusses the DTMF interface and how it's used by callers to locate users and to navigate the Exchange 2010 Unified Messaging menu system.

Contents

DTMF Overview

DTMF requires a caller to press a key on the telephone keypad that corresponds to a Unified Messaging menu option or to input a user's name by using the letters on the keys to spell the user's name or e-mail alias. Callers might use DTMF because Automatic Speech Recognition (ASR) hasn't been enabled or because they tried to use voice commands and failed. In either case, DTMF inputs are used to navigate menus and search for users.

By default, in Exchange 2010 Unified Messaging, DTMF inputs are used on dial plans and are the default caller interface for UM auto attendants.

Note:
Only auto attendants configured to use English can be speech-enabled.

DTMF inputs can be used by callers for:

- Dial plan subscriber access by using Outlook Voice Access.

- Dial plan directory lookups and searches to locate users.
- Auto attendants that aren't speech-enabled.
- Auto attendants that are speech-enabled that do or don't have a DTMF fallback auto attendant configured.
- DTMF fallback auto attendants (not speech-enabled).

UM Dial Plans and Dial by Name

When you create a UM dial plan, you can configure the primary and secondary input method that callers will use to look up names when they search for a user or want to contact a user. These settings are located on the dial plan's **Settings** tab and are called **Dial by name primary method** and **Dial by name secondary method**. The following options are available for the **Dial by name primary method** and the **Dial by name secondary method**:

- Last First
- First Last
- SMTP Address

Additionally, **None** is an available option on the **Dial by name secondary method**.

By default, **Last First** is selected for the **Dial by name primary method** and **SMTP Address** is selected as the **Dial by name secondary method.** Therefore, when a caller dials in to the subscriber access number configured on the UM dial plan, the dial plan's welcome message is played and the operator says something like, "Welcome to Contoso Outlook Voice Access. To access your mailbox, enter your extension. To contact someone, press the # key." After the caller presses the # key, the system responds with "Spell the name of the person you are calling, last name first, or to spell their e-mail alias, press the # key twice." In this scenario, depending on how your dial plan is configured, the system then prompts the caller to enter the user's last name first and then the user's first name (Last First) or to spell the e-mail alias, excluding the domain name.

For example, if the user's e-mail alias is tsmith@contoso.com, the caller would enter tsmith. If you want to change this configuration because the default setting doesn't meet your needs, you can change it to enable callers to enter the user's e-mail alias first or the user's first name followed by the last name. In this case, you would configure the **Dial by name primary method** with the **SMTP Address** setting and configure the **Dial by name secondary method** with the **First Last** setting. The settings for the dial by name methods will also apply to any UM auto attendants that are associated with the dial plan. For callers to be able to enter the name of the user by using DTMF inputs or the keys on the telephone keypad, a DTMF map and values for the user must exist within the Active Directory directory service.

For more information about how to change the dial by name primary and secondary methods on a UM dial plan, see Configure the Dial by Name Primary Method on a Unified Messaging Dial Plan and Configure the Dial by Name Secondary Method on a UM Dial Plan.

Return to top

DTMF Maps

In an Exchange 2010 organization, an attribute named **msExchUMDtmfMap** is associated with each user created in Active Directory. This attribute is used by Unified Messaging to map the user's first name, last name, and e-mail alias to a set of numbers. This mapping is referred to as a DTMF map. A DTMF map enables a caller to enter the digits on the telephone keypad that correspond to the letters of the user's name or e-mail alias. This attribute contains the values needed to create a DTMF map for the user's first name followed by the last name, for the user's last name followed by the first name, and for the user's e-mail alias.

The following table shows the DTMF map values that would be stored in Active Directory on the **msExchUMDtmfMap** attribute for a UM-enabled user named Tony Smith with an alias of tsmith@contoso.com.

DTMF values stored in Active Directory for a UM-enabled user named Tony Smith

Active Directory entry	User's name
• firstNameLastName:866976484	tonysmith
• lastNameFirstName:764848669	smithtony
• emailAddress:876484	tsmith

- Names and e-mail aliases may contain other characters that aren't alphanumeric, such as commas, hyphens, underscores, or periods. Characters such as these won't be used in a DTMF map for a user. For example, if the e-mail alias for Tony Smith is tony-smith@contoso.com, the DTMF map value would be 866976484, and the hyphen wouldn't be included. However, if a user's e-mail alias contains a number or numbers, for example, tonysmith123@contoso.com, the numbers would be used in the DTMF map that's created. The DTMF map for tonysmith123 would be 866976484123.

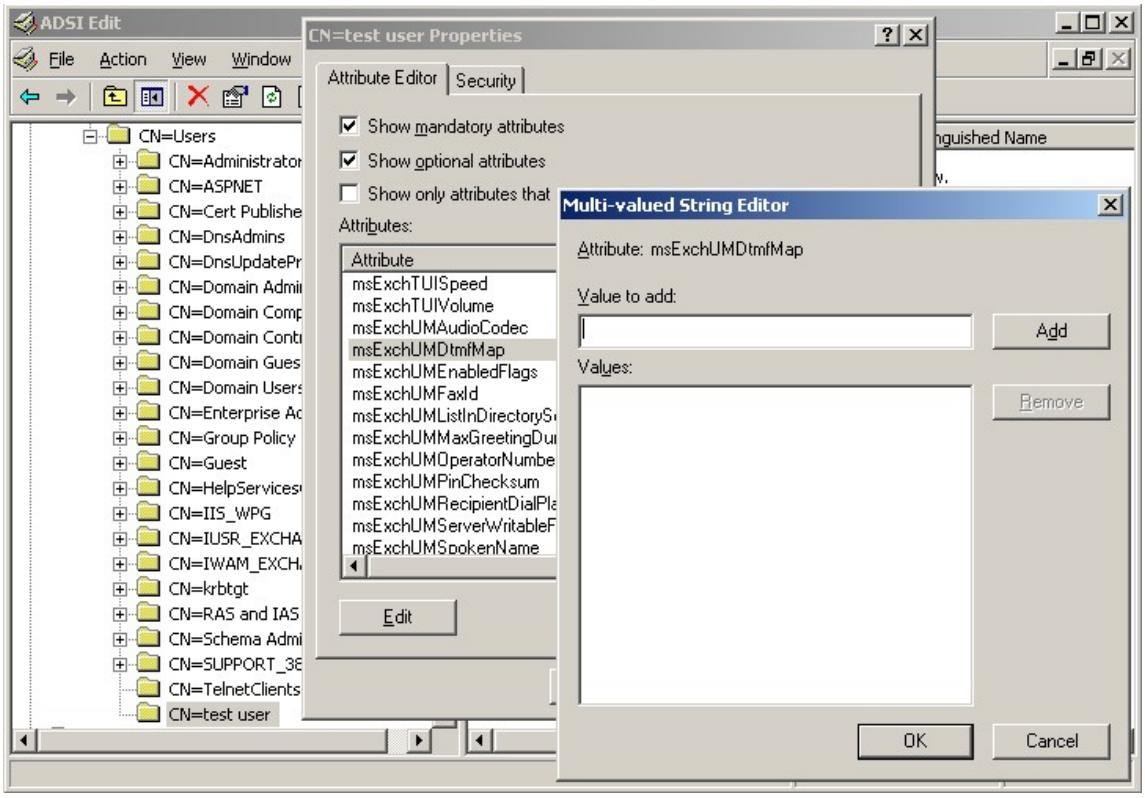
A DTMF map must exist for a user for callers to be able to enter the user's name or e-mail alias. However, in some cases, not all users will have a DTMF map associated with their user account.

Return to top

DTMF Maps for Users Who Aren't Enabled for Unified Messaging

Users, including mailbox-enabled users, aren't enabled for Unified Messaging by default. Therefore, the **msExchUMDtmfMap** attribute isn't populated with the values needed for a DTMF map for those users. The following figure illustrates the properties of a user for which the **msExchUMDtmfMap** attribute hasn't been populated.

msExchUMDtmfMap attribute without values



Because the user shown in the previous figure doesn't have DTMF map values defined for the user account, callers will be unable to contact the user when they press a telephone key from a UM auto attendant menu or perform a directory search. Also, UM-enabled users will be unable to send messages or transfer calls to users who don't have a DTMF map unless they can use ASR. To enable callers to transfer calls or contact users who aren't UM-enabled by using the telephone keypad, you must create the necessary values for the DTMF map for users. To create the values for a DTMF map for users who aren't enabled for Unified Messaging, you can run the **galgrammargenerator.exe -u** command. This command updates the DTMF maps for all users within your Exchange organization. The **galgrammargenerator.exe** command updates or creates DTMF maps for all users who aren't UM-enabled. You can use the **Set-User** cmdlet with the *-CreateDtmfMap* parameter to create and update a single user's DTMF map or update a DTMF map for a user if the name of the user was changed after a DTMF map was created. Optionally, you can create an Exchange Management Shell script by using this cmdlet to update the DTMF map values for multiple users.

For more information about the **Set-User** Exchange Management Shell cmdlet, see Set-User.

For more information about galgrammargenerator.exe, see Understanding Automatic Speech Recognition Directory Lookups.

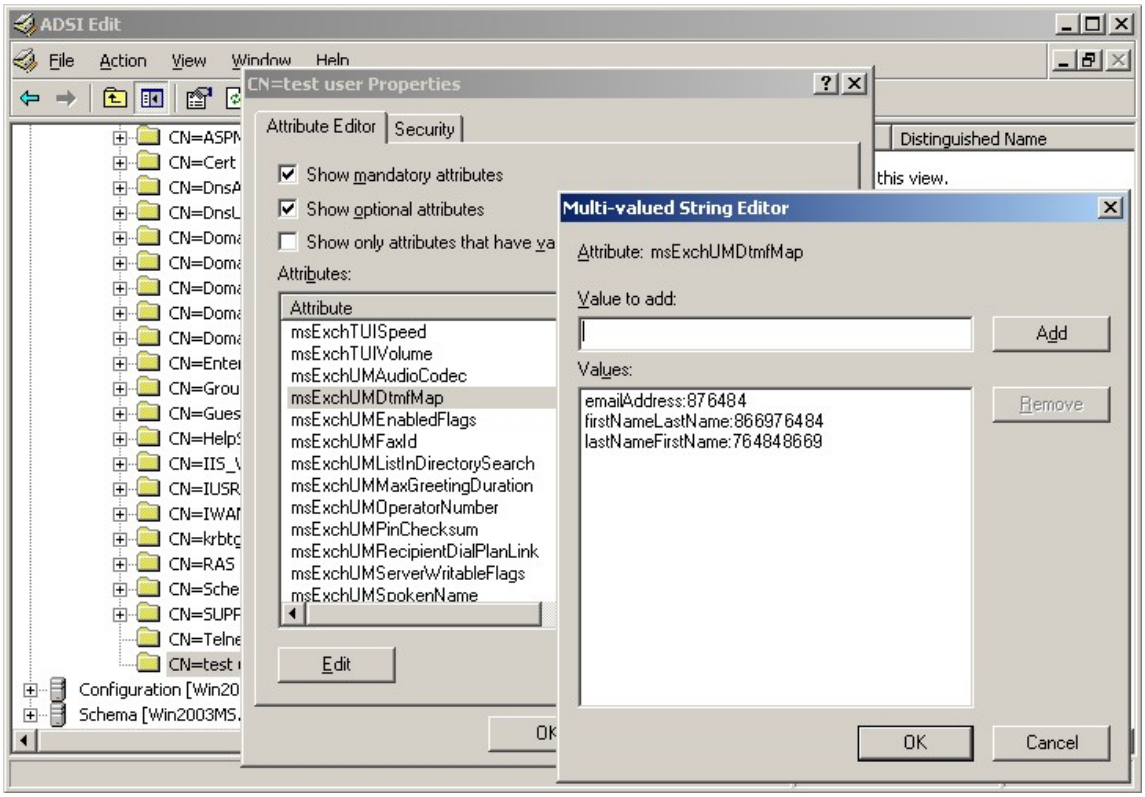
Return to top

DTMF Maps for Users Who Are Enabled for Unified Messaging

A DTMF map is created for UM-enabled users so that callers can contact them. By default, a DTMF map is created for users when they are enabled for Unified Messaging. This makes

it possible for calls to be transferred to a UM-enabled user from external callers, from users who aren't enabled for Unified Messaging, and from other UM-enabled users who use the telephone keypad to spell the user's name or e-mail alias. The following figure illustrates the properties on a user account where the **msExchUMDtmfMap** attribute has been populated with DTMF map values.

msExchUMDtmfMap attribute with values



After the DTMF map values have been created for a UM-enabled user, callers can use the directory search feature. Callers use directory search when they use the telephone keypad in the following situations:

- To identify or search for a user when they call in to the subscriber access number.
- To locate or transfer calls to a UM-enabled user when they call in to a UM auto attendant.

For more information about how to enable a user for Unified Messaging, see Enable a User for Unified Messaging.

Sometimes a user's first name, last name, or e-mail alias changes after the user is enabled for Unified Messaging. The user's DTMF map values aren't updated automatically in Active Directory. If a caller enters the user's new last name or e-mail alias and the user's DTMF map hasn't been updated to reflect the change to the name or e-mail alias, the caller will be unable to locate the user in the directory, send a message to the user, or transfer calls to the user. If you have to update a user's DTMF map after the user has been enabled for Unified Messaging, you can use the **Set-User** cmdlet with the -*CreateDtmfMap* parameter. You can also create an Exchange Management Shell script using this cmdlet if you want to update the DTMF maps for multiple UM-enabled users.

Note:

You can also use the **galgrammargenerator.exe -u** command to update the DTMF map

for UM-enabled users. However, if you use the **galgrammargenerator.exe -u** command, it will update or create DTMF maps for all users.

Caution:
We recommend that you don't manually change the DTMF values for users using a tool such as ADSI Edit because it might result in inconsistent configurations or other errors. We recommend that you only use **galgrammargenerator.exe** or the **Set-User** cmdlet to create or update DTMF maps for users.

For More Information

Adsiedit Overview

1.9.1.3.12 Understanding Automatic Speech Recognition Directory Lookups

Understanding Automatic Speech Recognition Directory Lookups

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-10*

Microsoft Exchange Server 2010 Unified Messaging (UM) offers a voice user interface (VUI) that uses Automatic Speech Recognition (ASR). This is the telephone interface callers use to navigate the menu systems and access their mailbox using speech inputs. ASR enables callers to use speech inputs instead of dual tone multi-frequency (DTMF), also known as touchtone, inputs to navigate the UM auto attendant menus or when UM-enabled users accesses their mailbox. This topic discusses how ASR is used in Exchange 2010 Unified Messaging and how grammar files are used with ASR.

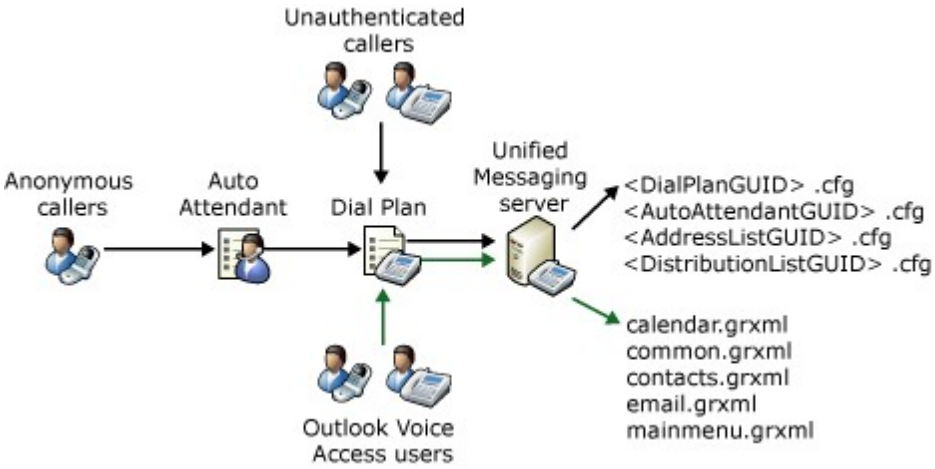
Note:
ASR for directory lookups and searches is currently available only in English for Outlook Voice Access users and for calls to UM auto attendants. However, support for ASR in other languages is planned for a future release.

Contents

Overview of Grammar Files

A speech grammar file contains words and phrases that the speech engine will try to recognize when the grammar file is being used. Grammar files define things such as the

commands available to users while they're reviewing their mail or their calendar or the names of people recognized by the speech engine when a caller searches the directory. Speech grammar files are first generated as files that have a .grxml extension. They're then processed into a compiled form with a .cfg extension before they're loaded into the speech engine. Because the .cfg file is loaded into the memory of the Microsoft Exchange Speech Engine service, there is no .cfg file created and saved to a disk. The following figure shows how the grammar files are used by callers.



Note:

If you want to locate the .grxml file that corresponds to a .cfg file, look in the event log for events that have the IDs 1040 or 1041. The event will show which .grxml file was used to produce a particular .cfg file.

Default Grammar Files

When the Unified Messaging server role is installed, many files are copied to the server. These files include the default grammar files that are used by ASR to enable the VUI. By default, these grammar files are installed in the <Program Files>\Microsoft\ Exchange Server\V14\UnifiedMessaging\grammars\<*language*> folder. However, when these grammar files are used by the Unified Messaging server, they're loaded and compiled into a .cfg file by the Microsoft Exchange Speech Engine service.

The default grammar files include the following files:

- Calendar.grxml
- Common.grxml
- Contacts.grxml
- Email.grxml
- Mainmenu.grxml

Custom Grammar Files

Several custom grammar files are created when the Unified Messaging server role is installed and then again when you create UM objects in the Active Directory directory service and the Microsoft Exchange Unified Messaging service runs grammar generation at its scheduled time, once each day. These grammar files contain the names of users and other objects, for example distribution lists, that are in Active Directory. For each name, there is additional data, for example an e-mail alias. This data lets the name be associated with a unique object.

The following grammar files are created when the Microsoft Exchange Unified Messaging service runs grammar generation at the scheduled time:

- Gal.grxml

- *<DialPlanGUID>*.grxml
- *<AddressListGUID>*.grxml
- DistributionList.grxml

Note:
UM-enabled users may not be immediately available for callers. You must either wait until the next scheduled grammar generation to occur or manually run **galgrammargenerator.exe** to include the UM-enabled user's name in a grammar file.

When the Unified Messaging server creates a speech grammar file, it examines many directory objects to determine which names should be added to the speech grammar file. The types of objects it processes are based on the scope of the grammar being created. However, for all these objects, Unified Messaging won't add the object to the grammar if the object is hidden from the Exchange 2010 address lists or the **msExchHideFromAddressLists** attribute is set to true for the object.

- For the global address list grammar file, Unified Messaging will consider the following:
  - Mail-enabled users
  - Mail-enabled contacts
- For dial plan grammar files, Unified Messaging will consider the following:
  - UM-enabled users in the specified dial plan
- For the distribution list grammar file, Unified Messaging will consider the following:
  - Distribution lists that are visible in address lists

A default global address list is created when the Mailbox server role is installed on a computer running Exchange 2010. When the Unified Messaging server role is installed, it creates a grammar file for the global address list based on the speech grammar filters that are configured. If you create custom address lists or distribution lists in your Exchange 2010 organization, additional grammar files will be created for each custom address list or distribution list you create.

If you create an address list that contains, for example, all recipients in a particular department, and then later add a new user in this department, the recipient won't be included as a member of the address list until you run the **Update-AddressList** cmdlet.

If you create an address list that contains, for example, all recipients in a particular department, and then the membership of the address list changes, you must run the **Update-AddressList** cmdlet before Unified Messaging name speech grammar generation occurs. This ensures that, when the grammar is generated or updated, it will contain all the recipients currently in the address list. When you run the **Update-AddressList** cmdlet, it will include each recipient in every address list that the recipient is a member of.

If a UM-enabled user isn't stamped as a member of an address list before grammar generation occurs, the user won't be added as a member. The next time grammar generation occurs, either on the defined schedule or manually when you run **galgrammargenerator.exe**, the UM-enabled user won't be added to the grammar for the address list. Therefore, their name won't be available when the directory is searched.

Note:
For a grammar file to be generated for a distribution list, the distribution list must not be hidden.

When you first create a UM dial plan, no grammar files are created. However, when a Unified Messaging server joins a dial plan for the first time, a single grammar file for the UM dial plan is created in the appropriate language folder. The UM dial plan speech grammar file is then filtered to include only UM-enabled users associated with the dial plan. The grammar files for these objects are named using the GUIDs of the objects they represent after they're compiled, for example, 2da514a1-06f4-44a1-9ce5-

610854f7d2ee.grxml or the corresponding .cfg file.

When the grammar files for UM dial plans, the global address list, address lists, and distribution lists are created, they're created in a language-specific folder on the local Unified Messaging server. The language folder used is selected based on the default language that is configured on the UM dial plan. For example, if the default language on the dial plan is set to US-English (en-US), a grammar file will be created in the <Program Files>\Microsoft\ Exchange Server\V14\UnifiedMessaging\grammars\en folder. After the grammar file is created, it will be updated according to the schedule that is configured on the Unified Messaging server.

For more information, see the following topics:

- Add a UM Server to a Dial Plan
- Create a UM Dial Plan
- Create a UM Auto Attendant

Grammar Generation

Frequently, the default grammar generation schedule will meet your needs. However, there are times when you must manually generate grammar files or update existing grammar files before the scheduled grammar generation task runs. There may also be times when you want to change the default grammar generation schedule.

Grammar generation occurs in the following situations:

- When the Unified Messaging server is added to a UM dial plan, and daily after that at a scheduled interval.
- When you run the **galgrammargenerator.exe** command to manually update or create grammar files.

The grammar file that is created is then updated when the scheduled grammar generation task runs. To display the default grammar generation schedule for a UM server, use the following cmdlet in the Exchange Management Shell:

```
(Get-UMServer $env:COMPUTERNAME).GrammarGenerationSchedule
```

For more information about the **Get-UMServer** cmdlet, see Get-UMServer.

By default, grammar generation occurs daily at the time specified by the *GrammarGenerationSchedule* parameter of the UM server. By default, the schedule is defined so that grammar generation starts at 2:00 A.M. each day. However, the grammar generation schedule can be changed and is controlled using the **Set-UMserver** cmdlet in the Shell. There is no graphical user interface that you can use to control the grammar generator schedule. This schedule can be controlled only by using the **Set-UMserver** cmdlet in the Shell. For more information about how to change the phonetic display name using the **Set-UMServer** cmdlet, see Set-UMServer.

By default, the grammar generation schedule is set to start once a day at 2:00 A.M. local time on the UM server. After it starts, grammar generation will run until it is completed, whether this is before the scheduled end time for the active period or not. Grammar generation won't run if there is another grammar generation that is running. Although you can configure additional scheduled times, grammar generation won't run within one hour of a previously scheduled grammar generation period. Because grammar generation uses lots of system resources, we recommend that you configure all grammar generation schedules so that grammar generation will occur during off-peak hours. However, you can stagger the grammar generation schedules on multiple UM servers, for example, Umserver1 starts at 2:00 A.M., Umserver2 starts at 2:30 A.M., and Umserver3 starts at 3:00 A.M. This helps minimize the effect of grammar generation on the Active Directory domain controllers.

Note:
A log file named UMSpeechGrammar.log will be created in the %ExchangeRoot%\UnifiedMessaging\temp folder. This log file contains information about all grammar files created or updated on a UM server. This file will be overwritten every time that scheduled grammar generation runs.

In the following circumstances, you can wait for the next scheduled grammar generation for the changes to be reflected, or you can force an update using the **galgrammargenerator.exe** command:

- When you complete a new installation of the UM server role and enable users for Unified Messaging
- When a UM dial plan, UM auto attendant, custom address list, or custom distribution list is created
- When you create UM-enabled users
- If you change a UM dial plan or UM auto attendant

Note:
When an Outlook Voice Access user tries to locate a UM-enabled user using the directory search feature with ASR immediately after you complete a new installation of the Unified Messaging server role and enabled users for UM, the caller will hear a system prompt that says, "I'm sorry I couldn't help." Then they are disconnected. This occurs because a grammar file for the global address list hasn't been generated. Use the **galgrammargenerator.exe** command to create the required grammar file for the global address list.

Each grammar file is overwritten every time that the Microsoft Exchange Unified Messaging service automatically runs or when you manually run the galgrammargenerator.exe program to force an update of the grammar files. This ensures that users who have just been enabled for UM can be accessed from the directory search in a time-efficient manner when a caller uses ASR. You can use **galgrammargenerator.exe** to force an update, or to generate or overwrite the grammar files used by Unified Messaging if they become corrupted. For example, when you first enable users for Unified Messaging, those users won't be available to callers who use ASR to perform a directory search until the scheduled grammar generation task runs. To make sure that those new users who were recently UM-enabled are visible to callers, run the galgrammargenerator.exe program to force the .grxml files to be created or updated and to compile the appropriate .cfg files so that callers can use ASR to move through the menu systems or locate users using ASR. For detailed steps, see Update the Speech Grammar Files on a UM Server.

Galgrammargenerator.exe is also useful when a UM server has joined a dial plan and one or more speech-enabled auto attendants are associated with the dial plan. By default, callers who call into a speech-enabled auto attendant can only reach UM-enabled users who are associated with the dial plan. Before callers can be transferred to UM-enabled users using voice inputs, a grammar file must be generated. The grammar file isn't generated automatically when the server joins a dial plan. Instead, it is generated the next time grammar generation is scheduled. Grammar generation occurs according to the default schedule, at 2:00 AM local time each day, unless the schedule has been changed.

If you want UM-enabled users to be available from a directory search from the speech-enabled auto attendant immediately after you create the auto attendant, you must generate the required grammar file for the auto attendant using galgrammargenerator.exe with the *–d* option.

A grammar file isn't required with auto attendants that aren't speech-enabled. This is because a DTMF map is added to Active Directory for each user when they're enabled for Unified Messaging. DTMF maps enable callers to enter the digits that correspond to the letters of the user's name or e-mail alias on a telephone keypad.

However, a DTMF map won't automatically be created for users who aren't UM-enabled. By using galgrammargenerator.exe with the *-u* option, you can generate a DTMF map for all users who are mail-enabled but not UM-enabled. This lets users who are mail-enabled but not UM-enabled be reached from the auto attendant when their name or e-mail alias is entered by a caller using DTMF inputs. For more information about the DTMF interface, see Understanding the DTMF Interface.

The following table lists the switches and descriptions for the switches for galgrammargenerator.exe.

Galgrammargenerator.exe and the switches

Switch	Description
-d <dialplan>	Creates a grammar file that contains the names of UM-enabled users only in the specified UM dial plan.
-g	Generates the grammar file.
-l	Generates a grammar file for a distribution list.
-o	Generates a log file. The path can be an absolute path, for example, C:\Logfiles. By default, the UM server will also automatically create a log file in the \UnifiedMessaging \Temp folder.
-p	Preloads all generated grammars into the Microsoft Speech Server platform.
-s <UMserver>	Creates a grammar file for each UM dial plan to which the specified UM server belongs.
-u	Creates or updates DTMF maps for users who are enabled for UM and who aren't enabled for UM. **Note:** If mailbox-enabled users or mail-enabled contacts have a character in their e-mail alias that isn't valid and you run the **galgrammargenerator.exe /u command** to create a DTMF map for users, the command won't complete successfully and Unified Messaging will report an error. To ensure that all mailbox users and mail-enabled contacts have no characters in their e-mail addresses that aren't valid, use the **Get-User** cmdlet to view all users. The **Get-User** cmdlet will perform a validation check for the user attributes. If any field has a character that isn't valid, an error will be generated that identifies the recipient and the field that contains the character.
-x	Defines the speech filter list that is used in XML format.

Note:
The default speech grammar filter list (SpeechGrammarFilterList.xml) is installed in the

<Program Files>\Microsoft\ Exchange Server\V14\Bin folder on each server that has the Unified Messaging server role installed. The contents of the speech filter list file must be the same on each UM server. The speech grammar filter list contains several rules that specify input patterns against which display names are matched and output patterns that define transformations of the matched name. If the name matches a pattern, it will be replaced in the speech grammar by the name or names generated from the associated output pattern or patterns. If the name doesn't match a pattern, it is passed through unchanged to the speech grammar. Names will be rejected from insertion in the speech grammar if they to have two or more distinct ways of being said. We recommend that you don't manually modify the SpeechGrammarFilterList.xml file.

Customizing Grammar Files

Currently, ASR is available only in English and includes the prerecorded prompts and Text-to-Speech (TTS) support for English. Although ASR support is included in the English language pack, there are times when it is difficult for speech recognition to locate the correct UM-enabled user because the user has a name that is difficult to pronounce, the caller's speech is matched against the wrong name, or the caller speaks a form of the user's name that differs from the name that exists in the speech grammar. However, adding an additional UM language pack won't resolve this problem.

Note:

Because ASR is enabled by default for U.S. English, a folder named \grammars\en is created on each Unified Messaging server. A folder is created for each language pack you install on the Unified Messaging server.

Unified Messaging uses two Active Directory attributes to generate names to use with ASR grammar files: Display name (**displayName**) and Phonetic display name (**msDS-PhoneticName**). By default, Unified Messaging uses the **displayName** attribute to recognize the name of a user when a caller speaks their name. This works well if the user's name is easy to pronounce. However, in some cases, users have names that are difficult to pronounce. To help Unified Messaging find users whose names are difficult to pronounce, we recommend that you configure the Unified Messaging system by supplying a phonetic display name for users who have names that ASR has trouble recognizing. However, to supply a phonetic display name, you must predict how the speech engine would perceive a certain spelling of a name to provide an accurate pronunciation for the phonetic name.

Note:

By default, the UM server will try to insert both the phonetic display name, if one exists, and the display name into the speech grammar file.

For example, the display name "Kweku Ako-Adjei" could be given a phonetic display name of "Quaykoo Akoo Oddjay", and UM would insert that into the speech grammar file. The drawback to creating phonetic names for users is that it is difficult to do on a large scale. It would be very time-consuming to create and test phonetic display names for every user whose name isn't correctly recognized by ASR, especially in large enterprise environments.

To add or change the phonetic display name for a UM-enabled user, you must use ADSI Edit (AdsiEdit.msc) or the **Set-User** cmdlet in the Shell. You can't use Active Directory Users and Computers or the Exchange Management Console to change a user's phonetic display name. For more information about how to change a phonetic display name using the **Set-User** cmdlet, see Set-User.

The *PhoneticDisplayName* parameter specifies a phonetic pronunciation for the display name. The display name is specified using the *DisplayName* parameter. If the display name isn't easy for the UM server to pronounce or recognize, you can use the *PhoneticDisplayName* parameter to specify a phonetic version. If you specify a value, it is

used by ASR to recognize the user's name and by the TTS engine to pronounce the user's name. If you don't specify a value, the UM server uses the *DisplayName* parameter. The maximum length of this parameter value is 255 characters.

For more information about ADSI Edit, see Adsiedit Overview.

For More Information

Update the Speech Grammar Files on a UM Server

Understanding Unified Messaging Dial Plans

Understanding Unified Messaging Auto Attendants

1.9.1.3.13 Understanding Telephony Concepts and Components

Understanding Telephony Concepts and Components

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-22*

If you're planning and deploying Microsoft Exchange Server 2010 Unified Messaging (UM) on your network, you must understand Unified Messaging and telephony networks. This topic provides an overview of telephony infrastructure concepts and components that will help you plan and deploy a server running Exchange 2010 Unified Messaging.

Contents

Overview

In versions of Microsoft Exchange before Exchange Server 2007, the Exchange administrator's main responsibility was managing e-mail messages and, sometimes,

managing a network infrastructure. Earlier versions of Exchange didn't have Unified Messaging capabilities. Exchange Server version 5.5, Exchange 2000 Server, and Exchange Server 2003 administrators focused on the Exchange environment and the network infrastructure, and relied heavily on telephony consultants to manage their telephony environment and infrastructure.

Concepts and Components

To successfully deploy a Unified Messaging server in Exchange 2010, you must have a good understanding of basic telephony concepts and telephony components. After you gain a good understanding of telephony basics, you can successfully integrate Exchange 2010 Unified Messaging into an Exchange 2010 organization. Basic concepts and components include the following:

- Circuit-switched and packet-switched networks
- Private Branch eXchange (PBX)
- IP PBX
- Voice over Internet Protocol (VoIP)
- IP gateways

Circuit-Switched Networks

In circuit-switched networks, such as the Public Switched Telephone Network (PSTN), multiple calls are transmitted across the same transmission medium. Frequently, the medium used in the PSTN is copper. However, fiber optic cable might also be used.

A circuit-switched network is a network in which there exists a dedicated connection. A dedicated connection is a circuit or channel set up between two nodes so that they can communicate. After a call is established between two nodes, the connection may be used only by these two nodes. When the call is ended by one of the nodes, the connection is canceled.

Note:

PSTN is a grouping of the world's public circuit-switched telephone networks. This grouping resembles the way that the Internet is a grouping of the world's public IP-based packet-switched networks.

There are two basic types of circuit-switched networks: analog and digital. Analog was designed for voice transmission. For many years, the PSTN was only analog, but today, circuit-based networks such as the PSTN have transitioned from analog to digital. To support an analog voice transmission signal over a digital network, the analog transmission signal must be encoded or converted into a digital format before it enters the telephony WAN. On the receiving end of the connection, the digital signal must be decoded or converted back into an analog signal format.

There are advantages and disadvantages to circuit-switched networks. Circuit-switched networks have several disadvantages. Circuit-switched networks can be relatively inefficient, because bandwidth can be wasted. This isn't the case when VoIP is used on a packet-switched network. VoIP shares the available bandwidth with all other network applications and makes more efficient use of the available bandwidth. Another disadvantage to circuit-switched networks is that you have to provision for the maximum number of telephone calls that will be required for peak usage times and then pay for the use of the circuit or circuits to support the maximum number of calls.

Circuit switching has one big advantage over packet-switched networks. In a circuit-switched network when you use a circuit, you have the full circuit for the time that you're using the circuit without competition from other users. This isn't the case with packet switched networks.

Note:

Synchronous Digital Hierarchy (SDH) has become the primary transmission protocol for most PSTN networks. SDH is carried over fiber optic networks.

Return to top

Packet-Switched Networks

Packet switching is a technique that divides a data message into smaller units called packets. Packets are sent to their destination by the best route available, and then they are reassembled at the receiving end.

In packet-switched networks such as the Internet, packets are routed to their destination through the most expedient route, but not all packets traveling between two hosts travel the same route, even those from a single message. This almost guarantees that the packets will arrive at different times and out of order. In a packet-switched network, packets (messages or fragments of messages) are individually routed between nodes over data links that may be shared by other nodes. With packet switching, unlike circuit switching, multiple connections to nodes on the network share the available bandwidth.

Note:

With circuit switching, all packets go to the receiver in order and along a single path.

Packet-switched networks exist to enable data communication on the Internet throughout the world. A public data network or packet-switched network is the data counterpart to the PSTN.

Packet-switched networks are also found in such network environments as LAN and WAN networks. A WAN packet-switched environment relies on telephone circuits, but the circuits are arranged so that they retain a permanent connection with their endpoint. In a LAN packet-switched environment, such as with an Ethernet network, the transmission of the data packets relies on packet switches, routers, and LAN cables. In a LAN, the switch establishes a connection between two segments only long enough to send the current packet. Incoming packets are saved to a temporary memory area or buffer in memory. In an Ethernet-based LAN, an Ethernet frame contains the payload or data portion of the packet and a special header that includes the media access control (MAC) address information for the source and destination of the packet. When the packets arrive at their destination, they are put back in order by a packet assembler. A packet assembler is needed because of the different routes that the packets may take.

Packet-switched networking has made it possible for the Internet to exist and, at the same time, has made data networks—especially LAN-based IP networks—more available and widespread.

Return to top

PBX

A legacy PBX is a telephony device that acts as a switch for switching calls in a telephony or circuit-switched network.

Note:

A legacy PBX is a PBX that cannot pass IP packets. In many businesses, legacy PBXs have been replaced by IP PBXs.

A PBX is a telephony device used by most medium-size and larger-size companies. A PBX enables users or subscribers of the PBX to share a certain number of outside lines for making telephone calls considered external to the PBX. A PBX is a much less expensive

solution than giving each user in a business a dedicated external telephone line. Telephone sets, in addition to fax machines, modems, and many other communication devices, can be connected to a PBX.

The PBX equipment is typically installed at a business's premises and connects calls between the telephones located and installed in the business site. A limited number of outside lines, also known as trunk lines, are typically available for making and receiving calls external to the business from an external source such as the PSTN.

Internal business calls made to external telephone numbers using a PBX are made by dialing 9 or 0 in some systems followed by the external number. An outgoing trunk line is automatically selected to complete the call. Conversely, the calls placed between users within the business don't ordinarily require special dialing digits or use of an external trunk line. This is because the internal calls are routed or switched by the PBX between telephones physically connected to the PBX.

In medium-size and larger-size businesses, the following PBX configurations are possible:

- A single PBX that supports the whole business.
- A grouping of two or more PBXs not networked or connected to each other.
- A grouping of two or more PBXs connected together or networked.

Note:
An Exchange 2010 UM dial plan can span more than one PBX and one IP gateway.

Return to top

IP PBX

An IP PBX is a PBX that supports the IP protocol to connect phones using an Ethernet or packet-switched LAN and sends its voice conversations in IP packets. A hybrid IP PBX supports the IP protocol for sending voice conversations in packets, but also connects traditional analog and digital circuit-switched Time Division Multiplex (TDM) telephones. An IP PBX is telephone switching equipment that resides in a private business instead of the telephone company.

IP PBXs are frequently easier to administer than legacy PBXs, because administrators can easily configure their IP PBX services using an Internet browser or another IP-based utility. Plus, no additional wiring, cabling, or patch panels must be installed. With an IP PBX, moving an IP-based telephone is as simple as unplugging a telephone and plugging it in at a new location, instead of the costly service calls to move a telephone from legacy PBX vendors. Additionally, businesses that own an IP PBX don't have the additional infrastructure costs required to maintain and manage two separate circuit-switched and packet-switched networks.

VoIP

Voice over Internet Protocol (VoIP) is a technology that contains hardware and software that enables people to use an IP-based network as the transmission medium for telephone calls. In VoIP, voice data is sent in packets using IP instead of traditional circuit transmissions or the circuit-switched telephone lines of the PSTN. An IP gateway that you connect to your IP network uses VoIP to send voice data packets between an Exchange 2010 Unified Messaging server and a PBX system.

IP Gateways

An IP gateway is a third-party hardware device or product that connects a legacy PBX to

your LAN. The IP gateway lets the PBX system communicate with your Exchange 2010 Unified Messaging server running IP.

Note:

The IP gateway can also connect to PBX systems that use VoIP instead of PSTN circuit-switched protocols.

Exchange 2010 Unified Messaging relies on the gateway's abilities to translate or convert TDM or telephony circuit-switched based protocols like ISDN and QSIG from a PBX to IP-based or VoIP-based protocols like Session Initiated Protocol (SIP), Realtime Transport Protocol (RTP), or T.38 for Realtime Facsimile Transport. The IP gateway is integral to the functionality and operation of Unified Messaging.

Important:

After you install the IP gateway, you must create an IP Gateway object in Active Directory to represent the IP gateway. After you create a UM IP Gateway object, the Unified Messaging server associated with the UM IP gateway will send a SIP OPTIONS request to the IP gateway to ensure that the IP gateway is responsive. If the IP gateway doesn't respond to the SIP OPTIONS request from the Unified Messaging server, the Unified Messaging server will log an event with ID 1088 stating that the request failed. To resolve this issue, ensure that the IP gateway is available and online and that the Unified Messaging configuration is correct.

For more information about IP PBX and PBX configurations, see Understanding PBX and IP PBX Configurations.

Return to top

For More Information

PBX Configuration Notes Tested by Microsoft or IP Gateway Vendor Partners

1.9.1.3.14 Understanding Protocols, Ports, and Services in Unified Messaging

Understanding Protocols, Ports, and Services in Unified Messaging

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-05-09*

Microsoft Exchange Server 2010 Unified Messaging (UM) requires that several TCP and User Datagram Protocol (UDP) ports be used to establish communication between servers running Exchange 2010 and other devices. By allowing access through these IP ports, you enable Unified Messaging to function correctly. This topic discusses the TCP and UDP ports used in Exchange 2010 Unified Messaging.

Unified Messaging Protocols and Services

Exchange 2010 Unified Messaging features and services rely on static and dynamic TCP and UDP ports to ensure correct operation of the computer running the Unified Messaging server role.When Exchange 2010 is installed, static Windows Firewall rules are added for Exchange. If you change the TCP ports that are used by the Unified Messaging server role, you may also need to reconfigure the Windows Firewall rules to allow Unified

Messaging to work correctly.

Important:

On Exchange 2010 Unified Messaging servers, Exchange setup creates the **SESWorker (TCP-In)** and **SESWorker (GFW) (TCP-In)** rules which allow inbound communication without any TCP port restrictions. We recommend you disable these two rules after you've setup the Unified Messaging server, and create a new rule to allow only the ports required for the SESWorker process which include 5065 and 5067 for TCP (unsecured). 5066 and 5068 for mutual TLS (secured). For details, see Exchange Network Port Reference.

Session Initiation Protocol

Session Initiation Protocol (SIP) is a protocol used for initiating, modifying, and ending an interactive user session that involves multimedia elements such as video, voice, instant messaging, online games, and virtual reality. It's one of the leading signaling protocols for Voice over IP (VoIP), together with H.323. Most VoIP standards-based solutions use either H.323 or SIP. However, several proprietary designs and protocols also exist. The VoIP protocols typically support features such as call waiting, conference calling, and call transfer.

SIP clients such as IP gateways and IP Private Branch eXchanges (PBXs) can use TCP and UDP port 5060 to connect to SIP servers. SIP is used only for setting up and tearing down voice or video calls. All voice and video communications occur over Realtime Transport Protocol (RTP).

Realtime Transport Protocol

RTP defines a standard packet format for delivering audio and video over a specific network, such as the Internet. RTP carries only voice/video data over the network. Call setup and teardown are generally performed by the SIP protocol.

RTP doesn't require a standard or static TCP or UDP port to communicate with. RTP communications occur on an even number UDP port, and the next higher odd number port is used for TCP communications. Although there are no standard port range assignments, RTP is generally configured to use ports 1024 and 65535. It's difficult for RTP to traverse firewalls because it uses a dynamic port range.

Unified Messaging Web Services

The Unified Messaging Web services installed on a Client Access server use IP for network communication between a client, the Unified Messaging server, the Client Access server, and computers running other Exchange 2010 server roles. There are several Exchange 2010 Outlook Web App and Microsoft Office Outlook 2007 client features that rely on Unified Messaging Web services to operate correctly.

The following Unified Messaging client features rely on Unified Messaging Web services:

- Voice mail options available with Exchange 2010 Outlook Web App, including the Play on Phone feature and the ability to reset a PIN.
- Play on Phone feature found in the Outlook 2007 client.

Note:

When an organization uses the Play on Phone and other client features in Exchange 2010 Unified Messaging, a computer running the Client Access, Hub Transport, and Mailbox server roles within the same Active Directory site is required in addition to the computer or computers that have the Unified Messaging server role installed.

Port Assignments

The following table shows the IP ports that Unified Messaging uses for each protocol and whether the IP ports used for each protocol can be changed.

IP ports used for Unified Messaging protocols

Protocol	TCP port	UDP port	Can ports be changed?
SIP (Microsoft Exchange Unified Messaging service)	5060 (unsecured) 5061 (secured) The service listens on both ports.		Ports can be changed in the msexchangeum.config configuration file. The msexchangeum.config file is located in the \Program Files \Microsoft\Exchange \V14\bin folder on an Exchange 2010 Unified Messaging server.
SIP (UM worker process)	5065 and 5067 for TCP (unsecured). 5066 and 5068 for mutual TLS (secured)		Ports can be changed in the msexchangeum.config configuration file. The msexchangeum.config file is located in the \Program Files \Microsoft\Exchange \V14\bin folder on an Exchange 2010 Unified Messaging server.
RTP		Ports between 1024 and 65535	Ports can be changed in the msexchangeum.config configuration file. The msexchangeum.config file is located in the \Program Files \Microsoft\Exchange \V14\bin folder on an Exchange 2010 Unified Messaging server.
Unified Messaging Web service	443		The port is configured on the Web site that hosts the Unified Messaging virtual directory. The port can be changed using IIS Manager.

Exchange 2010 Unified Messaging supports Network Address Translation (NAT) traversal and allows for the RTP media to be tunneled through a NAT firewall. However, for this to work, you must also have Microsoft Office Communications Server 2007 deployed in your environment. If you deploy both Exchange 2010 and Communications Server 2007 on your network, this deployment will enable Unified Messaging servers to communicate with endpoints outside a NAT firewall. The Unified Messaging server is associated with a Communications Server 2007 pool and obtains the appropriate authentication tokens from the Communications Server 2007 A/V Authentication Service on a computer serving that particular Communications Server 2007 pool.

The A/V Authentication Service is used to allow voice media to traverse NAT devices and

firewalls. This is necessary because media gateways handle signaling only and cannot transport voice securely across a NAT device or firewall. When you configure a mediation server in Communications Server 2007, you specify the A/V Edge server on which the A/V Authentication Service is running so that the mediation server will know where to forward the incoming media packets.

For more information about how to deploy Communications Server 2007 and Exchange 2010 Unified Messaging, see the following:

- Office Communications Server and Client Documentation Rollup
- Deploy Unified Messaging and Communications Server 2007 R2
- Understanding Unified Messaging and Communications Server 2007 R2

1.9.1.3.15 Understanding PBX and IP PBX Configurations

Understanding PBX and IP PBX Configurations

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Increasingly, organizations are purchasing, installing, and maintaining the hardware components, for example, Private Branch eXchanges (PBXs) or IP PBXs, which are required to support their own telephony system. Many organizations are buying their own telephony equipment and training their staff to reduce expenses associated with maintaining their telephony systems and because they want more control over the telephony features they offer.

For an organization to own and maintain their telephony network, they must buy the required telephony hardware components. They must also consider the day-to-day maintenance of the telephony equipment and the training required for their staff to support their telephony system. This topic discusses the different types of telephony business or organizational systems and the telephony hardware components they require. The topic also gives examples of the different types of telephony configurations.

Important:

We recommend that all customers who plan to deploy Microsoft Exchange Server 2010 Unified Messaging obtain the help of a UM specialist. This will help ensure a smooth upgrade from a legacy voice mail system. Rolling out a new UM deployment or performing an upgrade of an existing voice mail system requires significant knowledge about PBXs, IP PBXs, and Unified Messaging. For more information about who to contact, see the Microsoft Exchange Server 2007 Unified Messaging (UM) Specialists Web site.

Contents

Overview of Telephony Systems

In circuit-switched networks, such as the Public Switched Telephone Network, multiple calls are transmitted across the same transmission medium. Frequently, the medium that's used in the PSTN is copper. However, fiber optic cable might also be used.

A circuit-switched network is a network in which there exists a dedicated connection. A dedicated connection is a circuit or channel that's set up between two nodes so they can communicate. After a call is established between two nodes, the connection may be used only by these two nodes. When the call is ended by one of the nodes, the connection is canceled.

Different types or categories of telephone systems found in businesses and organizations include a circuit-based network, an IP-based network, or both. Each type of telephone system has distinct advantages and disadvantages you need to consider when planning and implementing a telephony system.

- **Centrex** Centrex is a type of telephone service that telephone companies lease to businesses and organizations. A traditional Centrex telephone system eliminates the need for a business or organization to purchase the telephony hardware used onsite to support the organization's telephone system. Typically, Centrex systems are used by small offices that rent Centrex services from a telephone company on a line-by-line and month-by-month basis. Centrex telephony systems are sometimes used by larger organizations, but are most frequently found in government, public, and private organizations. Centrex frequently uses analog telephone lines for the connections to a business or organization. But it can also use T1-circuits with a demultiplexer onsite to support analog and digital telephones or ISDN lines. In a Centrex-based telephony system, the telephone company's central office acts as the telephone exchange. It's designed specifically to support the needs of a given organization. The central telephone office routes the calls that originate from inside the company to the appropriate internal or external telephone number. Centrex uses the telephone company’s central office exchange to route internal calls back to an extension. For example, with Centrex, the telephone exchange or telephone company's central office knows which extensions are internal. So an employee who's located within the organization's telephony network can dial another employee in the same telephony network or dial plan by using a 4-digit extension number. When a call is dialed to the internal telephone extension number, it's forwarded to the telephone company’s central office and then routed back to the extension number that initiated the call.

A variation of a traditional Centrex telephony system is called *IP Centrex*. In an IP Centrex telephone system, the call is sent through an IP gateway located at a telephone company’s central office or located onsite at a service provider. In this kind of telephone system, the IP gateway translates the call into IP-based data packets that can be sent over the Internet or over a Voice over IP–based network. However, if the call is sent over the Internet, there's typically another IP gateway that receives the call and then translates the call back to a traditional circuit-switched call.

Organizations that currently have a traditional Centrex telephone system in place have to install, deploy, and maintain one or more IP gateways for Unified Messaging to work correctly. Unified Messaging may require that you install, deploy, and maintain IP gateways to work with IP Centrex. Several variables will determine whether you need an IP gateway. These variables include the type of telephones used in your organization (analog, digital, or IP) and the protocols supported by the IP Centrex system.

- **Key telephone** In a Key telephone system, the telephone company’s central office is connected to the organization using standard analog or digital telephone lines. A single telephone extension number is connected to multiple telephones so when a call is placed into the organization using this telephone

number, all the telephones associated with that line or extension number will ring at the same time.

With Key telephone systems, individual users share lines across telephones. Therefore, callers won't experience frequent busy signals when they try to call into an organization. Key telephone systems are typically used by small offices where internal call volume is high but external call volume is low.

Key telephone systems have become more sophisticated over time and can work with Unified Messaging if an IP gateway is added. However, some less sophisticated systems may not work even if a supported IP gateway is used.

- **PBX** A legacy PBX is a telephony device that switches calls in a telephony or circuit-switched network. A legacy PBX is a PBX that doesn't have a network adapter and can't pass IP packets. Because they can't pass IP packets, some businesses and organizations have replaced legacy PBXs with IP PBXs. For a list of PBXs supported by Unified Messaging, see Telephony Advisor for Exchange 2010.
  PBXs are used by most medium- and larger-sized companies. A PBX enables users or subscribers of the PBX to share a certain number of outside lines for making telephone calls considered external to the PBX. A PBX is a much less expensive solution than giving each user in a business a dedicated external telephone line. Telephones, in addition to fax machines, modems, and many other communication devices, can be connected to a PBX.
  The PBX equipment is typically installed on an organization's premises and connects calls between the telephones located onsite and the telephone company. A limited number of outside lines, also known as trunk lines, are typically available for making and receiving calls external to the business from an external source such as the PSTN.
  To enable a legacy PBX to be used with Unified Messaging, you need to deploy a supported IP gateway. For a list of supported IP gateways, see Telephony Advisor for Exchange 2010.
- **IP PBX** An IP PBX is a PBX that has a network adapter that supports the IP protocol. It's a piece of telephone switching equipment that generally resides in an organization or business instead of being located at a telephone company office. There are two types of IP PBXs: traditional IP PBXs and hybrid IP PBXs. Both traditional IP PBXs and hybrid IP PBXs support the IP protocol for sending voice conversations in packets to VoIP-based telephones. However, hybrid IP PBXs also connects traditional analog and digital telephones.
  IP PBXs are frequently easier to administer than legacy PBXs, because administrators can more easily configure IP PBX services using an Internet browser or another IP-based tool. Also, no additional wiring, cabling, or patch panels has to be installed. With an IP PBX, you can move an IP-based telephone by merely unplugging a telephone and plugging it in at a new location. This lets you avoid the costly service calls required to move a telephone from legacy PBX vendors. Additionally, organizations that own an IP PBX don't have to incur the additional infrastructure costs required to maintain and manage separate circuit-switched and packet-switched networks. For a list of IP PBXs supported for Unified Messaging, see Telephony Advisor for Exchange 2010.

Return to top

Legacy and Traditional PBX Configurations

On telephony networks that have legacy or traditional PBXs, a PBX does the following:

- Creates connections or circuits between the telephone sets of two users
- Maintains the connection as long as the users need the connection
- Provides information for accounting purposes (for example, meters calls)

In addition to the three functions included in the previous list, PBXs may offer other calling features such as:

- Auto attendants
- Call accounting
- Call pick-up
- Call transfer
- Call waiting
- Conference calling
- Direct Inward Dialing (DID)
- Do Not Disturb (DND)

Although there are several manufacturers of PBXs, they all fit into two basic categories: analog and digital. These types of PBXs are frequently known as *legacy* or *traditional* PBXs.

Typically, PBX systems are connected to the telephone company's central office by using special telephone lines, known as T1- and E1-lines. T1- and E1-lines have multiple channels. These telephone lines are also known as *trunk lines.* They let the central office or the PBX send multiple calls over the same line for better efficiency using a simplified wiring layout. A PBX can also work with analog or ISDN lines.

By correctly configuring your PBX, you can control how many channels or lines you want to configure to receive calls that come from external callers and how many channels or lines to devote to calls that come from callers inside your organization. Configuring the number of channels or lines helps prevent busy signals and lets you configure the number of channels or lines devoted to applications such as call centers. Correctly configuring your PBX is a cost effective method for managing the channels or lines in your organization because it reduces the number of leased lines required.

A PBX can route a specific dialed telephone number to a specific telephone so users can have their own individual telephone number or extension number. This is known as a Direct Inward Dialing number. When the telephone number is dialed for a user, the telephone company sends the DID number to the PBX by using Dialed Number Identification Service. Because the telephone company uses DNIS to send the number, there's no need for operator intervention to route the call. The PBX has the information about the call to correctly route it to the number that was dialed by the caller. For a list of PBXs supported by Unified Messaging, see Telephony Advisor for Exchange 2010.

Return to top

Analog and Digital PBXs

Analog PBXs send voice and call signaling information, such as the touch tones of a dialed telephone number, as an analog sound. Therefore, the sound is never digitized. To correctly direct the call, the PBX and the telephone company's central office have to listen for the signaling information.

Note:

Touchtone is more technically known as dual tone multi-frequency. When a caller presses a key on a telephone keypad, the telephone produces two separate tones: a high frequency tone and a low frequency tone. When a person speaks into the telephone, only a single tone or frequency is emitted. Sending two tones with different frequencies at the same time reduces the possibility that the signaling tones will be interpreted as a human voice or that a human voice will be interpreted as the signaling tones.

Digital PBXs encode or digitize the analog sound into a digital format. Digital PBXs typically encode the voice sounds using a standard industry audio codec like G.711 or G.729. After the digitized voice is encoded, it's sent over a channel by using circuit switching. Circuit switching sets up an end-to-end open connection. It leaves the channel open for the length of the call and for the caller's exclusive use. However, the signaling method that's used by the PBX depends on the manufacturer. PBX manufacturers may have their own

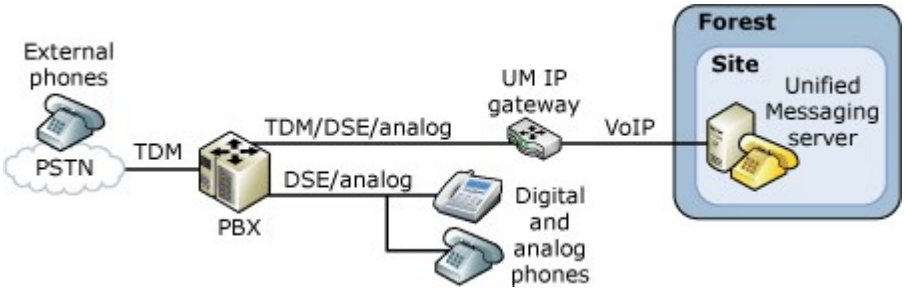
proprietary signaling method for call setup. For more information about the audio codecs used, see Understanding Unified Messaging Audio Codecs.

Note:
Digital PBXs can support both digital and analog trunk lines.

In larger organizations, PBXs make it possible for employees in separate physical locations to contact one another by dialing an extension number for a user. This can be done by using a single PBX or may involve multiple PBXs networked together. PBXs at different office locations can be connected to a single transparent circuit-switched network by using T1- or E1-lines. When these lines connect PBXs together, they are frequently known as *tie lines*. The PBXs communicate with one another across the tie lines using a PBX-to-PBX protocol, such as QSIG. QSIG lets a set of PBXs act as if they are a single PBX.

This kind of PBX environment can also include advanced features, such as call transferring and telephone conferencing. In addition to allowing for advanced features, having two connected PBXs can also save the organization money because long distance charges between employees in the different locations will be reduced. This is because a call made between two employees remains on a tie line between the PBXs and requires that the user dial only an extension number for the other user instead of placing a long distance call.

The following figure illustrates a typical telephony and data network that includes legacy or traditional PBXs.



In a telephony environment that includes a single or multiple analog or digital PBXs, an IP gateway is required between the PBX and the Exchange 2010 computer that has the Unified Messaging server role installed to convert the circuit-based protocols found on a telephony network into the IP-based protocols found on a data network. For more information about IP gateways, see the following topics:

- Understanding Unified Messaging IP Gateways
- Managing IP Gateways

For a list of IP gateways supported for Unified Messaging, see Telephony Advisor for Exchange 2010.

Return to top

IP PBX Configurations

An IP PBX is a PBX that supports the IP protocol to connect telephones by using an Ethernet or packet-switched LAN. It sends voice conversations in IP or data packets. An IP PBX may have multiple interfaces. These include interfaces for a data network and other interfaces that allow for a connection to a telephony or circuit-switched network.

The development of real-time Internet protocols has made it possible to successfully send

voice and fax messages over a data network. Such real-time Internet protocols include the VoIP protocols used with Unified Messaging: Session Initiation Protocol (SIP) over Transmission Control Protocol (TCP) for voice messaging. These protocols have made it possible to successfully send voice and fax messages over a data network. Real-time VoIP protocols are required to send voice messages over a packet-switched or data network so the delivery order and timing of data packets can be maintained and controlled. If these protocols weren't used to maintain and control the delivery and timing of the data packets, a person's voice would be broken up and sound incoherent or the images might appear garbled. For more information about VoIP protocols used in Unified Messaging, see Understanding Protocols, Ports, and Services in Unified Messaging. For a list of IP PBXs supported for Unified Messaging, see Telephony Advisor for Exchange 2010.

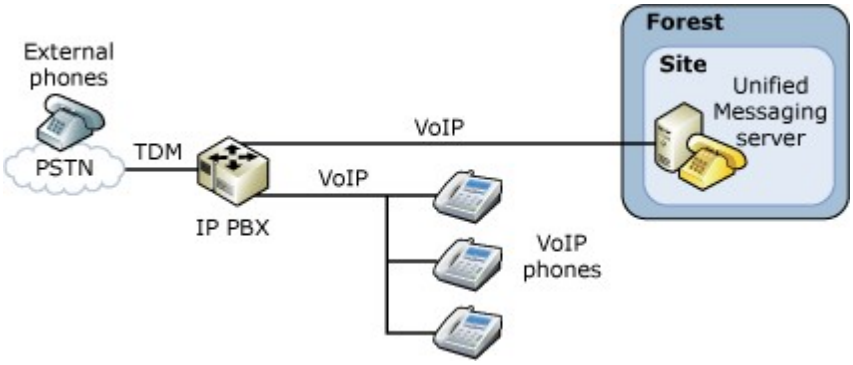
Note:

Unified Messaging supports only SIP over TCP.

Traditional IP PBX Configurations

A standard or traditional IP PBX contains at least a single network interface that connects to a data network using VoIP protocols. It may also contain additional network interfaces or other telephony interfaces that enable it to connect to an existing telephony network such as the PSTN. The connection to the data network allows for communication with other VoIP hosts located on the data network by using IP data packets. These VoIP hosts include other IP PBXs, VoIP-based telephones, IP gateways, and Unified Messaging servers. A traditional IP PBX is doesn't support analog or digital telephones. It supports only VoIP telephones.

The following figure illustrates a typical telephony and data network that includes a traditional IP PBX.



Because the IP PBX can already connect to a data network and can convert the circuit-based protocols from the PSTN to packet-switched VoIP protocols, an IP gateway may not be required to enable communication with UM servers on the data network.

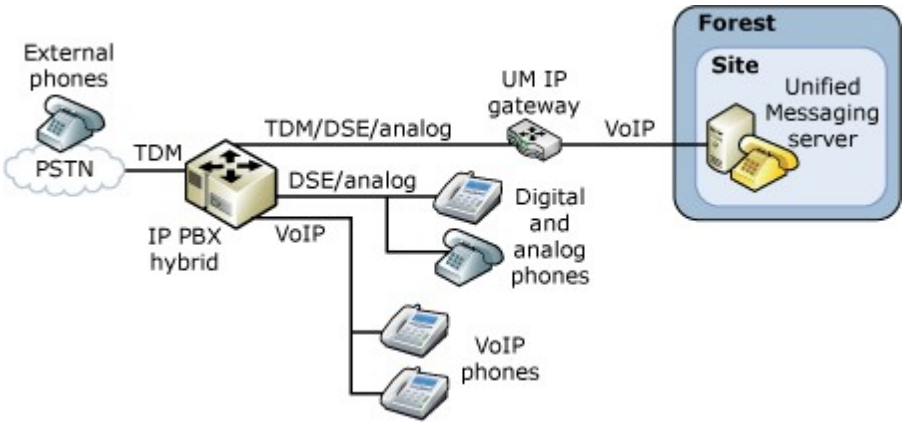
IP PBX Hybrid Configurations

Hybrid IP PBXs can provide analog, digital, and VoIP-based capabilities. If the correct interfaces are installed on an IP PBX and the software that supports multiple types of interfaces is installed correctly, the IP PBX is considered a hybrid IP PBX. An IP PBX hybrid makes it possible to use a mixture of analog, digital, and IP-based telephones.

Most modern IP PBXs can support and provide all three types of voice communication or a traditional IP PBX can be upgraded to a hybrid IP PBX by installing the necessary interfaces and software or firmware updates.

The mixture of analog, digital, and IP-based telephones makes it possible for users in your organization to use many new features and also provides great flexibility in your telephony environment. Using an IP PBX hybrid also allows for a more gradual migration to a completely VoIP-based telephony environment and voice messaging system for your organization.

The following figure illustrates a typical telephony and data network that includes an IP PBX hybrid configuration.



Several factors determine whether an IP gateway will be required when you connect with an UM server. One of these factors is the compatibility of the VoIP protocols used by the IP PBX or hybrid IP PBX and Unified Messaging. If an IP gateway isn't required, it will reduce the complexity of the telephony infrastructure, and the support that you must have for Unified Messaging will be simpler.

Return to top

Calling or Called Party Identification

Calling or called party identification is a telephone company service that can tell the person who is receiving the call the telephone number and sometimes the name of the person who is calling and other information about the call. This information is sent over a serial cable by using call signaling. When a call is received by a PBX or IP PBX from a telephone company, the call includes calling identification information such as the following:

- The calling party's number
- The called party's number
- Status codes such as a ring-no-answer, the state or condition of the line, line busy, and call forward always
- The line or port number that's being used for the call
- In telephony, the signaling information is used to exchange information between endpoints on a network to set up, control, and end calls. Several signaling methods used by IP gateways and IP PBXs are supported by Unified Messaging. The signaling method that's used depends on the type of device that's being used and the type of signaling method that's used by the telephone company. The most important factor is that the device that's connecting to the telephone company and to the IP gateway or IP PBX must support at least one of the signaling methods that enable calling or called party information to be sent and received by callers. For more information about signaling configuration information for a supported IP gateway, see Telephony Advisor for Exchange 2010.

Although other signaling methods can be used, the two most popular signaling methods are as follows:

- **Simplified Message Desk Interface (SMDI)** SMDI is a protocol that's used to provide signaling, call control, and calling identification information from an interface between a telephone system and a voice mail system. It's used to provide the voice mail system with the information it needs to process an

incoming call. Every time an incoming call is sent by using SMDI over a serial interface or RS-232 interface, the information that's sent will identify the line or port, the type of call, and the calling or called party numbers. The SMDI cable connects from a device such as a PBX to a serial connection on the IP gateway. However, SMDI is also used with IP PBXs. The SMDI protocol allows for a maximum of only 10 digits for each calling and called number. This is a limitation of the protocol and can't be changed.

- **In-band** In-band signaling allows for the exchange of signaling, call control, and calling identification information from a telephone company. This information is sent over the same channel and in the same band (300 Hz to 3.4 kHz) as the voice and other sounds that are being made during the call. For example, when a user places a call by using DTMF or touchtone dialing and talks to the called party, both the touchtone and the voice conversation use the same channel and band. In-band signaling is less secure because the control signals are exposed to the user and is a less popular signaling method than SMDI. In-band signaling applies only to Channel Associated Signaling (CAS).

Important:

We recommend that all customers who plan to deploy Unified Messaging obtain the assistance of a UM specialist. A UM specialist will help make sure there's a smooth upgrade to Unified Messaging from a legacy voice mail system. Performing a new deployment or upgrading a legacy voice mail system requires significant PBX and UM knowledge. For more information about how to contact a Unified Messaging specialist, see the Microsoft Exchange Server 2007 Unified Messaging (UM) Specialists Web site.

Return to top

1.9.1.3.16 Understanding Faxing in Unified Messaging

Understanding Faxing in Unified Messaging

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-22*

Microsoft Exchange Server 2010 Unified Messaging (UM) enables voice mail messages to be delivered to a user's Exchange 2010 mailbox and also lets users receive fax messages in their Exchange 2010 mailbox. In Exchange 2010 Unified Messaging, a fax message is sent to the user's mailbox as an e-mail message that has an image file with a .tif extension attached. The user can open the attached file using a software application that can open and view image files that have a .tif extension. This topic discusses faxing and how it works in Exchange 2010 Unified Messaging.

Note:

Although Unified Messaging doesn't let users send outgoing faxes, many third-party solutions, such as an Internet fax service, e-mail faxing service, or a third-party fax server application, can be used to send outgoing faxes.

Contents

Overview of Faxing

Fax is an abbreviation for the word facsimile. It's a technology that's used to electronically transfer documents. Generally, faxes are sent and received by fax machines or computer fax/modems by using the Public Switched Telephone Network (PSTN), which is a telephony or circuit-based network. However, there are other faxing options that can be used to send and receive faxes.

Most organizations today want their users to be able to send and receive faxes. Organizations use one or more of the methods described in the following list to send or receive faxes over the PSTN or over the Internet. There are advantages and disadvantages to each of these methods.

- Traditional fax machines and computer-based faxing
- Faxing by using fax servers or gateways
- Faxing by using a Voice over IP (VoIP) network
- Faxing by using an e-mail client application

To send a fax message, users in an organization may have to do the following:

- Print a hard copy of the document to be faxed and use a physical fax machine to send it.
- Save the document on their computer and use a fax modem to send the fax.
- Use an Internet fax service that lets them fax a document from a software application.
- Send an outgoing fax to a fax server by using a software application that's configured to use the fax server.

To receive a fax, users in an organization may have to do the following:

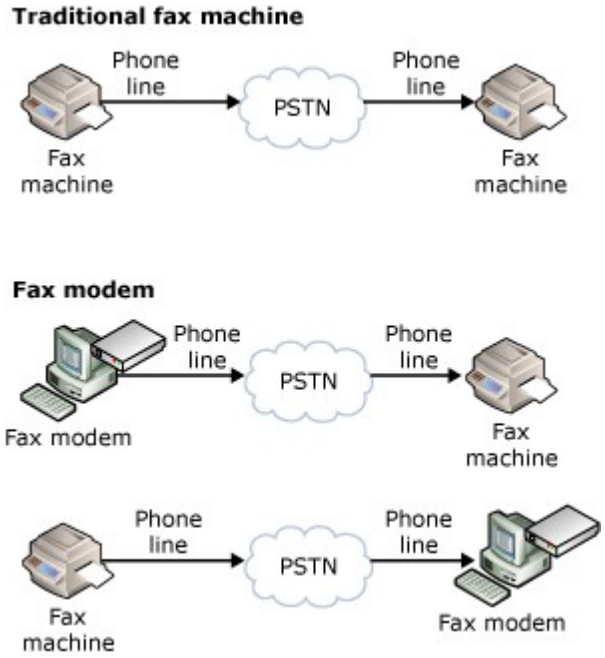
- Receive a fax on a physical fax machine within the organization.
- Receive a fax by using a fax modem that's installed on their computer.
- Receive a fax from an Internet faxing service.
- Receive a fax from a fax server that's configured on a network.
- Receive a fax from a Unified Messaging server on a VoIP network.

Faxing Methods

There are several options for sending and receiving faxes, including the following:

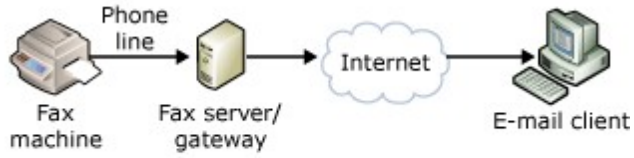
Traditional fax machines and computer-based faxing Scanners, a fax modem in a computer, a printer with built-in faxing capabilities, or a dedicated fax machine can be used to send and receive faxes. All of these can be used to transmit data in the form of pulses by using a telephone line to another fax device, usually another fax machine or computer that has a fax modem. The pulses are then transformed into images or used to print the image on paper.

The traditional fax method requires at least a single telephone line on the sending and receiving device, and only one fax can be sent or received at a time. A disadvantage of sending and receiving faxes by using a fax modem is that the computer must be turned on and running fax software or a fax service. This kind of computer-based faxing doesn't use the Internet to send or receive faxes. The following figure shows how traditional and computer-based faxing are used to send and receive faxes.

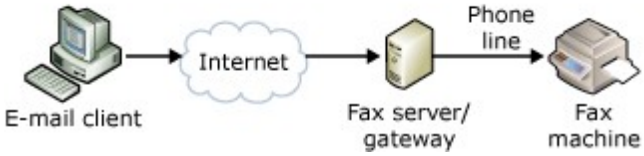


Fax servers or gateways and Internet fax services There are several ways to send and receive faxes over the Internet. These include using a software application on a computer or using an e-mail client to receive faxes. In most cases, this kind of faxing involves using a fax server or fax gateway to convert between faxes and e-mail. This has become increasingly popular because it enables organizations to remove or avoid purchasing additional fax machines. It also eliminates the need to install additional telephone lines. This kind of faxing involves creating a document, including a fax cover page with the correct identifying information, and then sending the document to a traditional fax machine. For example, the user uses a software application such as Microsoft Office Word or Outlook to create and send the fax to the fax server or gateway. The fax server or gateway receives the fax and then sends it by using a traditional telephone line to a fax machine or fax modem that's installed on a computer. The following figure shows how fax servers, gateways, and Internet fax services can be used to send and receive faxes.

Fax Receiving



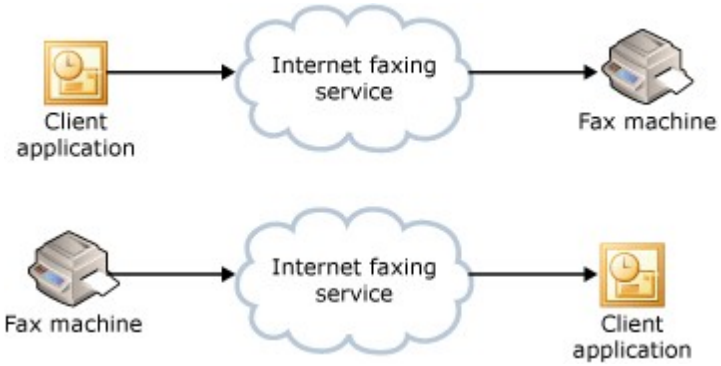
Sending a fax



Internet fax services let a user send faxes from a computer by using the Internet. A software application such as Word or Outlook can be used to create and send the fax to an Internet fax service. There are many companies that offer Internet faxing services on a subscription basis or by charging for each fax message that's sent. Internet fax services offer the following advantages:

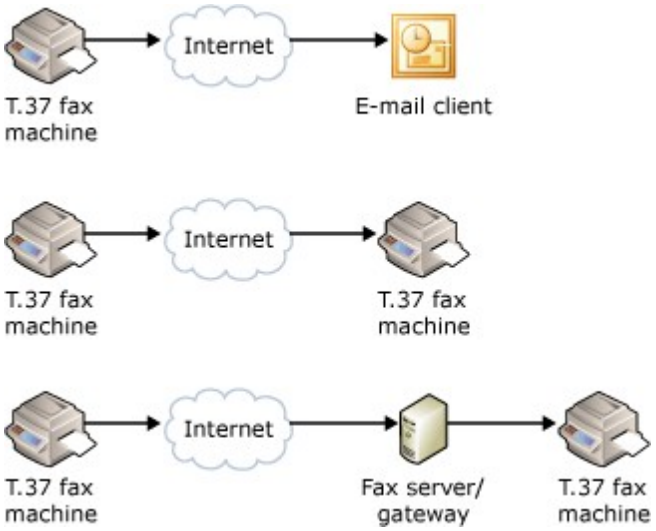
- No fax machine is required.
- No software or hardware must be installed.
- No dedicated telephone lines are required.
- Confidentiality.
- Multiple faxes can be sent at the same time.
- Faxes can be received when the computer is shut off.

The following figure shows how Internet fax services can be used to send and receive faxes.



Faxing by using an e-mail client application Faxes can be sent and received by a fax machine over the Internet and then received by an e-mail client such as Outlook.

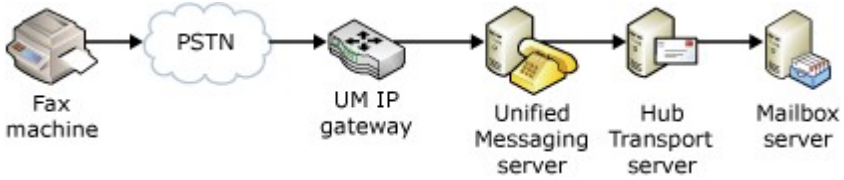
The T.37 protocol was designed to enable a fax machine to send fax messages over the Internet to an e-mail client. The faxes are sent over the Internet as an e-mail attachment, typically as .tif or .pdf files. In this kind of faxing, a fax machine that supports iFax or T.37 is required, in addition to an e-mail address for the sending and receiving fax machines. To work with existing traditional fax machines and fax modems, all T.37 fax machines support standard faxing by using a telephone line. However, in some cases, T.37 fax machines can be used when a fax gateway is also being used. The following figure shows how T.37-based fax machines and e-mail clients can be used to send and receive faxes.



Faxing by using a VoIP network VoIP is a technology that contains hardware and software that enables people to use an IP-based network as the transmission medium for telephone calls. On a VoIP network, voice and fax data is sent in packets by using IP instead of traditional circuit transmissions or the circuit-switched telephone lines of the PSTN. An IP gateway that you connect to your IP network uses VoIP to send voice data packets between an Exchange 2010 Unified Messaging server and a Private Branch eXchange (PBX) system. Or, you can use an IP PBX to perform the functions of both an IP gateway and a PBX.

There are two basic types of networks: circuit-switched and packet-switched. A circuit-switched network is a network in which there exists a dedicated connection. A dedicated connection is a circuit or channel that's set up between two nodes so that they can communicate. After a call is established between two nodes, the connection may be used only by these two nodes. When the call is ended by one of the nodes, the connection is canceled. In circuit-switched networks, such as the PSTN, multiple calls are transmitted across the same transmission medium. Frequently, the medium that's used in the PSTN is copper. However, fiber optic cable might also be used.

In packet-switched networks such as the Internet or a local area network (LAN), packets are routed to their destination through the most expedient route, but not all packets traveling between two hosts travel the same route, even those from a single message. This almost guarantees that the packets will arrive at different times and out of order. In a packet-switched network, packets (messages or fragments of messages) are individually routed between nodes over data links that may be shared by other nodes. With packet switching, unlike circuit switching, multiple connections to nodes on the network share the available bandwidth. Packet-switched networking has made it possible for the Internet to exist and, at the same time, has made data networks—especially LAN-based IP and VoIP networks—more available and widespread. The following figure shows how a VoIP network and Exchange Unified Messaging can be used to deliver faxes.



T.38

T.38 is a faxing standard and protocol that enables faxing over an IP-based network. An

IP-based network that uses the T.38 protocol uses Simple Mail Transfer Protocol (SMTP) and MIME to send the message to a recipient's mailbox. T.38 allows for IP fax transmissions for IP-enabled fax devices and fax gateways. The devices can include IP network-based hosts such as client computers and printers. In Exchange 2010 Unified Messaging, the fax images are separate documents encoded as .tif files and attached to an e-mail message. Both the e-mail message and the .tif file attachment are sent to the recipient's Exchange 2010 UM-enabled mailbox.

Exchange 2010 Unified Messaging relies on the gateway's abilities to translate or convert Time Division Multiplex (TDM) or telephony circuit-switched based protocols like Integrated Services Digital Network (ISDN) and QSIG from a PBX to IP-based or VoIP-based protocols like Session Initiation Protocol (SIP), Real-Time Transport Protocol (RTP), or T.38 for receiving fax messages. The IP gateway is integral to the functionality and operation of Unified Messaging. The IP gateway is responsible for sensing fax tones. Unified Messaging servers rely on the IP gateway to send a notification that a fax has been detected. Then the Unified Messaging server will renegotiate the media session and use the T.38 protocol.

Return to top

Overview of Faxing with Exchange 2010 Unified Messaging

In Exchange 2010 Unified Messaging, the user receives the fax images as separate documents encoded as .tif image files that are attached to an e-mail message. Both the e-mail message and the .tif attachment are sent to the recipient's Exchange 2010 UM-enabled mailbox.

There are several advantages to sending a fax message to the user's mailbox. These advantages include the following:

- You can reduce the number of physical or traditional fax machines.
- The number of telephone lines used for faxing in an organization can be reduced, because the Unified Messaging server can queue many faxes and send each fax when one of the telephone lines becomes available.
- Faxes that are received as a .tif image file are better quality than a traditional fax. Incoming faxes can be printed by a local or shared printer.
- Faxes sent to the user's mailbox are more secure because they're less likely than hard copy faxes to be picked up by someone other than the recipient.
- Users can receive faxes without leaving their desk.
- Fax messages that are received can be monitored to make sure that they comply with an organization's security policies.

A single fax message can be sent only to a single UM-enabled user. Exchange 2010 Unified Messaging can't forward fax messages to a distribution list. If you need to have this functionality, you must follow these steps:

1. Create a mailbox to answer the fax call. This will be the mailbox for the distribution list.
2. UM-enable the distribution list mailbox.
3. Create a rule for this UM-enabled mailbox. The rule will be configured to forward all messages to the selected distribution list.

Note:

If you’re using the RTM version of Exchange 2010 Unified Messaging, you may have to enable inband fax tone detection for fax receiving to work correctly with some IP PBXs. You do this by changing the *EnableInbandFaxDetection* setting to True in the msexchangeum.config file. The msexchangeum.config file is located in the \Program Files\Microsoft \Exchange\V14\bin folder on an Exchange 2010 Unified Messaging server. If

you don't configure this setting, Unified Messaging servers must rely on IP gateways to perform inband fax tone detection.
Changing the *EnableInbandFaxDetection* setting to True in the msexchangeum.config file isn't required in Exchange 2010 Service Pack 1 (SP1). Enabling fax tone detection isn't necessary on a Unified Messaging server with Exchange 2010 SP1 installed because the Unified Communications Managed API v. 2.0 (UCMA) enables the Unified Messaging server to listen to both inband and out-of-band fax events.

Return to top

Receiving Incoming Faxes

Receiving a fax on a VoIP network differs from receiving a fax on a standard fax machine or by using a fax server that's located on an IP-based network. To enable faxes to be sent and received over a VoIP network, you must have an IP gateway or an IP PBX that supports the T.38 protocol and a server that also supports T.38. T.38 allows for IP-based fax transmissions for IP network-based hosts, for example, client computers, printers with built-in faxing capabilities, and servers such as a Unified Messaging server.

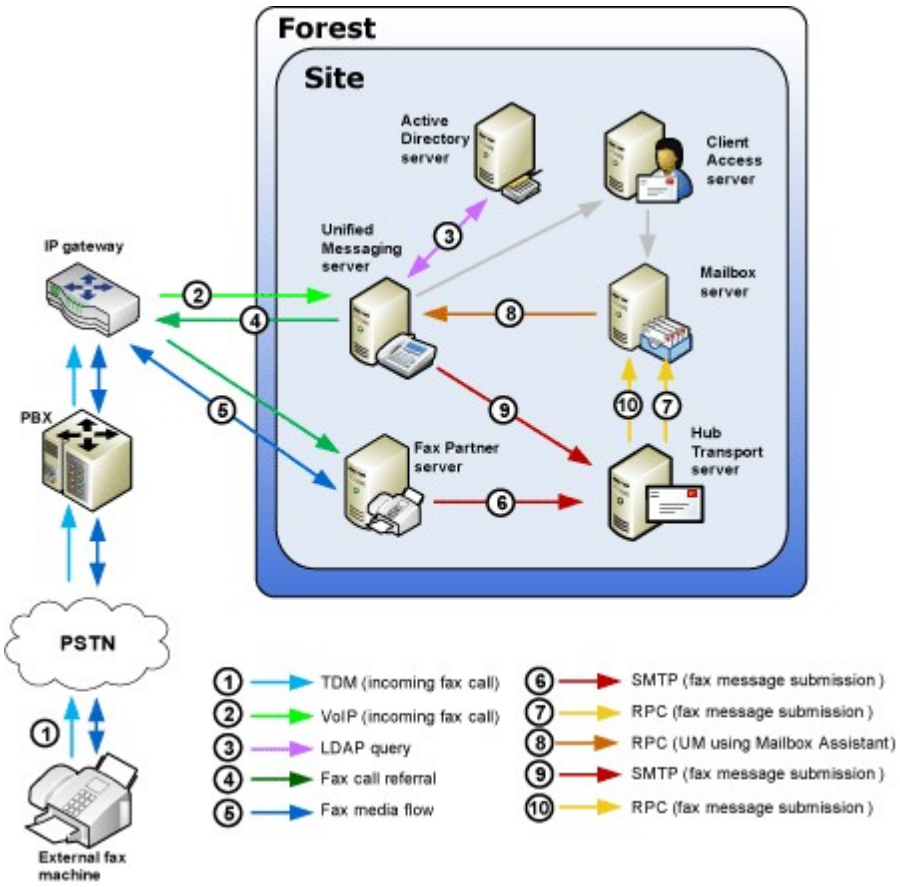
Important:

Sending and receiving faxes using T.38 or G.711 isn't supported in an environment where Unified Messaging and Microsoft Office Communications Server 2007 are integrated.

When a call is received into a PBX, the PBX forwards the call to the appropriate extension. If a ring-no-answer occurs at the user's extension number, the PBX forwards the call to an IP gateway, and the IP gateway forwards the fax call to the appropriate Unified Messaging server. When the call is received by the Unified Messaging server, the Unified Messaging server must decide whether it's a voice call or a fax call. When the SIP protocol is used, the Unified Messaging server processes the call as a voice message. However, if the T.38 protocol is used from the IP gateway, the Unified Messaging server recognizes that the call is for a fax and processes the call. Exchange 2010 Unified Messaging forwards incoming fax calls to a dedicated fax partner server, which then establishes the fax call with the fax sender and receives the fax on behalf of the UM-enabled user. The fax partner's server then sends the fax included as a .tif attachment in the SMTP message to the recipient's mailbox.

When an incoming T.38 fax signal is sent from the IP gateway to the Exchange 2010 UM server, the UM server queries Active Directory using LDAP to determine if the intended recipient of the incoming fax call is allowed to receive incoming fax messages and to determine the SIP address of the fax partner server. After these have been checked, the UM server sends a fax call referral request to the IP gateway or SIP peer, which then forwards the fax request on to the fax partner server. After the fax call has been successfully established, the fax sender sends the fax media and data to a fax partner server. After the fax media and data has been received by the fax partner server, the fax partner server sends an e-mail message to a Hub Transport server using SMTP that contains a .tif image of the fax message and special X-headers to the intended fax recipient.

After the fax message is authenticated and is sent from a valid fax partner server, the UM mailbox assistant on the Mailbox server issues an RPC call to the UM server. By doing this, the UM server ensures that the fax message properties match those of fax messages that are created by an Exchange 2010 Unified Messaging server. Finally, the UM server again submits the final fax message, which includes the e-mail message and .tif attachment for the incoming fax, to a Hub Transport server. Then, using MAPI RPC, the completed and formatted version of the fax message is delivered to the intended recipient. The following figure shows the steps that are involved when an incoming fax is received.



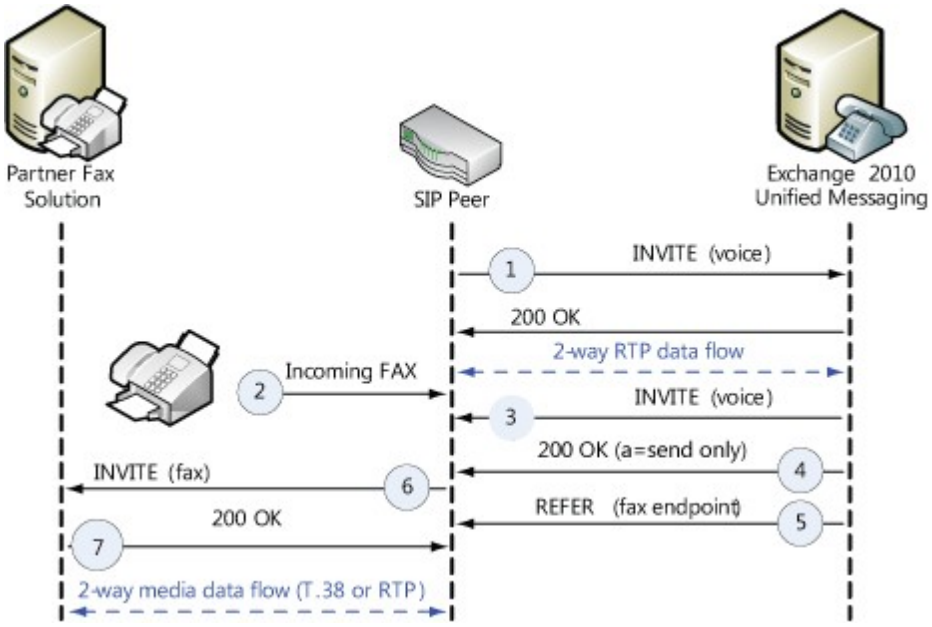
Return to top

Fax Call Referral Methods

An incoming fax call can be signaled to Exchange 2010 UM through either SIP re-INVITE from the IP gateway or SIP peer (media gateway), CNG notification by the SIP peer, or CNG detection by the UM server. The following subsections detail the fax call referral in each case.

Re-INVITE from a SIP Peer

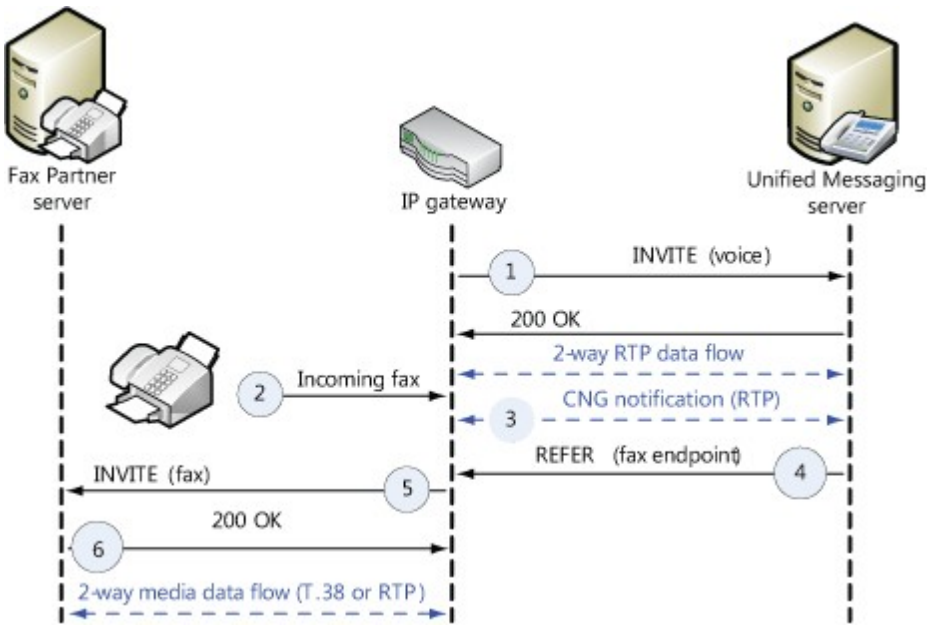
The call flow in this scenario proceeds as shown in the following figure.



An incoming call to a UM pilot number is directed to UM as an INVITE with a voice (RTP/ audio) SDP profile (1). UM accepts the invitation and media streams are established. After the call has been established, fax transmission is initiated by the caller (2). The SIP peer detects the calling fax tone (CNG). The SIP peer issues a re-INVITE to the UM server, this time specifying a fax (T.38 or G.711) profile in the SDP (3). UM responds to the invitation with a 200 OK that places the SIP peer "on hold" (4). UM issues a REFER, referring the SIP (CNG) peer to a fax partner solution end point, obtained from its configuration data (5). The SIP peer sends the fax session INVITE to the fax partner solution (6). The fax partner solution accepts the invitation, and a media session is established with the SIP peer.

CNG Notification by a SIP Peer

The call flow in this scenario proceeds as shown in the following figure.

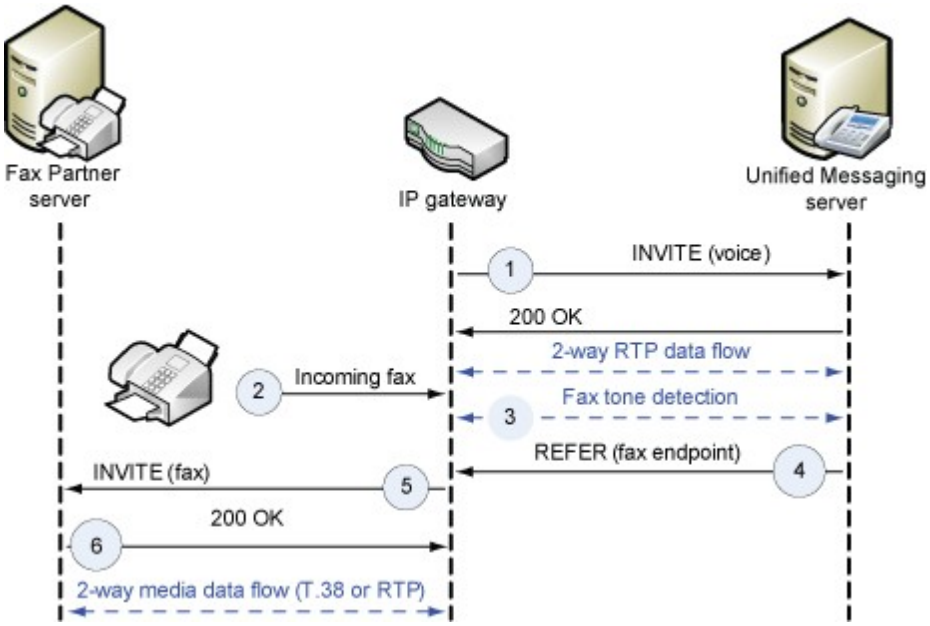


An incoming call to a UM pilot number is directed to UM as an INVITE with a voice (RTP/

audio) SDP profile (1). UM accepts the invitation and media streams are established. After the call has been established, fax transmission is initiated by the caller (2). The SIP peer detects the calling fax tone (CNG).The SIP peer notifies the UM server of the fax by sending a CNG notification in the RTP stream, compliant with RFC 4733 (3). UM responds to the notification by immediately issuing a REFER, therefore referring the SIP peer to a fax partner solution end point, obtained from its configuration data (4). The SIP Peer sends the fax session INVITE to the Fax Partner Solution (5). The fax partner solution accepts the invitation (6), and a media session is established with the SIP peer.

CNG Detection by a UM Server

The call flow in this scenario proceeds as shown in the following figure.



An incoming call to a UM pilot number is directed to UM as an INVITE with a voice (RTP/ audio) SDP profile. UM accepts the invitation and media streams are established (1). After the call has been established, fax transmission is initiated by the caller (2). The UM server detects the fax tone (CNG) in the RTP audio stream (3). UM responds to the notification by immediately issuing a REFER and therefore referring the SIP peer to a fax partner solution end point, obtained from its configuration data (4). The SIP peer sends the fax session INVITE to the fax partner solution (5). The fax partner solution accepts the invitation (6), and a media session is established with the SIP peer.

Return to top

Configuring Faxing

By default, when you install the Unified Messaging server role, the server isn't configured to allow incoming fax calls to be processed or delivered to a UM-enabled user. To configure Exchange 2010 UM with a fax partner server, you must configure the UM mailbox policy and configure authentication between the UM server and the fax partner server. For more information, see Deploy and Configure Incoming Faxing.

Telephone Numbers and Faxing

Exchange 2010 Unified Messaging offers the following options when you're configuring

UM-enabled users to receive fax messages:

- A Direct Inward Dial (DID) telephone number that's used with voice mail.
- A separate DID telephone number that's used for receiving faxes.
- A central fax telephone number that will receive all faxes.

A Single DID Telephone Number

When you enable a user for Unified Messaging by using the Enable Unified Messaging wizard or the **Enable-UMMailbox** cmdlet, you must specify at least a single extension number for the user. This extension number is enabled on a per-user basis and must be unique within a given dial plan. The extension is used by Unified Messaging to locate the correct user in Active Directory and to deliver voice and fax messages to the user's Exchange 2010 mailbox. For more information, see Enable-UMMailbox.

In this scenario, the user will use a single DID number for voice and fax. This configuration is easy to administer and doesn't waste additional DID numbers. If the user is away or on the phone when a fax call arrives, UM answers the call, detects the fax tone, creates the fax message, and sends it to the user.

However, in this scenario, the user may receive calls from fax machines. The user can:

- Not answer the telephone when it rings so that the fax call will be forwarded and answered by a Unified Messaging server and the fax message will be created and forwarded to the user's mailbox.
- Answer the fax call, and then transfer it to himself or herself so that the call will be forwarded and answered by a Unified Messaging server and the fax message will be created and forwarded to the user's mailbox.
- Wait for the caller to retry sending the fax and let the fax call be transferred to a Unified Messaging server.

In summary, using a single DID number requires the user to perform additional actions to be able to receive fax messages.

Return to top

Multiple DID Telephone Numbers

When you enable a user for Unified Messaging, you must enter at least a single extension number for that user. However, you can also add multiple extension numbers for a UM-enabled user by using the *SecondaryAddress* parameter with the **Set-Mailbox** cmdlet. For more information, see Set-UMMailbox.

Important:

In Exchange 2007 SP1, you can use the **Set-Mailbox** cmdlet or the Exchange Management Console to add multiple extension numbers. For more information, see Modify an Extension Number for a UM-Enabled User.

Adding multiple extension numbers is useful when a UM-enabled user:

- Receives many faxes
- Doesn't want to be bothered with answering the phone to receive a fax
- Doesn't want to hear a fax tone when they answer their phone

Adding multiple extensions is more complex than using a single extension and may require additional configuration settings on a PBX. To configure multiple extension numbers for a UM-enabled user, you must have DID extension numbers that are available but aren't being used in your organization. Therefore, it isn't a good idea to use multiple numbers for a UM-enabled user if your organization has a limited number of available DID extension numbers.

The benefit of using multiple DID telephone numbers is that the UM-enabled user receives voice calls on one DID extension number and fax calls on the other DID extension number. Although, this may be more complex and requires additional configuration steps, using

separate DID numbers for voice mail and fax calls is easier for the user.

If you configure two DID extension numbers for a specific user, the DID extension numbers can come from separate UM dial plans. In this scenario, you can create a dial plan, add Unified Messaging servers to the dial plan, and use a Unified Messaging server as a dedicated server that will receive fax calls and forward fax messages to the users. For more information, see Create a UM Dial Plan.

You have the following options for configuring multiple DID extension numbers for UM-enabled users:

- **Multiple DID numbers (one for fax without Unified Messaging and one for voice)** This type of configuration is enabled on a per-user basis and is used when you have extra or unused DID extension numbers available. One DID extension number is published as the user's voice mail number and the other DID extension number is published as the user's fax number. In this scenario, voice calls that are answered by a ring-no-answer or busy signal are forwarded to a Unified Messaging server, and a voice message is created and sent to the UM-enabled user's mailbox. The other extension number can be connected to a fax machine or to another computer that has a fax modem. Although this configuration is possible, it doesn't require that Unified Messaging servers process the fax calls, and fax messages won't be sent to the UM-enabled user's mailbox.
- **Multiple DID numbers (one for fax and one for voice)** This type of configuration is enabled on a per-user basis and can be used when your organization has many DID extension numbers available. In this scenario, both DID extension numbers that are answered by a ring-no-answer or a busy signal are forwarded to a Unified Messaging server that will create a voice or fax message depending on the DID extension number that's called. Although the user will publish one number for voice and one for fax, the Unified Messaging server detects the type of call that's being received on the DID extension number and can create a voice or fax message from calls to either of the DID extension numbers. This is very useful when a user doesn't have a separate fax machine or dedicated computer that has a fax modem to answer incoming fax calls.
- **Two DID numbers (one "phantom" extension for fax and one for voice)** This type of configuration is enabled on a per-user basis. It's basically the same as the configuration that uses two DID numbers (one for fax and one for voice). However, in this configuration, the number that's published for fax calls for the UM-enabled user is configured on the PBX as a "phantom" extension. Incoming calls that are received on this "phantom" DID extension number are always forwarded to a Unified Messaging server.
  The advantage of this kind of configuration is that incoming fax calls are answered by a Unified Messaging server. When a ring-no-answer occurs, a fax is created and forwarded by the Unified Messaging server to the UM-enabled user's mailbox without disturbing the user. This happens because no telephone or fax device is positioned close to the user, and the user doesn't hear the ring of an incoming call.
  The disadvantages of this kind of configuration are that you must have additional DID extensions available and you must configure the PBX to forward the call to a Unified Messaging server.

Central Fax Telephone Number

When you enable a user for Unified Messaging by using the Enable Unified Messaging wizard or the **Enable-UMMailbox** cmdlet, you must specify at least a single extension number for the user. This kind of fax configuration is defined on each Unified Messaging dial plan.

In some organizations, especially those that receive many faxes each day, you might have to publish one fax number for the whole organization. This fax number would be

used by all callers when they submit faxes to users in the organization. This kind of configuration is useful in the following situations:

- A user within the organization receives too many faxes in their mailbox to manage them effectively.
- A user receives too many spam faxes in their mailbox.
- Business logic is too complex to warrant creating a transport rule. This might be the case if your organization requires that you route certain faxes to one group and other faxes to another group. For more information, see the following topics:
  - Understanding Transport Rules
  - Understanding How Transport Rules Are Applied
- Filtering fax messages by using Outlook isn't effective.

Publishing one fax number for the whole organization enables your organization to control the types of faxes that are received by users. The advantage of this configuration is that it requires only a single DID extension number or an external telephone number. Also, it doesn't require a separate DID number for faxing for each UM-enabled user. However, it does require a "fax secretary" or other person to distribute the incoming faxes to users within the organization based on information that's included on the fax cover page or in the fax message itself.

Note:

Using a central fax number with optical character recognition (OCR) is not available in Exchange 2010 Unified Messaging. This kind of configuration can use a central fax number. However, instead of having to be routed to the recipient by a person, the faxing software receives the fax, performs OCR, and then tries to locate the recipient based on the information on the cover page or fax message.

Journaling UM Fax Messages

Many organizations that implement journaling may also use Unified Messaging to consolidate their e-mail, voice mail, and fax infrastructure. However, you may not want the journaling process to generate journal reports for messages that are generated by Unified Messaging. In this case, you can decide whether to journal voice mail messages and missed call notification messages that are handled by an Exchange 2010 Unified Messaging server or to skip such messages. If your organization doesn't require journaling of such messages, you can reduce the hard disk space that's required to store journal reports by skipping such messages. When you enable or disable the journaling of voice mail messages and missed call notification messages, your change is applied to all Hub Transport servers in your organization. For more information, see Understanding Journaling.

Note:

Messages that contain faxes that are generated by a Unified Messaging server are always journaled, even if you configure a journal rule that specifies not to journal Unified Messaging voice mail and missed call notification messages.

Return to top

1.9.1.3.17 Understanding Quality of Service (QoS) in Unified Messaging

Understanding Quality of Service (QoS) in Unified Messaging

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-20*

Microsoft Exchange Server 2010 Unified Messaging (UM) supports DiffServ through Differentiated Services Code Point (DSCP) marking.

In Windows Server 2008, TCP/IP performs DiffServ marking when you've installed the Quality of Service (QoS) Packet Scheduler. When you install the Unified Messaging server role on a computer that's running Windows Server 2008 with the QoS Packet Scheduler installed, all outgoing Unified Messaging packets will be marked with a DSCP value that's configured. However, you can change this value for the packets by using Registry Editor or by modifying the Group Policy. For more information about DSCP marking, see Differentiated Services Code Point (DSCP) overview. By default, the QoS Packet Scheduler is installed on Windows Server 2008.

The Microsoft Exchange Unified Messaging service doesn't perform any classification of network packets. However, the media platform that's included with Unified Messaging instructs the Microsoft Windows networking stack that all audio packets are to be marked as *Guaranteed Service*. The operating system will then use Group Policy settings to determine how the data packets should be marked and then mark the TOS field of the IP header. For more information about QoS in Windows, see How QoS Works.

Note:

The media stack QoS marking is performed on UDP traffic only because TCP traffic has its own flow control.

You can enter IP addresses and IP address ranges in the Internet Protocol Version 4 (IPv4) format, Internet Protocol Version 6 (IPv6) format, or both formats. However, when you install the Unified Messaging server role on Windows Server 2008, you must have the IPv4 protocol stack enabled with or without having the IPv6 protocol stack enabled. This is because there are limitations with the telephony and speech components that are required and used by Unified Messaging.

Note:

Layer 3 network devices, such as routers, must also support DiffServ.

1.9.1.3.18 Understanding Unified Messaging Subscriber Access

Understanding Unified Messaging Subscriber Access

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

When you're deploying Microsoft Exchange Server 2010 Unified Messaging (UM), you must understand subscriber access and the features included with Exchange 2010 that depend on subscriber access. This topic describes subscriber access and how it's used in Exchange 2010 Unified Messaging to let subscribers, also known as UM-enabled users, access their Exchange 2010 mailbox.

Subscriber Access

A subscriber is an internal business user or network user who's enabled for Exchange 2010 Unified Messaging. Subscriber access is used by users to access their individual

mailboxes to retrieve e-mail, voice messages, contacts, and calendaring information. Outlook Voice Access is an Exchange 2010 Unified Messaging feature that lets subscribers access their Exchange 2010 mailbox.

When you enable subscriber access for Exchange 2010 UM-enabled users, you must install the Exchange 2010 Unified Messaging server role on the computer that's running Exchange 2010 and verify that at least one of each of the following have been created:

- A UM dial plan
- A UM mailbox policy
- A UM IP gateway
- A UM hunt group

When you configure subscriber access, you configure the UM dial plan to have a subscriber access number. The telephone number or number that's configured on the UM dial plan is the telephone number that subscribers will use to access their Exchange 2010 mailboxes over the telephone using Outlook Voice Access. The subscriber access feature included with Exchange 2010 Unified Messaging resembles other unified messaging solutions. However, Exchange 2010 offers more advanced features than other unified messaging solutions. For more information about how to create or modify UM dial plans and enable subscriber access, see Create a UM Dial Plan

Note:
A UM dial plan must contain at least one subscriber access number, but can contain multiple subscriber access numbers.

For more information about how to enable a user for Unified Messaging, see Enable a User for Unified Messaging.

Return to top

Outlook Voice Access

There are two Exchange 2010 Unified Messaging user interfaces available to subscribers: the Telephone User Interface (TUI) and the Voice User Interface (VUI). These two interfaces together are called Outlook Voice Access. Outlook Voice Access can be used when subscribers access the Unified Messaging system from an external or internal telephone to access their individual mailbox, including their personal e-mail, voice messages, contacts, and calendaring information in their Exchange 2010 mailbox.

If you want to prevent users from receiving voice mail but want to allow them access to their Exchange 2010 mailbox using Outlook Voice Access, you can enable users for Unified Messaging and configure the users' mailbox with an extension number that isn't currently being used by another user in the organization.

Important:
For the VUI or Automatic Speech Recognition (ASR) to be used for subscriber access, it must be enabled on the UM dial plan to enable the VUI functionality as described in the earlier scenarios.

For a copy of the Microsoft Exchange 2010 Unified Messaging Outlook Voice Access Quick Start Guide, see the Microsoft Download Center.

The following scenarios demonstrate how Outlook Voice Access can be used for subscriber access from a telephone:

- **Access e-mail** An Outlook Voice Access user places a call to the subscriber access number from a telephone and wants to access voice mail. The voice prompt says, "Welcome. You're connected to Microsoft Exchange. To access your mailbox, please enter your extension. To contact someone, press the # key." After the user enters a mailbox extension number, the voice prompt

says, "Please enter your PIN and press the # key." After the user enters a PIN, the voice prompt says, "You have 2 new voice mails, 10 new e-mail messages, and your next meeting is at 10:00 A.M. Please say voice mail, e-mail, calendar, personal contacts, directory, or personal options." When the user says "E-mail," Unified Messaging reads the message header and then the name, subject, time, and priority for the messages that are in the subscriber's mailbox.

- **Access calendar** An Outlook Voice Access user places a call to the subscriber access number from a telephone and wants to access voice mail. The voice prompt says, "Welcome. You're connected to Microsoft Exchange. To access your mailbox, please enter your extension. To contact someone, press the # key." After the user enters a mailbox extension, the voice prompt says, "Please enter your PIN and press the # key." After the user enters a PIN, the voice prompt says, "You have 2 new voice mails, 10 new e-mail messages, and your next meeting is at 10:00 A.M. Please say voice mail, e-mail, calendar, personal contacts, directory, or personal options." When the user says "Calendar," Unified Messaging says, "Sure, and which day should I open?" The user says, "Today's calendar." Unified Messaging responds by saying, "Opening today's calendar." Unified Messaging reads each of the calendar appointments for that day for the user.

  Note:
  If a Unified Messaging server encounters a corrupted calendar item in a user's mailbox, it will fail to read the item, but will return the caller to the Outlook Voice Access main menu and will skip reading any additional meetings that may be scheduled for the rest of the day.

- **Access voice mail** An Outlook Voice Access user places a call to the subscriber access number from a telephone and wants to access voice mail. The voice prompt says, "Welcome. You're connected to Microsoft Exchange. To access your mailbox, please enter your extension. To contact someone, press the # key." After the user enters a mailbox extension number, the voice prompt says, "Please enter your PIN and press the # key." After the user enters a PIN, the voice prompt says, "You have 2 new voice mails, 10 new e-mail messages, and your next meeting is at 10:00 A.M. Please say voice mail, e-mail, calendar, personal contacts, directory, or personal options." The user says "Voice mail" and Unified Messaging reads the message header and then the name, subject, time, and priority for the voice messages that are in the user's mailbox.

  Note:
  If speech recognition is enabled, users can access their UM-enabled mailbox using speech input. However, subscribers can also use touchtone, also known as dual tone multi-frequency (DTMF), by pressing 0. Speech recognition is not enabled for PIN input.

- **Locate an e-mail alias** An Outlook Voice Access user places a call to the subscriber access number from a telephone and wants to locate a person in the directory by spelling the e-mail alias. The voice prompt says, "Welcome. You're connected to Microsoft Exchange. To contact someone, press the # key." The user presses the # key, and then spells the name of the person using DTMF or touchtone inputs.

  Note:
  The directory search feature with subscriber access is not speech-enabled. Users will be able to spell the name of the person who they want to contact only using DTMF inputs.

  Important:
  In some companies (especially in East Asia), office telephones may not have letters on the keys of the telephone. This makes the spell-the-name feature that uses the DTMF interface almost impossible to use, without a working

knowledge of the key mappings. By default, Exchange 2010 Unified Messaging uses the E.161 key mapping. For example, 2=ABC, 3=DEF, 4=GHI, 5=JKL, 6=MNO, 7=PQRS, 8=TUV, 9=WXYZ.
When inputting a combination of letters and numbers, for example, Mike1092, the numeric digits are mapped to themselves. For an e-mail alias of Mike1092 to be entered correctly, the user must press the numbers 64531092. Also, for characters other than A-Z and 0-9, there won't be a telephone key equivalent. Therefore, these characters shouldn't be entered. For example, the e-mail alias mike.wilson would be entered as 6453945766. Even though there are 11 characters to be input, only 10 digits are entered by the user because the period (.) does not have a digit equivalent.

Important:
If you need to access the e-mail message after you delete it using Outlook Voice Access, you can use Outlook Web App or Outlook to move the e-mail message back into the appropriate folder from the Deleted Items folder. You can't use Outlook Voice Access to access the Deleted Items folder.

Return to top

1.9.1.3.19 Understanding Protected Voice Mail

Understanding Protected Voice Mail

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-09-24*

Some legacy PBX telephony systems allow the caller to mark a voice mail message as private, blocking the intended recipient of the message from forwarding it to others when they listen to the message. In integrated voice mail systems, a voice message can be accessed in multiple ways, which makes it more of a challenge to prevent voice messages marked private from being exposed to unintended listeners.

Unified Messaging (UM) in Exchange Server 2010 can be configured to use Active Directory Rights Management Services (AD RMS) to protect voice messages for an organization. This feature is known as Protected Voice Mail.

When a voice message is protected, the recipient is not only blocked from forwarding the message, but UM also assures that only the intended recipient or recipients of the message can access its content. Protected voice messages can be accessed by using Microsoft Office Outlook 2010, Office Outlook Web App, and Exchange Server 2010 Outlook Voice Access.

Contents

UM Mailbox Policies

SMS Notifications and Protected Voice Mail

Overview of Protected Voice Mail

The Protected Voice Mail feature is available with Exchange 2010 Unified Messaging (UM). It can be configured on a UM mailbox policy, and all Protected Voice Mail settings can be configured using the Exchange Management Console (EMC) or cmdlets in the Exchange Management Shell.

Note:
In a deployment where both Exchange 2010 servers and Microsoft Exchange Server 2007 servers exist, Voice Mail Preview isn't available to UM-enabled users who have an Exchange 2007 mailbox.

Protected Voice Mail is implemented by applying Information Rights Management (IRM) to voice messages. When voice messages are protected by UM:

- Users can reply to protected voice messages.
- Recipients of a voice message can't forward it.
- Users can't save a copy of the voice message.
- Users can't save or copy the attached audio of the voice message.
- A voice mail message can be opened only by the intended recipient or recipients.

Both call answering voice mail messages and interpersonal voice messages (voice messages that are sent to a user using Outlook Voice Access) can be protected by UM. However, protection won't be applied to the following types of messages:

- Fax messages.
- Non-voice messages. For example, e-mail messages or meeting requests, even when they're created using Outlook Voice Access (voice replies).

Overview of Active Directory Rights Management Services

AD RMS, a component of Windows Server 2008, is available to help protect files so that only the users who the sender intends to view a file can do so. AD RMS protects a file by specifying the rights that a user must have to access the file. Rights can be configured to allow a user to open, modify, print, forward, or take other actions with the rights-managed information. With AD RMS, you can safeguard data when it's distributed outside your network.

An AD RMS system has both a server and a client component, including the following:

- A Windows Server 2008 R2–based server running the Active Directory Rights Management Services server role, which handles certificates and licensing.
- A database server.
- The AD RMS client. The latest version of the AD RMS client is included as part of the Windows 7 and Windows Vista operating systems.

The server component is made up of several Web services that run on a Microsoft server such as Windows Server 2008. The client component can be run on either a client or server operating system and includes functions that enable an application to encrypt and decrypt content, retrieve templates and revocation lists, and acquire licenses and certificates from a server.

By using AD RMS and the AD RMS client, you can augment an organization's security

strategy by protecting information through persistent usage policies that remain with the information, regardless of where it's moved. You can use AD RMS to help prevent sensitive information—such as financial reports, product specifications, customer data, and confidential e-mail and voice mail messages—from intentionally or accidentally getting into the wrong hands. For detailed information, see AD RMS Overview.

In Exchange 2010, you can use Information Rights Management (IRM) features to apply persistent protection to messages and attachments. IRM uses AD RMS, an information protection technology in Windows Server 2008 and Windows Server 2008 R2. To use IRM to implement Protected Voice Mail, you need Windows Server 2008 R2 with AD RMS.

Using the IRM features in Exchange 2010, and Protected Voice Mail, your organization and your users can control the rights recipients have to access e-mail and voice mail messages. IRM can be also used to restrict recipient actions such as forwarding a message to other recipients, printing a message or attachment, or extracting message or attachment content by copying and pasting. For details, see Understanding Information Rights Management.

IRM Requirements

Before you can implement IRM in Exchange 2010, you must first deploy and configure your AD RMS infrastructure. For detailed information, see Active Directory Rights Management Services. To implement IRM to support Protected Voice Mail in your Exchange 2010 organization, your deployment must meet the following requirements.

Return to top

Server	Requirement
AD RMS Cluster	• **Windows Server 2008 Service Pack 2 (SP2)** with the following hotfix. For more information, see A hotfix is available for the Active Directory Rights Management Services role in Windows Server 2008. • **Service connection point (SCP)** Exchange 2010 and AD RMS-aware applications use the SCP registered in Active Directory to discover AD RMS clusters and URLs. AD RMS allows you to register the SCP within AD RMS setup. If the account used to set up AD RMS isn't a member of the Enterprise Admins security group, SCP registration can be performed after setup. There is only one SCP for AD RMS in an Active Directory forest. • **Permissions** Servers in the Exchange servers group or individual Exchange servers must be assigned Read and Execute permissions to the AD RMS server certification pipeline (The default path is \inetpub\wwwroot_wmcs \certification\ServerCertification.asmx on AD RMS servers). • **AD RMS super users** To enable transport decryption, journal report decryption, IRM in Outlook Web App, and IRM for Exchange Search, you must add the Federated Delivery Mailbox, a system mailbox created by Exchange

	2010 Setup, to the AD RMS super users group on the AD RMS cluster. For detailed information, see Add the Federation Mailbox to the AD RMS Super Users Group.
Exchange Server	• **Exchange Server 2010** • Recommended: This hotfix for the Microsoft .NET Framework 2.0 Service Pack 2 (SP2). For information, see FIX: ArgumentNullException exception error message when a .NET Framework 2.0 SP2-based application tries to process a response with zero-length content to an asynchronous ASP.NET Web service request: "Value cannot be null".

Configuring and Testing IRM

You must use the Shell to configure IRM features in Exchange 2010. To configure individual IRM features, use the Set-IRMConfiguration cmdlet. For more information about how to configure IRM features, see Managing Information Rights Management.

After you've set up an Exchange 2010 server, you can use the Test-IRMConfiguration cmdlet to perform end-to-end tests of your IRM deployment. This cmdlet verifies the IRM configuration for an organization and should be run before enabling Protected Voice Mail. The **Test-IRMConfiguration** cmdlet performs the following tests:

- Inspects the IRM configuration for your Exchange 2010 organization
- Checks the AD RMS server for version and hotfix information
- Verifies whether an Exchange server can be activated for RMS by retrieving a Rights Account Certificate and Client Licensor Certificate (CLC)
- Acquires AD RMS rights policy templates from the AD RMS server
- Verifies that the specified sender can send IRM-protected messages
- Retrieves a super user use license for the specified recipient
- Acquires a pre-license for the specified recipient

Client Support and End User Features

The e-mail client software that's used to listen to a Protected Voice Mail message must support IRM and know how to read a UM-protected voice message. E-mail clients that are supported include Microsoft Outlook 2010, Outlook Web App, and Exchange 2010 Outlook Voice Access. The following table contains a list of e-mail clients and whether or not they're supported.

E-mail client	Description
Microsoft Outlook	• Protected voice messages are supported in Outlook 2010 only.
Outlook Web App	• Outlook Web App in Exchange 2010 supports Protected Voice Mail messages. Earlier versions of Outlook Web App or Microsoft Outlook Web Access don't support them.
Outlook Voice Access	• Outlook Voice Access in Exchange 2010 supports Protected Voice Mail. Outlook Voice Access included with Exchange 2007 doesn't support Protected Voice Mail. • The user's mailbox must reside on an Exchange 2010 Mailbox server.
Windows Mobile	• Windows Mobile doesn't currently support Protected Voice Mail.

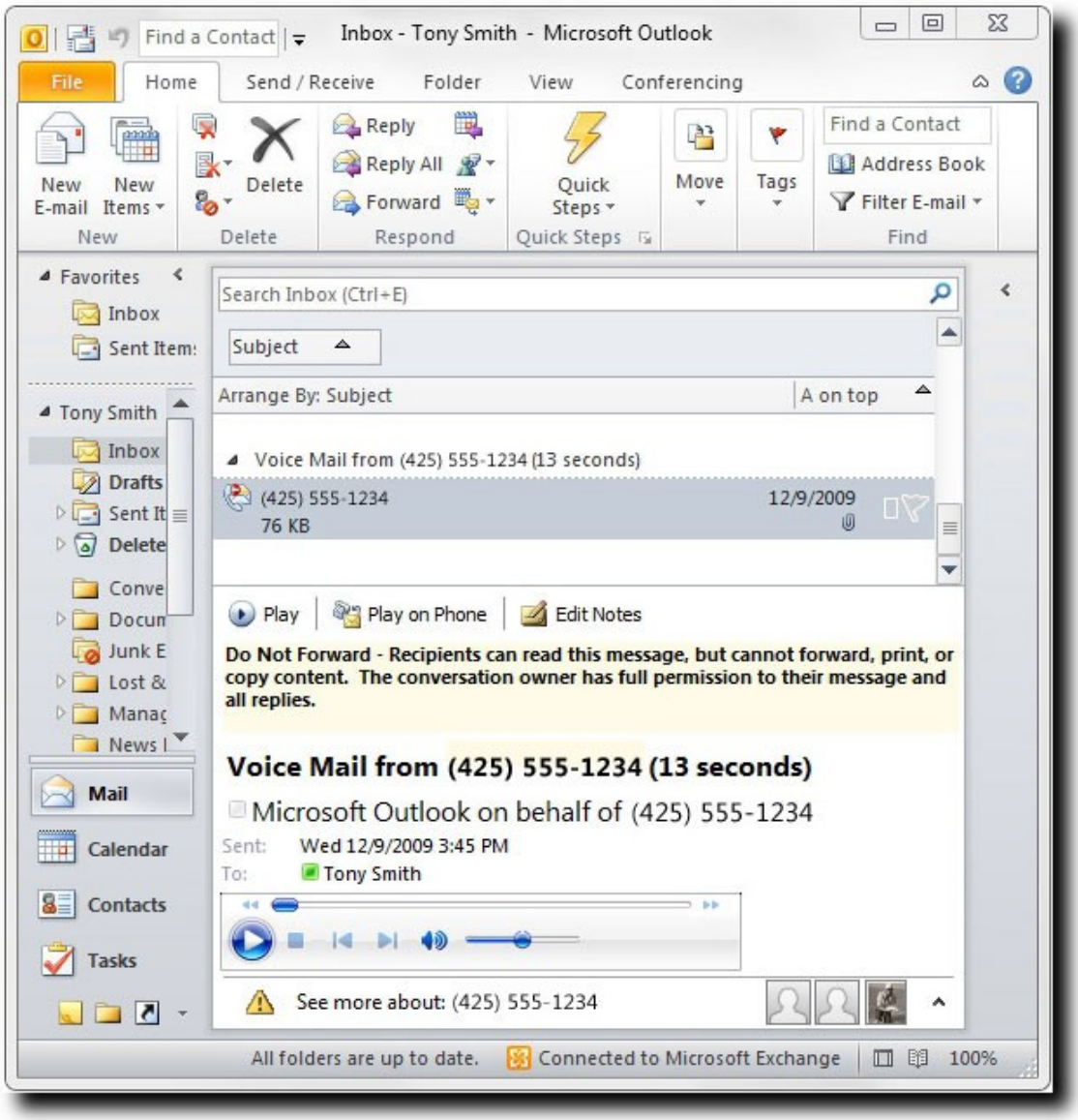
Other e-mail clients	• Protected Voice Mail isn't supported.

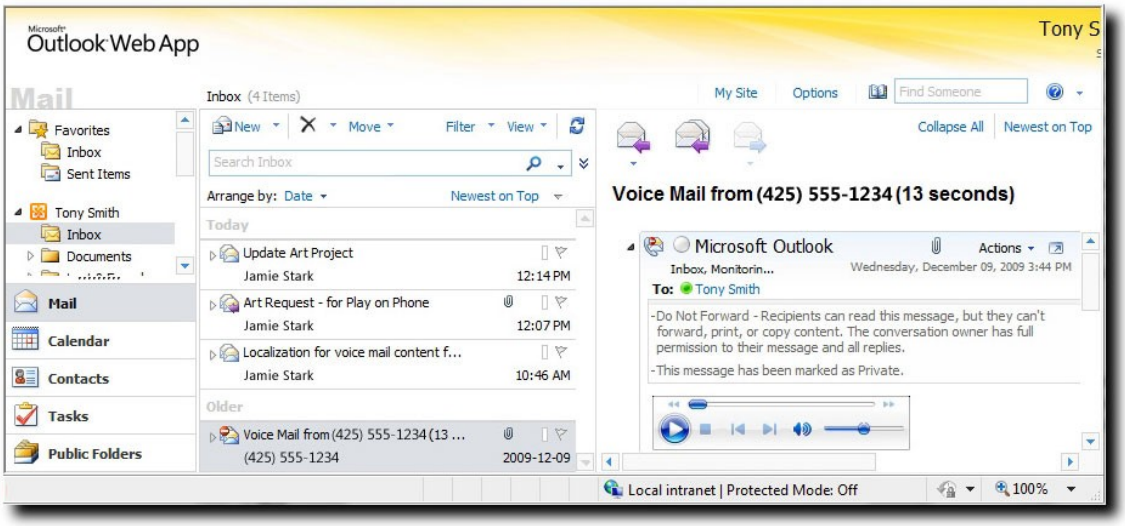
Return to top

Protected Voice Message Structure

There are actually two messages involved for each Protected Voice Mail message. The first message is the outer message, which isn't encrypted. It contains an attachment named message.rpmsg. The attachment contains the IRM-protected voice message and internal rights management control data. The Rights Management Control data includes a content key, and rights information that specifies who can access the voice message and how those users can access it.

Protected voice messages are shown in the user's Inbox in the **Voice Mail** search folder. The user can listen to the voice messages by using the embedded audio player just as they would listen to a regular voice message, except that the Forward button will be disabled and a note will be shown at the top of the message stating that it's protected and that it can't be forwarded.


Inbox - Tony Smith - Microsoft Outlook
Find a Contact
File
Home
Send / Receive
Folder
View
Conferencing
New E-mail
New Items
Delete
Reply
Reply All
Forward
Quick Steps
Move
Tags
Find a Contact
Address Book
Filter E-mail
New
Delete
Respond
Quick Steps
Find
Favorites
Inbox
Sent Item:
Tony Smith
Inbox
Drafts
Sent It
Delete
Conve
Docun
Junk E
Lost &
Manag
News I
Mail
Calendar
Contacts
Tasks
Search Inbox (Ctrl+E)
Subject
Arrange By: Subject
A on top
Voice Mail from (425) 555-1234 (13 seconds)
(425) 555-1234
76 KB
12/9/2009
Play
Play on Phone
Edit Notes
Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.
Voice Mail from (425) 555-1234 (13 seconds)
Microsoft Outlook on behalf of (425) 555-1234
Sent: Wed 12/9/2009 3:45 PM
To: Tony Smith
See more about: (425) 555-1234
All folders are up to date.
Connected to Microsoft Exchange
100%



For e-mail clients that don't support Protected Voice Mail, the body of the outer message will be displayed. Default text is provided by UM when the protected voice message is being created. Administrators can overwrite this text by using the UM mailbox policy configuration objects.

If the user is using an e-mail client that doesn't support Protected Voice Mail, the following default text will appear on the user's client application e-mail form: "*Your e-mail program doesn't support opening voice messages that are sent with restricted permission. To listen to this message, use Outlook 2010 or Outlook Web App in Exchange 2010. Or, if you're using Exchange 2010 Unified Messaging, you can use Outlook Voice Access*."

You can customize the default text that's included in the e-mail message by configuring a UM mailbox policy. For example, you could configure the UM mailbox policy with customized text such as, *"You can't open this voice mail message because it's protected. To view or listen to this voice message, sign in to your mailbox at https://mail.contoso.com or call +1 (425) 555-1234 to call in to Outlook Voice Access."*

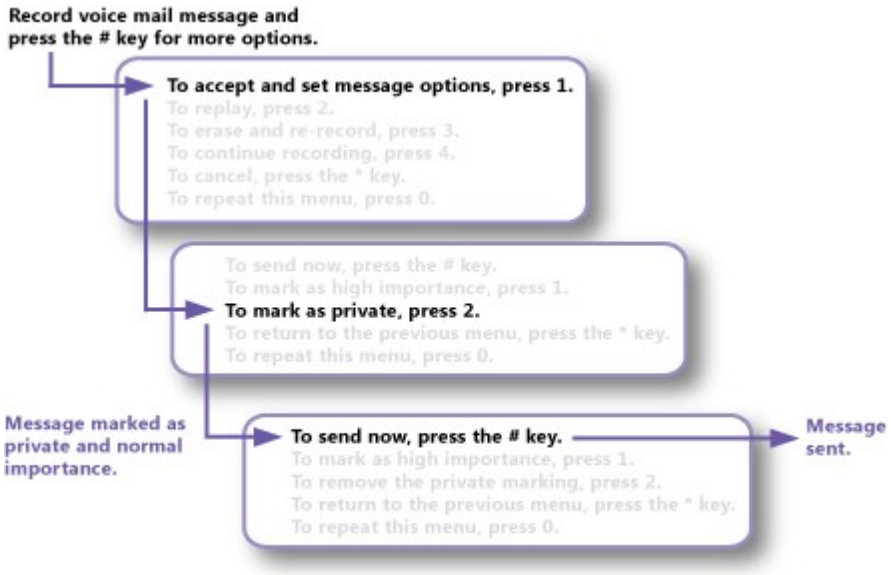
Composing a Protected Voice Mail Message

There are two situations in which protected voice messages can be created:

- **Call Answering** Call answering occurs when a caller calls a UM-enabled user, but the user isn't available to answer the call or forwards it directly to his or her voice mail. In call answering scenarios, the voice mail system will play a series of voice prompts after the caller records their voice mail message. The caller can then choose from additional message options, including the option to mark the voice message as private by pressing the pound (#) key. If the caller pressed the # key, they can follow the instructions provided by UM to mark the message as private, remove the private marking from the private voice message, or mark the voice message with High importance. The following diagram shows the menu options that are available to callers when they leave a private voice message for a user.

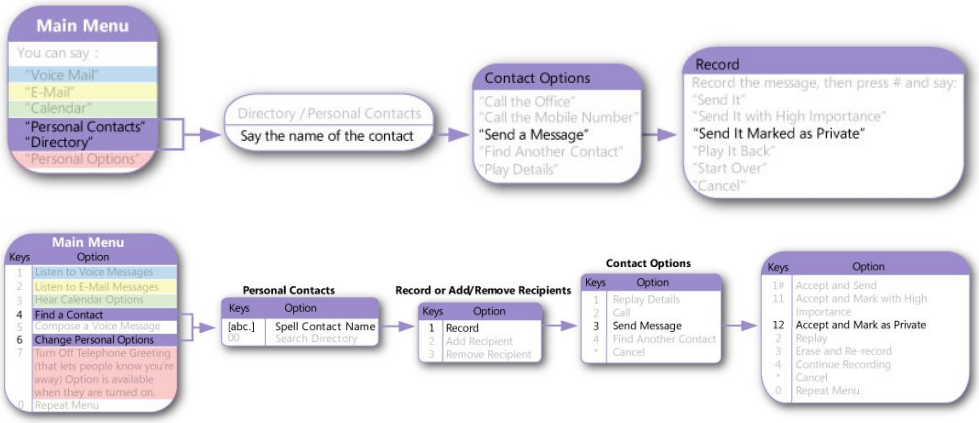
  Note:

  For call answering calls, the Protected Voice Mail settings on the UM mailbox policy of the intended recipient of the message are used by UM, because the caller isn't authenticated.



- **Outlook Voice Access** Outlook Voice Access lets UM-enabled users access their Exchange 2010 mailbox using analog, digital, or cellular telephones by dialing their Outlook Voice Access number. There are two Exchange 2010 Unified Messaging user interfaces available to UM-enabled users: the telephone user interface (TUI) and the voice user interface (VUI). Outlook Voice Access users can search for contacts in the directory and send them voice messages. If Protected Voice Mail has been enabled for the UM-enabled recipients, callers can mark the messages as private after they're recorded. Alternatively, administrators can configure a UM mailbox policy to ensure that all voice messages sent by authenticated users are protected by UM.

Note:
If a caller is authenticated, the Protected Voice Mail settings on the UM mailbox policy that is linked to the caller are applied, regardless the UM mailbox policy settings for the intended recipient of the voice mail message.



Return to top

UM Mailbox Policies

You can create a Unified Messaging mailbox policy to apply a common set of UM policy

settings, such as PIN policy settings, dialing restrictions, and Protected Voice Mail settings to a collection of UM-enabled mailboxes. To learn more about UM mailbox policies, see Managing UM Mailbox Policies.

You can use the EMC or the Exchange **Set-UMMailboxPolicy** cmdlet to configure Protected Voice Mail options. The following table lists the settings that can be configured for Protected Voice Mail.

Protected Voice Mail settings

Shell Parameter	Setting available in EMC?	Description
ProtectAuthenticatedVoiceMail	Yes	The *ProtectAuthenticatedVoiceMail* parameter specifies whether UM-enabled users can send protected voice messages when they're accessing their mailbox using Outlook Voice Access. The default setting is `None`. This means that no protection is applied when voice mail messages are composed and that callers won't have the option to mark voice messages as Private. If the value is set to `Private`, only messages marked as Private by the caller are protected. If the value is set to `All`, every voice message is protected, regardless of the option chosen by the caller.
ProtectUnauthenticatedVoiceMail	Yes	The *ProtectUnauthenticatedVoiceMail* parameter specifies whether the Unified Messaging servers that answer calls for UM-enabled users associated with a UM mailbox policy create protected voice messages. This setting also applies when a message is sent from a UM auto attendant to a UM-enabled user. The default setting is `None`. This means that no protection is applied to voice messages and that the caller won't be offered the option to mark the message as Private. If the value is set to `Private`, only messages marked as Private by the caller are protected. If the value is set to `All`, every voice message is protected, regardless of whether if the message has been marked

		as private by the caller.
ProtectedVoiceMailText	Yes	The *ProtectedVoiceMailText* parameter specifies the text to be included in the body of the outer message of a Protected Voice Mail message. This text will be shown in all e-mail client applications that don't support Protected Voice Mail messages. Note that a default message is always provided by UM when this property is set to `Null` or is empty.
RequireProtectedPlayOnPhone	Yes	The *RequireProtectedPlayOnPhone* parameter specifies whether users associated with the UM mailbox policy will be forced to listen to the protected voice message over the phone (using Play On Phone). The default value is `$false`. When the value is set to `$true`, the audio media player on Protected Voice Mail forms in Outlook or Outlook Web App will be shown as disabled. Note that the preview text for the voice message can always be accessed. The user can't play the audio file using any media player software or use the embedded media player to listen to the voice message.
AllowVoiceResponseToOtherMessageTypes	Yes	The *AllowVoiceResponseToOtherMessageTypes* parameter specifies whether callers who have authenticated to Outlook Voice Access to access their e-mail will be able to compose a voice reply to e-mails and meeting requests.

For more information about how to manage Protected Voice Mail settings, see the following topics:

- Configure Protected Voice Mail from Authenticated Callers on a UM Mailbox Policy
- Configure Protected Voice Mail from Unauthenticated Callers on a UM Mailbox Policy
- Enable or Disable Multimedia Playback of Protected Voice Messages on a UM

Mailbox Policy
- Specify the Text to Display for E-Mail Clients that Don't Support Windows Rights Management on a UM Mailbox Policy
- Set-UMMailboxPolicy

Return to top

SMS Notifications and Protected Voice Mail

Users who configure their UM account to send SMS (also called text message) notifications to their mobile phone when voice messages are received will also receive audio transcription (Voice Mail Preview) text as part of the body of the text message. However, for protected voice messages, this represents a security issue because the content of the voice messages should always be protected.

When UM creates a text message notification for a voice message that's protected, it checks whether the voice message is marked as Private. If so, it won't add the transcribed audio text to the text message that it sends to the mobile phone. The following text will be included in the text message instead: "Use Outlook Voice Access to access this protected voice mail message."

1.9.1.3.20 Understanding Message Waiting Indicator

Understanding Message Waiting Indicator

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-24*

Message Waiting Indicator (MWI) is a feature that's found in most legacy voice mail systems. In its most common form, this feature lights up a lamp on a user's phone to indicate the presence of a new or unheard voice mail message. In general, this is the way that legacy voice mail systems let voice mail subscribers know that they have new or unheard voice mail messages. However, in the context of Microsoft Exchange Unified Messaging (UM), MWI refers to a feature that's available in traditional IP gateway, PBX, and Microsoft Exchange Server 2010 Unified Messaging and Microsoft Lync Server 2010 deployments.

In a traditional telephony environment, MWI allows for a lamp or some other mechanism to notify the UM-enabled user that they have a new voice mail message. In environments where Microsoft Office Communications Server 2007 R2 or Lync Server 2010 and VoIP phones are used, the mechanism for letting a user know that a new voice message was received is different than in a traditional telephony environment. Enterprise Voice UM-enabled users see different lights than users in a traditional telephony environment, or other types of notifications.

Contents

MWI Resilience

MWI Administration

Overview

In general, Message Waiting Indicator (MWI) can refer to any mechanism that indicates the existence of a new or unheard voice message. The message can be new or marked as an unread e-mail message, or it can be new or marked as an unheard voice message. The message-waiting indicator mechanism could be:

- A new voice mail message as seen from Outlook or Microsoft Office Outlook Web App.
- A text or SMS message sent to a registered mobile phone.
- An outbound call made from Exchange UM to a preconfigured number.
- A light or phone lamp on a phone.
- A special dial tone.
- Icons or buttons on the display screen of a phone.
- A highlighted notification within a software application.

In Microsoft Exchange Server 2007 and Exchange 2010, a UM-enabled user's voice mail is stored in an Exchange mailbox. It can be accessed from a telephone using Outlook Voice Access, from a desktop or portable computer using Outlook and Outlook Web App, and mobile phone clients. When a UM-enabled user receives a new voice message, the message appears in their Voice Mail search folder. If the voice message is accessed using Outlook or Outlook Web App, an e-mail message will be included with the voice message. UM-enabled users who access their Inbox via Outlook and Outlook Web App already have a very efficient mechanism to let them know that they have a new voice message. However, not all UM-enabled users access their voice mail and e-mail messages using Outlook and Outlook Web App.

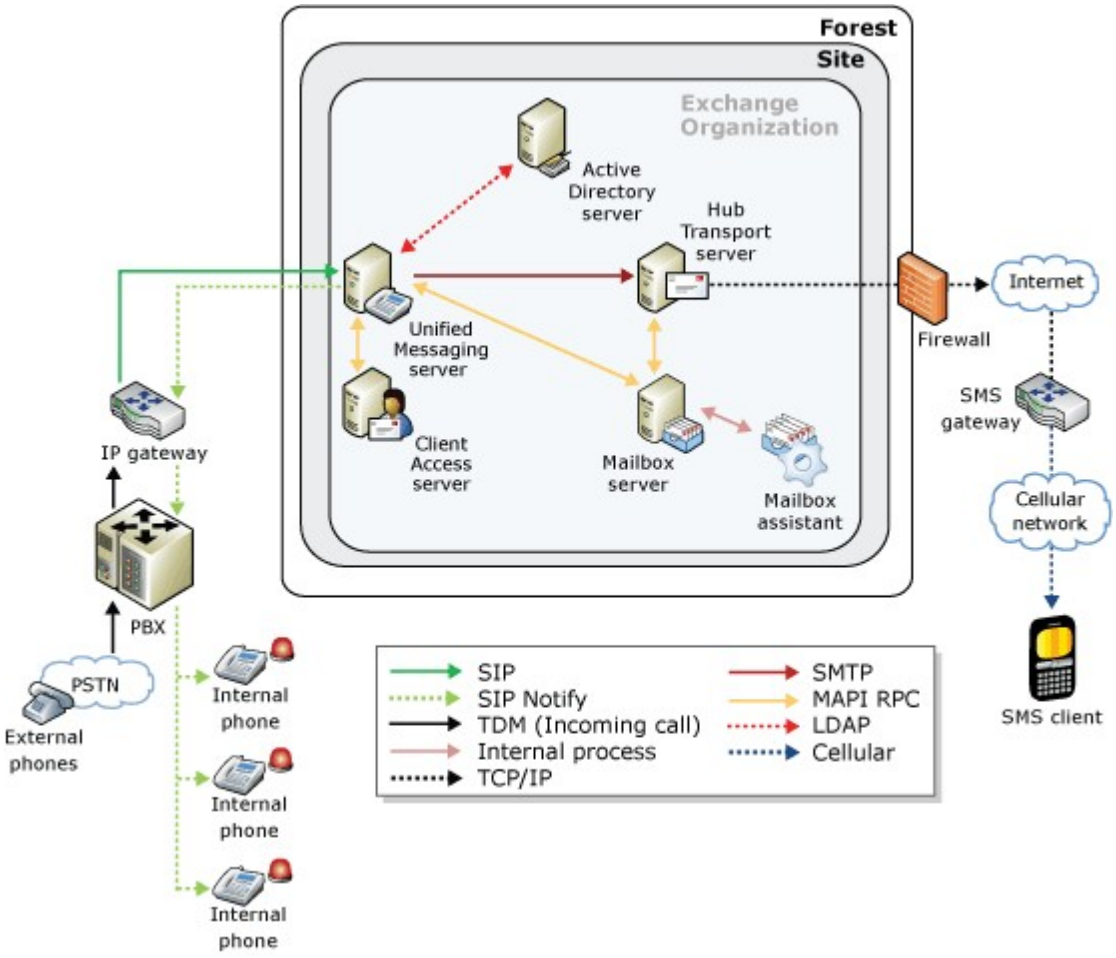
In Exchange 2007, MWI was supported in a traditional or an IP PBX environment by using a third-party solution or application. Exchange 2010 includes built-in support for MWI. Office Communications Server 2007 R2 and Lync Server 2010 also support MWI. However, the actual MWI mechanism depends on the type of IP-based phone that's used by the Enterprise Voice and UM-enabled user. The following examples show message-waiting indicators from IP-based phones used with Communications Server 2007 R2 or Lync Server 2010:

In Exchange 2010, MWI doesn't require that any additional server roles or services be installed. By default, MWI is turned on. It's controlled through settings on a UM mailbox policy or on the UM-enabled user's mailbox. MWI also works with protected voice messages and is a feature found only in Exchange 2010.

To implement MWI in Exchange 2010 in a traditional telephony environment, a UM server

sends an MWI SIP NOTIFY message to a SIP peer or an IP gateway that's represented by a UM IP gateway in Active Directory. The SIP peer or IP gateway sends the notification to the PBX. The PBX, in turn, lights up the lamp on the desktop phone to notify the user of a new or unheard voice message.

There are two voice-mail scenarios: call answering and Outlook Voice Access. With call answering, the UM server answers an incoming call and allows the caller to leave a voice message for a UM-enabled user. With Outlook Voice Access, when a caller calls a subscriber access number, they can leave a voice message for a UM-enabled user. The following figure shows an overview of how MWI in Exchange 2010 Unified Messaging works in a call-answering scenario.



Note:
The Mailbox Assistant only looks for Voice Mail search folder events.

Return to top

The UM Server's Role in Message Waiting Indicator

After a caller calls a UM-enabled user and the user doesn't answer their phone, the UM server sends a SIP NOTIFY message to an IP gateway or a SIP peer. The UM server receives MWI state change information over RPC from the Mailbox server and sends the request for a change of notification to an IP gateway or IP PBX using a SIP NOTIFY message. The RPC request to the Mailbox server will include the following information:

- Message waiting indicator enabled (Yes or No).
- Number of new/marked unheard voice messages.

- Number of old/marked heard voice messages.
- Number of new/marked unheard urgent voice messages.
- Number of old/marked heard urgent voice messages.
- The primary extension number on the primary UM dial plan.
- The IP address or fully qualified domain name (FQDN) of the SIP peer or IP gateway to be used for SIP NOTIFY messages.
- The security type of the UM dial plan (Unsecured, SIP secured, or Secured). This information will be used by the UM server to determine whether the connection to the IP gateway must be SIP over TCP or SIP over TLS. TLS is supported for MWI SIP Notify.

The UM server uses the diversion information on the header of the incoming call to determine the extension number or phone number of the UM-enabled user. When the extension or phone number is determined, the UM server sends the request to the SIP peer, and the SIP peer sends the message on to the PBX. The PBX then changes the state of the MWI and lights the phone's lamp.

Note:

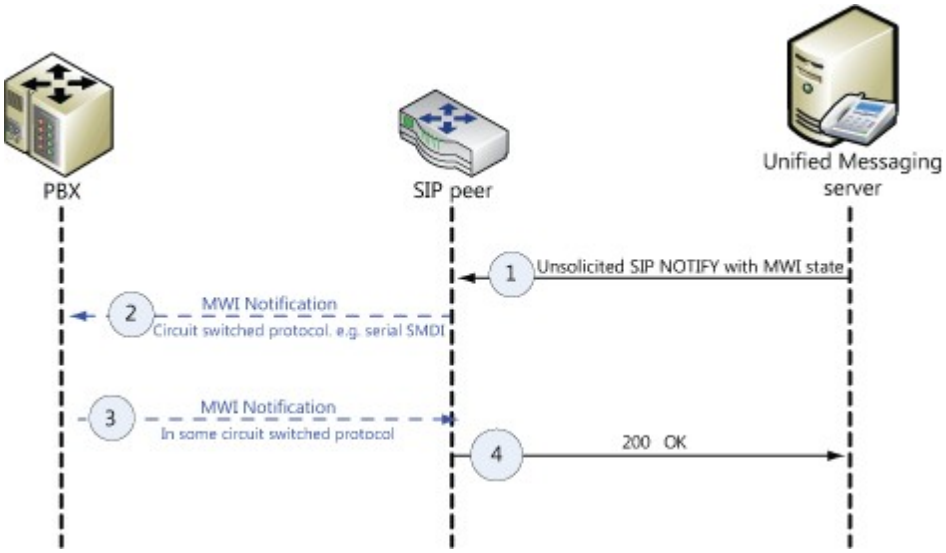
Although PBX outages should be rare, Exchange UM will automatically refresh the MWI status for every mailbox at least once every 12 hours. There is no way to force a refresh, but if the PBX is powered off and all the MWI lamps go off, it should be a maximum of 6 hours until all lamps are restored to the correct state.

Return to top

MWI SIP NOTIFY Messages

MWI notifications use SIP NOTIFY messages to communicate with SIP peers or IP gateways. These messages are sent to the SIP peer with MWI state change information. MWI state change information is included in the SIP NOTIFY message and indicates whether or not MWI notifications will be sent to users. Whenever there's a change in MWI state, the Mailbox Assistant sends this information to a UM server over RPC. After the UM server receives this information, it parses the message to obtain the target SIP peer or IP gateway and the MWI state change information. It will then form a SIP NOTIFY message with the MWI state change information in the message body and send this information on to the SIP peer or IP gateway.

MWI in Exchange 2010 is based on RFC 3842. RFC 3842 states that SIP event notifications must be used for message-waiting notifications. MWI is based on the SIP model, and is driven by the endpoints found in a unified messaging system. SIP endpoints, either IP gateways or IP PBXs, which obtain MWI information must send a SIP SUBSCRIBE message to the Unified Messaging system. The SIP SUBSCRIBE message will be replied to with a NOTIFY message that accepts the subscription. All MWI state change information will be conveyed from the unified message system to a SIP endpoint using NOTIFY messages that are embedded within the subscription that was previously created. The exact syntax of the SIP NOTIFY message to be sent to the SIP peer is based on the format described in RFC 3842. The call flow is shown in the following figure.



The UM server sends an MWI NOTIFY message to the SIP peer. The event header is set to "message-summary", which indicates that this is an MWI-related NOTIFY message. The To header field indicates the SIP endpoint for which the MWI service must be provided. The Subscription-State header must be set to "terminated" instead of "active".

- The SIP peer or IP gateway conveys this information to the PBX using a circuit-switched protocol such as SMDI.
- The PBX sends a success message over a circuit-switched protocol.
- The SIP peer or IP gateway can respond with any of the following messages: 200 OK (Success) or 480 (Temporarily Unavailable). A UM server can handle both these responses and additional failure responses.

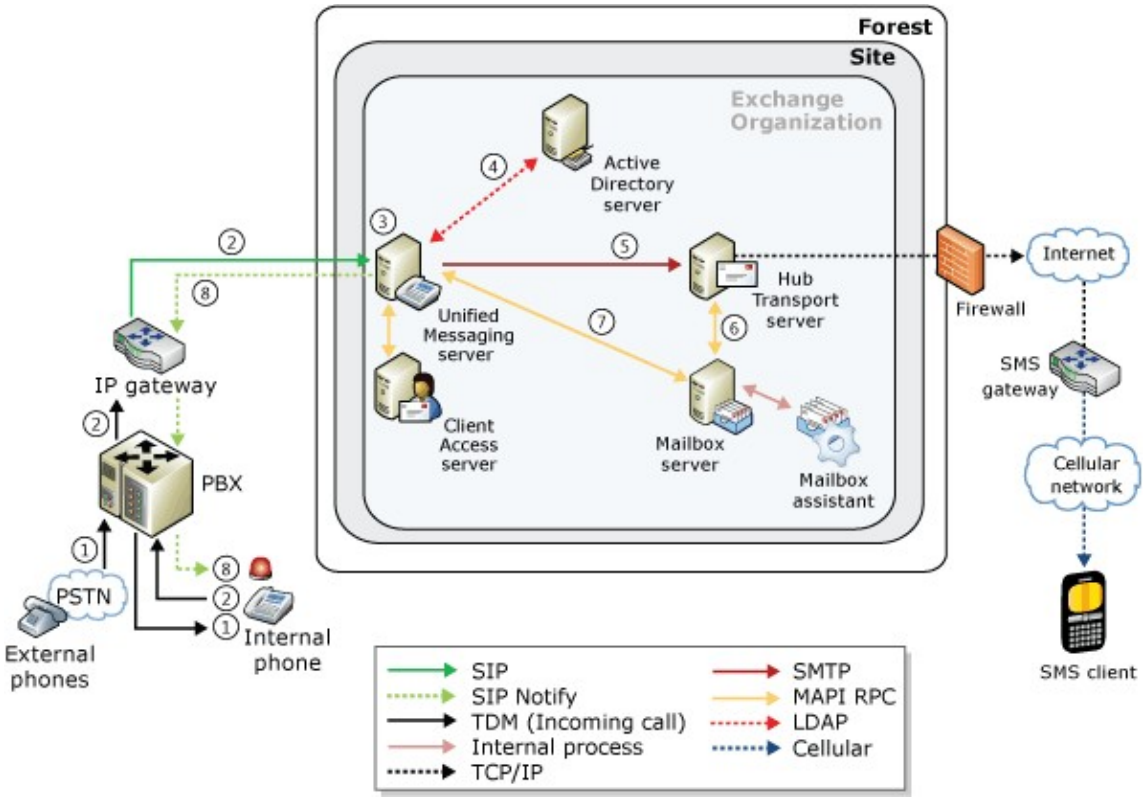
MWI in a Traditional Telephony Environment

In a traditional telephony environment, an incoming call is received by the PBX and then sent on to the IP gateway. The UM server and the Mailbox Assistant are used to determine the MWI state for the UM-enabled user. They're responsible for delivering the SIP notification back to the IP gateway and PBX. In a traditional telephony environment, the call flow and MWI notification are as follows:

1. The incoming call is received by the PBX, and then sent from the PBX to the phone of the UM-enabled user. The user doesn't answer and the caller is prompted to leave a voice message.
2. The call is first sent from the PBX to the IP gateway.
3. The IP gateway then submits the call to a UM server.
4. The UM server performs an LDAP query to locate the UM-enabled user's information, such as the extension number and the greetings for the user. The greeting or greetings for the UM-enabled user are played.
5. The voice message that was created by the UM server is submitted to a Hub Transport server within the same site.
6. The Hub Transport server submits the voice message to a Mailbox server. The Mailbox Assistant receives a MAPI event for a new voice message.
7. The Mailbox Assistant reads the UM dial plan and the UM mailbox policy to determine whether MWI notifications should be sent to the UM-enabled user. The Mailbox Assistant queries for all UM servers that are associated with the UM dial plan of the UM-enabled user. The Mailbox Assistant tries to send the RPC event to the first UM server that's returned. If this fails, it tries the next one. It will keep retrying for 5 minutes, or until all servers have been tried. If all the RPC calls fail, the Mailbox Assistant logs the error in Event Viewer. The UM server queries for all UM IP gateways that are associated with the UM dial plan of the UM-enabled user's mailbox.
8. UM sends a SIP NOTIFY message to the first IP gateway that's returned from

the query. If this fails, the UM server will choose the next IP gateway. The UM server will keep trying for an IP gateway for 5 minutes. If all attempts to find an IP gateway fail, the UM server will log an error. If an IP gateway is located successfully, the IP gateway will send the notification to the PBX, and the PBX in turn will send a notification of the MWI event to the user's phone to light the phone lamp.

The following figure shows the call flow in a traditional telephony environment.



Return to top

MWI in a Lync Server 2010 Environment

In telephony environments that include Lync Server 2010, an incoming call can be sent from an external phone to the mediation server, sent from a Lync 2010 client, or from a Unified Communications (UC)-based phone. After the call is received, it's sent on to the Lync Server 2010 front-end server pool. The UM server and the Mailbox Assistant are used to determine the MWI state for the UM-enabled user and to deliver this notification to the client or UC-based phone.

Note:

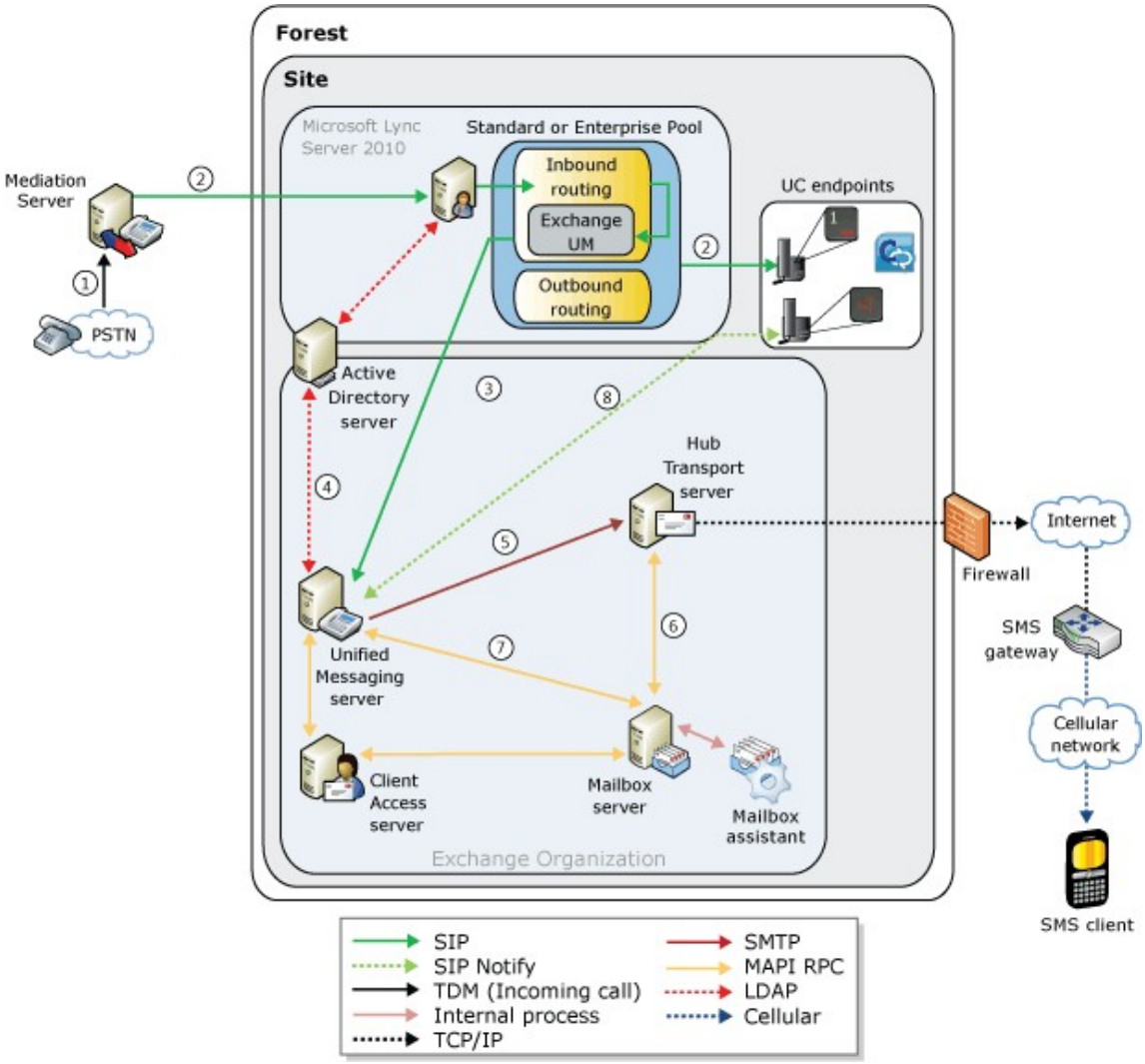
Message waiting notification is only supported in Lync Server 2010 deployments. It is also available in cross-premises deployments that include Lync Server 2010. Office Communications Server 2007 R2 doesn't support MWI and isn't supported in cross-premises deployments.

In a telephony environment with Lync Server 2010, the call flow and MWI notification is as follows:

1. The call is sent from one of the following:
   1.a. An external phone to a mediation server
   1.b. A Lync 2010 client
   1.c. A UC-based phone.

2. The incoming call is received by the Lync Server 2010 front-end server pool and sent on to the phone of the UM-enabled user. The user doesn't answer and the caller is prompted to leave a voice message.
3. The Lync Server 2010 front-end server pool then submits the call to a UM server.
4. The UM server performs an LDAP query to locate information for the UM-enabled user, such as their extension number and greetings. The greetings are played, and the caller is prompted to leave a voice message.
5. The voice message that was created by the UM server is submitted to a Hub Transport server within the same site.
6. The Hub Transport server submits the voice message to a Mailbox server. The Mailbox Assistant receives a MAPI event for a new voice message.
7. The Mailbox Assistant reads the UM dial plan and the UM mailbox policy to decide whether MWI notifications should be sent to the user. The Mailbox Assistant queries for all UM servers that are associated with UM dial plan of the user. The Mailbox Assistant tries to send the RPC event to the first UM server that's returned. If this attempt fails, the Mailbox Assistant tries the next one. It will keep trying to find a UM server for 5 minutes or until all servers have been tried. If all the RPC calls fail, the Mailbox Assistant will log an error in the Event Viewer. The UM server queries for all UM IP gateways associated with the UM dial plan of the UM-enabled user's mailbox.
8. UM sends a SIP NOTIFY message to the first IP gateway that's returned from the query. If this fails, the UM server will choose the next IP gateway. The UM server will keep trying to find an IP gateway for 5 minutes. If all attempts to contact an IP gateways fail, the UM server will log an error. If it's successful, the IP gateway will send the notification to the Lync Server 2010 front-end server pool, which in turn will send a notification of the MWI event to the user's phone or Lync 2010 client.

The following figure shows the call flow in a traditional telephony environment.



Return to top

MWI Resilience

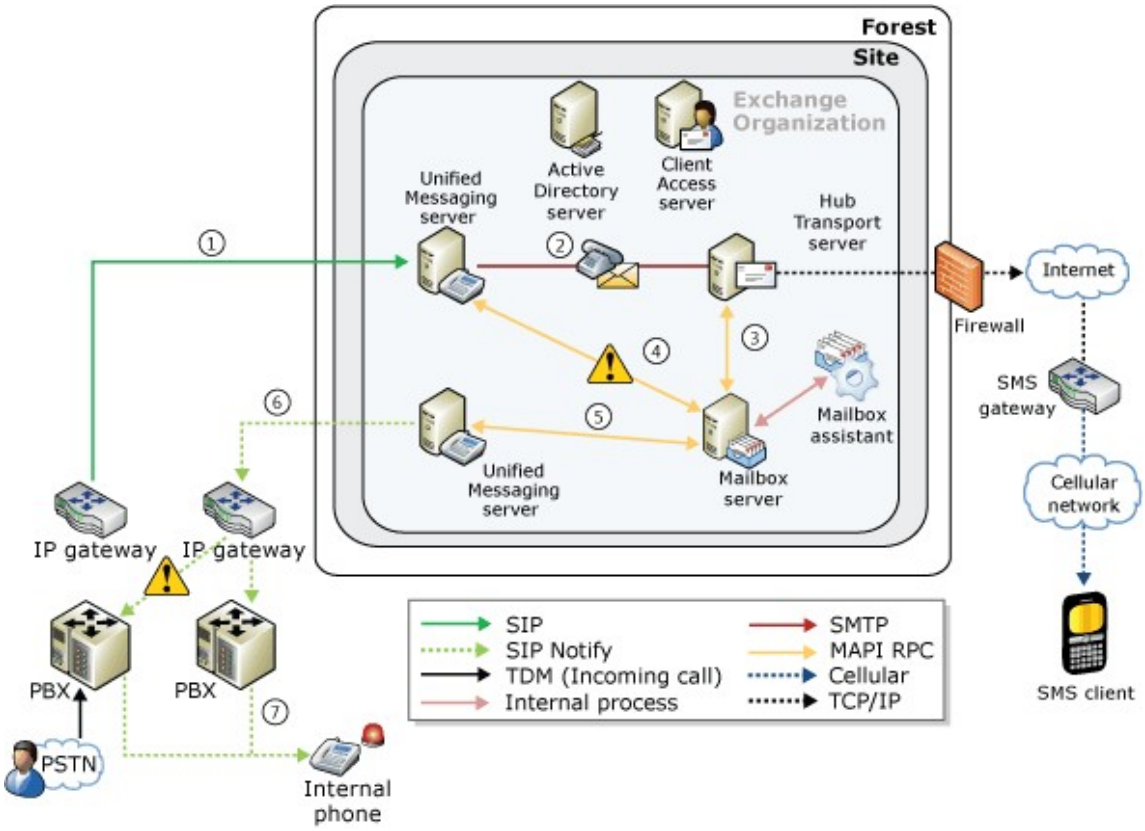
When you're deploying UM servers, UM dial plans, and UM IP gateways, and are using MWI for UM-enabled users, it's best to deploy multiple UM servers and multiple IP gateways to create fault tolerance and resiliency. Doing this also creates MWI resilience. When you deploy multiple UM servers and UM IP gateways, if a UM server or IP gateway isn't available and the Mailbox server can't connect, the next UM server will be used. If the UM server can't connect to the IP gateway, the next IP gateway will be used. In both cases, a round robin mechanism is used.

To enable fault tolerance for MWI in Unified Messaging, you must create and configure one or more of the following:

- A UM dial plan that's associated with the UM-enabled user who will receive MWI notifications.
- A UM mailbox policy that's associated with the UM-enabled user who will receive MWI notifications.
- A UM IP gateway that's associated with the UM dial plan that's associated with the UM-enabled user who will receive MWI notifications.

- A UM server that's added to the UM dial plan that's associated with the UM-enabled user who will receive MWI notifications.

The following figure shows that MWI can use multiple paths to send SIP NOTIFY messages.



MWI Administration

MWI can be administered by configuring settings on two Active Directory objects: UM mailbox policies and UM IP gateways. For both Active Directory objects, you can enable or disable MWI by using the **Set-UMMailboxPolicy** cmdlet or the **Set-UMIPgateway** cmdlet, or by configuring the settings using the Exchange Management Console (EMC). You can view the status of the MWI notification by using the **Get-UMMailboxPolicy** cmdlet and the **Get-UMIPgateway** cmdlet, or by viewing the settings in the EMC.

UM Mailbox Policies and MWI

You can create a Unified Messaging mailbox policy to apply a common set of UM policy settings to a collection of UM-enabled mailboxes. For example, you can use a UM mailbox policy to apply PIN policy settings, dialing restrictions, and MWI settings. If you enable MWI, it will be enabled for all users who are associated with the UM mailbox policy. If you disable MWI on a UM mailbox policy, MWI will be disabled for all UM-enabled users who are associated with the UM mailbox policy. Thus, disabling MWI can disable MWI for all UM-enabled users associated with a single or multiple UM dial plans or a single or multiple UM mailbox policies. If you enable or disable MWI on a UM mailbox, you can affect large groups of UM-enabled users in your Exchange organization. The MWI setting will apply to a subset of the users who are associated with a UM dial plan. To learn more about UM mailbox policies, including how to enable or disable MWI for a group of UM-enabled users, see Managing UM Mailbox Policies.

You can use the EMC and the **Set-UMMailboxPolicy** cmdlet to configure the MWI setting.

The following table lists the setting that can be configured for MWI.

Message Waiting Indicator setting on a UM mailbox policy

Shell parameter	Setting available in the EMC?	Description
AllowMessageWaitingIndicator	Yes	The *AllowMessageWaitingIndicator* parameter specifies whether users who are associated with a UM mailbox policy can receive notifications when they receive a new voice message. The default value is `$true`. Enabling this setting will allow voice mail notifications to be sent to users who are associated with a single UM mailbox policy for calls taken by a UM IP gateway. This setting allows the UM IP gateway to receive and send SIP NOTIFY messages to UM-enabled users' phones. This option isn't available to UM-enabled users who have a mailbox on an Exchange 2007 server.

For more information about how to manage MWI settings, see the following topics:

- Managing UM Mailbox Policies
- View or Configure the Properties of a UM Mailbox Policy
- Enable or Disable Message Waiting Indicator on a UM Mailbox Policy
- Set-UMMailboxPolicy

UM IP Gateways and MWI

If you disable MWI on a UM IP gateway, you'll disable MWI for all users who connect to the IP gateway that's represented by the UM IP gateway. Therefore, disabling MWI can disable MWI for all UM-enabled users associated with a single or multiple UM dial plans or a single or multiple UM mailbox policies. If you enable or disable MWI on a UM IP gateway, you can affect large groups of users in your Exchange organization. To learn more about UM mailbox policies, including how to enable or disable MWI for a group of UM-enabled users, see Managing UM Mailbox Policies.

You can use the EMC and the **Set-UMMailboxPolicy** cmdlet to configure the MWI setting. The following table lists the setting that can be configured for MWI.

Message Waiting Indicator setting on a UM IP gateway

Shell parameter	Setting available in the EMC?	Description
MessageWaitingIndicatorAllowed	Yes	The *MessageWaitingIndicatorAllowed* parameter specifies whether to enable the UM IP gateway to allow SIP NOTIFY

		messages to be sent to users associated with a UM dial plan. The default value is `$true`. When this setting is enabled, voice mail notifications can be sent to users for calls that are received by the UM IP gateway. This setting allows the UM IP gateway to send message-waiting notifications to UM-enabled users. This option isn't available to UM-enabled users who have a mailbox on an Exchange 2007 server.

For more information about how to manage MWI settings, see the following topics:

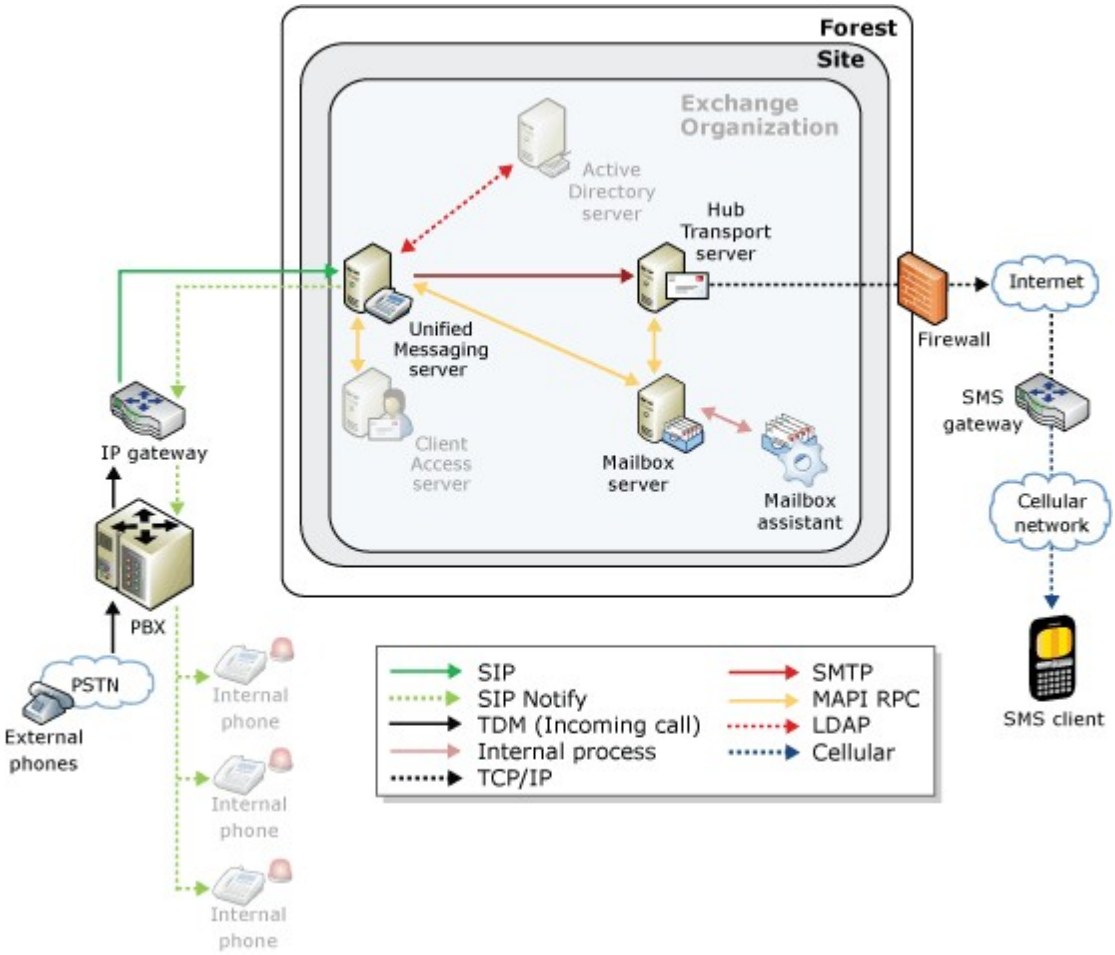
- Managing UM IP Gateways
- View or Configure the Properties of a UM IP Gateway
- Allow or Prevent Message Waiting Indicator on a UM IP Gateway
- Set-UMIPGateway

Return to top

SMS MWI Notifications

Message Waiting Indicator can refer to any mechanism that indicates the existence of a new voice mail message. It can take the form of a Short Messaging Service (SMS) message, also known as a text message. The text message can be sent to the user's registered mobile phone along with other MWI notifications such as a light on their phone, a light on their phone keypad, or a light on a UC-based phone display.

The following figure shows an overview of how SMS MWI notifications work in an in Exchange 2010 Unified Messaging call answering scenario.



Note:

The SMS or text message that's sent to a UM-enabled user includes voice mail preview.

SMS MWI notifications can be administered by configuring settings on two Active Directory objects: UM mailbox policies and UM mailboxes. For both Active Directory objects, you can enable or disable SMS MWI by using the **Set-UMMailboxPolicy** cmdlet and the **Set-UMMailbox** cmdlet. You can view the status of SMS MWI notifications by using the **Get-UMMailboxPolicy** cmdlet and the **Get-UMMailbox** cmdlet.

You can only use the **Set-UMMailbox** cmdlet to configure the SMS MWI setting. This setting can't be configured by using the EMC. The following table lists the setting that can be configured for MWI.

SMS and Message Waiting Indicator setting on a UM mailbox

Shell parameter	Setting available in the EMC?	Description
UMSMSNotificationOption	No	The *UMSMSNotificationOption* parameter specifies whether a UM-enabled user can receive text messaging notifications for voice mail only, for voice mail and missed calls, or isn't allowed to receive notifications. The values for this parameter

		are: `VoiceMail`, `VoiceMailAndMissedCalls`, and `None`. The default value is `None`. This option isn't available to UM-enabled users who have a mailbox on an Exchange 2007 server.

For more information about how to manage SMS MWI settings, see the following topics:

- Managing Unified Messaging Users
- View or Configure the Properties of a UM-Enabled User
- Set-UMMailbox

You can only use the **Set-UMMailboxPolicy** cmdlet to configure the MWI setting. This setting isn't available using EMC. The following table lists the setting that can be configured for MWI.

SMS and Message Waiting Indicator setting on a UM mailbox policy

Shell parameter	Setting available in the EMC?	Description
AllowSMSNotification	No	The *AllowSMSNotification* parameter specifies whether UM-enabled users whose mailboxes are associated with the UM mailbox policy are allowed to receive SMS or text messages sent to their mobile phones. If this parameter is set to $true, you must also use the **Set-UMMailbox** cmdlet and set the *UMSMSNotificationOption* parameter for the UM-enabled user to either `voicemail` or `VoiceMailAndMissedCalls`. The default value is $true. This option isn't available to UM-enabled users who have a mailbox on an Exchange 2007 server.

For more information about how to manage MWI settings, see the following topics:

- Managing UM Mailbox Policies
- View or Configure the Properties of a UM Mailbox Policy
- Set-UMMailboxPolicy

Return to top

Understanding Secondary Dial Plans

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-08*

When you enable a user for Unified Messaging (UM) in Microsoft Exchange Server 2007 or the RTM version of Exchange Server 2010, you're required to assign at least a single extension number and associate a single UM dial plan to that UM-enabled user. You can assign additional extension numbers for that user within the same dial plan but you can't add a secondary dial plan with a single or multiple extension numbers. In Exchange 2010 Service Pack 1 (SP1), in addition to being required to assign the user a single primary UM dial plan with a single or multiple extension numbers, you can add a secondary UM dial plan with single or multiple extension numbers. This can be very useful, for example, if the user has two physical phones or travels between locations.

Contents

Overview

When you enable a user for Unified Messaging in the RTM version of Exchange 2010, you must define at least one extension number and one UM dial plan for Unified Messaging to use to locate the user when a voice mail message is submitted to the user's Exchange 2010 mailbox. After you've enabled the user for Unified Messaging, you can add additional extension numbers or EUM proxy addresses to the user's mailbox, but you can't associate the UM-enabled user with a secondary dial plan. In Exchange 2010 SP1, after you enable the user for Unified Messaging, add the required extension number, and associate the user with a single dial plan, you can add a secondary UM dial plan with a single or multiple extension numbers.

Note:

There's no limit to the number of secondary extension numbers that you can add for a UM-enabled user.

There may be times when a user travels between locations, has two or more phones, or wants to receive voice mail on one Direct Inward Dial (DID) extension number and to receive faxes on a different DID extension number. To achieve this, you must add an additional DID extension to the user's mailbox and, in some cases, add a secondary dial plan.

In some configurations, after you add a second extension on a primary dial plan or add a single or multiple extension numbers to a secondary dial plan, the user can receive voice messages or faxes using one or more of the extension numbers. If you want a Unified Messaging server to answer these fax calls and send them to the second DID extension number, you must configure the telephony equipment in your organization to forward the fax call to the second DID extension number.

The mailbox of a UM-enabled user can be assigned the following:

- A single extension number, Session Initiation Protocol (SIP) address, or E.164 address on a single dial plan.
- Multiple extension numbers on a single dial plan.
- Multiple extension numbers on two separate dial plans.

When an Exchange 2010 user's mailbox is enabled for Unified Messaging, the administrator must specify an extension number and a UM mailbox policy. The extension number is required by a UM server to identify the user when they log on to Outlook Voice Access to retrieve messages. The UM mailbox policy contains a collection of configuration properties, with values that UM applies to any user who is UM-enabled under that policy. The UM mailbox policy is similar to the "class of service" found in other systems (for example, voice mail or PBX), in the sense that a change to a UM mailbox policy value can affect the behavior for a large number of associated users.

One property on a UM mailbox policy refers to a UM dial plan. This is a configuration object that represents a set of telephony-capable extensions. This set has a numbering plan in which duplicate extension numbers aren't allowed.

Therefore, a user's extension number is unique within the UM dial plan in which they're UM enabled. In fact, the UM dial plan and extension number pair must be unique within the Exchange organization. This is one way that UM uniquely identifies a UM-enabled user in an Exchange organization. Using a secondary dial plan makes it easier to keep the dial plan and extension number unique within an organization. For example, imagine an organization has two UM dial plans: Dial Plan A and Dial Plan B. A user's extension number in Dial Plan A is 55555 and, in Dial Plan B, it's 66666. When a secondary dial plan is used, the user's extension for Dial Plan A can be 55555 and their extension in Dial Plan B can also be 55555. In both cases, the user's extension within the dial plan that's used is unique.

The following table defines terms that are used when discussing primary and secondary extensions, pilot numbers, and UM dial plans.

Term	Definition
primary extension	The extension number that's specified when the user is UM enabled.
primary dial plan	The UM dial plan that's specified when the user is UM enabled. The UM-enabled user is associated with the dial plan when the user is linked to the UM mailbox policy.
primary pilot number	The pilot number for the user's primary dial plan. The user's calls are forwarded to this number if there's no answer or their line is busy. It's also the number that the user calls when they want to log on to Outlook Voice Access.
secondary extension	One or more extension numbers that may be added to a UM-enabled user's configuration.
secondary dial plan	A UM dial plan other than the primary dial plan in which one or more secondary extensions can be configured.
secondary pilot number	The pilot number of a user's secondary dial plan. A user can call this number from their

	secondary extension number when they want to log on to Outlook Voice Access.

Return to top

Use of Secondary Extensions

In most deployments, only one extension is configured per UM-enabled user. However, there are some more advanced deployments that require you to add secondary extensions for your users.

When Microsoft Lync Server 2010 and Microsoft Office Communications Server R2 are used for Enterprise Voice, Exchange Unified Messaging can provide the voice mail system. However, the UM dial plan used for Enterprise Voice must be a SIP URI dial plan that's specific to UM configurations with Lync Server 2010 and Office Communications Server R2. In these deployments, the user's extension is provided by a Microsoft Unified Communications endpoint, such as Microsoft Office Communicator, running on the user's computer, or Office Communicator Phone Edition, running on a supported IP phone device. Thus, in most cases, the user's primary dial plan must be the same SIP URI dial plan used with Lync Server and Office Communications Server. But if the user requires more extension numbers, you shouldn't add another secondary extension to the primary dial plan. You must add a secondary dial plan and then add the secondary extension or EUM proxy address to the UM-enabled user.

Call Answering

Exchange Unified Messaging provides both of the following:

- **Call answering** Occurs when a user doesn't answer their phone and UM takes the call**.**
- **Outlook Voice Access** Used by users when they dial in to the Unified Messaging system to access to their mailbox.

Two configurations are used frequently:

- A UM-enabled user has two extension numbers (one primary, one secondary) in the primary dial plan. These extensions correspond to different phones on the user's desk and are connected to the same PBX. These different numbers are available to two separate audiences. In this configuration, the primary extension is the "general" work number and the secondary extension is the "task-specific" number, possibly a helpdesk line, or a dedicated fax number.
- A UM-enabled user spends a certain length of time, perhaps 3 weeks out of 4, in their company's main office and the rest of the time in another office at one of the company's remote locations. The two offices have different PBXs, and the extension numbers are unique to each PBX. In this example, the user is configured to have a primary extension in their primary dial plan on the main office PBX and a secondary extension in a secondary dial plan on the PBX of the other office.

In either configuration, voice messages or missed call notification messages that are generated by unanswered calls to either extension will be sent to the user's Inbox.

Outlook Voice Access

You may want UM-enabled users to be able to log on to Outlook Voice Access from any extension, primary or secondary. While this is possible, there may be some architectural restrictions that keep this from working identically from all extensions. To log on to Outlook Voice Access in the RTM version of Exchange 2010 or Exchange 2010 SP1, UM-enabled users must perform the following steps:

1. Call a UM pilot number (subscriber access number).
2. Key in their extension number if they're calling from another phone number.
3. Key in their PIN if they aren't enabled for Enterprise Voice and are calling from

a Unified Communications phone, Office Communicator or Lync Server.

Usage Scenarios

- **Single extension with Outlook Voice Access** If the user has a single primary extension, they must always call the pilot number for their primary UM dial plan. If they call from their extension number, they won't be prompted to enter the extension number, and step 2 of the preceding steps will be skipped.
- **Two extensions in the primary dial plan with Outlook Voice Access** If the user has only two extensions, primary and secondary, and both the primary and secondary extension are in the same UM dial plan, they must always call the pilot number of the dial plan. If they call from either the primary or secondary extension, they won't be prompted to enter the extension number, and step 2 of the preceding steps will be skipped. Outlook Voice Access features will work the same way, whichever extension is used to log on.
- **Extensions in the primary dial plan and in a secondary dial plan with Outlook Voice Access** If the user has only two extensions, primary and secondary, and both primary and secondary extensions are in different UM dial plans (primary and secondary); they should call the pilot number appropriate to their dial plan. From their primary extension, they should call the pilot number of the primary dial plan, and from their secondary extension, they should call the pilot number of the secondary dial plan. If they do this, they won't be prompted to enter the extension number, and step 2 of the preceding steps will be skipped.
  Outlook Voice Access features that don't involve outbound dialing (for example "Call the sender" or "Call the office") will work the same way, whichever extension is used to log on. However, Outlook Voice Access features that do require outbound dialing won't work as expected when the user logs on to the secondary dial plan unless the outbound dialing rules are exactly the same in both dial plans. For the behavior of outbound dialing to be exactly the same, you must ensure that the following properties are configured identically on the primary and secondary dial plans:
  - Dialing codes (trunk access, national, and international)
  - In-country or region dialing codes
  - Dialing rules
  - Dialing rule group names

A UM-enabled user is associated with a UM mailbox policy, and this UM mailbox policy is associated with the user's primary dial plan. The UM mailbox policy settings that are associated with the UM-enabled user's primary dial plan will be applied to the user. If a user is associated with a secondary dial plan with a second extension number in the secondary dial plan, the UM mailbox policy settings associated with the primary dial plan will still be applied. In Outlook Voice Access, the same UM mailbox policy settings associated with the primary dial plan are applied whether the user calls in to the primary dial plan or to a secondary dial plan.

The **AllowedInCountryOrRegionGroups and AllowedInternationalGroups** properties on the UM mailbox policy contain the names of groups of dialing rules that are configured on the **ConfiguredInCountryOrRegionGroups** and **ConfiguredInternationalGroups** properties of a UM dial plan. When a UM-enabled user calls in to Outlook Voice Access, the outbound calling rules from the UM mailbox policy associated with the primary or secondary dial plan will apply to calls the user makes, depending on whether the UM-enabled user has called in to the primary or secondary dial plan's subscriber access or pilot number.

For example, if a primary dial plan named "Contoso Dial Plan 1" has a dialing rule named "US and Canada" in its **ConfiguredInCountryOrRegionGroups** property, the UM mailbox policy "Contoso UM Policy 1" might also have "US and Canada" in its **AllowedInCountryOrRegionGroups** property. If you want to add a secondary extension in "Contoso Dial Plan 2" for a user in "Contoso UM Policy 2", you would have to ensure that the **ConfiguredInCountryOrRegionGroups** property of "Contoso Dial Plan 2" also

contains a rule named "US and Canada". Otherwise, if the user logs on to Outlook Voice Access from their secondary extension, UM won't be able to find a rule on the secondary dial plan named "US and Canada". If this happens, Unified Messaging will only allow the user to call numbers allowed to any caller to the secondary dial plan, which could be more restrictive.

Return to top

UM Features That Operate Differently for Secondary Dial Plans

There's a set of UM features that can use secondary dial plans but may not work correctly in certain situations. It's important that you understand how each of these features is affected when you configure UM-enabled users to use a secondary dial plan.

Play on Phone

In Microsoft Outlook 2010 or Office Outlook Web App in Exchange 2010, Play on Phone uses the IP gateway that's associated with the user's primary dial plan to make the outbound call. It applies dialing rules from the primary dial plan and the UM mailbox policy that's associated with the user's mailbox.

Directory Search (Outlook Voice Access)

A search of the directory for a user who's been authenticated will follow these rules:

- The ability to search for a user and then leave a voice message or call an Exchange 2010 user will be available only if the user conducting the search is UM enabled and has a primary extension on the same dial plan as the user that's being called. If so, a search by name, alias, and primary extension will locate the user. However, searching by using the secondary extension won't locate the user.
- If the user being searched for is UM enabled and has a secondary extension on the called dial plan, then a search by name, alias, and secondary extension will find the user. However, although options to leave a voice message and call the contact will be offered, the call contact option won't succeed. In this case, a search by primary extension won't find the user.
- To find and be able to either call or leave a voice message for the user they're searching for, the UM-enabled user should use Outlook Voice Access through their primary dial plan's pilot number and search by name, alias, or primary extension. If the searched-for user is called using the secondary dial plan's pilot number, the user will only be found if the search is made by name, alias, or secondary extension. If the primary extension is used, the only option that will be available is for the user to leave a voice mail.

Directory Search (Subscriber Access)

A search of the directory for a user who hasn't been authenticated will follow these rules:

- The user being searched for will be found and the option to leave a voice message or call the user will be offered only if the user is UM enabled and has a primary extension on the called dial plan. If so, a search by name, alias, and primary extension will find the user. However, a search by secondary extension won't find the user.
- If the user being searched for is UM enabled, has a secondary extension on the called dial plan, and the option **Features** > **Callers can contact** > **Anyone on the default global address list** is selected on the called dial plan, then a search by name, alias, and secondary extension will find them. However, the option to leave voice mail will be offered to the caller, and there will be no option to call them.
- To find and be able to either call or leave a voice message for a user, the caller

must call the pilot number of the user's primary dial plan and search by name, alias, or the user's secondary extension. If the user's secondary pilot number is called, they will only be found if the **Callers can contact** option is set to **global address list (GAL)**. In this case, only the option to leave a voice message will be provided.

Call the Sender (Outlook Voice Access)

When a user calls in to Outlook Voice Access and chooses the option to Call the Sender, they can send either an e-mail message or a voice mail message to a UM-enabled user. The options available depend on whether the caller is associated with the same dial plan as the sender they're calling. Calls to a UM-enabled user when the caller dials in to a subscriber access number, pilot number, or Outlook Voice Access number and the caller is authenticated will follow these rules:

- **E-mail messages** If the sender of the e-mail message is a UM-enabled user, choosing the option to call the sender will result in a call to the sender's primary extension that's configured on the user's primary dial plan. In the case where the sender's primary extension is on a dial plan that's different from the caller's, the prompt to "Call the Sender" will only be provided if there's a business, home, or mobile phone configured for the sender in Active Directory and the dialing rules are configured to allow the call.
- **Voice mail messages** If the caller is a UM-enabled user, the option to call the sender will always result in a call to the extension that the sender uses to leave their voice message. If this extension has a number of digits different from the called dial plan, the prompt to call the sender won't be provided unless there are dialing rules in place that would permit the call. For example:
  - The "Call the sender" option will be offered if the sender uses an extension on the dial plan that was used to send the voice message.
  - The "Call the sender" option will be played if the sender uses an extension from a different dial plan than the dial plan that's used with Outlook Voice Access to send the voice message and both dial plans have the same number of digits. The success of the call will depend on whether the IP gateway and PBX infrastructure permit the call transfer.
  - The "Call the sender" option won't be played if the sender uses an extension from a different dial plan than the dial plan that's used with Outlook Voice Access to send the voice message, the dial plans have a different number of digits, and there are no outdialing rules that match the sender's extension.

Return to top

1.9.1.3.22 Understanding Client Features in Unified Messaging

Understanding Client Features in Unified Messaging

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Features >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

This topic describes Unified Messaging (UM) client features that give UM-enabled users access to their e-mail and UM messages in their Microsoft Exchange Server 2010 mailbox. The Unified Messaging client capabilities enable you to provide users simplified voice mail and e-mail access options and an improved overall user experience.

Contents

Outlook Voice Access

Outlook Voice Access is an Exchange 2010 feature that enables subscribers to retrieve e-mail messages from their individual mailbox using an analog, digital, or mobile telephone. They can then interact with their mailbox using touchtone or voice commands. When UM-enabled users access their Exchange 2010 mailbox using a telephone, they are presented with a series of voice prompts. These voice prompts help users navigate the Unified Messaging system and enable users to access their Exchange 2010 Inbox. Outlook Voice Access lets users retrieve, listen to, reply to, create, and forward voice or e-mail messages and listen to or change calendar information. For a copy of the Microsoft Exchange Server 2010 Unified Messaging Outlook Voice Access Quick Reference Guide, visit the Microsoft Download Center.

Important:

If you need to access the e-mail message after you delete it using Outlook Voice Access, you can use Outlook Web App or Microsoft Outlook to move the e-mail message back into the appropriate folder from the Deleted Items folder. You can't use Outlook Voice Access to access the Deleted Items folder.

Unified Messaging and ActiveSync Clients

The Microsoft Exchange ActiveSync protocol is used to connect mobile clients, such as those found on Internet capable mobile phones, to an Exchange 2010 server and mailbox. There are many mobile phones that users can use to access their Exchange 2010 mailbox and view e-mail messages, view and change calendar information, and listen to their voice messages. Many wireless and mobile phones used today enable users to continually be connected to their Exchange 2010 mailbox.

Return to top

Unified Messaging Integration with Outlook 2007 and Outlook 2010 Clients

Using Microsoft Office Outlook 2007, users can access their individual Exchange 2010 mailbox and view e-mail messages in their Inbox, view and change calendar information, and listen to voice messages using a Microsoft Windows Media Player, which is embedded inside the e-mail messages on their portable device or computer. Using the Exchange 2010 client, users gain additional features, such as the Play on Phone functionality. For more information about the Outlook features for Exchange Unified Messaging, see Outlook 2007 Features for Exchange Unified Messaging.

Note:

When you install Outlook 2007 on a client computer, the Outlook 2007 Unified Messaging voice mail features are included. The Unified Messaging features for configuring voice mail are available only with Outlook 2007 and aren't available with earlier versions of Outlook.

Unified Messaging Integration with Outlook Web App Clients

Outlook Web App provides users with a set of Unified Messaging interfaces and tools comparable to a full-featured e-mail client like Exchange 2010. As in earlier versions, known as Outlook Web Access, users can access their Exchange 2010 mailbox using a compliant Web browser. However, similar to the Exchange 2010 e-mail client, Outlook Web App offers users a Windows Media Player embedded in the e-mail message, which can be used to listen to voice messages, and enables users to access other features such as Play on Phone.

Note:

When you use Exchange ActiveSync on a mobile phone, you can listen to the attached .wma file that contains the voice mail message. The advanced Unified Messaging features found in the Outlook Web App Premium client, such as the voice mail configuration options, aren't available in Outlook Web App Light.

Caution:

When you use the light version of Outlook Web App and Pocket Internet Explorer on a mobile phone, you may be able to listen to the .wma attachment in a voice message. However, this isn't a supported configuration.

1.9.1.3.22.1 Understanding Outlook Voice Access

Understanding Outlook Voice Access

Understanding Unified Messaging > Understanding Unified Messaging Features > Understanding Client Features in Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-30*

Outlook Voice Access lets Unified Messaging (UM)–enabled users access their Microsoft Exchange Server 2010 or Exchange Server 2007 mailbox using analog, digital, or cellular telephones.

A subscriber is an internal business user or network user who's enabled for Exchange 2010 Unified Messaging. Subscriber access is used by users to access their individual mailboxes to retrieve e-mail, voice messages, contacts, and calendaring information. Outlook Voice Access is an Exchange 2010 Unified Messaging feature that lets subscribers access their Exchange 2010 mailbox.

Outlook Voice Access Overview

In Exchange Server 2007 and also in Exchange 2010, a UM-enabled user can call in to an internal or external telephone number that's configured on a UM dial plan to access their mailbox and use the menu system found in Outlook Voice Access. Using this menu system, UM-enabled users can read e-mail, listen to voice messages, interact with their Outlook calendar, access their personal contacts, and perform tasks such as configuring their Outlook Voice Access PIN or recording their voice mail greetings.

Outlook Voice Access Interfaces

There are two Exchange 2010 Unified Messaging user interfaces available to subscribers:

the telephone user interface (TUI) and the voice user interface (VUI). These two interfaces together are called Outlook Voice Access. For a list of all the commands that are available in Outlook Voice Access, see Outlook Voice Access Command Reference.

You can prevent users from receiving voice mail, but let them retain the ability to access their Exchange 2010 mailbox using Outlook Voice Access. You can enable users for Unified Messaging and configure the users' mailbox with an extension number that isn't currently being used by another user in the organization.

Important:

For the VUI or Automatic Speech Recognition (ASR) to be used for subscriber access, it must be enabled on the UM dial plan to enable the VUI functionality as described in the scenarios in the following section.

For a copy of the Microsoft Exchange 2010 Unified Messaging Outlook Voice Access Quick Start Guide, see the Microsoft Download Center. You can also see Outlook Voice Access Quick Start Guide for a copy.

Outlook Voice Access Scenarios

The following scenarios demonstrate how Outlook Voice Access can be used for subscriber access from a telephone:

- **Access e-mail** An Outlook Voice Access user places a call to the subscriber access number from a telephone and wants to access their e-mail. The voice prompt says, "Welcome. You're connected to Microsoft Exchange. To access your mailbox, please enter your extension. To contact someone, press the # key." After the user enters a mailbox extension number, the voice prompt says, "Please enter your PIN and press the # key." After the user enters a PIN, the voice prompt says, "You have 2 new voice mails, 10 new e-mail messages, and your next meeting is at 10:00 A.M. Please say voice mail, e-mail, calendar, personal contacts, directory, or personal options." When the user says "E-mail," Unified Messaging reads the message header and then the name, subject, time, and priority for the messages that are in the subscriber's mailbox.
- **Access calendar** An Outlook Voice Access user places a call to the subscriber access number from a telephone and wants to access their calendar. The voice prompt says, "Welcome. You're connected to Microsoft Exchange. To access your mailbox, please enter your extension. To contact someone, press the # key." After the user enters a mailbox extension, the voice prompt says, "Please enter your PIN and press the # key." After the user enters a PIN, the voice prompt says, "You have 2 new voice mails, 10 new e-mail messages, and your next meeting is at 10:00 A.M. Please say voice mail, e-mail, calendar, personal contacts, directory, or personal options." When the user says "Calendar," Unified Messaging says, "Sure, and which day should I open?" The user says, "Today's calendar." Unified Messaging responds by saying, "Opening today's calendar." Unified Messaging reads each calendar appointment for that day for the user.

  Note:

  If a Unified Messaging server encounters a corrupted calendar item in a user's mailbox, it will fail to read the item, but will return the caller to the Outlook Voice Access main menu and will skip reading any additional meetings that may be scheduled for the rest of the day.

- **Access voice mail** An Outlook Voice Access user places a call to the subscriber access number from a telephone and wants to access voice mail. The voice prompt says, "Welcome. You're connected to Microsoft Exchange. To access your mailbox, please enter your extension. To contact someone, press the # key." After the user enters a mailbox extension number, the voice prompt says, "Please enter your PIN and press the # key." After the user

enters a PIN, the voice prompt says, "You have 2 new voice mails, 10 new e-mail messages, and your next meeting is at 10:00 A.M. Please say voice mail, e-mail, calendar, personal contacts, directory, or personal options." The user says "Voice mail" and Unified Messaging reads the message header and then the name, subject, time, and priority for the voice messages that are in the user's mailbox.

Note:
If speech recognition is enabled, users can access their UM-enabled mailbox using speech input. However, subscribers can also use touchtone, also known as dual tone multi-frequency (DTMF), by pressing 0. Speech recognition isn't enabled for PIN input.

- **Locate an e-mail alias** An Outlook Voice Access user places a call to the subscriber access number from a telephone and wants to locate a person in the directory by spelling their e-mail alias. The voice prompt says, "Welcome. You're connected to Microsoft Exchange. To contact someone, press the # key." The user presses the # key, and then spells the name of the person using touchtone inputs.

Note:
The directory search feature with subscriber access isn't speech-enabled. Users will be able to spell the name of the person who they want to contact only by using touchtone inputs.

Important:
In some companies (especially in East Asia), office telephones may not have letters on the keys of the telephone. This makes the spell-the-name feature that uses the touchtone interface almost impossible to use without a working knowledge of the key mappings. By default, Exchange 2010 Unified Messaging uses the E.161 key mapping. For example, 2=ABC, 3=DEF, 4=GHI, 5=JKL, 6=MNO, 7=PQRS, 8=TUV, 9=WXYZ.

When inputting a combination of letters and numbers, for example, Mike1092, the numeric digits are mapped to themselves. For an e-mail alias of Mike1092 to be entered correctly, the user must press the numbers 64531092. Also, for characters other than A-Z and 0-9, there won't be a telephone key equivalent. Therefore, these characters shouldn't be entered. For example, the e-mail alias mike.wilson would be entered as 6453945766. Even though there are 11 characters to be input, only 10 digits are entered by the user because there's no digit equivalent for the period (.). For details, seeOutlook Voice Access User Scenarios.

Public and Personal Contact Groups

You can use Outlook Voice Access to send or forward a voice message, an e-mail message, or a meeting request. You can send or forward the message or meeting request to any of the following:

- A person in your personal Contacts folder
- A person in your organization’s shared address list
- A group you’ve created in your personal Contacts folder
- A public group included in your organization’s shared address list

You can send messages and meeting requests using the voice user interface (VUI) (if automatic speech recognition has been turned on by your voice mail administrator) or using touchtone inputs on your telephone keypad. You can also use Outlook Voice Access to listen to details about a group, including the members included in the group.

Note:
When sending a message to a public group in your shared address list, or a group in your personal Contacts folder that doesn’t include any members, the voice mail system won't give you the option to send or forward the message or meeting request. However, if you try to add a group as one of the recipients of a message or meeting request that you are

creating over the phone, the voice mail system will not add the group and say "The message could not be sent because the contact does not appear to have a valid e-mail address" because the group doesn't contain any valid e-mail addresses.

Choosing a Language

You can't change the language that Outlook Voice Access uses to speak to you and to reply to you when you speak to it. The voice mail system will try to find and use the best match for the language you chose when you first signed in to Microsoft Office Outlook Web App or the language that you've chosen on the Regional tab in Outlook Web App. If the language you choose isn't supported by Outlook Voice Access, the voice mail system will use the same language that callers hear when they're prompted to leave a voice message for you.

Outlook Voice Access User Scenarios

Understanding Unified Messaging Features > Understanding Client Features in Unified Messaging > Understanding Outlook Voice Access >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-11*

Outlook Voice Access is a feature in Microsoft Exchange Server 2010 Unified Messaging (UM) that enables users to retrieve e-mail messages from their mailbox using an analog, digital, or mobile telephone. They can then interact with their mailbox using touchtone or voice commands.

The Outlook Voice Access Quick Reference Guide includes a graphic representation of all the Outlook Voice Access menu options and how to navigate the menu system. To download a copy of the Quick Reference Guide, see the Microsoft Download Center.

When UM-enabled users access their Exchange 2010 mailbox using a telephone, they are presented with a series of voice prompts. These voice prompts help them navigate the Unified Messaging system and enable them to access their mailbox. Outlook Voice Access lets users do the following:

- Retrieve, listen to, reply to, create, and forward voice or e-mail messages.
- Listen to or change calendar information.
- Change personal options, such as changing a PIN, or call or send a voice message to a personal contact.

Contents

Reading and Reviewing E-Mail

Users can listen to, reply to, create, and forward unread e-mail messages using the telephone. For example, if users are expecting an important e-mail message, and do not have access to the Internet, they can use a mobile phone to dial the subscriber access number or the number that is used for Outlook Voice Access. After users enter their extension number, enter their PIN, and then say, "E-mail," the Unified Messaging server

will access the users' mailbox and read their unread e-mail. While the Unified Messaging server reads an e-mail message, the user can say one of the following:

- "Reply" to reply to the sender.
- "Reply all" to reply to all recipients on the e-mail message.
- "Forward" to forward the e-mail message to another user.
- "Flag" to flag the message for follow up.
- "Hide" to hide the conversation.

Listen to E-Mail Messages

To listen to e-mail messages using the voice user interface (VUI), users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Say "E-mail" to access e-mail.
2. The Unified Messaging server will read the name, subject, time, and priority of the first unread e-mail message.
3. The user can then say one of the following options:
   - "Next message" to mark the message as Read and go to the next e-mail message.
   - "Mark unread" to keep the message marked as Unread and go to the next message.
   - "End" to jump to the end of the message.
   - "Delete" to delete the message.

This process is shown in the following figure.

To listen to e-mail messages using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 2 to access e-mail.
2. The Unified Messaging server will read the name, subject, time, and priority of the first unread e-mail message.
3. The user can then press one of the following options:
   - Pound (#) key to mark the message as Read and go to the next e-mail message.
   - 9 to keep the message marked as Unread and go to the next message.
   - 33 to jump to the end of the message.
   - 7 to delete the message.

This process is shown in the following figure.

Return to top

Reply to E-Mail Messages

To listen to e-mail messages and then reply using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Say "E-mail" to access e-mail.
2. Say "Next message" repeatedly until they reach the e-mail message to which they want to reply.
3. Listen to the message or say "End" to go to the end of the message.

4. Say one of the following:
   - "Reply" to reply to the sender.
   - "Reply all" to reply to the sender and all other recipients.
   - "Forward" to forward the message to another user or group.
5. Record a reply and then hang up, remain silent, or press any key. To accept the reply message and send it, say "Send it."

This process is shown in the following figure.

To listen to e-mail messages and then reply using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 2 to access e-mail.
2. Press # repeatedly until they user reach the e-mail message to which they want to reply. Press 9 to mark the message as Unread.
3. Listen to the message or press 33 to go to the end of the message.
4. Press 8 to reply to the sender, press 88 to reply to the sender and all other recipients, or press 6 to forward the message to another user or group.
5. Record a reply, and then press #. To accept the reply message and send it, press 1.

This process is shown in the following figure.

Return to top

Listen to the Next Unread E-Mail Message

To listen to an e-mail message and then go to the next unread message using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Say "E-mail."
2. Say "Next unread." Say "Mark unread" if they want to mark the message as Unread.

This process is shown in the following figure.

To listen to an e-mail message and then go to the next Unread message using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 2 to access e-mail.
2. Press ## to listen to the next unread message. Press 9 to mark the message as Unread.

This process is shown in the following figure.

Return to top

Flag an E-Mail Message for Follow Up

To listen to e-mail messages and flag messages for follow up using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

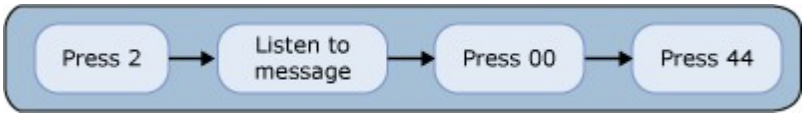
1. Say "E-mail" to access e-mail.
2. Say "Next message" repeatedly until they reach the e-mail message that they want to flag for follow up. Say "Mark unread" to mark the message as Unread.
3. Listen to the message or say "End" to go to the end of the message.
4. Say "Flag" or "Flag for follow up" to flag the message for follow up.

This process is shown in the following figure.

To listen to e-mail messages and flag messages for follow up using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 2 to access e-mail.
2. Press # repeatedly until they reach the e-mail message that they want to flag for follow up. Press 9 to mark the message as Unread.
3. Listen to the message or press 33 to go to the end of the message.
4. Press 0 (zero) twice to access more options.
5. Press 44 to flag the message for follow up.

This process is shown in the following figure.



Return to top

Hide a Conversation

To listen to e-mail messages and hide a conversation so that Unified Messaging will not continue to read other e-mail messages that are in the same e-mail conversation using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Say "E-mail" to open e-mail.
2. Say "Next message" repeatedly until they reach the e-mail message that they want. Say "Mark unread" to mark the message as Unread.
3. Listen to the message or say "End" to go to the end of the message.
4. Say "Hide" or "Hide conversation" to hide the conversation. The next e-mail message will be read.

This process is shown in the following figure.

To listen to e-mail messages and hide a conversation so that Unified Messaging will not continue to read other e-mail messages that are in the same e-mail conversation using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 2 to access e-mail.
2. Press # until they reach the e-mail message that they want to hide. Press 9 to mark the message as Unread.
3. Listen to the message or press 33 to go to the end of the message.
4. Press 99 to hide the conversation. The next e-mail message will be read.

This process is shown in the following figure.

Note:
When a conversation is hidden, it is hidden only for the current session. If users log off and then log on to their mailbox again, Unified Messaging will read e-mail messages that are in the same conversation.

Return to top

Managing Calendar Items

Users can listen to, reply to, create, and forward items in their calendar over the telephone.

For example, a user has a meeting at 10:00 A.M. However, because of some unexpected delays, the user will be 15 minutes late. The user can inform the other meeting attendees by calling the telephone number for Outlook Voice Access, logging on to the Exchange 2010 mailbox, and then accessing the list of meetings for that day in the calendar. After Unified Messaging reads the meeting request for the 10:00 A.M. meeting, the user can use the *I'll be late* feature to inform all the meeting attendees that the user will be 15 minutes late. Each attendee will receive an e-mail message that informs them that the user will be 15 minutes late. The user also has the option to attach a voice mail message.

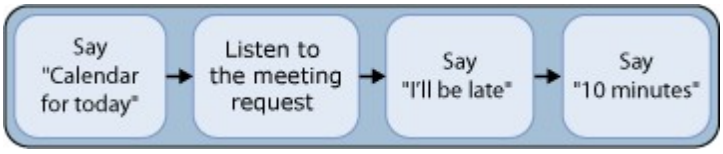
In another example, a user may have an important client who decides to schedule an all-day meeting on very short notice. The user must cancel all other meetings for that day in the simplest possible way. Using the *Clear my calendar* feature, users can quickly and easily clear their calendar for the whole day.

Send an I'll Be Late Message

To send an I'll be late message to meeting participants using the VUI, users must dial the Unified Messaging subscriber access number, enter their extension number and PIN, and then do the following:

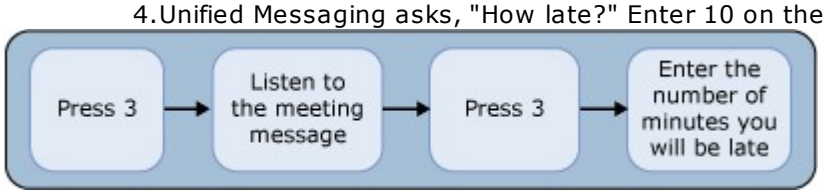
1. Say "Calendar for today."
2. Listen to the meeting request.
3. After the meeting request has been read, say "I'll be late."
4. Unified Messaging asks, "How late?" Say "10 minutes."
5. Unified Messaging asks, "Do you want to record a message?" Say "Yes." Record the message, and then say "Send it."

This process is shown in the following figure.



To send an I'll be late message to meeting participants using the touchtone interface, users must dial the Unified Messaging subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 3 to access their calendar.
2. Listen to the meeting requests to locate the meeting for which to send an I'll be late message.
3. After the meeting request has been read, press 3.
4. Unified Messaging asks, "How late?" Enter 10 on the telephone key pad.



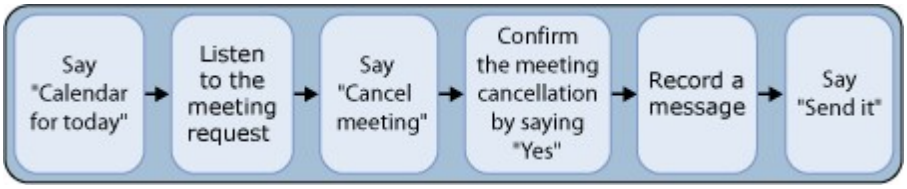
Return to top

Cancel a Meeting

To cancel a meeting, the user must be the meeting organizer. To cancel the meeting using the VUI, meeting organizers must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Say "Calendar for today" to access their calendar.
2. Listen to the meeting request.
3. After the meeting request has been read, say "Cancel meeting."
4. Confirm the meeting cancellation by saying "Yes."
5. After Unified Messaging asks whether the meeting organizer wants to attach a recorded message, say "Yes." Record the message, and then say "Send it."

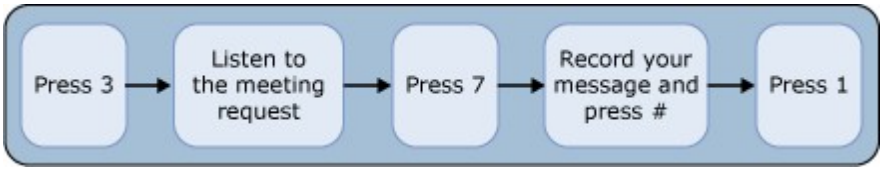
This process is shown in the following figure.



To cancel a meeting, the user must be the meeting organizer. To cancel the meeting using the touchtone interface, meeting organizers must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 3 to access their calendar.
2. Listen to the meeting requests to locate the meeting to cancel.
3. Press 7 to cancel the meeting.
4. If meeting organizers choose to send a voice message, they can then press one of the following options:
   - # to stop recording the message.
   - 1 to accept the recorded message.

This process is shown in the following figure.



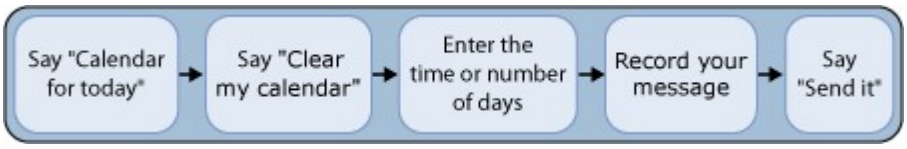
Return to top

Clear a Calendar

To clear their calendar using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Say "Calendar for today" to access their calendar.
2. Say "Clear my calendar."
3. Enter the time or the number of days to be cleared.
4. After Unified Messaging asks whether they want to attach a recorded voice message, they say "Yes," record the message, and then say "Send it." If they do not want to send an attached recorded voice message, they say "No."

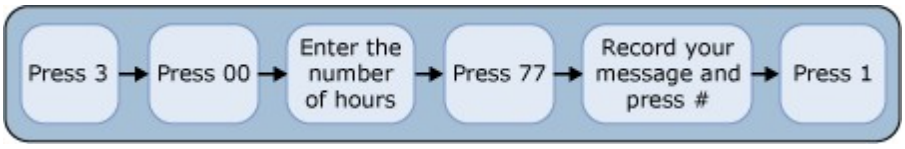
This process is shown in the following figure.



To clear their calendar using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 3 to access their calendar.
2. Press 00 to go to the More Options menu.
3. Press 77 to clear their calendar.
4. Enter the number of hours to clear from the calendar.
5. If users choose to send a voice message, they can do one of the following:
   - Press # to not send a voice message
   - Record the voice message when prompted, press # to stop recording the message, and then press 1 to accept the recorded message.

This process is shown in the following figure.



Return to top

Accept a Meeting Request

To accept a meeting request using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Say "E-mail" to access their e-mail.
2. Listen to the e-mail message that contains a meeting request.
3. Say "Accept" to accept the meeting request.

This process is shown in the following figure.

To accept a meeting request using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 2 to access their e-mail.
2. Listen to the e-mail message that contains a meeting request.
3. Press 4 to accept the meeting request.

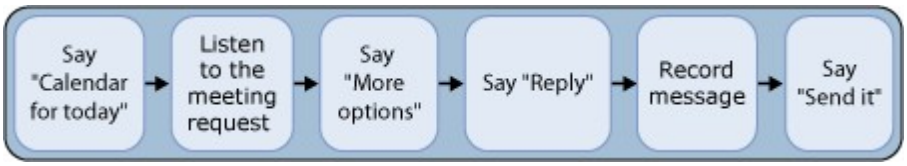
This process is shown in the following figure.

Reply to a Meeting Request

To reply to a meeting request using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

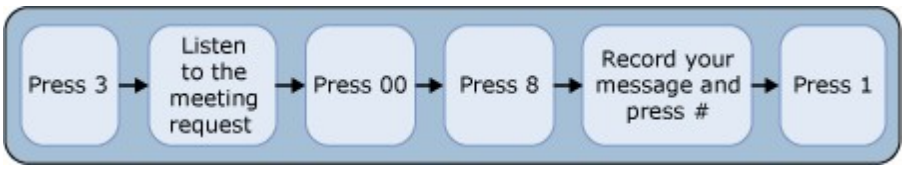
1. Say "Calendar for today."
2. Listen to the meeting requests to locate the meeting request to reply to.
3. Say "More options" to open the More Options menu.
4. Say "Reply" to reply to the meeting organizer.
5. Record a message.
6. Say "Send it."

This process is shown in the following figure.



1. To reply to a meeting request using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:
2. Press 3 to access their calendar.
3. Listen to the meeting requests to locate the meeting request to reply to.
4. Press 00 for more options.
5. Press 8 to reply to the meeting organizer.
6. Record a message, and then press #.
7. Press 1 to accept the recording and send the message.

This process is shown in the following figure.



Return to top

Managing Personal Options and Contacts

Users can manage their personal options and contacts using Outlook Voice Access. They can:

- Call a personal contact.
- Locate and call a user in the directory.
- Configure personal options, such as changing their PIN over the telephone.

When users first set up their mailbox, they must create personal and Away greetings that callers will hear when users are unable to answer their telephone. If, for example, users realize that they have forgotten to turn on an Away voice greeting that will give callers an alternative number to call if they have an immediate issue, users can use Outlook Voice Access to access their personal options and record and turn on an Away greeting from any telephone.

If a user has to contact an account manager with important information about a client, the user can call the number that is used for Outlook Voice Access, use the directory search feature to locate the account manager, and then place the call.

Note:

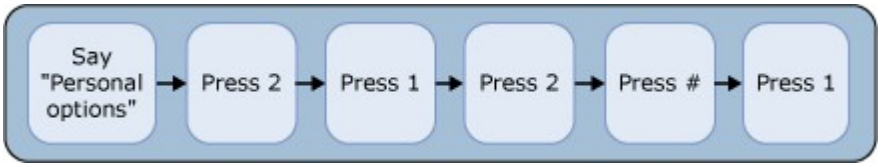
When users access the Personal Options menu, they must use the touchtone interface.

Record a Personal Greeting

To record a personal greeting using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

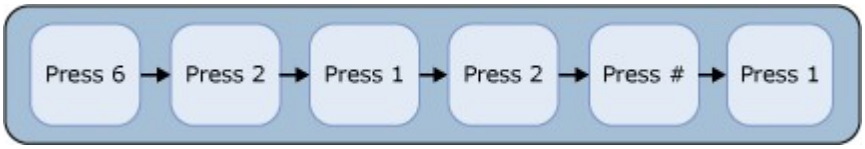
1. Say "Personal options" to access the Personal Options menu.
2. Press 2 to record greetings.
3. Press 1 to record a personal greeting.
4. Press # to stop recording the personal greeting.
5. If they have to re-record their personal greeting, they should press 2.
6. Press 1 to accept the personal greeting.

This process is shown in the following figure.



1. To record a personal greeting using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:
2. Press 6 to access personal options.
3. Press 2 to record greetings.
4. Press 1 to record a personal greeting.
5. Press 2 to re-record the personal greeting.
6. Press # to stop recording the personal greeting.
7. Press 1 to accept the personal greeting.

This process is shown in the following figure.



Note:

When users change their telephone greeting, they are also given the option to turn on or

off their e-mail automatic reply message.

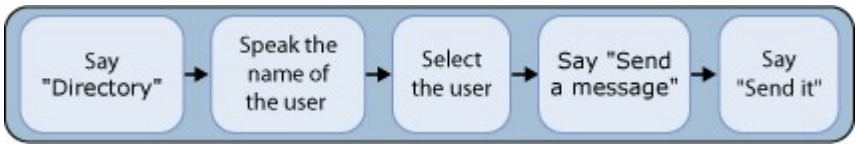
Return to top

Send a Voice Message to a User

Users can locate and send a voice message to another UM-enabled user. To send a voice message to another user using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

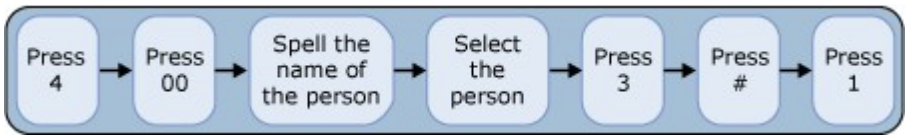
1. Say "Directory."
2. Say the name of the person to locate.
3. Select the correct person from the list.
4. Say "Send a message," and then record the voice message.
5. Say "Send it" to send the message.

This process is shown in the following figure.



1. Users can locate and send a voice message to another UM-enabled user. To send a voice message to another user using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:
2. Press 4 to search for a contact.
3. Press 00 to locate the person in the directory.
4. Spell the name of the person to locate using the telephone keypad.
5. Select the correct person from the list.
6. Press 3 to send a voice message to the person.
7. Record the voice message, and then press # to stop recording.
8. Press 1 to accept the voice message and send it.

This process is shown in the following figure.

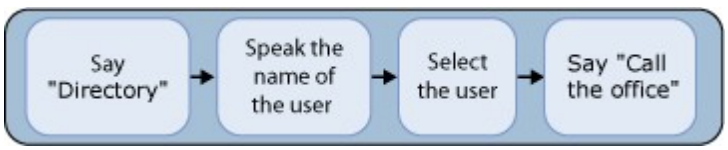


Locate and Call a User in the Directory

To locate and call a user in the directory using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Say "Directory."
2. Say the name of the person to locate.
3. Select the correct person from the list.
4. Say "Call the office."

This process is shown in the following figure.

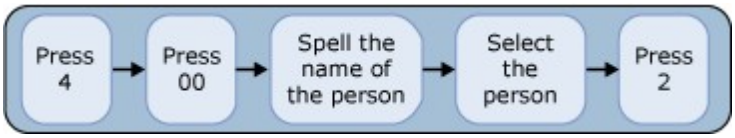


To locate and call a user in the directory using the touchtone interface, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Press 4 to access personal contacts.

2. Press 00 to locate a person in the directory.
3. Spell the name of the person to locate using the telephone keypad.
4. Select the correct person from the list.

This process is shown in the following figure.



Return to top

Change a PIN

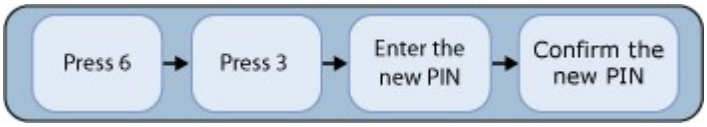
To change their PIN using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:

1. Say "Personal options."
2. Press 3 to change the PIN.
3. Enter the new PIN, and then press #.
4. Press # to confirm the new PIN.

This process is shown in the following figure.

1. To change their PIN using the VUI, users must dial the UM subscriber access number, enter their extension number and PIN, and then do the following:
2. Press 6 to change personal options.
3. Press 3 to change the PIN.
4. Enter the new PIN, and then press #.
5. Press # to confirm the new PIN.

This process is shown in the following figure.



Outlook Voice Access Quick Start Guide

Understanding Unified Messaging Features > Understanding Client Features in Unified Messaging > Understanding Outlook Voice Access >

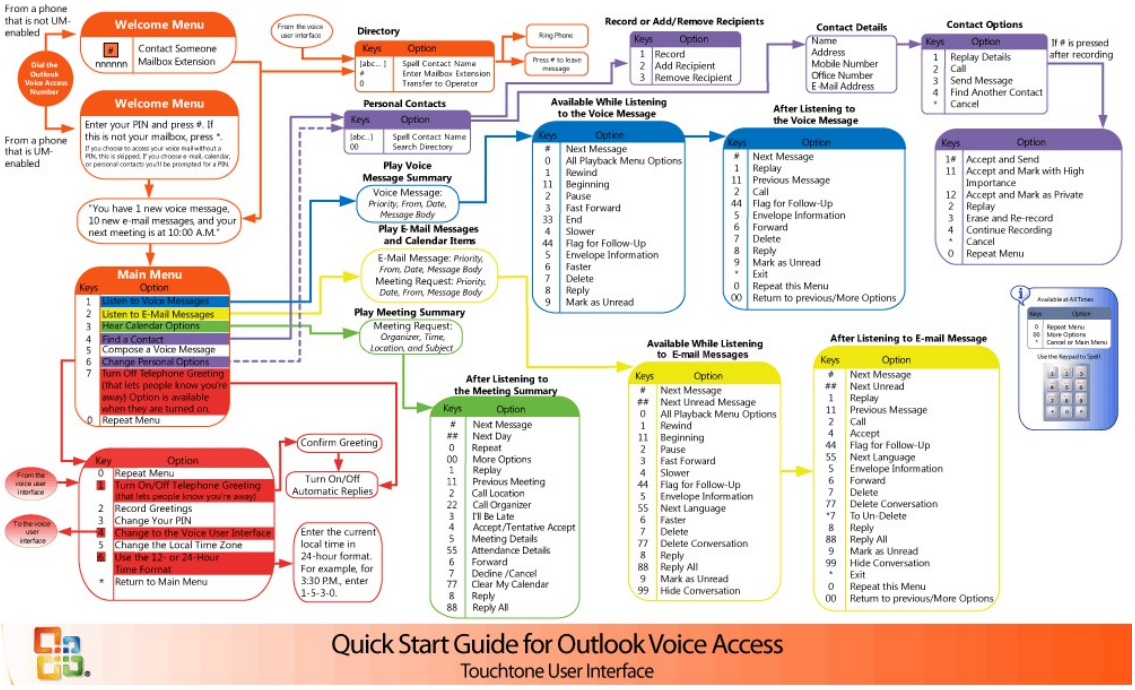
Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

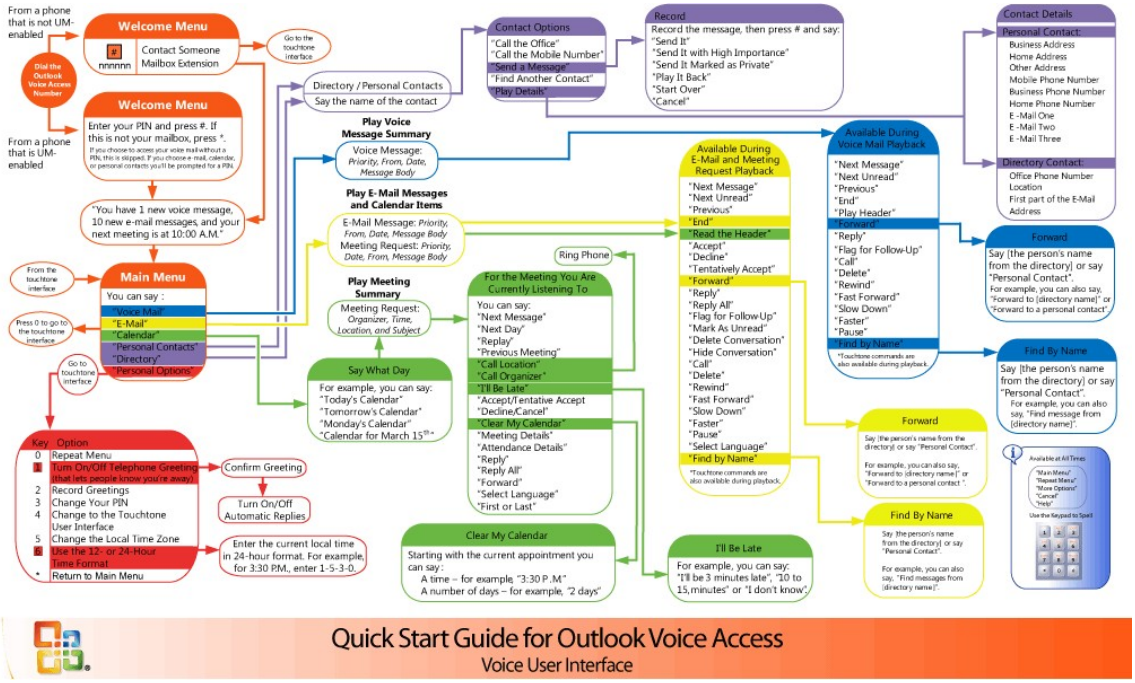
Topic Last Modified: *2009-09-15*

Outlook Voice Access lets Unified Messaging (UM)-enabled users access their Microsoft Exchange Server 2010 mailbox using analog, digital, or mobile telephones. Using the menu system found in Outlook Voice Access, UM-enabled users can read e-mail, listen to voice messages, interact with their Microsoft Outlook calendar, access their personal contacts, and manage personal options, for example, configuring their Outlook Voice Access PIN or recording their voice mail recordings. This quick start guide shows the navigation tree and the options that are available to UM-enabled users when they use Outlook Voice Access.

Outlook Voice Access Quick Start Guide

The following figures illustrate the touchtone interface and Voice User Interface (VUI) commands and menus that are used with Outlook Voice Access.





You can download a printable version of the Outlook Voice Access Quick Start Guide for Exchange 2010 Unified Messaging by visiting the Microsoft Download Center.

For More Information

- For more information about common user scenarios in Exchange 2010 Unified Messaging, see Outlook Voice Access User Scenarios.
- For more information about client features in Exchange 2010 Unified Messaging, see Understanding Client Features in Unified Messaging.
- For more information about subscriber access in Exchange 2010 Unified Messaging, see Understanding Unified Messaging Subscriber Access.
- For more information about the voice prompts that are used with subscriber access in Exchange 2010 Unified Messaging, see Understanding Unified Messaging Audio Prompts.

Outlook Voice Access Command Reference

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Outlook Voice Access lets Unified Messaging (UM)-enabled users access their Microsoft Exchange Server 2010 mailbox using analog, digital, or mobile telephones. Using the menu system found in Outlook Voice Access, UM-enabled users can read e-mail, listen to voice messages, interact with their Outlook calendar, access their personal contacts, and manage personal options such as configuring their Outlook Voice Access PIN or recording their voice mail recordings. This topic contains a list of the commands and how they are used by Outlook Voice Access users when they call in to a subscriber access number to access their Exchange 2010 mailbox.

Outlook Voice Access User Interfaces

There are two Exchange 2010 Unified Messaging user interfaces available to subscribers: the Telephone User Interface (TUI) and the Voice User Interface (VUI). In Exchange 2010, these two interfaces together are called Outlook Voice Access. Outlook Voice Access can be used when subscribers access the Unified Messaging system from an external or internal telephone to access their personal e-mail, voice messages, contacts, and calendaring information in their Exchange 2010 mailbox.

For more information about the user interfaces that are used by Outlook Voice Access users, see the following topics:

- Understanding the DTMF Interface
- Understanding Automatic Speech Recognition Directory Lookups

E-Mail and Voice Mail Commands Reference

As an Outlook Voice Access user, when you dial in to a subscriber access number, you are presented with menu options that enable you to access your Exchange 2010 mailbox and manage your e-mail and voice mail. The following table lists the commands that are available for managing your e-mail and voice mail.

E-mail and voice mail commands

Voice command	Touchtone command	Description
"Play"		Plays the current e-mail or voice mail message.
"Next"	#	Reads the next e-mail or voice mail message.
"Next unread"	00 followed by ##	Reads the next unread e-mail message. Available only for e-mail.
"Delete"	7	Deletes the current e-mail or voice mail message.
"Reply"	8	Replies to the user who sent the current e-mail or voice mail message.
"Reply all"	00 followed by 88	Replies to the user of the current e-mail message. Not an available option for voice mail messages.
"Mark as unread"	9	Marks the e-mail message as Unread.
"End"	33	Stops reading and goes to the end of the current e-mail or voice mail message.
"More options"	00	Opens the More Options menu.
"Previous"	00 followed by 11	Reads the previous e-mail or voice mail message.
"Read the header"		Reads the header of the e-mail or voice mail message.
"Call sender"	00 followed by 2	Places a call to the user who sent the current e-mail or voice mail message.
"Forward"	00 followed by 6	Forwards the current e-mail or voice mail message to other e-mail recipients or groups.
"Flag for follow up"	00 followed by 44	Marks or flags the current e-mail or voice mail message for follow up.
"Find by name"		Uses the user's name to locate e-mail or voice mail messages in the user's mailbox.
"Delete conversation"	00 followed by 77	Deletes all the e-mail messages that are associated with an e-mail

		conversation. Available only for e-mail.
"Hide conversation"	00 followed by 99	Hides additional e-mail messages that are contained within the same e-mail conversation. Available only for e-mail.
"Envelope information"	00 followed by 5	Reads the envelope information for the e-mail or voice mail message.
"Select language"	00 followed by 55	Lets you select the language in which you want the e-mail or voice mail message to be read.
"Rewind" or "Repeat"	1	Rewinds or repeats the current e-mail or voice mail message. Available only while the message is being played.
"Pause"	2	Pauses the current e-mail or voice mail message. Available only while the message is being played.
"Fast forward"	3	Fast forwards the current e-mail or voice mail message. Available only while the message is being played.
"Slow down"	4	Plays or reads the current e-mail or voice mail message more slowly. Available only while the message is being played.
"Faster"	6	Plays or reads the current e-mail or voice mail message faster. Available only while the message is being played.
"Previous"	11	Reads the previous e-mail message from the beginning. Available only for e-mail.
"Replay"	00 followed by 1	Replays the current e-mail or voice mail message.
"Repeat"	0	Repeats the current menu options.
"Main menu"	*	Exits to the main menu.

Important:

If you need to access the e-mail message after you delete it using Outlook Voice Access, you can use Outlook Web App or Outlook to move the e-mail message back into the appropriate folder from the Deleted Items folder. You cannot use Outlook Voice Access to access the Deleted Items folder.

Calendar Options Command Reference

As an Outlook Voice Access user, when you dial in to a subscriber access number, you are presented with menu options that enable you to access your Exchange 2010 mailbox and manage your calendar. The following table lists the commands that are available for managing your calendar.

Calendar commands

Voice command	Touchtone command	Description
"Next"	#	Reads the next calendar appointment.
"Next day"	##	Opens and reads the calendar appointments for the next day.
"Repeat"	0	Repeats the menu options that are available. Or, if you are using the VUI, the system reads the calendar appointment again.
"More options"	00	Plays the more calendar options menu.
"Repeat"	1	Reads the calendar appointment again.
"Previous meeting"	00 followed by 11	Opens the previous meeting that is scheduled.
"Call location"	2	Calls the telephone number that is listed for the meeting location.
"Call organizer"	00 followed by 22	Calls the telephone number that is listed for the organizer of the meeting.
"I'll be late"	3	Sends an I'll be late message to all the meeting attendees.
"Accept" or "Tentative accept"	4	Accepts or tentatively accepts the meeting request.
"Meeting details"	5	Reads or plays back the details of the meeting that is currently being read.
"Attendance details"	00 followed by 55	Reads or plays the details of a meeting that is scheduled.
"Forward"	00 followed by 6	Forwards a meeting request for the meeting to another user.
"Decline" or "Cancel"	7	Declines or cancels the meeting request.
"Clear my calendar"	00 followed by 77	Clears your calendar for a

		specific time period for that day.
"Reply"	00 followed by 8	Replies to the meeting organizer.
"Reply all"	00 followed by 88	Replies to all the meeting attendees.
"Repeat menu"	5 followed by 0	Repeats the menu options that are available.
"Rewind"	5 followed by 1	Rewinds the meeting details.
	5 followed by 11	Returns to the beginning of the meeting details.
	5 followed by 2	Pauses and resumes playback of the meeting details.
"Fast forward"	5 followed by 3	Skips forward within the meeting details.
"End"	5 followed by 33	Skips to the end of the meeting details.
	5 followed by 4	Plays or reads the meeting details slower.
	5 followed by 55	Selects the language that will be used to read the meeting details.
	5 followed by 6	Plays or reads the meeting details faster.
"Main menu"	*	Exits to the main menu.

Personal Contacts Options Commands Reference

As an Outlook Voice Access user, when you dial in to a subscriber access number, you are presented with menu options that enable you to access your Exchange 2010 mailbox and call or send a message to a personal contact. If you choose to use the VUI, which is selected by default, and select the personal contacts menu option, the system will prompt you to input the name of the personal contact. However, to locate a user in the directory, you must use the touchtone or dual tone multi-frequency (DTMF) interface. The following table lists the commands that are available for managing your contacts.

Personal contact commands

Voice command	Touchtone command	Description
"Directory"	00	Searches the directory for a user.
"Play details"	1	Plays the details of the personal contact, such as the telephone numbers that are

		listed for the personal contact.
"Send a message"	3	Sends a message to the personal contact that is selected.
"Find another contact"	4	Finds another personal contact.
"Call the cell"	2 followed by 1	Calls the mobile telephone number that is listed for the personal contact.
"Call the office"	2 followed by 2	Calls the business or office telephone number that is listed for the personal contact.
"Call home"	2 followed by 3	Calls the home telephone number that is listed for the personal contact.
	##	Lets you enter the e-mail alias or name for the user in the directory if using the directory search feature.
"Main menu"	*	Exits to the main menu.

Personal Options Commands Reference

As an Outlook Voice Access user, when you dial in to a subscriber access number, you are presented with menu options that enable you to access your Exchange 2010 mailbox and manage your personal options. When you configure personal options using Outlook Voice Access, the DTMF or touchtone interface is the only interface that is available. The VUI or Automatic Speech Recognition (ASR) is not available for configuring personal options. The following table lists the commands that are available for managing your personal options.

Personal options commands

Voice command	Touchtone command	Description
	1	Turns on or off the telephone Out of Office greeting.
	2	Records the personal voice mail or Out of Office voice mail greeting.
	3	Changes the PIN that is used for Outlook Voice Access.
	4	Starts using the VUI or touchtone interface.
	5	Sets the local time zone to use.
	6	Chooses the 12-hour or 24-hour time format.

	*	Returns to the main menu.
	0	Repeats the menu options that are available.

For More Information

- For more information about subscriber access in Exchange 2010 Unified Messaging, see Understanding Unified Messaging Subscriber Access.
- For more information about the voice prompts that are used with subscriber access in Exchange 2010 Unified Messaging, see Understanding Unified Messaging Audio Prompts.
- For more information about client features in Exchange 2010 Unified Messaging, see Understanding Client Features in Unified Messaging.
- For more information about common user scenarios in Exchange 2010 Unified Messaging, see Outlook Voice Access User Scenarios.

1.9.1.3.22.2 Understanding Call Answering Rules

Understanding Call Answering Rules

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-04-12*

Call Answering Rules is a new feature in Microsoft Exchange Server 2010. Using this feature, end users can dictate how their incoming call answering calls should be handled. Call answering rules are applied to incoming calls similar to the way Inbox rules are applied to incoming e-mail messages.

Call answering rules are stored in the mailboxes of users who are enabled for Exchange 2010 Unified Messaging. Nine call answering rules can be set up for each mailbox. These rules are independent of the Inbox rules that are set up by users and don't consume a part of the Inbox rules quota for the user. By default, no call answering rules are configured. If an incoming call is answered by a Unified Messaging (UM) server, the caller can be prompted to leave a voice message or if the caller doesn't prompt the system, the caller will also be able to leave a voice message for the called party.

Anatomy of Call Answering Rules

A call answering rule consists of two parts: conditions and actions. You can associate one or more conditions with a single call answering rule. The call answering rule will only be processed if all the conditions for the rule are met. You can also associate one or more actions with a single call answering rule. These actions determine what options will be offered to the caller when the call answering rule is processed.

Call Answering Rules support the following conditions:

- Who the incoming call is from
- The time of day
- Calendar free/busy status

- Whether automatic replies are turned on for e-mail

The following actions are supported:

- Find me
- Transfer the caller to someone else.
- Leave a voice message

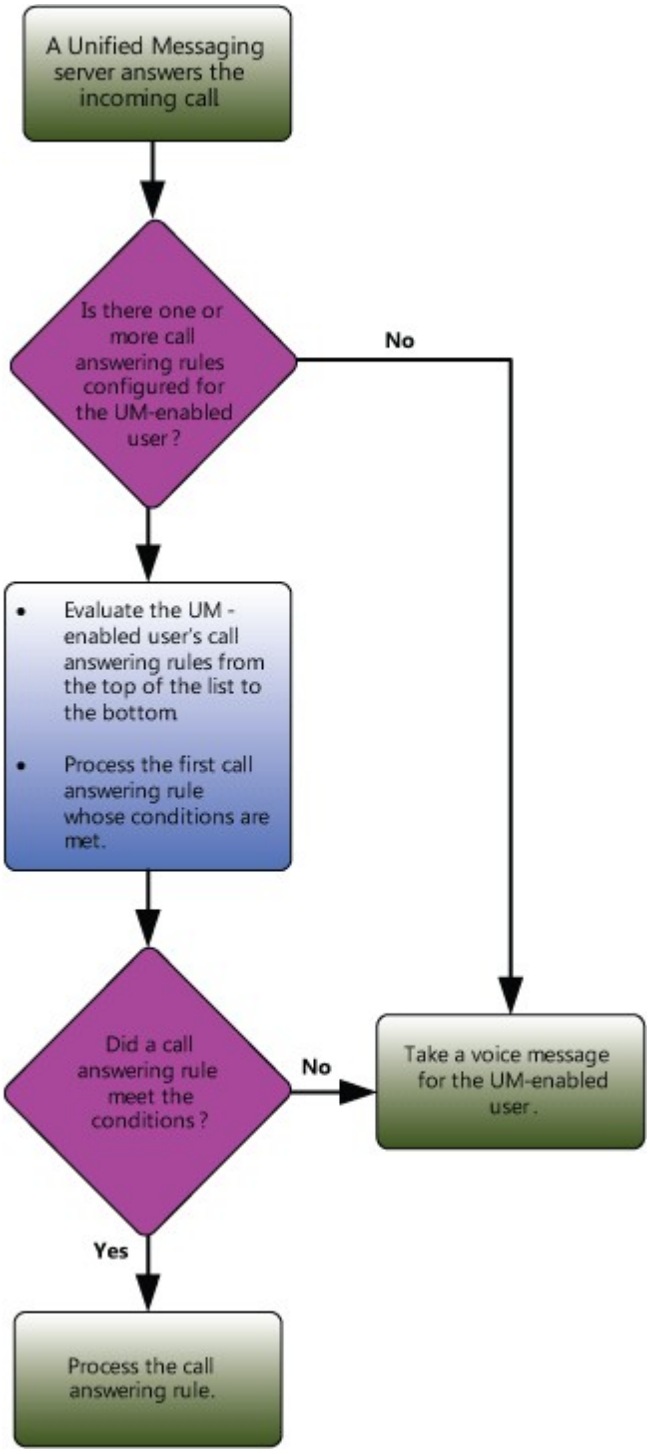
Note:
If a user records a custom greeting for a call answering rule, they must include the menu option as part of the custom greeting when they configure the call answering rule. If they don't, the Unified Messaging server won't generate a menu prompt that lets the caller know what his or her choices are. After UM plays the custom greeting, the server will wait for the caller's input. If the menu option isn't included in the greeting, the caller won't input anything and the server will prompt them, asking "Are you still there?"

For more information on the conditions and actions, see Call Answering Rules for the End User.

Selecting a call answering rule for each incoming call

As shown in the following diagram, when an incoming call is received for a UM-enabled user, UM will:

1. Determine whether the user has created any call answering rules. If not, UM will offer the caller the option of leaving a voice message.
2. If one or more call answering rules have been configured, UM will evaluate each of these rules. The first rule whose conditions are met will be processed.
3. After evaluating all the rules, if UM doesn't find a rule whose conditions are met, UM will ask the caller to leave a voice message.



Dialing Rules

Depending on how a call answering rule is configured, an incoming call may result in a call transfer. When this happens, the transfer target phone number will be subject to the dialing rules and restrictions on the UM mailbox policy that the called party is associated with. For more information about outdialing and dialing rules and restrictions, see the following topics:

- Configure Dialing Rule Groups on a UM Dial Plan
- Create a Dialing Rule Entry on a UM Dial Plan
- Enable Dialing Restrictions on a UM Mailbox Policy

Enabling/Disabling Call Answering Rules

By default, call answering rules are automatically enabled for UM-enabled users. However, you can disable call answering rules for users by disabling the feature on a UM dial plan, a UM mailbox policy, or the user's mailbox. For details about how to enable or disable call answering rules, see the following topics:

- Allow or Prevent Call Answering Rules on a UM Dial Plan
- Enable or Disable Call Answering Rules on a UM Mailbox Policy
- Enable or Disable Call Answering Rules for a UM-Enabled User

Important:
Call answering rules aren't available for UM-enabled users who have a mailbox on a Microsoft Exchange Server 2007 Mailbox server.

Call Answering Rules for the End User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-04-12*

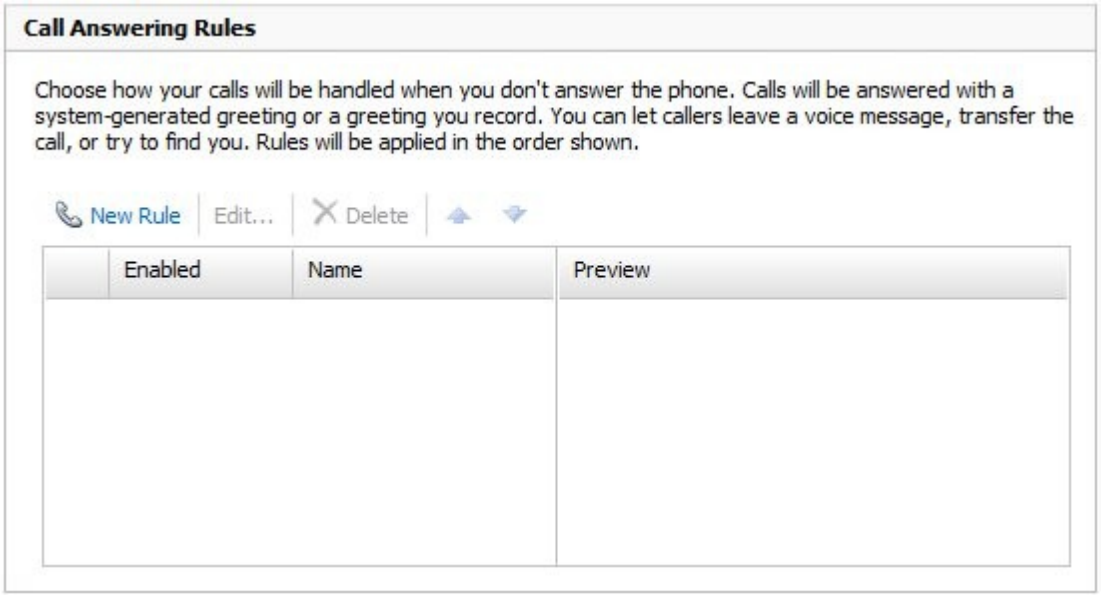
One of the main functions of Exchange Unified Messaging is to answer incoming calls, take a voice mail message, and send it to your Inbox. Call Answering Rules let you tell the voice mail system how to handle your incoming calls. You can set the voice mail system to just answer your incoming calls and record a voice message, or you can set up conditions and actions so that the incoming call will be handled in a different way.

Contents

Call Answering Rules Overview

If your mailbox is enabled for Exchange 2010 Unified Messaging, you can set up to nine call answering rules. These rules are different from the Inbox rules that you set up. By default, no call answering rules have been created for you. All callers will be prompted to leave you a voice message until you set up call answering rules. If you're satisfied with having the voice mail system just answer your incoming calls and record a voice message, you don't have to create any call answering rules. However, if you decide that you want to set up conditions or actions, you can set them up by using the **Call Answering Rules** section on the **Voice Mail** tab in Outlook Web App. Use the **Call Answering Rules** section,

shown below, to create, edit, and delete call answering rules.



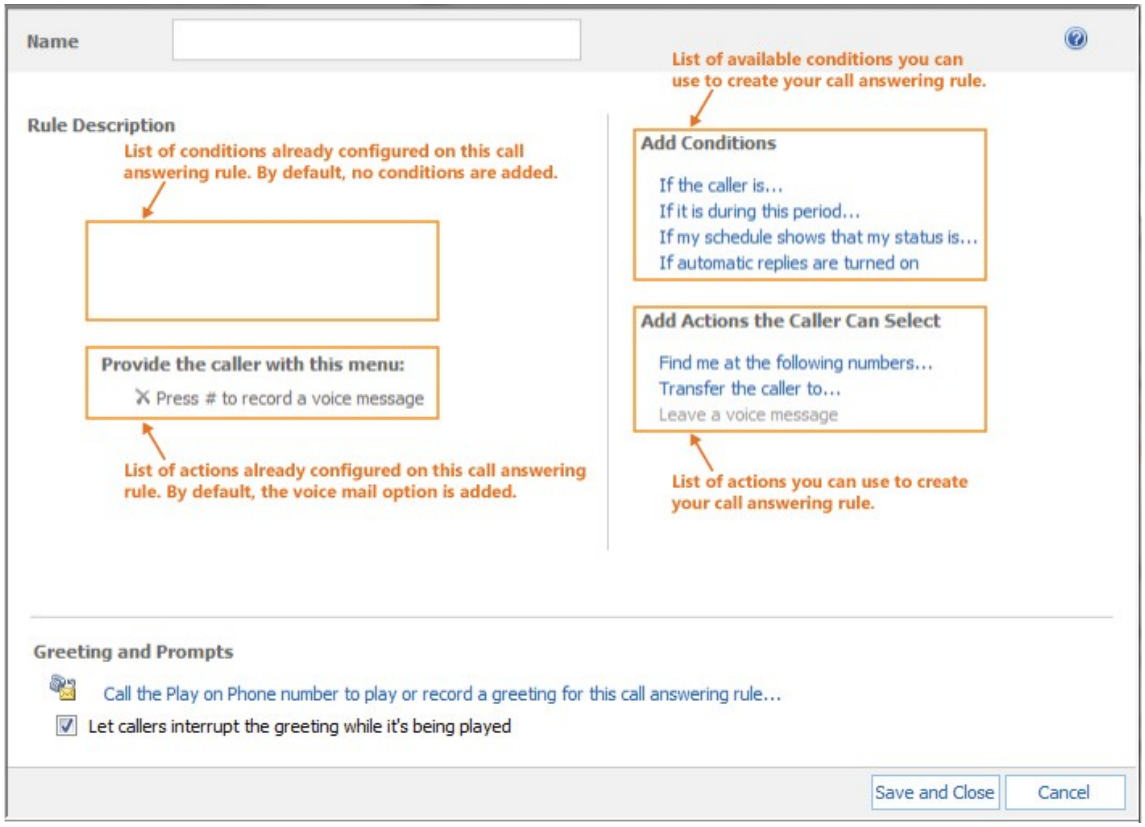
To create a new call answering rule, click New Rule.

Anatomy of a Call Answering Rule

Each call answering rule that you create contains two key parts:

- Conditions – The criteria that must be met before the rule can be applied to an incoming call.
- Actions – The options that should be presented to the caller when all the conditions are met. These actions will be read to the caller over the phone, and the caller can then choose what they want to do using the keypad on their phone.

The following figure shows the form for creating a call answering rule. The form is divided into two columns. The right column displays the list of available conditions and actions you can use to build the rule. The left column displays the list of conditions and actions that have been added to the rule.



Return to top

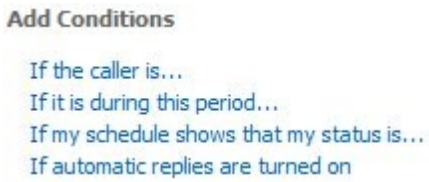
Conditions

Conditions are rules that you can apply to call answering rules. By using a combination of conditions, you can create multiple call answering rules that will trigger when the conditions are met. To create a default rule that will be applied to every call, you create a rule that doesn't contain any conditions.

There are four conditions that can be used when you set up call answering rules, including:

- Caller ID
- Time-of-the-day
- Free/busy status
- Automatic e-mail reply is enabled/disabled

Use one of the following options to add a condition for a call answering rule:



Actions

Actions are used to define what you want to happen when a condition is met. The three kinds of actions are:

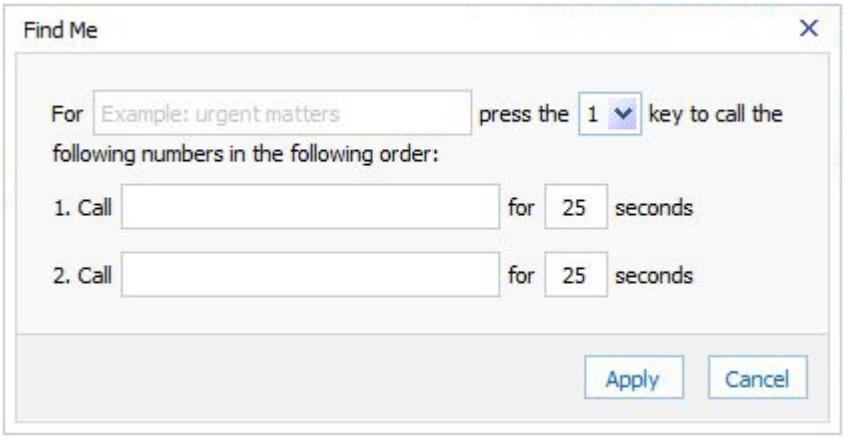
- Find-Me
- Call Transfer
- Leave a Voice Mail

Use one of the following options to add an action for a call answering rule:

Adding a Find-Me Action

When a caller selects Find-Me, the voice mail system will attempt to locate you at up to 2 different phone numbers, and then connect the caller to you if you're available at one of the phone numbers. To add Find-Me to your list of actions, click Find me at the following numbers...

In the Find-Me dialog box, specify the phone numbers and other settings. The settings that are available are listed below:



You can specify text that will be read to the caller. For example, if you enter "Urgent Matters" to inform your callers that they should only select this action if they have important things to discuss with you, the voice mail system will say "For Urgent Matters, press the 1 key."

You have to associate the Find-Me action with the number on the telephone keypad that the caller will have to press to select this action. In the example above, the **1** telephone key is the number callers will press to reach you at one of the phone number or numbers you specify.

Next you have to specify the one or two phone numbers that the voice mail system will dial. If you specify two telephone numbers, the second number will be dialed if you're not available at the first. Each phone number that you specify has an associated duration. The duration is the time period during which the voice mail system will try to dial the phone number before it moves on to the next number. Or, if you can't be contacted, the voice mail system will go back to the options menu.

After you've entered this information, click **Apply** to save the Find-Me settings.

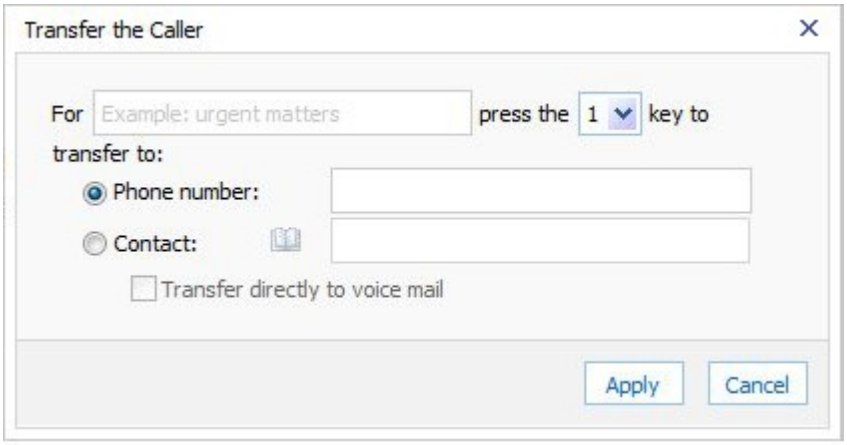
Return to top

Adding Call Transfer Options

By setting a Call Transfer action, you provide callers with the option to be transferred to another person's phone number. To add Call Transfer to your list of actions, click

Transfer the caller to...

There are several options that are available when you want to transfer an incoming call to another phone or Contact. The **Transfer the Caller** dialog box is shown below.



- You can specify text that will be read to the caller. For example, you can enter "Important Matters" to inform your callers that they should choose this option if they have an important matter to discuss and need to speak to someone.
- You have to associate the **Call Transfer** action with the number on the telephone keypad that the caller will have to press to select this action.
- When you choose the Call Transfer action, you have to specify a person or phone number for the caller to be transferred to. You can choose a phone number or select a Contact to be called when the caller presses the correct key on the telephone keypad. If you specify a contact who's within your company directory, the voice mail system will try to transfer the call to the extension number of that contact.
- In addition to specifying a person or number for the caller to be transferred to, you also need to specify the number on the telephone keypad that the caller will have to press to select the Call Transfer action.
- After you've entered this information, click **Apply** to save the Call Transfer settings.

Adding and Removing the Leave a Voice Mail Action

By default, the voice mail option is automatically added to each call answering rule. If you don't want to offer this option, you can remove it by clicking . Press the # key to record a voice message. If you've removed the option for receiving a voice message, you can add it back by clicking the Leave a voice message option.

Return to top

Recording a Personalized Voice Mail Greeting

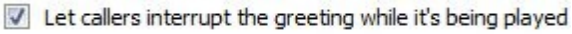
You can record a custom greeting for each call answering rule you create. By default, Unified Messaging will generate a default greeting based on the actions you've configured. To record a custom greeting, you can click the

Call the Play on Phone number to play or record a greeting for this call answering rule...

in the **Call Answering Rule** window and the voice mail system will call you so you can

record a greeting. In your recording, you should include any actions you've configured on the rule itself. The voice mail system won't list the actions if you've recorded a custom greeting.

You can also allow callers to interrupt your voice mail greeting while it's being played for callers, or prevent them from doing so, by selecting or clearing the



check box.

Saving Your Call Answering Rules

Before you save your rule, you have to give it a meaningful name. After you do this, click **Save and Close** to create the rule. Next, you should test to make sure the call answering rule is working you want it to by trying to call your phone extension and waiting for the call to be answered by Unified Messaging.

Return to top

1.9.1.3.22.3 Outlook 2007 Features for Exchange Unified Messaging

Outlook 2007 Features for Exchange Unified Messaging

Understanding Unified Messaging > Understanding Unified Messaging Features > Understanding Client Features in Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-26*

When you enable users for Microsoft Exchange Server 2010 Unified Messaging (UM), users can receive e-mail, voice, and fax messages in their individual Exchange Inbox. This topic discusses the Microsoft Office Outlook 2007 features for Exchange 2010 Unified Messaging that let a UM-enabled user who is using Outlook 2007:

- Play a voice message from Microsoft Windows Media Player, which is integrated into an Outlook mail form, or from a message list.
- Play a voice message on a telephone.
- Configure individual voice mail settings.

Note:

Unified Messaging is only available for Exchange recipients who have mailboxes located on a server that's running Exchange 2010.

Third-Party Unified Messaging Solutions

In the past, with many third-party Unified Messaging solutions, voice mail was received and then stored in a single location. It was retrieved by a user who was using a telephone, or routed to the user's Inbox to be played from an Outlook or Outlook Web App client computer. Even if the Unified Messaging system was using a legacy version of Microsoft Exchange to store the voice mail data, the voice mail system and the client computer weren't closely integrated and therefore didn't provide a seamless voice mail experience for the user.

In voice mail environments such as these, when a user received a voice message, it arrived as an e-mail message with the voice mail message contained inside an attachment. Users had to open an instance of Windows Media Player or another media

player installed on the client computer to play and listen to their voice mail messages. Because the Outlook or Outlook Web App client computer and the third-party Unified Messaging system weren't integrated, in addition to having to open an individual instance of a media player application, users couldn't configure their individual voice mail settings from their e-mail client software. They had to change individual voice mail settings through a different software application or by using their telephone.

Legacy Clients and Exchange

When UM-enabled users use Outlook 2007 or the version of Outlook Web App that's included with Exchange 2010, they are given more voice mail options than Microsoft Exchange recipients who are using legacy versions of Outlook, Outlook Web App, or Exchange. Outlook or Outlook Web App users, or users who connect to a legacy version of Exchange, still receive their voice mail as a standard e-mail sound file attachment (*.wav or *.wma), and no voice mail configuration options are available to them.

Note:

When you use Microsoft Exchange ActiveSync on a mobile phone, you can listen to the attached *.wma file that contains the voice mail message. The advanced Unified Messaging features found in the Outlook Web App client, such as the voice mail configuration options, aren't available in the light version of Outlook Web App.

Caution:

When you use the light version of Outlook Web App and Pocket Internet Explorer on a mobile phone, you may be able to listen to the .wma attachment in a voice message. However, this is not a supported configuration.

Outlook 2007 Features for Exchange Unified Messaging

To offer a seamless voice mail experience for the user, Outlook 2007 and the version of Outlook Web App included with Exchange 2010 offer Exchange 2010 UM-enabled users a full set of voice mail features. These features include many voice mail configuration options, and the ability to play a voice message from either the reading pane using an integrated Windows Media Player or from the message list.

Note:

Users must use a version of Windows Media Player no earlier than Windows Media Player version 7.0 to use the integrated media player and controls. If you are running Outlook 2007 on a computer that's running Windows Server 2008 64-bit Edition, you must install the most recent version of the Windows Media Audio Voice Codec and the Windows Media Encoder. To install the most recent version of the Windows Media Audio Voice Codec, see FIX: Availability of the Windows Media Audio 9 Voice codec for x64-based computers. To install the most recent version of the Windows Media Encoder, see Windows Media Encoder 9 Series x64 Edition.

The Outlook 2007 features for Exchange Unified Messaging are included with the installation of Outlook 2007.After the Outlook 2007 software is installed and the user is UM-enabled, a voice mail tab with voice mail configuration settings will be made available to the user from the **Options** menu.

Note:

The Outlook features for Exchange Unified Messaging are available only with Outlook 2007 and are not available with earlier versions of Outlook.

Using the **Voice Mail** tab, the user can configure settings such as telephone access

numbers and the voice mail Play on Phone number, and can reset a voice mail access PIN.

Note:
The Outlook 2007 **Voice Mail** tab will only be available if the user is enabled for Unified Messaging.

With Outlook features for Exchange Unified Messaging, UM-enabled users can:

- Listen to voice messages without changing their context to another application.
- Configure individual voice mail settings.
- View all their voice mail in one location.
- Distinguish voice and fax messages from e-mail messages within their individual Inboxes using new icons. This includes unique notifications for new e-mail, voice, and fax messages.
- Determine whether a voice message has already been played.
- Add annotations to a voice mail message in a text box.
- Reply to a voice message with e-mail when the sender's contact information is known.
- Add received phone numbers to Contacts using the shortcut menu.

Note:
The Outlook features for Exchange Unified Messaging are included when you install Outlook 2007. However, the settings for the Unified Messaging features are maintained per user and not per computer.

The topics in the following list introduce and more fully discuss the Unified Messaging features found in Outlook 2007 and in Outlook Live in Exchange 2010:

- Outlook 2007 Features for Exchange Unified Messaging: Voice Mail Form
- Outlook 2007 Features for Exchange Unified Messaging: Play on Phone
- Outlook 2007 Features for Exchange Unified Messaging: Voice Mail Options

For More Information

- For more information about Exchange 2010 Unified Messaging, see Unified Messaging.
- For more information about how to enable users for Unified Messaging, see Enable a User for Unified Messaging.
- For more information about Outlook Live in Exchange 2010, see Managing Outlook Web App

Outlook 2007 Features for Exchange Unified Messaging: Voice Mail Form

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-01*

This topic discusses the Outlook features for Microsoft Exchange Server 2010 Unified Messaging (UM) available with Microsoft Office Outlook 2007. Using the Outlook features for Exchange Unified Messaging, a UM-enabled user who is using Outlook 2007 can play a voice mail message from Microsoft Windows Media Player using an Outlook voice mail

form. After a voice message is received and opened, a voice mail form will be used. Other message types with voice attachments, for example, calendar replies, are treated as standard items and use default Outlook forms.

Contents

Voice Mail Form

The Outlook 2007 voice mail form resembles the default e-mail form, but gives users an interface for performing actions such as playing, stopping, or pausing voice messages, playing voice messages on a telephone, and adding and editing notes.

The voice mail form includes the embedded Windows Media Player and a notes field. The embedded Windows Media Player and notes field are displayed in either the preview pane when previewing a voice message or in a separate window when the voice message is opened by the user. If users aren't enabled for Unified Messaging or Outlook 2007 hasn't been installed on the client computer, users receive voice messages only as attachments, and the voice mail form isn't available.

Note:

To use the Windows Media Player in the voice mail form, users must use a version of Windows Media Player no earlier than Windows Media Player version 7.0. If the appropriate version of Windows Media Player isn't installed, the player won't be rendered in the form, but other Unified Messaging features will be available on the client computer.

Important:

If you're running Outlook 2007 on a computer running Windows Server 2008 64-bit Edition, you need to install the most recent version of the Windows Media Audio Voice codec and the Windows Media Encoder. To install the most recent version of the Windows Media Audio Voice codec, see FIX: Availability of the Windows Media Audio 9 voice codec for x64-based computers. To install the most recent version of the Windows Media Encoder, see Windows Media Encoder 9 Series x64 Edition.

Voice Mail Form Options

The following three options are available in the voice mail form options:

- **Play** Users can play and listen to voice messages using computer speakers or headphones. After **Play** is clicked, the Windows Media Player goes into play mode.
- **Play on Phone** Users send a request to the Unified Messaging server to play the selected voice message on the user's phone or send the voice message to another telephone number specified by the user. After **Play on Phone** is clicked, the **Play on Phone** dialog box appears so that the user can configure and control the Play on Phone operation.
- **Edit Notes** The user opens the voice message and can add or edit notes or comments in the **Notes** field.

Outlook 2007 Features for Exchange Unified Messaging: Play on Phone

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

After a voice mail message arrives, users can choose either to listen to the voice mail message through their computer speakers or headphones or to use the Play on Phone feature. The Play on Phone feature is included with the Outlook features for Microsoft Exchange Server 2010 Unified Messaging (UM) in Microsoft Office Outlook 2007. This topic discusses how a UM-enabled user can use the Play on Phone feature provided by Exchange 2010.

What Is Play on Phone?

The Play on Phone feature lets UM-enabled users play voice messages over a telephone. If a UM-enabled user works in an office cubicle, is using a public computer or a computer that isn't enabled for multimedia, or is listening to a voice message that's confidential, the user might not want to or be able to listen to a voice message through computer speakers. Alternatively, the user can play back the voice mail message using any telephone, including home, office, or mobile telephones.

The Play on Phone feature is available in Outlook 2007 and also in Exchange 2010 Outlook Web App.

When the user clicks the **Play on Phone** toolbar option in the Outlook 2007 voice mail form, the **Play on Phone** dialog box appears. The **Play on Phone** dialog box provides the controls for selecting or inputting the telephone number to use to play a voice message, for starting and ending the call, and for displaying a status message for monitoring the call.

Note:

Only one voice message can be played at one time. If the user tries to start a second Play on Phone call while a previous call is still in progress, an error message will appear.

Most Recently Used Telephone Number List

Users can see a list of telephone numbers they used most recently in the **Play on Phone** dialog box. The telephone number specified on the **Voice Mail** tab is always displayed as the top entry and is automatically selected for the user as the primary number. Users can use the menu options to select other telephone numbers to dial instead of the telephone number configured as the primary number.

Note:

To enable users who are using the Play on Phone feature to dial an external telephone number without using an outside line access code, for example 425-555-0123 instead of 9-425-555-0123, configure in-country/region dialing rules on a UM dial plan that include the following line: group1, 9xxxxxxxxxx, 91xxxxxxxxxx. After you configure the in-country/region dialing rules, add this list to the UM mailbox policy.

Play on Phone Buttons

The **Play on Phone** dialog box gives users the option to **Dial** and **Hang-up**. When the **Play on Phone** dialog box is first opened, the **Dial** button is enabled and the **Hang-up** button is disabled. After a call is placed, the **Dial** button becomes disabled until the call has ended. The call can be ended either by clicking the **Hang-up** button or by physically hanging up the telephone. Closing the **Play on Phone** dialog box using the **Close** button ends the call if one is in progress.

Subject, Sent, and Status Field

The bottom section of the **Play on Phone** dialog box displays the subject of the voice message, the date and time sent, and a message that displays the current state of the call. Any errors specific to the Play on Phone operation are displayed to the user in this section of the **Play on Phone** dialog box.

Phone Number Validation

Play on Phone only performs simple validation on your input into the **Play on Phone** dialog box. Play on Phone doesn't validate telephone numbers. If a telephone number isn't valid, the Microsoft Exchange Unified Messaging service returns a meaningful error code to the user.

For More Information

- For more information about the Outlook features for Exchange Unified Messaging, see Outlook 2007 Features for Exchange Unified Messaging.
- For more information about the Unified Messaging voice mail form, see Outlook 2007 Features for Exchange Unified Messaging: Voice Mail Form.
- For more information about how to configure Unified Messaging voice mail options, see Outlook 2007 Features for Exchange Unified Messaging: Voice Mail Options.

Outlook 2007 Features for Exchange Unified Messaging: Voice Mail Options

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

A user who is enabled for Microsoft Exchange Server 2010 Unified Messaging (UM) can configure several voice mail options in the Outlook features for Exchange Unified Messaging available with Microsoft Office Outlook 2007. This topic discusses the Outlook 2007 Unified Messaging features that let a UM-enabled user who is using Outlook 2007 select and configure available voice mail options.

Note:

The voice mail configuration options on the **Voice Mail** tab in Outlook 2007 appear dimmed if a Unified Messaging server cannot be located on the network. These voice mail options are also unavailable if the user's mailbox is located on a server running an earlier version of Microsoft Exchange.

Note:
When you log on to a computer joined to a domain and you access the **Voice Mail** tab in Outlook 2007, you may be prompted to enter your credentials. This occurs because the default security settings in Microsoft Internet Explorer are configured to allow an automatic logon only for Web sites listed in the **Local intranet** zone. To correct this issue, add the fully qualified domain name (FQDN) of the Client Access server to the **Local intranet** zone or configure the user authentication to use an automatic logon using the current user credentials in Internet Explorer.

Telephone Access

Using the options in the **Telephone Access** section on the **Voice Mail** tab, users can set telephone access numbers, reset their voice mail PIN, and select the e-mail folder that they will access when they use Outlook Voice Access.

Telephone Access Numbers

The **Telephone Access Numbers** box specifies the telephone number or telephone numbers that users can dial to access their messages, calendar, and contacts using Outlook Voice Access. The numbers in this box are referred to as subscriber access numbers, pilot ID numbers, pilot IDs, or pilot numbers, and are configured on a UM dial plan. The telephone access numbers listed in this box are configured in the **Telephone access numbers** section on the **Subscriber Access** tab of a UM dial plan. These telephone numbers apply to all users who are members of the UM dial plan. For more information about how to configure a UM dial plan, see View or Configure the Properties of a UM Dial Plan.

Resetting Voice Mail PIN

The **Reset PIN** button lets users reset their voice mail PIN. The PIN is used to access their mailbox and calendar information.

Selecting an E-Mail Folder

The **Choose the folder to read when accessing e-mail messages from a phone** option lets users specify which e-mail folder to read e-mail, voice mail, or other messages from, when they use Outlook Voice Access. The **Change Folder** button lets users select which mailbox folder will be read. By default, the Inbox is selected as the folder to use when users access messages from a telephone using Outlook Voice Access.

Voice Mail

Users can configure several voice mail options in the **Voice Mail** section of the **Voice Mail** tab. These options include the Play on Phone telephone number and voice mail greetings.

Play on Phone Number

The telephone number in the **Play on Phone number** box determines the telephone number that the Unified Messaging system calls when the user is using the Play on Phone feature. By default, the telephone number is set to the user's extension number, but can be changed by the user.

Voice Mail Greetings

Users can use the **Choose the greeting played to callers when leaving a message** option on the **Voice Mail** tab to select the type of greeting that callers hear when they reach the user's voice mail.

- **Voice-mail greeting** is the default selection and is the regular voice mail greeting. It's the greeting used when the user is in the office but away from the desk for a short time.
- The **Out of Office voice mail greeting** is generally used when a user is not in the office or is away for an extended time.

Play or Record a Greeting on Your Telephone

Clicking the **Call** button calls the Play on Phone number and plays the greeting to users on their telephone. Users can also use this option to play or record a new greeting from a telephone.

Missed Call Notifications

Users can specify whether they want to receive missed call notification messages from the Exchange 2010 Unified Messaging server using the **Send an e-mail to my Inbox when I miss a phone call** check box. When this box is selected, users receive notifications when callers try to contact them but do not leave voice messages. By default, the **Send an e-mail to my Inbox when I miss a phone call** box is selected.

Note:
For many of the voice mail options included in Outlook 2007 and Exchange 2010 Outlook Web App to function correctly, the Client Access server role must be installed on a computer running Exchange 2010, and Autodiscover must be configured correctly.

Voice Mail Shortcut Keys

There are keyboard shortcuts to help users configure or select voice mail options. The following table lists the keyboard shortcuts available for voice mail options.

To do this	Press
Reset the telephone access PIN	ALT+R
Select the e-mail folder to read when you use Outlook Voice Access	ALT+F
Enter the Play on Phone number	ALT+P
Select the voice mail greeting	ALT+V
Select the Out of Office greeting	ALT+O
Dial the number to play or record a greeting on the telephone	ALT+D
Enable or disable Missed Call Notifications	ALT+S

For More Information

- For more information about the Unified Messaging voice mail form, see Outlook 2007 Features for Exchange Unified Messaging: Voice Mail Form.
- For more information about the Unified Messaging Play on Phone feature, see Outlook 2007 Features for Exchange Unified Messaging: Play on Phone.
- For more information about Outlook features for Exchange Unified Messaging, see Outlook 2007 Features for Exchange Unified Messaging.

Outlook 2010 and Outlook Web App Features in Unified Messaging

Understanding Unified Messaging > Understanding Unified Messaging Features > Understanding Client Features in Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

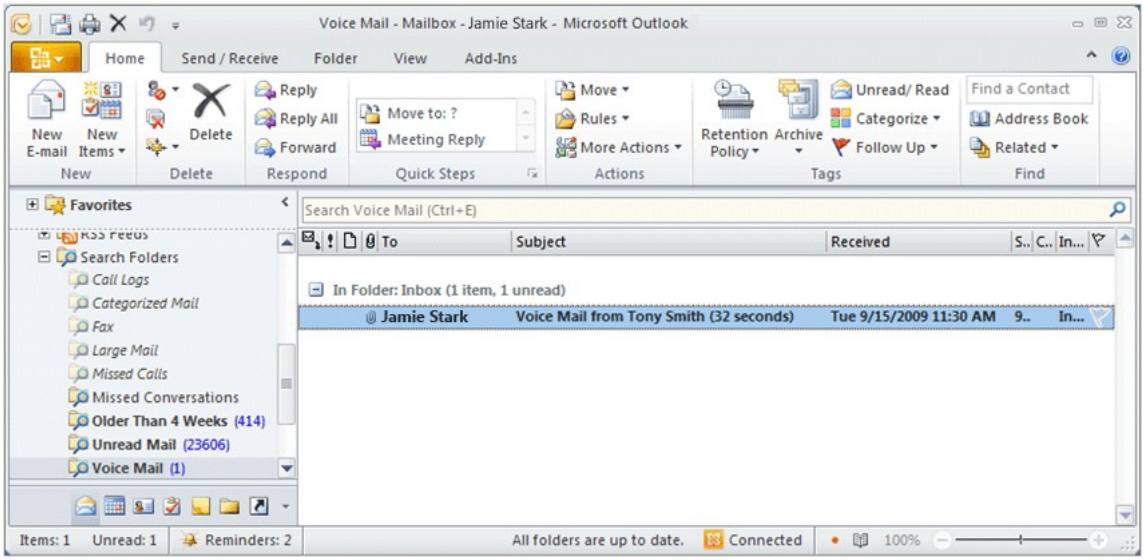
Topic Last Modified: *2010-04-15*

When you enable users for Microsoft Exchange Server 2010 Unified Messaging (UM), users can receive e-mail, voice mail, and fax messages in their individual Exchange Inbox. This topic discusses the Microsoft Outlook 2010 features for Exchange 2010 Unified Messaging that let a UM-enabled user who's using Outlook 2010 do the following:

- See the transcription for voice messages.
- Play a voice message from Windows Media Player, which is integrated into an Outlook mail form, or from a message list.
- Play a voice message on a telephone.
- Configure individual voice mail settings.
- Reply to a voice message with e-mail when the sender's contact information is known.
- Add received phone numbers to Contacts using the shortcut menu.

To offer a seamless voice mail experience for the user, Outlook 2010 and Microsoft Office Outlook Web App in Exchange 2010 offer Exchange 2010 UM-enabled users a full set of voice mail features. These features include many voice mail configuration options, Voice Mail Preview, and the ability to play a voice message from either the Reading Pane using an integrated Windows Media Player or from the message list.

- The Outlook 2010 features for Exchange Unified Messaging are installed with Outlook 2010. After Outlook 2010 is installed and a user is enabled for Unified Messaging, a Voice Mail tab with voice mail configuration settings is available to the user from the **Options** menu and they can receive their voice mail in their mailbox.
- When the UM-enabled user receives a voice message, the voice message will be sent to the **Voice Mail** search folder in their Outlook 2010 **Search Folders**. The following screenshot shows a new voice message that's been sent to the **Voice Mail** search folder:



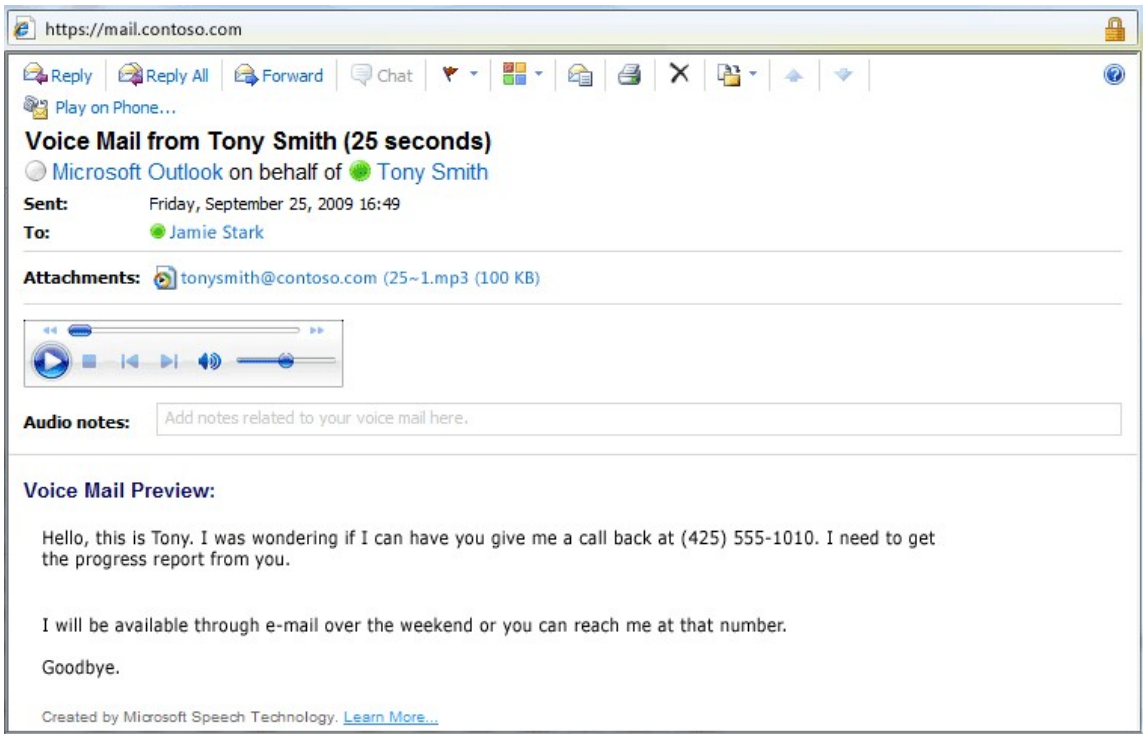
Voice Mail Message Form and Voice Mail Preview

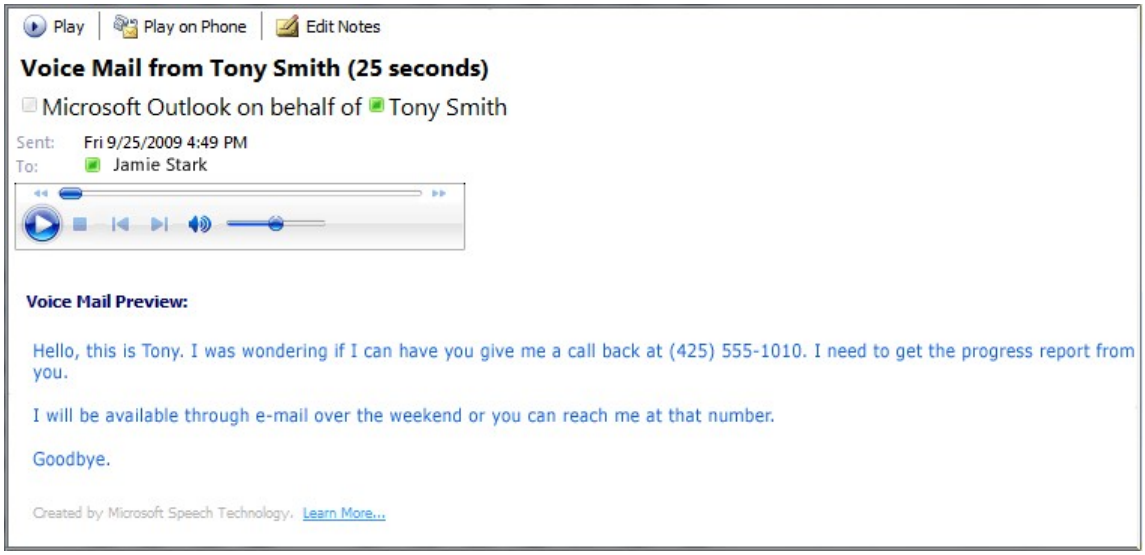
The Outlook 2010 and Outlook Web App voice mail form resembles the default e-mail form, but gives users an interface for performing actions such as playing, stopping, or pausing voice messages, playing voice messages on a telephone, and adding and editing notes.

The voice mail form includes the embedded Windows Media Player and a notes field. The embedded Windows Media Player and notes field are displayed in either the Reading Pane when the user previews a voice message or in a separate window when they open a voice message. If users aren't enabled for Unified Messaging, they won't receive voice mail in their mailbox. Or, if they don't have Outlook 2010 installed, they'll receive voice messages only as attachments, and the voice mail form won't be available.

Voice Mail Form Options

The voice mail form options are available when a user accesses their voice mail using Outlook Web App or Outlook 2010. The following screenshots show the voice mail form in Outlook Web App and Outlook 2010.





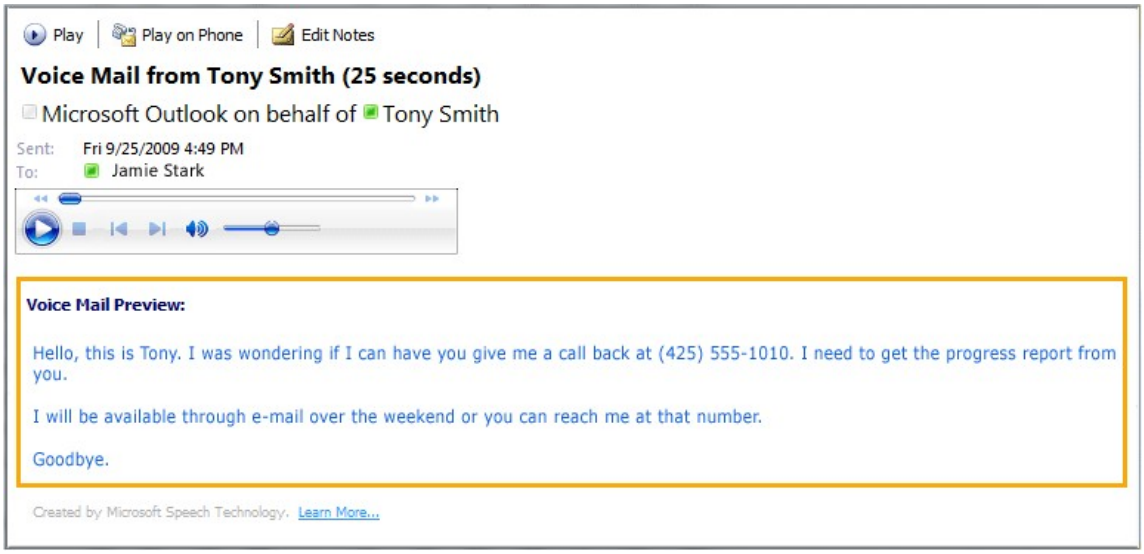
In both Outlook Web App and Outlook 2010, the following three options are available in the voice mail form:

- **Windows Media Player Controls** Users can play and listen to voice messages using computer speakers or headphones. After **Play** is clicked, the Windows Media Player goes into play mode.
- **Play on Phone** Users send a request to the Unified Messaging server to play a selected voice message on their phone or send the voice message to another telephone number they specify. After **Play on Phone** is clicked, the **Play on Phone** dialog box appears so that the user can configure and control the Play on Phone operation.
- **Voice Mail Preview** The user can view the text transcription of the actual voice mail message that was left by a caller.
- **Audio Notes** The user opens the voice message and can add or edit notes or comments in the **Audio notes** field.

Return to top

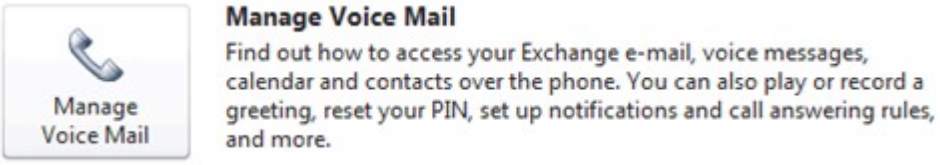
Voice Mail Preview

When users receive a voice mail, they receive a message that contains not just a recording, but also text that's been created from the voice recording. Users see the voice mail text displayed in the e-mail message within Outlook Web App or in the next version of Outlook. The following screenshot shows an example of a voice mail preview for a voice message:



Voice Mail Settings

After a user has been enabled for voice mail access, they can change settings for Call Answering Rules, Outlook Voice Access, text message and e-mail notifications, and Voice Mail Preview. They can click the button shown next to the **Manage Voice Mail** option in the following figure to view and set up their voice mail settings.



Call Answering Rules

Using the options in the **Call Answering Rules** section, users can create rules that specify how they want incoming calls to be handled. They can set up call answering rules to handle calls based on a condition such as the time of the day, transfer an incoming call to another phone number, or use the Find Me feature to call other phone numbers that they set up.

If they don't create call answering rules, incoming callers will be sent directly to their voice mail.

New Rule	• The **New Rule** button is used to add a new call answering rule. By default, no rules are set up, so all callers will be forwarded to their voice mail when they're not available.
Edit...	• The **Edit** button is used to change an existing call answering rule.
Delete	• The **Delete** button is used to remove an existing call answering rule.
	• This arrow is used to move a call answering rule up in the processing order.
	• This arrow is used to move a call

	answering rule down in the processing order.

Reset PIN

You can use this option to reset your Outlook Voice Access PIN.

Reset my Voice Mail PIN...	• Use this setting to reset your voice mail PIN. After you do this, you'll receive a new temporary PIN in your Inbox. You use your PIN to access your mailbox and calendar information.

Outlook Voice Access

Using the options in the **Outlook Voice Access** section on the **Voice Mail** tab, you can set telephone access numbers, reset your voice mail PIN, and select the e-mail folder that you'll access when you use Outlook Voice Access.

You can access your new voice messages in the order of your prefer. (•) From newest to oldest ( ) From oldest to newest	• You can access your new voice messages in the order in which you want to hear them read. This option lets you play unread voice messages from the newest to the oldest or from the oldest to the newest.
Read this folder: Inbox	• Use this setting to select which e-mail folder to read e-mail, voice mail, or other messages from when you use Outlook Voice Access • If you want Outlook Voice Access to read from a different folder than the one that's currently specified, click the name of the folder next to **Read this folder**. Then, in the **Select Folder** window, select the folder you want from the list. Or, you can click **Create New Folder** to create a different folder for Outlook Voice Access to read from. After you've

	selected the correct folder, click **OK**.

Greetings

You can choose which greeting will be played to callers when you're not available or you don't answer your phone. To record a greeting, call the Play on Phone number.

Default voice mail greeting	• Use this setting to select the default voice mail greeting to use when you don't answer your phone.
Inform callers that you will be away for an extended period of time	• Use this setting to select a voice mail greeting that lets people know you're away for an extended period of time. For example, you would use this setting when you're on vacation or away on business.
Call me to play or record the selected greeting...	• Use this setting to call the Play on Phone number and play the default voice mail greeting or the greeting you use when you'll be away for an extended period of time to you over a phone. • You can use this setting to play or record a new greeting from a telephone.

Play on Phone

Use Play on Phone to have the voice mail system call you at the number that you define in this box.

The voice mail system calls this number when you click the Play on Phone button to listen to a voice message. 11111	• The telephone number you add in this box determines the telephone number that the voice mail system calls when you use Play on Phone and click **Call me on my Play on Phone number to play or record the selected greeting**. • By default, this telephone number is your extension number, but you can change it.

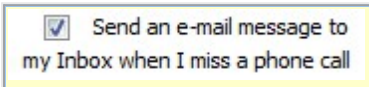
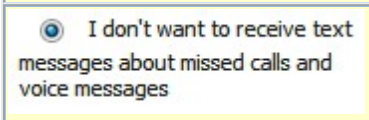
	• If this box contains something other than a phone or extension number, such as an e-mail address, the call will be sent to you where you're signed in.

Return to top

Notifications

Users can receive notifications about missed calls and voice messages on their mobile or office phone. They can receive an e-mail notification when someone calls them on their office or mobile phone but doesn't leave a voice message. They can also receive a text message notification to alert them when they miss a phone call or receive a voice message on their mobile phone.

The following settings allow users to set up notifications for missed calls and voice mail messages they receive:

	• If this check box is selected, the user will receive an e-mail notification in their Inbox when a caller tries to contact them but doesn't leave a voice message. • In most cases, the user will also see a missed call notification on their mobile phone from their mobile phone provider. • By default, this box is selected.
	• When a user selects this option button, they won't receive a text message notification on their mobile phone when they miss a call or receive a voice message. • In most cases, they'll see a missed call notification on their mobile phone from their mobile phone provider, but they won't see a notification on their mobile phone that they have a voice message. • By default, the option to receive text message notifications isn't available until a user sets up text message notifications. They can set up text message notifications by clicking the **Set up notifications** link and following the

	required steps.
I only want to receive text message notifications when I have voice messages	• When a user selects this option button, they'll receive text message notifications on their mobile phone when they have a voice message but won't receive missed call notifications. • In most cases, they'll see a missed call notification on their mobile phone from their mobile service provider, but they won't see a notification from their mobile phone provider that they have a voice message. • By default, this option isn't available until the user sets up text message notifications. They can set up text message notifications by clicking the **Set up notifications** link and following the required steps.
I want to receive text message notifications about missed calls and voice messages	• When a user selects this option button, they'll receive missed call and voice message notifications in a text message on their mobile phone. • In most cases, they'll also see a missed call notification and a voice mail notification on their mobile phone from their mobile service provider. • By default, this option isn't available until the user sets up text message notifications. They can set up text message notifications by clicking the **Set up notifications** link and following the required steps.

Return to top

Voice Mail Preview

Users can preview the text of voice messages they receive. They can also have text previews included with voice messages they send. To turn on Voice Mail Preview, they select from the following options. Users can use the settings in the Voice Mail Preview section to turn on or turn off voice mail previews or to allow preview text to be sent using

Outlook Voice Access.

☑ Include preview text with voice messages I receive.	• When this check box is selected, the user will receive a text preview of the voice messages they receive in an e-mail message. • By default, this box is selected.
☑ Include preview text with voice messages I send through Outlook Voice Access	• When this check box is selected, a text preview will be sent along with voice messages that the user sends. • By default, this box is selected.

1.9.1.3.22.5 Voice Mail Preview for End Users

Voice Mail Preview for End Users

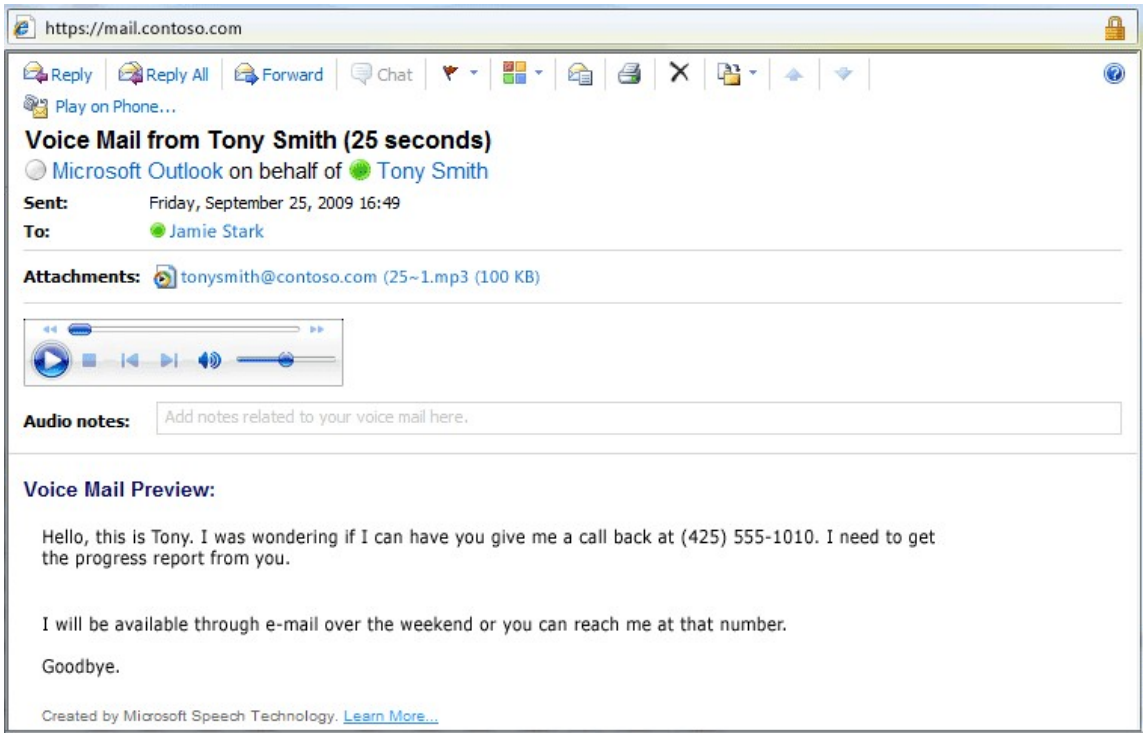
Understanding Unified Messaging > Understanding Unified Messaging Features > Understanding Client Features in Unified Messaging >

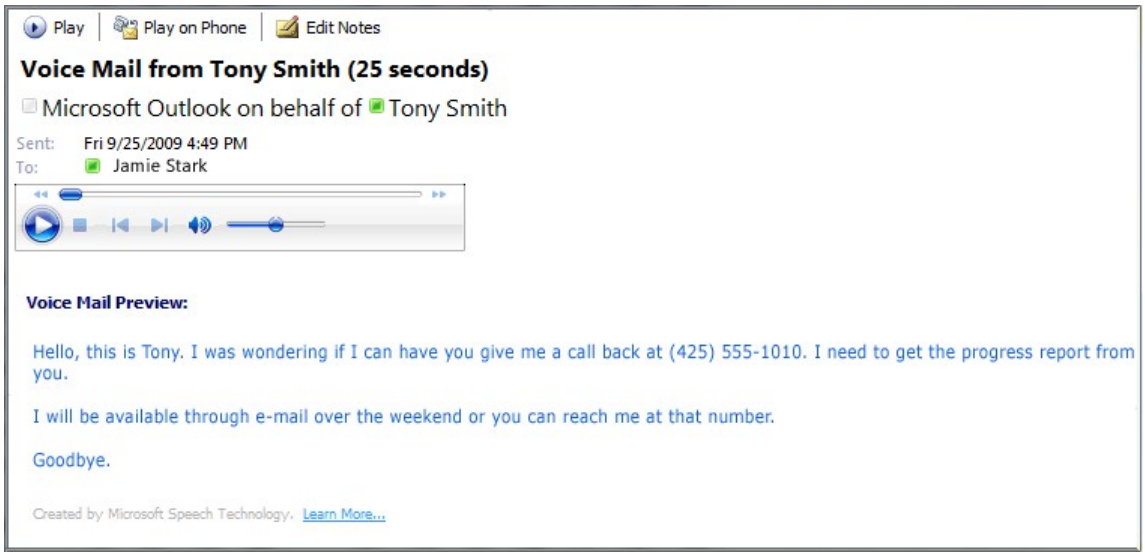
Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-17*

Voice Mail Preview is a feature that's available to users who receive their voice mail messages from Microsoft Exchange Server 2010 Unified Messaging (UM). Voice Mail Preview enhances the existing UM voice mail functionality by providing a text version of audio recordings. The voice mail text is displayed in e-mail messages within Microsoft Office Outlook Web App, Outlook 2010, and in other e-mail programs. For more information, see Microsoft Speech Technologies.

The following examples show how Voice Mail Preview is displayed in Outlook Web App and Outlook 2010:





Do users need to use a specific e-mail program?

No. Voice Mail Preview is included in the message body text of any e-mail program, including mobile programs. Although users can use other e-mail programs to receive voice messages, Outlook and Outlook Web App provide a better experience. For example, in Outlook 2010, when a specific word is clicked in the Voice Mail Preview text, the audio playback of the voice message will start to play at that word. This is useful for listening to a specific part of a voice message.

Can users search for specific voice mail messages?

Yes. Words and phrases in the Voice Mail Preview text are automatically indexed, so voice messages will appear in search results. In Microsoft Office Outlook 2007 or later versions or in Outlook Web App in Exchange 2010, users can also use the **Audio Notes** field to add text about a voice message. These notes are also included in searches, to make it easier to locate a message.

Why is this feature called 'Voice Mail Preview'?

It’s important to set users’ expectations correctly. Voice Mail Preview doesn't necessarily produce text that’s the same as what callers say in their voice messages. In fact, it's usually inaccurate in some way. To call it transcription would suggest a more perfect result can generally be achieved. Preview suggests that the reader should be able to gain an idea of the voice content, which is closer to the real capability of the feature.

What makes the Voice Mail Preview text more or less accurate?

The accuracy of the Voice Mail Preview text is controlled by many factors and sometimes those factors can't be controlled. However, Voice Mail Preview text is likely to be more accurate when:

- The caller leaves a simple voice message that doesn't include slang terms, technical jargon, or unusual words or phrases.
- The caller uses a language that's easily recognized and translated by the voice mail system. Generally, voice messages left by callers who don't speak too quickly or too softly and who don't have strong accents will produce more accurate sentences and phrases.
- The voice message is free of background noise, echo, and the audio doesn't drop-out.

Which languages can be used with Voice Mail Preview?

Voice Mail Preview text is available in the following languages:

- English (US) (en-US)
- English (Canada) (en-CA)
- French (France) (fr-FR)
- Italian (it-IT)
- Polish (pl-PL)
- Portuguese (Portugal) (pt-PT)
- Spanish (Spain) (es-ES)

You can download the Exchange 2010 UM language packs from the Microsoft Download Center.

After you install a UM language pack on a UM server, the dial plans and auto attendants can be configured to use the language you've chosen. Many companies have only one UM dial plan. UM will try to create a voice mail preview in the default dial plan language, but

the default language must support Voice Mail Preview. A UM dial plan can only be configured to create voice mail previews in one language at a time.

To configure UM to provide voice mail previews in a language other than en-US, follow these steps:

1. Verify that Voice Mail Preview is supported in the language you want to use.
2. If so, download and install the appropriate UM language pack on each UM server that's associated with the dial plan. Downloading and installing the language pack doesn't configure the dial plan default language.
3. Configure the dial plan with the language that will be used for Voice Mail Preview. For more information, see Configure the Default Language on a UM Dial Plan.

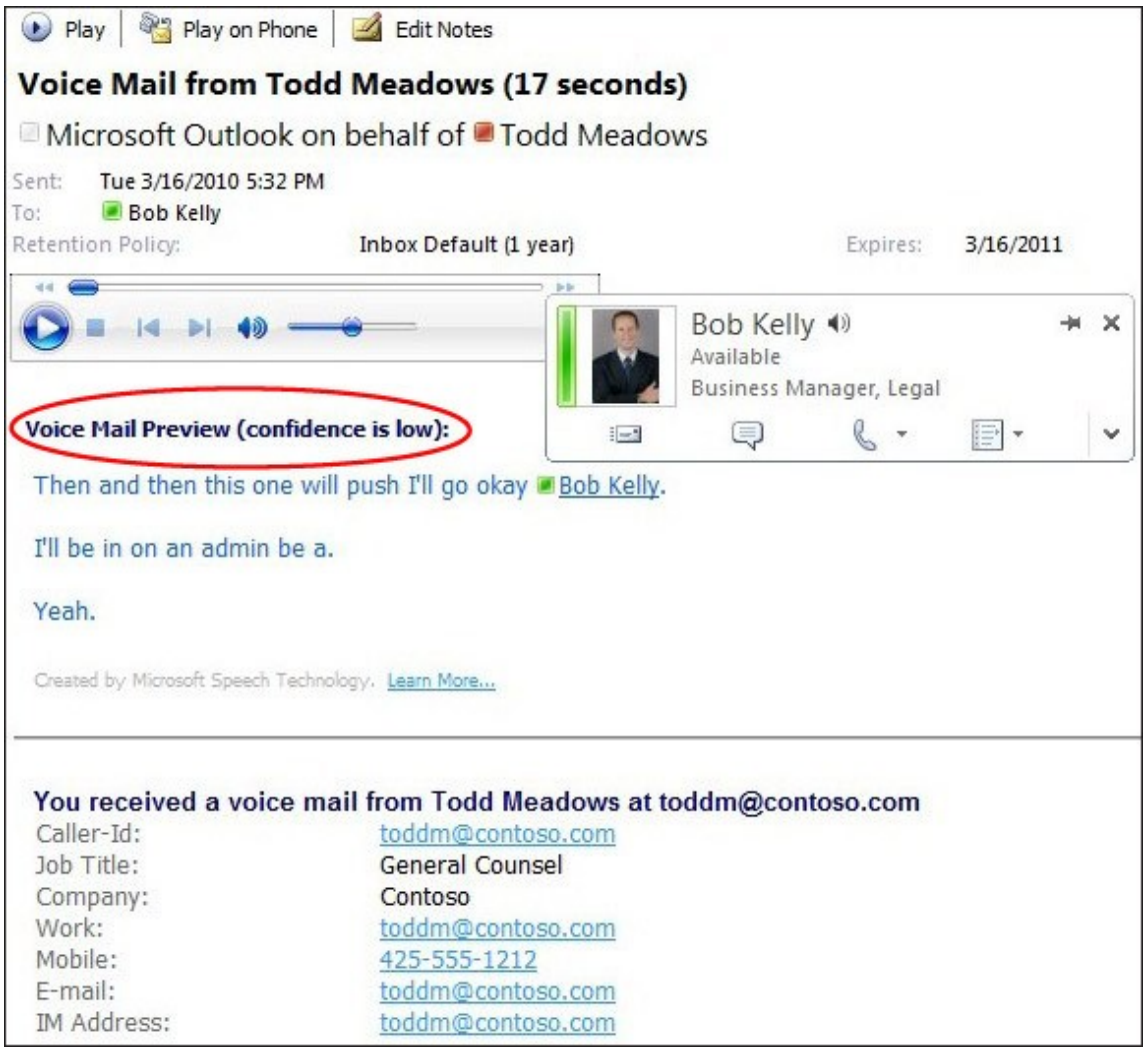
- How Voice Mail Preview displays text in the supported languages depends on the type of voice message that's sent. There are two types:
- **Voice messages that are recorded when the called party doesn't answer their phone**
  In this scenario, the language used for Voice Mail Preview is determined by the caller's spoken language and whether the language is supported. For example, if a caller leaves a voice message in Italian, the Voice Mail Preview text will appear in Italian if Italian has been configured on the dial plan. However, if a caller leaves a message in Japanese, no Voice Mail Preview text will be included with the message because Japanese isn't available.
- **Voice messages that are sent to by an Outlook Voice Access user**
  The language that's used for voice mail preview of messages sent by an Outlook Voice Access user is controlled by the voice mail administrator. Thus, the language used for Voice Mail Preview text will be in the same language of the voice mail system. However, if a caller speaking a language that's not supported for Voice Mail Preview uses Outlook Voice Access to leave a message, no Voice Mail Preview text will be included with the message. To learn more about Outlook Voice Access, see Understanding Outlook Voice Access.

For more information about UM language packs, see Understanding Unified Messaging Languages and Client Language Support for Unified Messaging.

Does the voice mail system know when a voice mail preview is inaccurate?

The voice mail system determines a confidence level for each voice mail preview included with a voice message. The voice mail system measures how well the sounds in the recording matched with words, numbers, and phrases. If the system was able to find matches easily, the confidence level will be high. A higher level of confidence is generally associated with a higher accuracy.

If the confidence level is determined to be lower than a certain value, the voice mail system includes the phrase **Voice Mail Preview (confidence is low)** above the Voice Mail Preview text. If the confidence level is low, it's likely that the Voice Mail Preview text will be inaccurate. The following is an example of a low confidence voice mail preview.



Unified Messaging uses Automatic Speech Recognition (ASR) to calculate its confidence in the preview, but it has no way to decide which words are wrong and which are correct.

However, the system does try to learn to improve accuracy of its voice mail previews. For example, Exchange 2010 Unified Messaging tries to match the caller's telephone number (if provided) with the user's personal Contacts and Active Directory. If the UM finds a match, it will include the name of the caller, along with its standard lists of names and words, when running ASR on the voice recording.

Can Voice Mail Preview be used if it isn't completely accurate?

Users may have a better experience with Voice Mail Preview if they don't try to read the preview too carefully, word by word. Instead, they should look for names, phone numbers, and phrases such as "Call me back" or "I need to talk" that may provide clues about the purpose of the call.

Voice Mail Preview isn't expected to dictate messages exactly, but it can help users answer questions such as the following:

- Is this voice message related to my work?
- Is this voice message important to me?
- Did the caller leave a number? Is it different from any numbers that I may have listed for them?
- Does the caller consider this voice message urgent?

- Should I step out of a meeting to call this person back?
- I was expecting a call to confirm my request. Is this the confirmation call?

Can Voice Mail Preview be turned on or off?

Yes. If you've enabled Voice Mail Preview, users can turn it on or off using Outlook 2010 or Outlook Web App. However, the dial plan language must support Voice Mail Preview and the UM language pack for that language must be installed.

Although Voice Mail Preview settings are the same whether a user is using Outlook 2010 or Outlook Web App, they'll access them differently:

Outlook 2010

To access the Voice Mail Preview settings in Outlook 2010, on the **File** tab, they click **Manage Voice Mail**.

Manage Voice Mail
Find out how to access your Exchange e-mail, voice messages, calendar and contacts over the phone. You can also play or record a greeting, reset your PIN, set up notifications and call answering rules, and more.

Outlook Web App

To access the Voice Mail Preview settings in Outlook Web App, they click **Options** > Go to **Options** > **Phone** > **Voice Mail**. On the **Voice Mail** tab, the following settings are available in the **Voice Mail Preview** window.

☑ Include preview text with voice messages I receive.	When this check box is selected, the user will see a text preview of the voice messages they receive. By default, this box is selected.
☑ Include preview text with voice messages I send through Outlook Voice Access	When this check box is selected, a text preview will be sent along with voice messages that the user sends. By default, this box is selected.

By default, both Voice Mail Preview options are enabled when a user is enabled for Unified Messaging. If the UM dial plan is configured to use a UM language pack that supports Voice Mail Preview, a UM server will create voice mail previews for users when:

- A caller leaves a voice mail message because the called party doesn't answer their phone.
- A UM-enabled user signs in to Outlook Voice Access and records a voice message to one or more recipients.

When a caller leaves a voice message, and **Include preview text with voice messages I receive** is enabled, the UM server will create a voice mail preview in the e-mail message, attach the audio file, and send it to the recipient's mailbox. You may want to disable this option if the language that's configured on the dial plan doesn’t include Voice Mail Preview support and you don't want voice mail previews included in voice mail messages.

When users sign in to Outlook Voice Access and they send a voice message to another

user, they may want to disable the **Include preview text with voice messages I receive through Outlook Voice Access** option. For example, they might want to do this it if they're sending voice messages in a language that Voice Mail Preview doesn't support or if they don't want to include the voice mail preview with the voice message because it's too long.

1.9.1.4 Understanding Unified Messaging Call Processing

Understanding Unified Messaging Call Processing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Call processing is a term that describes how incoming calls are answered and handled by a Microsoft Exchange Server 2010 Unified Messaging server in different incoming call scenarios.

Unified Messaging handles the following sorts of incoming calls:

- Voice
- Outlook Voice Access
- Play on Phone
- Auto attendant

Incoming Calls Overview

When an incoming call is received by a Unified Messaging server, the call is answered and then routed using a message transport, for example, SMTP, MAPI, remote procedure call (RPC), or LDAP. The message transport protocol used to route messages depends on the type of incoming call the Unified Messaging server answers.

Unified Messaging depends on the Active Directory directory service to route incoming calls. Each UM-enabled recipient must have a telephone extension number listed in Active Directory for call answering to function correctly. The extension number for the recipient is listed in Active Directory and is mapped to the extension number that's configured on the user's UM-enabled Exchange mailbox. When a Unified Messaging server answers a call, an Active Directory lookup is performed to locate the appropriate UM-enabled recipient and the message is routed to the recipient's mailbox.

Message Flow

Message flow in Unified Messaging is the process by which a message received by a Unified Messaging server is routed in an Exchange 2010 organization.

Note:

In earlier versions of Exchange, routing groups were used to route messages between bridgehead servers—known in Exchange 2007 and Exchange 2010 as Hub Transport servers. There are no routing groups in Exchange 2010.

For example, in an incoming call scenario that includes incoming voice messages, a Hub Transport server uses the SMTP transport protocol to submit the voice mail message to the Mailbox server. In a routing scenario that includes multiple Hub Transport servers, the incoming voice mail message is first submitted to the closest Hub Transport server and is

then routed to the Mailbox server that contains the UM-enabled mailbox.

Note:
The Unified Messaging servers use a spooling or retry algorithm to make sure all incoming messages are transmitted and delivered to UM-enabled recipients. They try to connect to a Hub Transport server every 30 seconds to submit all messages stored on the Unified Messaging server.

For more information about how the Unified Messaging server handles incoming calls and how messages flow in Unified Messaging, see the following topics:

- Unified Messaging Voice Call Processing
- Unified Messaging Outlook Voice Access Call Processing
- Unified Messaging Auto Attendant Call Processing
- Unified Messaging Play on Phone Call Processing

1.9.1.4.1 Unified Messaging Voice Call Processing

Unified Messaging Voice Call Processing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

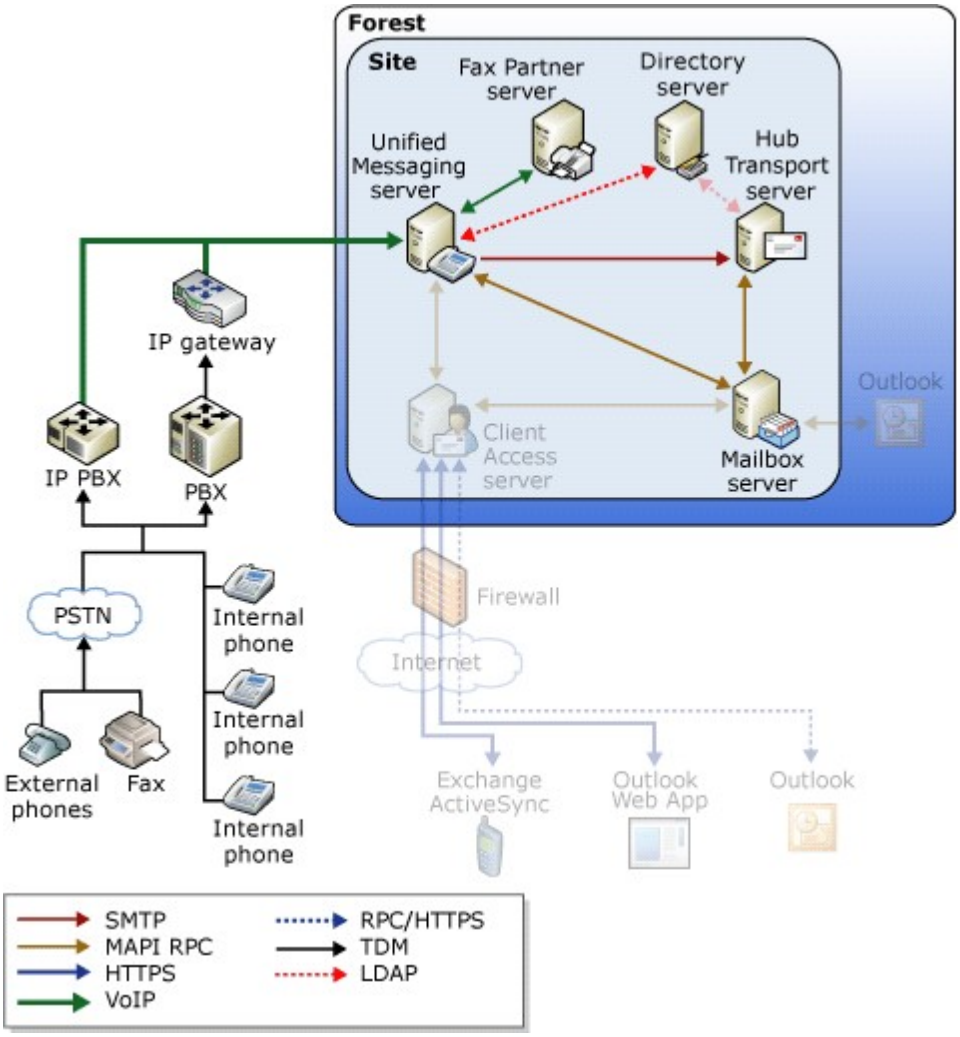
Topic Last Modified: *2011-04-28*

Incoming voice messages are received by your organization's telephony network and then passed to a Microsoft Exchange Server 2010 Unified Messaging (UM) server that handles and routes the incoming call. This topic discusses the message flow for incoming voice messages received by a Unified Messaging server.

Voice Incoming Messages

Voice calls that come in to an Exchange 2010 organization can be received from users who are inside or outside the organization. When a caller places a call to a UM-enabled user's telephone extension and the user is unavailable to answer the call, the Private Branch eXchange (PBX) forwards or routes the incoming call to an IP gateway and then to the Unified Messaging server. In a Unified Messaging system that uses an IP PBX, the IP PBX forwards the incoming message to the Unified Messaging server. The IP gateway or the IP PBX translates or converts the incoming stream into a Voice over IP (VoIP) protocol such as the Session Initiation Protocol (SIP) for incoming voice messages. The stream of IP data is then passed on to the Unified Messaging server. After the Unified Messaging server receives the call, the Unified Messaging server processes the message and determines how to route the message.

The following figure illustrates how incoming voice messages flow in an Exchange 2010 organization.



1.9.1.4.2 Unified Messaging Outlook Voice Access Call Processing

Unified Messaging Outlook Voice Access Call Processing

Unified Messaging > Understanding Unified Messaging > Understanding Unified Messaging Call Processing >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

When an authenticated UM-enabled user calls in to the Microsoft Exchange Server 2010 Unified Messaging (UM) system, the call is received by your organization's telephony network and then passed to an Exchange 2010 Unified Messaging server that handles and routes the incoming call. This topic discusses the message flow for incoming Outlook Voice Access calls to an Exchange 2010 Unified Messaging server.

Outlook Voice Access

With Exchange 2010 Unified Messaging, UM-enabled users or subscribers can access their e-mail, contacts, and calendaring information using a standard analog, digital, or mobile

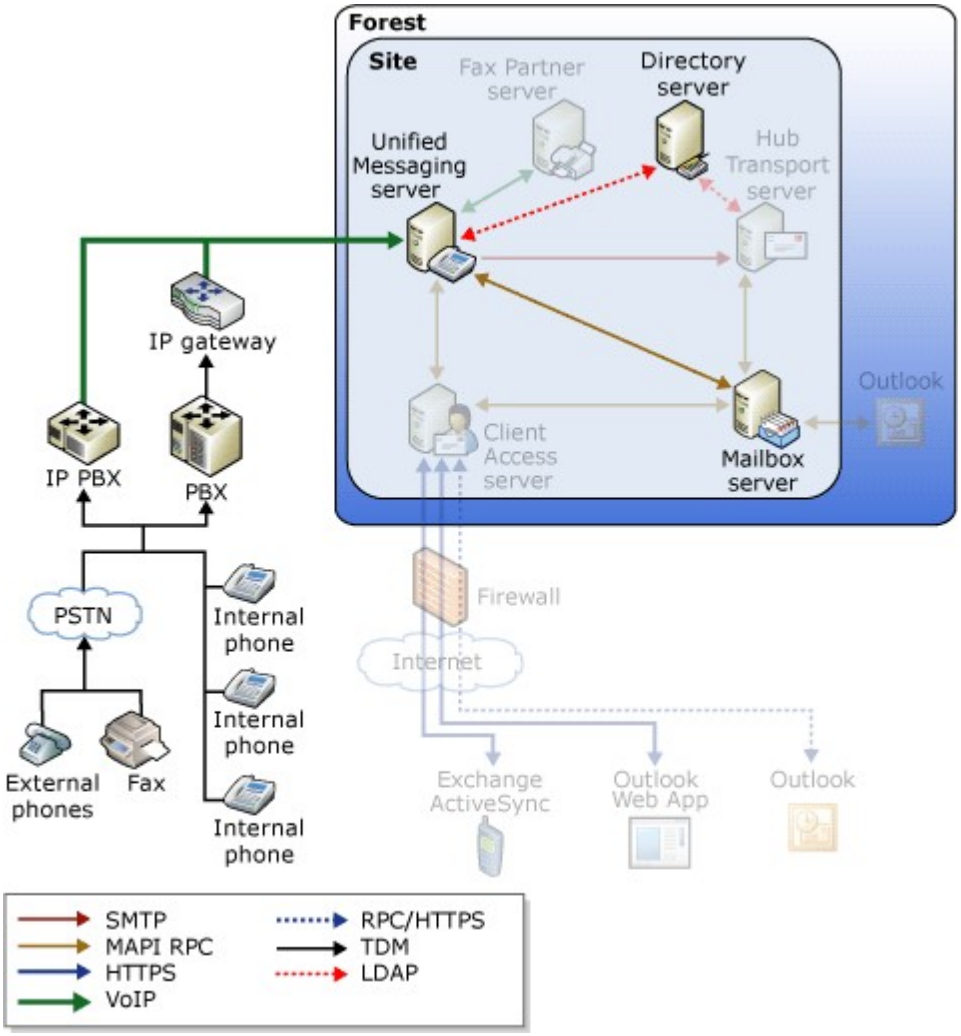
telephone. When UM-enabled users use Outlook Voice Access, they can perform the following tasks:

- Listen to new and saved e-mail and voice mail messages.
- Forward, reply, save, and delete e-mail and voice mail messages.
- Interact with their calendar.
- Locate a person in the global address list or personal contacts.
- Send a voice message to a person.
- Change their PIN, spoken name, or greetings.
- For more information about subscriber access in Exchange 2010 Unified Messaging, see Understanding Unified Messaging Subscriber Access.

Outlook Voice Access Message Flow

Outlook Voice Access incoming calls and messages created using Outlook Voice Access are routed to an Exchange 2010 Unified Messaging server and then to the Mailbox server. However, if a message is submitted using Outlook Voice Access, for example, a change in the schedule of a meeting from a subscriber, the message is submitted to a Hub Transport server before it's routed to the appropriate mailbox for the Exchange 2010 recipient or recipients.

The following figure illustrates how incoming calls and messages placed by subscribers or UM-enabled users flow in an Exchange 2010 organization.



1.9.1.4.3 Unified Messaging Auto Attendant Call Processing

Unified Messaging Auto Attendant Call Processing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Incoming calls received by a Unified Messaging (UM) auto attendant are first passed through your organization's telephony network and then to a Microsoft Exchange Server 2010 Unified Messaging server that handles and routes the incoming call. This topic discusses the message flow for incoming messages received by an Exchange 2010 Unified Messaging auto attendant.

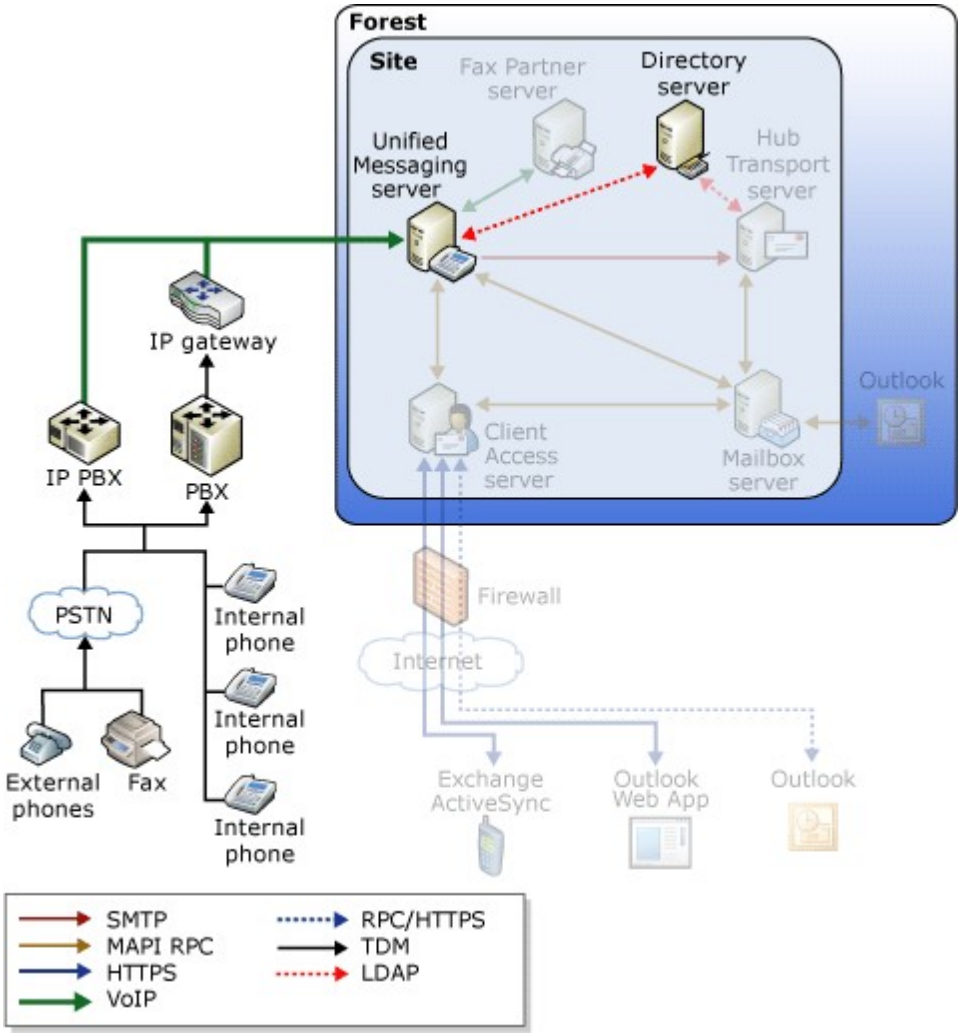
UM Auto Attendants

When external or anonymous callers place a call using an external business telephone number, or an internal anonymous caller places a call to an internal extension number, they are presented with voice prompts to help them navigate the Unified Messaging menu system. The UM auto attendant is a set of voice prompts or .wav files played to callers in place of a human operator or receptionist when they call into an organization that has Exchange 2010 Unified Messaging. Exchange 2010 Unified Messaging enables you to create one or more auto attendants depending on the needs of your organization. For more information about UM auto attendants, see Understanding Unified Messaging Auto Attendants.

Auto Attendant Message Flow

When a call is received by an Exchange 2010 Unified Messaging server, the Unified Messaging server performs an LDAP query to an Active Directory directory service domain controller to determine how to handle the incoming call.

The following figure illustrates the message flow process when Unified Messaging auto attendants are used in an Exchange 2010 organization.



1.9.1.4.4 Unified Messaging Play on Phone Call Processing

Unified Messaging Play on Phone Call Processing

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Incoming calls placed by users using the Play on Phone feature are received and routed by a Microsoft Exchange Server 2010 Unified Messaging server.

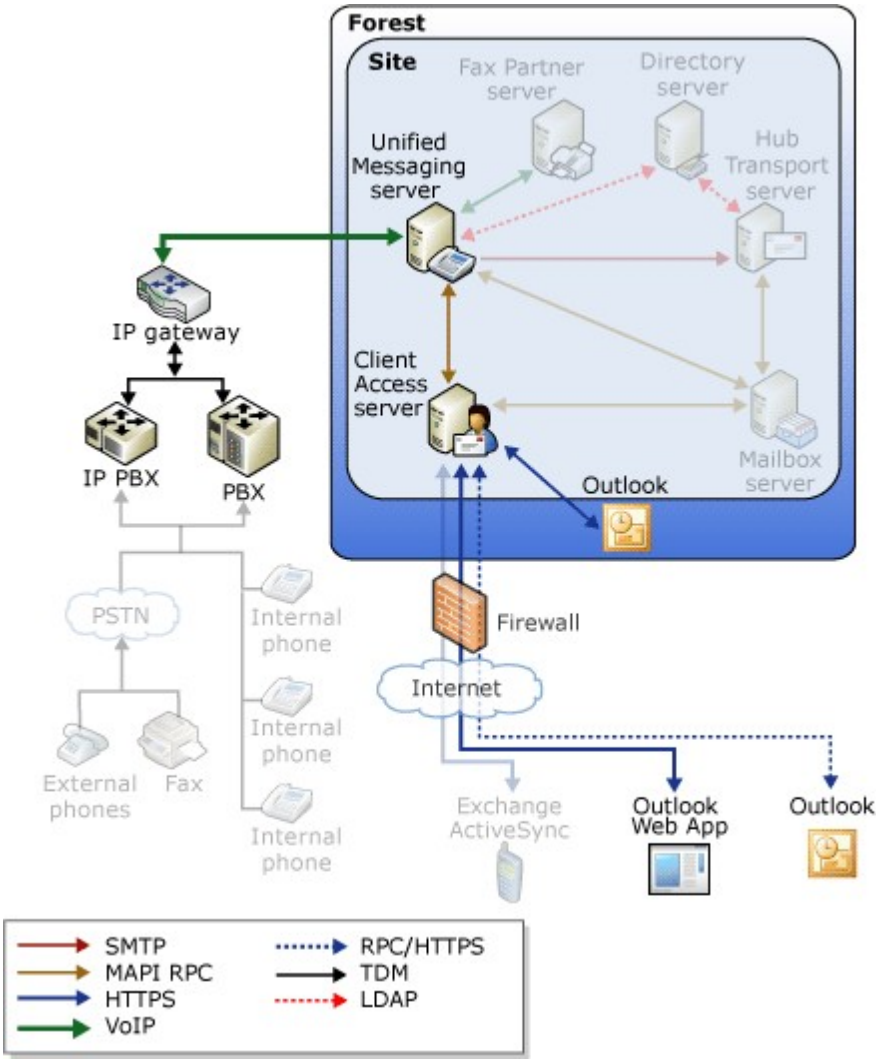
Play on Phone

The Exchange 2010 Unified Messaging Play on Phone feature enables UM-enabled users to access a voice mail message. However, instead of playing the media file over their computer speakers, they can listen to the message on a telephone.

When UM-enabled users work in office cubicles, use a public computer, have a computer

that isn't enabled for multimedia, or have a voice message that's confidential, they may not want to or may be unable to play a voice message over their computer speakers. The Play on Phone feature lets UM-enabled users play the voice message over a telephone. The Play on Phone feature is available in Exchange 2010 Outlook Web App and in Microsoft Office Outlook 2007.

The following figure illustrates how Exchange 2010 Unified Messaging routes the incoming calls for UM-enabled users who use the Play on Phone feature.



The Unified Messaging Web services are installed on Client Access server. Unified Messaging Web services enable Session Initiation Protocol (SIP) functionality on a Client Access server. This functionality enables a user to record a voice mail greeting or use the Play on Phone feature. The Unified Messaging server uses only SIP to communicate. Therefore, the UM Web service is installed on a computer running the Client Access server role and is required to enable the Client Access server to communicate with the Unified Messaging server.

Important:

By default, SIP data, which includes Unified Messaging server settings and other call information sent from a Unified Messaging server to a Client Access server, isn't encrypted. This could pose a security threat. To help protect all SIP traffic, use Transport

Layer Security (TLS) to encrypt the traffic between a Client Access server and a Unified Messaging server by configuring TLS security settings on the UM dial plan. For more information about SIP security and TLS, see Understanding Unified Messaging VoIP Security.

1.9.1.4.5 Call Routing with Office Communications Server 2007

Call Routing with Office Communications Server 2007

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-07*

Microsoft Exchange Server 2010 Service Pack 1 (SP1) or later Unified Messaging (UM) combines voice messaging and e-mail messaging into a single messaging infrastructure. Enterprise Voice in Microsoft Office Communications Server 2007 takes advantage of the UM infrastructure to provide call answering, subscriber access, call notification, and auto-attendant services. Implementing these services requires integration of Exchange UM and Communications Server 2007 in a shared Active Directory topology. Working together, Unified Messaging and Communications Server 2007 provide call answering, Outlook Voice Access, and auto-attendant services to Enterprise Voice deployments.

Deploying Exchange UM for Communications Server requires you to install the Exchange Mailbox, Hub Transport, Client Access, and Unified Messaging server roles in each forest where Unified Messaging is deployed. Exchange 2010 Unified Messaging requires that all Enterprise Voice users be configured with a Microsoft Exchange Server 2007, Exchange 2007 Service Pack 3 (SP3), or Exchange 2010 SP1 or later mailbox.

If you plan to move users from an existing telephony infrastructure to Enterprise Voice, moving them to Unified Messaging is the last step in the migration process.

Routing Components for Enterprise Voice

Enterprise Voice functionality is handled by services running on Communications Server 2007 Enterprise Edition and Communications Server 2007 Standard Edition. When a user is enabled for Enterprise Voice, Microsoft Office Communicator 2007 or Communicator Phone Edition becomes the user's primary phone, instead of his or her PBX phone. A unique phone number will be assigned to Communicator. In combination with a recommended USB audio device, Communicator will handle both the call control (or signaling) and the media (audio and video). In this scenario, Communications Server 2007 routes calls among Communicator endpoints on the IP network (IP-IP calls) and routes those calls to the Public Switched Telephone Network (PSTN).

To download the reference and Help documentation for Communications Server 2007, see Office Communications Server and Client Documentation Rollup.

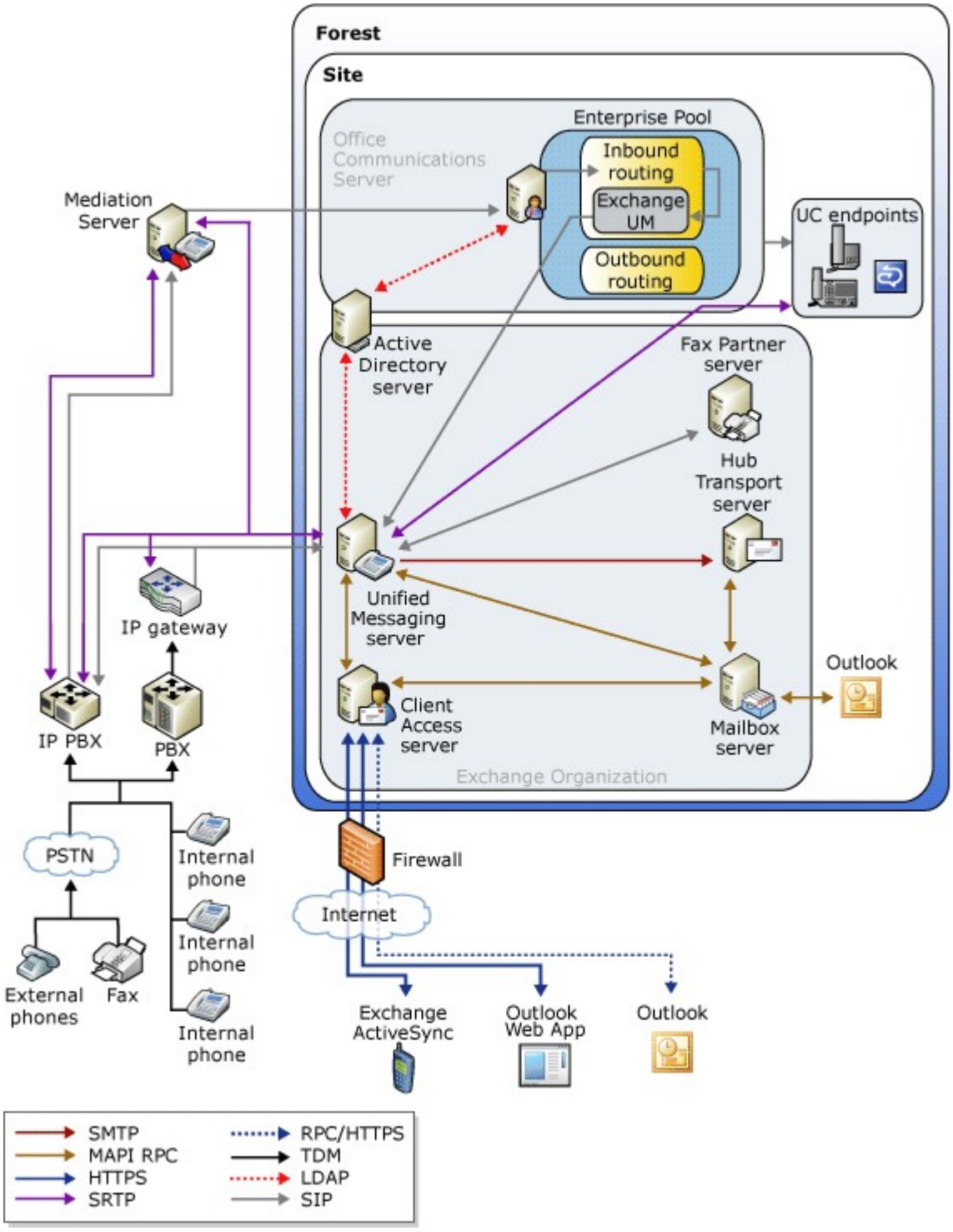
Enterprise Voice services include an Inbound Routing component. By default, the Inbound Routing component is installed on all Communications Server 2007 Standard Edition servers and Enterprise Edition front-end servers and is needed for routing incoming calls for Enterprise Voice users. Enterprise Voice services include the following, which control inbound and outbound calling:

Service	Description
Inbound Routing Component	Applies the target user's calling preferences.

Exchange Unified Messaging	Forwards the request to voice mail, as needed.
Outbound Routing Component	Determines the optimal route, based on URI and user policy.
Translation Service	Applies normalization rules, based on the location profile or phone context.
User Services	Performs reverse number lookup on the target phone number.

Inbound Routing and Exchange Unified Messaging

The Inbound Routing component determines how incoming calls to the server should be routed. When this component is used with Exchange UM, it enables voice mail services for Enterprise Voice enabled users. The following figure shows how the Inbound Routing component in Communications Server 2007 is used to send an incoming call to an Exchange Unified Messaging server.



The Inbound Routing component handles incoming calls largely according to preferences that are specified by users on their Enterprise Voice clients. For example, users specify whether unanswered calls are forwarded or only logged for notification. If call forwarding is enabled, users can specify whether unanswered calls should be forwarded to another number or to an Exchange 2007 SP3 or Exchange 2010 Unified Messaging server that's been configured to provide call answering.

The Inbound Routing component controls many options for Enterprise Voice users including options for voice mail such as:

- **Route Unanswered Calls to Voicemail** This is the default if the user is enabled for voice mail. The call is routed according to Inbound Routing rules.
- **Generate Missed Call Notifications when caller hangs up before call reaches voicemail** Notifies Exchange UM when this type of missed call is received.

Inbound routing rules specify how calls to a user should be routed in the presence or absence of registered clients in the system. The Inbound Routing component also takes care of applying presence-based rules to incoming calls. For example, it can send incoming calls to voice mail if the user has set the presence state to Do Not Disturb. Inbound routing is aware of the presence container levels and automatically rejects calls from users in blocked containers.

Inbound routing rules are uploaded to the server as an XML schema as part of an Enterprise Voice user's self-provisioning information. By default, if the incoming call isn't answered within the ring duration, the unanswered call is sent to voice mail. The user can choose to modify the default configuration by choosing whether to forward to a number immediately, forward to another person, or to send the caller directly to voice mail.

1.9.1.5 Understanding Unified Messaging Server Topologies

Understanding Unified Messaging Server Topologies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

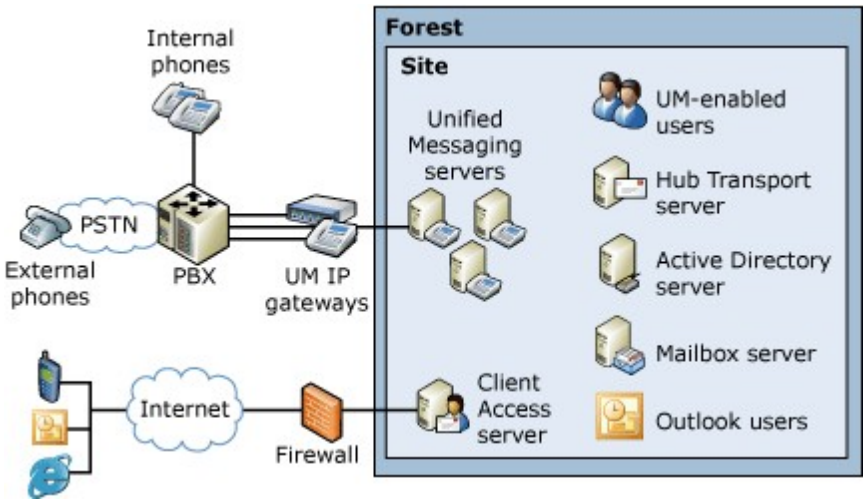
Topic Last Modified: *2010-05-13*

Microsoft Exchange Server 2010 supports a server architecture that distributes server tasks among different server roles. In this kind of architecture, a Unified Messaging (UM) server accepts incoming calls. The Unified Messaging server then routes the messages to the appropriate server for processing. This could be the Client Access server, the Mailbox server, or the Hub Transport server. The server that has the Hub Transport server role installed was formerly known as a bridgehead server.

This topic describes the relationship between the Unified Messaging servers on a typical network and the telephony components in an organization.

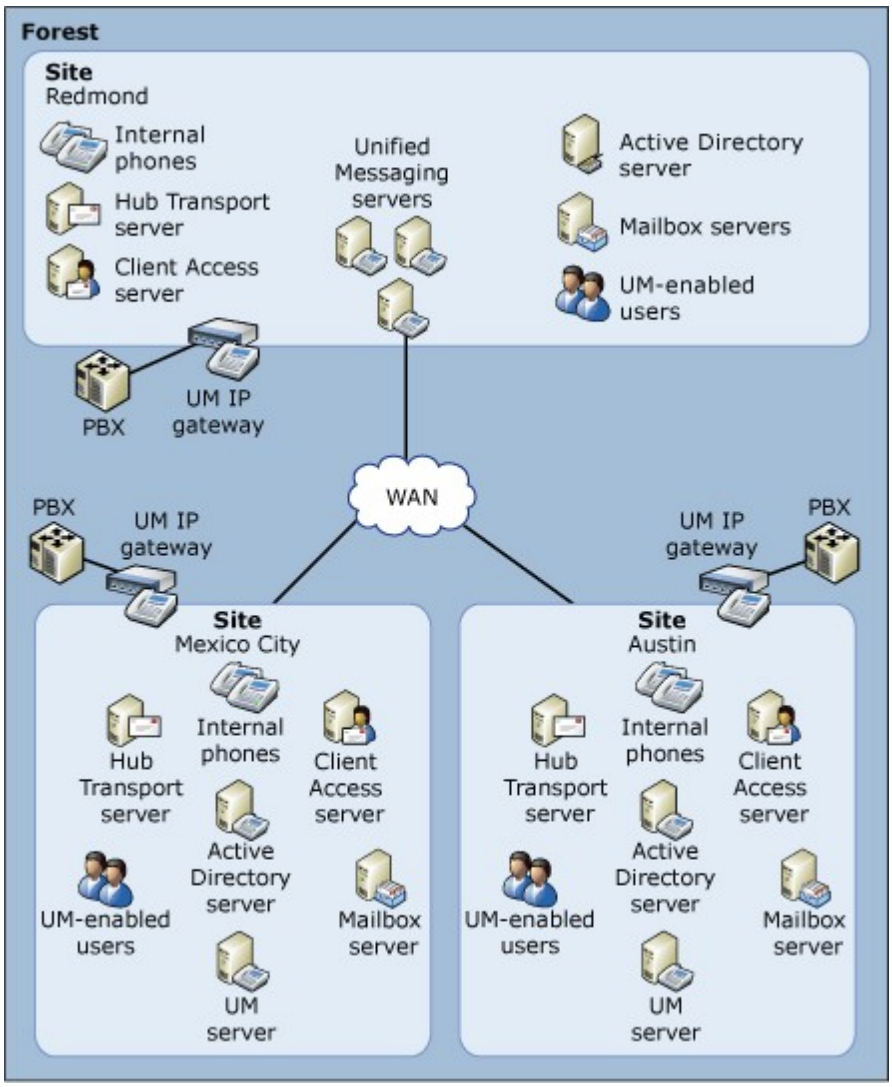
UM Topology That Has a Single PBX

The following figure illustrates an Exchange Server 2010 Unified Messaging topology that contains a single Private Branch eXchange (PBX).



UM Topology That Has Multiple PBXs

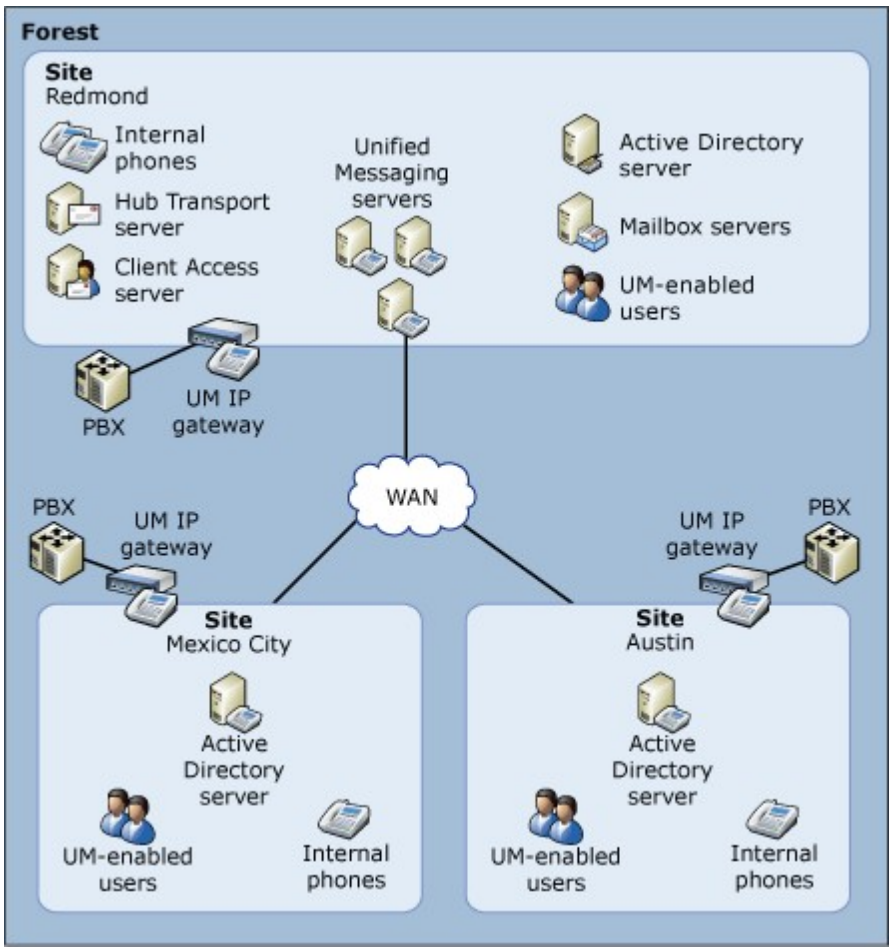
The following figure illustrates an Exchange 2010 Unified Messaging topology that contains multiple PBXs.



The following figure illustrates centralized management system for an Exchange 2010 Unified Messaging topology that contains multiple PBXs. This configuration enables the placement of all Unified Messaging servers in a single location. IP gateways are deployed in each branch office, and replace the legacy voice messaging system for each branch office. Because IP gateways are close to the PBX, the Hub Transport, Client Access, and the Mailbox servers can be removed from both the Mexico City and the Austin sites.

Note:

The round trip time between the IP gateways and UM servers should not be more than 300 milliseconds.



1.9.1.6 Understanding Unified Messaging and Communications Server 2007 R2

Understanding Unified Messaging and Communications Server 2007 R2

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Microsoft Exchange Server 2010 Unified Messaging (UM) can use the Microsoft Office Communications Server 2007 platform to combine voice messaging, instant messaging, enhanced presence, audio/video conferencing, and e-mail into a familiar, integrated communications experience. This communication method has the following benefits:

- Enhanced presence notifications across a variety of applications that keep users informed of the availability of contacts.
- Integration of instant messaging, voice messaging, conferencing, e-mail, and other communication modes that enables users to select the most appropriate mode for the task. Users can also switch from one mode to another as needed.
- Availability of communications alternatives from any location where an Internet connection is available.
- A smart client (Microsoft Office Communicator 2007) for telephony, instant

messaging, and conferencing.
- Continuity of user experience across multiple devices.

This topic discusses how Exchange 2010 Unified Messaging and Communications Server 2007 can be deployed together to provide voice messaging, instant messaging, enhanced presence, audio/video conferencing, and e-mail into an integrated communication experience for users in your organization.

Caution:
To use the features described in this topic, Exchange 2010 must be installed on the computers that have the Unified Messaging server role installed.

Contents

Overview

All Communications Server 2007 topologies support Enterprise Voice. Enterprise Voice is an implementation of IP telephony that uses Session Initiation Protocol (SIP) for signaling and Realtime Transport Protocol (RTP) for voice messaging. SIP is an industry standard, application layer signaling protocol for starting, controlling, and ending communication sessions in an IP-based network. SIP is formally described in the International Engineering Task Force (IETF) reference specification RFC 3261.

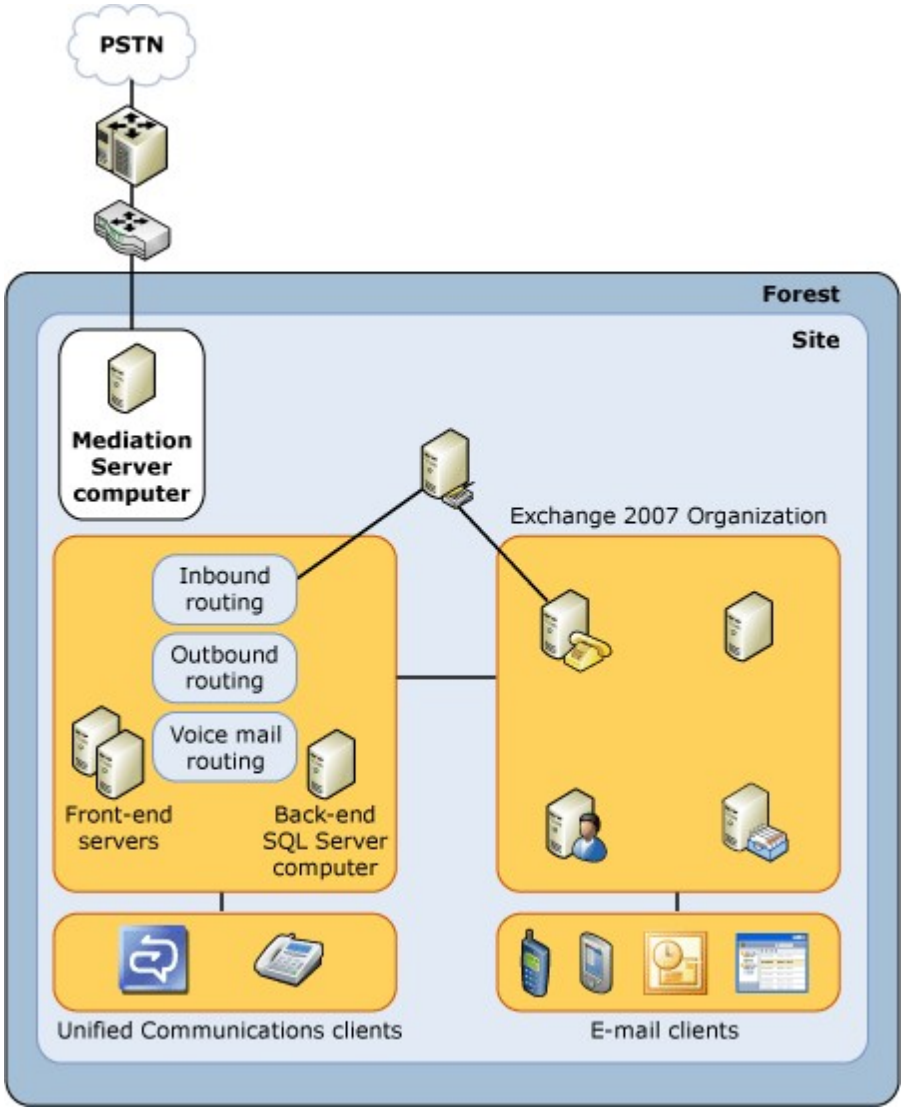
In Communications Server 2007, SIP is used for instant messaging, conferencing, presence subscriptions, video, and voice messaging. SIP enables Enterprise Voice clients to provide a common user experience across all these communication modes. Enterprise Voice uses RTP for media. Like SIP, RTP is an IETF standard. It defines a packet format for carrying audio and video over IP networks.

When a user places a call from an Enterprise Voice client to a Public Switched Telephone Network (PSTN) destination, the call moves through the Enterprise Voice infrastructure as follows:

1. The user places a call from an Enterprise Voice client by dialing the number or by clicking the name of a contact in Communicator or Microsoft Office Outlook 2007.
2. The Communications Server 2007 server normalizes the telephone number to E.164 format, and then uses the routing rules based on location profile and user policy to direct the call to the correct mediation server.
3. The Communications Server 2007 mediation server performs any necessary media translation and routes the call to the IP gateway.
4. The IP gateway applies local dialing rules or Private Branch eXchange (PBX) dialing rules and passes the call to the PSTN, PBX, or IP PBX.

The following figure illustrates a simple Unified Messaging and Communications Server 2007 topology.

Exchange 2010 Unified Messaging and Communications Server 2007 simple topology



Communications Server 2007 Overview

Communications Server 2007 Enterprise Voice takes advantage of the Unified Messaging infrastructure to provide voice mail, subscriber access, call notification, and auto attendant services. These include the following:

- **Phone number normalization** Phone number normalization translates number strings entered in various formats into a single standard format. Normalization rules specify how to convert telephone numbers dialed in various formats to standard E.164 format.
- **Location profiles** A location profile is a named set of normalization rules that translates telephone numbers for a location to a single standard (E.164) format for telephone authorization and call routing. The name of each location profile must match the fully qualified domain name (FQDN) of its corresponding Exchange 2010 UM dial plan.
- **Phone usage records** Phone usage records provide a quick, easy way to assign call permissions to users. To enable phone usage records to function correctly, you must assign a voice policy for the call to be correctly routed to the voice user.
- **Voice policies** Enterprise Voice policies are collections of phone usage

records assigned to one or more users. Most organizations will have multiple voice policies. Typically, organizations have a global policy that applies to all users and special policies applied on a per-user basis.

- **Call routing** The core routing components for Communications Server 2007 are the Inbound and Outbound Routing Components, as follows:
  - **Inbound Routing Component** The Inbound Routing Component handles incoming calls largely according to preferences specified by users on their Enterprise Voice clients. Users specify whether unanswered calls are forwarded or logged for notification.
  - **Outbound Routing Component** The Outbound Routing Component handles calls placed by Enterprise Voice users either to telephone numbers owned and managed by the enterprise or to telephone numbers on the PSTN or mobile networks. When an enterprise user places a call, the Outbound Routing Component looks up the target number in the Realtime Communication (RTC) database. If the dialed number matches a SIP Uniform Resource Identifier (URI) for an enterprise user, the call is routed through all SIP endpoints for that user.

Important:

When you are integrating Exchange Unified Messaging and Office Communications Server, you'll probably find it unnecessary to configure dialing rules or dialing rule groups in Exchange Unified Messaging. Office Communications Server is designed to perform call routing and number translation for users in your organization, and will also do this when the calls are made by Exchange Unified Messaging on behalf of users.

- **Services** The setup routing for Communications Server 2007 installs services that provide support for voice messaging with Exchange 2010 Unified Messaging, including the following:
  - **Translation Service** The Translation Service is the application responsible for translating the dialed number into an E.164 number based on the normalization rules defined by the administrator.
  - **Enterprise Services** Enterprise Services performs reverse number lookup on the target telephone number of each incoming call, matches that number to the SIP URI of the destination user, and sends the call to that user's SIP endpoints.
  - **User Replicator** The User Replicator extracts user telephone numbers from the Active Directory directory service and writes them to tables in the RTC database, where they are available to Enterprise Services and the Address Book Service.
  - **Address Book Service** The Address Book Service normalizes enterprise user telephone numbers written to the RTC database to E.164 format to provision user Contacts in Communicator.

To download the reference and Help documentation for Communications Server 2007, see Office Communications Server and Client Documentation Rollup.

Return to top

Exchange 2010 Unified Messaging

The Unified Messaging server role is one of several Exchange 2010 server roles that you can install and configure on a computer running Exchange 2010. For Enterprise Voice users, Unified Messaging combines voice messaging and e-mail messaging into a single store that can be accessed from a telephone or a computer. Unified Messaging and Communications Server 2007 work together to provide voice mail, subscriber access, and auto attendant services to Enterprise Voice deployments, including the following:

- **Voice mail** Voice mail includes answering an incoming call on behalf of a user, playing a personal greeting, recording a message, and submitting it for

delivery to the user's Inbox as an e-mail message. Notification of unanswered calls is sent to the user's Outlook and Outlook Web App Inboxes. The subject and priority of calls can be displayed in a way that resembles the way they are displayed for e-mail.

- **Subscriber access** A subscriber is an internal business user or network user who is enabled for Exchange 2010 Unified Messaging. Subscriber access is used by users to access their individual mailboxes to retrieve e-mail, voice messages, contacts, and calendaring information. Outlook Voice Access is an Exchange 2010 Unified Messaging feature that lets subscribers access their Exchange 2010 mailbox. Subscriber access enables an Enterprise Voice user to access voice mail, calendar, and contacts from a telephony interface. A subscriber access number is configured by you on a UM dial plan. For more information about Outlook Voice Access, see Understanding Unified Messaging Subscriber Access.
- **Auto attendant** In telephony or Unified Messaging environments, an automated attendant or auto attendant menu system transfers callers to the extension of a user or department without the intervention of a receptionist or an operator. In many auto attendant systems, a receptionist or operator can be reached by pressing or saying zero. The automated attendant is a feature in most modern PBXs and Unified Messaging solutions. For more information about auto attendants in Exchange 2010 Unified Messaging, see Understanding Unified Messaging Auto Attendants.

For more information about Exchange 2010 Unified Messaging, see Unified Messaging.

There are four user scenarios in which Communications Server 2007 and Exchange 2010 Unified Messaging can be used together. These are:

- **Call notification** User 1 calls User 2. User 2 doesn't answer the call. User 1 hangs up. User 2 receives an e-mail message in the Exchange 2010 mailbox that User 1 called. Call notifications are also sent when an inbound call is forwarded. User 1 calls User 2. User 2 sets call forwarding to User 3. User 1 calls User 2. The call is forwarded to User 3, and User 2 receives a call notification that the call was forwarded.
- **Leave a voice mail message** User 1 calls User 2. User 2 doesn't answer the call. Because User 2 hasn't configured call forwarding to another telephone number, the call from User 1 is diverted to the voice mail for User 2. User 1 is invited to leave a voice message for User 2. The voice mail greeting previously recorded by User 2 is played, inviting User 1 to leave a voice message for User 2. User 2 receives a voice mail message recorded by User 1.
- **Subscriber access** User 2 dials in to a subscriber access number and accesses the Exchange 2010 mailbox to check for voice messages. User 2 can listen to e-mail or voice mail messages or access the calendar. After listening to the voice message from User 1, User 2 decides to return the call from User 1. User 2 accesses the options menu and uses the callback option to place a call to User 1.
- **Auto attendant** User 1 doesn't know the extension number for User 2. User 1 dials in to a telephone number configured on a UM auto attendant. The welcome greeting and prompts configured on the auto attendant are played to User 1. User 1 uses the directory search feature to locate User 2 in the directory and places a call to the extension number for User 2.

Note:

Both subscriber access and those auto attendant services offered by Exchange 2010 Unified Messaging require users to dial specific telephone numbers. These numbers must be routable by Enterprise Voice. This means that each number must be mapped to a SIP address. Communications Server 2007 can route the SIP address to an address configured on the server that has the Exchange 2010 Unified Messaging server role installed.

Return to top

Exchange 2010 Unified Messaging Active Directory Objects

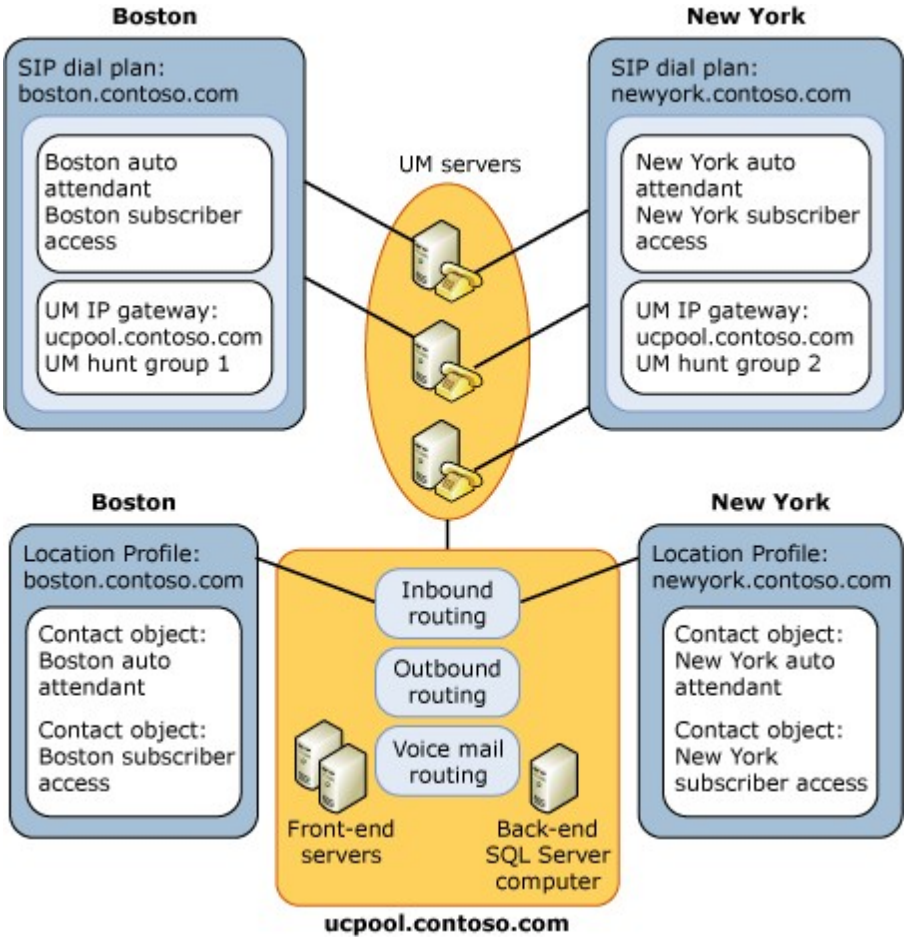
Exchange Unified Messaging Active Directory objects enable Exchange 2010 Unified Messaging to integrate with the Communications Server 2007 Enterprise Voice infrastructure. To successfully deploy Exchange 2010 Unified Messaging in your organization, you must fully understand the relationship between each of following UM Active Directory objects and their counterparts in Enterprise Voice:

- **UM Dial Plan object** A UM Dial Plan object is the basic unit of configuration in Exchange Unified Messaging. A UM dial plan can be of the following types: Telephone Extension, SIP URI, or E.164. When Exchange Unified Messaging is deployed with Communications Server 2007, the dial plan type is always SIP URI. Users in a UM dial plan reach all other users in the plan using SIP URIs or SIP addresses. Each SIP address must be unique within a specific SIP URI dial plan. Each dial plan must correspond to an Enterprise Voice location profile. The name of each location profile must match the forest FQDN of the SIP URI dial plan.
- **UM IP Gateway object** A UM IP Gateway object is a logical representation of a physical IP gateway or SIP-enabled IP PBX. The UM IP Gateway object logically represents each Communications Server 2007 pool and front-end server as if it were a physical IP gateway. Each UM IP Gateway object encapsulates configuration elements related to the corresponding pool or server. After a UM IP Gateway object is created, it's associated with one or more UM hunt groups.
- **UM Hunt Group object** The UM Hunt Group object associates a UM IP gateway with a UM dial plan. By creating multiple UM Hunt Group objects, you can associate a single UM IP gateway with multiple UM dial plans and, therefore, with multiple Enterprise Voice location profiles.

For more information about the Active Directory objects included in Exchange 2010 Unified Messaging, see Understanding Unified Messaging Components.

The following figure illustrates the relationships between Exchange 2010 Unified Messaging objects and Communications Server 2007 objects.

Unified Messaging and Communications Server 2007 objects and their relationships



Exchange 2010 Unified Messaging combines voice messaging and e-mail messaging into a single messaging infrastructure. Communications Server 2007 Enterprise Voice takes advantage of the Unified Messaging infrastructure to provide voice mail, subscriber access, call notification, auto attendant services and other enhanced features that include voice messaging, instant messaging, enhanced presence, audio/video conferencing, and e-mail into an integrated communication experience for users in your organization. Implementing these services requires integrating Unified Messaging and Communications Server 2007 in a shared Active Directory topology. For more information about the configuration steps required to correctly deploy and integrate Exchange 2010 Unified Messaging and Communications Server 2007, see Deploy Unified Messaging and Communications Server 2007 R2.

To download the reference and Help documentation for Communications Server 2007, see Office Communications Server and Client Documentation Rollup.

Return to top

1.9.1.7 Understanding Unified Messaging Performance and Scalability

Understanding Unified Messaging Performance and Scalability

Exchange Server 2010 > Unified Messaging > Understanding Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-30*

In many organizations today, the ability to access e-mail and voice mail is critical to the success of daily operations. To provide continuous access to e-mail and voice mail, you must correctly plan and implement a solution for Microsoft Exchange Server 2010 that will ensure the availability of the servers that provide these services. To provide a highly scalable solution in Exchange 2010 Unified Messaging (UM), you have to understand how the UM components can be scaled to support your users.

Unified Messaging Server Scalability

Scalability is defined as the capability to increase resources to increase the capacity of a given service. There are two types of scalability that can be used to increase the capacity of UM servers in your organization: horizontal and vertical. In Unified Messaging, when you scale vertically, you add hardware resources to a single UM server or multiple UM servers, by, for example:

- Adding more hard disk space for message storage
- Increasing the speed or number of processors
- Increasing the amount or speed of RAM
- Increasing the number of network adapters or increasing the number of local area network ports in a single network adapter

In Unified Messaging, when you scale horizontally, you install the Unified Messaging server role on new UM servers and add more UM servers to a dial plan to increase the number of incoming concurrent calls the system can accept. To scale your UM environment horizontally, you can also increase the number of IP gateways. This increases the number of ports available to be used for incoming calls.

Unified Messaging provides an efficient and simple deployment model that's highly scalable without increasing the complexity of the deployment. There are many deployment models for Unified Messaging in your organization. But the recommended deployment model for Unified Messaging is to centralize your UM servers. All the available deployment options for Unified Messaging have several steps in common that are required to create a scalable system to support large numbers of UM users. These steps are as follows:

1. **Provision PBX lines** The first step in building a highly scalable UM solution is to provision PBX lines.
2. **Organize channels** After you've provisioned PBX-based voice channels, you can organize the channels as hunt groups.
3. **Deploy IP gateways** After you've organized your voice channels as hunt groups, you end these channels at IP gateways. IP gateways are used with a legacy PBX to convert the circuit-switched protocols found on a telephony network to IP-based packet-switched protocols.
4. **Add more Unified Messaging servers to a dial plan** If you have to increase the number of calls that can be handled by Unified Messaging, you can install and set up additional UM servers and add them to a dial plan. In most cases, IP gateways will use DNS to load balance between the existing UM servers and the additional UM servers that have been installed.

Return to top

Network Traffic

Every incoming call received from an IP gateway will generate IP-based network traffic and consume some amount of your available network bandwidth. Before you deploy Unified Messaging, you should perform an analysis of the network traffic to determine current usage patterns and find any potential issues. On most networks, bandwidth demand isn't evenly distributed throughout business hours. Because all the IP-based calls are routed directly to your UM servers from the IP gateways on your network and this IP-

based network traffic consumes some available bandwidth, you should follow these recommendations and guidelines:

- Place your PBXs physically close to your IP gateways.
- Place your IP gateways and your UM servers on the same well-connected network or within the same physical site.
- Place your UM servers on the same well-connected network or within the same physical site as other computers that have Exchange 2010 server roles installed, including Mailbox, Hub Transport, and Client Access servers.
- End your Wide Area Network (WAN) connections close to where your telephony equipment is located.
- In branch office scenarios or over WAN connections, use the G.723.1 codec instead of the G.711u or G.711A codec to minimize the network traffic that's passed between your IP gateways and your UM servers.

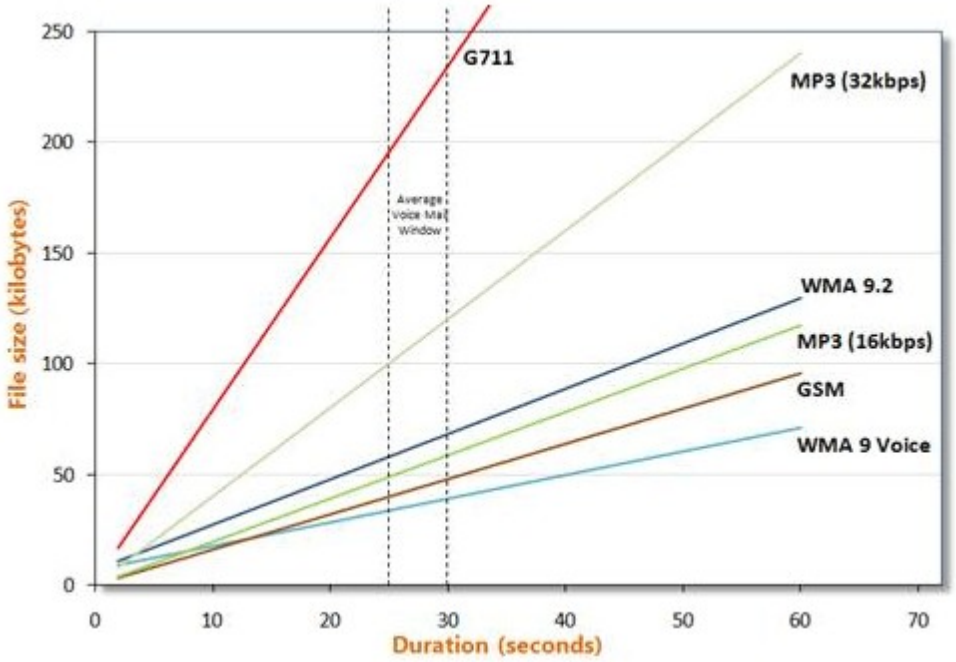
UM Servers

Generally, Unified Messaging scalability is determined by the number of concurrent calls. By default, a single UM server can accept a maximum of 100 concurrent voice calls. These calls can be either incoming or outgoing, and can be generated when a user leaves a voice mail message, when an Outlook Voice Access user accesses their Exchange 2010 mailbox, or when a user uses the Play on Phone feature to listen to their voice messages. Although the number of concurrent calls is an important factor to consider when you build a scalable UM infrastructure, you also have to determine the best codec to use to encode the voice messages and the types and number of users who you have to support.

- **Number of concurrent calls** Although, by default, a UM server can accept 100 concurrent voice calls, a single UM server can be set up to accept a maximum of 200 concurrent voice messages. The more you increase the number of concurrent connections on a single UM server, the more resources will be required. It's especially important to decrease this setting on low-end, slower computers on which the UM server role is installed. Performance counters are available, and the **Get-UMActiveCalls** cmdlet can also be used to monitor the number of calls that are currently connected to a UM server.
  If the number of concurrent calls required by your organization is larger than the number that's supported by a single UM server, you can scale horizontally and increase the capacity of concurrent calls by installing the Unified Messaging server role on an additional server and then adding the new UM server to the same dial plan.
- **Voice mail storage codec** The term "codec" is a combination of the words "coding" and "decoding" and relates to digital data. A codec is a computer program or software that transforms digital data into an audio file format or streaming audio format.
  In Microsoft Exchange Unified Messaging, there are two general types of codecs: the codec that's used between IP gateways and the codec that's used to encode voice messages. The MP3, Windows Media Audio (WMA), Group System Mobile (GSM) 06.10, and G.711 Pulse Code Modulation (PCM) Linear audio codecs are used to create mp3, .wma and .wav audio files for voice messages. But the file type that's used depends on the audio codec that's used to create the voice message audio file. In Microsoft Exchange Unified Messaging, the MP3 audio codec creates .mp3 audio files, the WMA audio codec creates .wma audio files, and the GSM 06.10 and G.711 PCM Linear audio codecs produce .wav audio files. Depending on the codec that's used, an audio file in .wma or .wav format is sent together with the e-mail message to the intended voice mail recipient. The size of UM voice messages depends on the size of the attachment that holds the voice data. Additionally, the size of the attachment depends on the following factors:
  - The duration of the voice mail recording
  - The audio codec that's used
  - The audio file storage format

  The following figure shows the four audio codecs you can use in Unified Messaging and how the size of the audio file depends on the duration of the

voice mail recording.



The sample bit rate (bit/sec) and compression properties for each audio codec that's used in Unified Messaging are as follows:

- MP3 - 16 bit - compressed file
- WMA – 16-bit – compressed file
- G.711 – 16-bit – uncompressed file
- GSM – 8-bit – compressed file

By default, the MP3 format is selected. The MP3 format is a common audio file format that's used to greatly reduce the size of the audio file and is most commonly used by personal audio devices or MP3 players. MP3 is a cross-platform type of audio codec and is used for compatibility with many mobile phones and devices and different computer operating systems.

When the WMA codec is used, we estimate that each UM server can handle 60 to 75 concurrent IP-based calls. This estimate is based on the assumption that 14 percent of all the IP-based calls arrive during the single busiest hour of a day. Based on the following assumptions:

- The WMA codec is used
- 14 percent of all IP-based calls arrive during the single busiest hour of a day
- Your users access their voice messages frequently using Outlook Voice Access

we estimate that each UM server can support between 2,000 and 10,000 users.

Generally, you should allow for the following number of concurrent calls per UM server:

- 60, if the default dial plan codec is WMA
- 75, if the default dial plan codec is GSM

- **Types of users** There are two types of users who access the UM system and consume UM resources: authenticated users and unauthenticated users. When you build a scalable UM environment, you have to consider the effect these users will have and the resources each of these users will consume.
  - **Authenticated** Authenticated users are UM-enabled and can access their mailbox using Outlook Voice Access. Authenticated users consume UM server resources in several ways, for example, by directly calling in to a subscriber access number, signing in to their mailboxes, accessing their messages, calendar, contacts, or the directory, and using a UM server to play voice

messages over a telephone with the Play on Phone feature. They can also indirectly consume resources by transferring a call, sending a voice message, or calling a user's extension number and leaving a voice message.

- **Unauthenticated** Users who call in to a UM auto attendant or call in to a subscriber access number but don't sign in to their mailbox are unauthenticated callers. UM resources are used to service their requests every time they call in to a UM auto attendant or use a subscriber access number. Even though they don't sign in to their mailbox, they still consume resources by transferring a call, sending a voice message, transferring to another auto attendant, transferring to another telephone number, or listening to recorded audio prompts.

IP Gateways

Unified Messaging relies on the ability of the IP gateway to translate TDM or telephony circuit-switched based protocols, such as Integrated Services Digital Network (ISDN) or QSIG, from a PBX to protocols based on VoIP or IP, such as SIP, RTP, or T.38 for real-time facsimile transport.

IP gateways are available from multiple manufacturers in sizes and models that range from 4 ports to 32 ports. You can deploy as many IP gateways as necessary to provide for capacity and fault tolerance. If the number of calls or ports required is larger than the number of calls or ports supported by a single IP gateway, you can scale horizontally and increase the number of calls that can be accepted or the number of ports by installing and setting up additional IP gateways, creating the UM IP gateway object, and setting up the appropriate hunt groups to support your environment.

It's equally important to match the number of IP gateways you have in your environment to the number of UM servers that are available. For example, you shouldn't set up 10 IP gateways that are each connected with a T-1 line to a single UM server. This would mean that the UM server would have to support 240 concurrent incoming calls. You should consider this and scale your IP gateways to UM servers appropriately.

Return to top

1.9.1.8 Understanding Unified Messaging Availability

Understanding Unified Messaging Availability

Exchange Server 2010 > Unified Messaging > Understanding Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-03*

In many organizations today, accessing e-mail and voice mail is critical to the success of daily operations. To provide continuous access to e-mail and voice mail, you have to correctly plan and implement a solution for Microsoft Exchange Server 2010 that will ensure the availability of the servers that provide these services. You need to understand how to implement a solution that will make your Unified Messaging servers highly available.

Unified Messaging Availability

Minimum uptime requirements may vary among organizations. But every organization wants to achieve a high level of up time, especially for their telephony system. An

organization's telephony system is frequently business-critical and must be highly available to users. One of the factors you need to consider when you deploy a UM system is the ability for the system to provide services for users when a key component, for example, a UM server or an IP gateway, becomes unavailable.

To provide a highly available UM system, you must include additional key components to protect against hardware failures for the following:

- **UM servers** Unified Messaging runs as a service and a worker process. This means that if the service is using lots of system resources or has become unresponsive, the worker process can be recycled. The UM worker process is responsible for dealing with outages in Mailbox servers, Hub Transport servers, and domain controllers. If, for example, a Mailbox server for a user is unavailable, the UM server will continue to accept calls on behalf of the user. But the user's custom greeting won't be played. Instead, a standard greeting will be used for calls to that user. Additionally, if the Hub Transport server is unavailable, the UM server will continue to accept calls and queue the calls, depending on how you've set up the queuing limit, until the Hub Transport server is available. In a situation where all domain controllers are unavailable, the UM server will be unable to accept calls.
  UM deployments can be made more resilient and more available by adding UM servers to a single dial plan in an N+1 configuration. This means that, if you need two UM servers, you'd install and set up an additional UM server so you'd have a UM server to take the place of a UM server that's failing or has to be taken offline.
  When you add multiple servers to a single dial plan, the IP gateway will try to connect to a UM server that's listed in the configuration on the IP gateway by IP address, or by fully qualified domain name for TLS deployments. If the UM server is unavailable, the IP gateway will try to connect to the UM server again after 5 seconds. If there is no response from the UM server, the IP gateway will try to connect to the next UM server in the list that's set up on the IP gateway.
- **IP gateways** If you want to create redundancy to provide for IP gateway availability, you should add multiple IP gateways in an N+1 configuration. This means that, if you need two IP gateways, you'd install and set up an additional IP gateway so that you'd have an IP gateway to take the place of an IP gateway that's failing or has to be taken offline.
  You have to set up your PBX to send the incoming calls it receives to different IP gateways. After you set up the PBX, the PBX will detect a failure or no signal or that a port isn't answering calls. This lets the PBX redirect calls to an IP gateway that can answer incoming calls.
  The IP gateways supported by Unified Messaging can be set up to route calls to UM servers in a round-robin manner. To enable an IP gateway, you need to set up each IP gateway with the IP addresses for your UM servers that will be answering calls from the IP gateway. These are the UM servers associated with the same dial plan as the UM IP gateway object that logically represents the IP gateway. This will let all the UM IP gateways to forward incoming calls to the UM servers associated with the same dial plan. Then, if an IP gateway fails, the PBX will send the call to an IP gateway that can answer the call. The IP gateway, in turn, will forward the call to a UM server within the same dial plan. If the call is sent to a UM server that isn't available, the IP gateway will try to contact the UM server again. If it's unsuccessful in contacting the UM server, it will then use the next UM server in the list that's set up on the IP gateway to answer the call. But not all supported IP gateways can be set up to support both load balancing and detecting when a server has been taken offline or is failing.

Return to top

Load Balancing in Unified Messaging

Unified Messaging deployments can be made more resilient by deploying multiple UM

servers to a single dial plan to balance the load of incoming calls. The IP gateways supported by Unified Messaging can be set up to route calls in a round-robin manner to balance the load between multiple UM servers in a dial plan.

Round robin is a method for distributing the workload among multiple servers. However, round robin doesn't by itself enable an IP gateway to detect a server failure. If one of the UM servers fails and if the IP gateway can't detect that a UM server is unavailable, the IP gateway will continue to send incoming calls to the UM server until you detect the failure and remove the server from the dial plan. After you remove the UM server from the dial plan, you should also remove the IP address or FQDN for the UM server from the configuration on the IP gateway.

Unified Messaging doesn't use round-robin DNS or Network Load Balancing to distribute incoming calls. Round-robin DNS can be used on multi-homed computers and can be used to distribute the load for other services, but not for Unified Messaging. NLB is used with other services to distribute client requests and to automatically detect whether a server is unavailable, and then to redistribute other client requests to the remaining server. But it also can't be used with Unified Messaging. The only way to distribute or balance the load between Unified Messaging servers in a dial plan is for the IP gateway to be set up with the IP addresses or FQDNs of the UM servers in the dial plan. The IP gateway will use the list to distribute the load across all the UM servers in the dial plan and can also detect a server failure if the IP/VoIP supports this functionality.

Another way to load balance your UM deployment is to set up PBX hunt groups to connect to multiple IP gateways and then set up the hunt groups to load balance across the IP gateways.

1.9.1.9 Understanding System Requirements for Unified Messaging

Understanding System Requirements for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-10*

To provide continuous access to e-mail and voice mail, you must correctly plan and implement a high performance, highly available, and scalable solution for Microsoft Exchange Server 2010. To implement a high performance voice mail solution that's highly available and scalable, you must understand the system requirements for Exchange Unified Messaging (UM) in Exchange 2010. This will help you to select the UM servers and other voice mail components that will have the greatest effect on system performance, scalability, and availability for your deployment.

As you plan your deployment, you can use this topic and other topics in this section to help design your Unified Messaging environment. For details, see Exchange 2010 System Requirements.

Unified Messaging System Hardware Overview

Choosing the correct system hardware is one of the most important steps when in planning and implementing voice mail solution. You must ensure that the hardware you choose will meet or even exceed the system requirements. You must consider the following when you plan and deploy Unified Messaging 2010:

- How to tune your high-performing UM servers for optimum performance

- How to make your Unified Messaging deployment scalable
- How to make your Unified Messaging deployment highly available

Performance

Tuning a Unified Messaging server for optimum performance is an ongoing process. You must understand all the variables that affect your system, including user profile, architecture, and the hardware that's used on a Unified Messaging server. When you know your requirements for a Unified Messaging server, you can establish baseline metrics for the server and make adjustments to improve overall system performance.

Generally, the maximum level of performance for a Unified Messaging server is determined by the component that has the lowest level of performance, which can cause a bottleneck in the system. The key to improving performance is learning to identify bottlenecks in your Unified Messaging system, determine the cause of the system bottlenecks, and then take the appropriate action or actions.

There are several tools you can use to measure performance of Exchange 2010 Unified Messaging, including Jetstress and Load Generator (LoadGen). For details, see Tools for Performance and Scalability Evaluation. The Windows Server 2008 operating system also includes some general performance tools, including Windows Performance Monitor.

Also, you should analyze your current loads to establish minimum server requirements. One of the biggest challenges in determining minimum server requirements is understanding how your users use your voice mail system. After you determine your hardware requirements, you should conduct a pilot test to make sure the Unified Messaging server performance levels are acceptable.

Availability

To provide a highly available UM system, you must protect against hardware failures for the following:

- **UM servers** Unified Messaging runs as a service and a worker process. This means that if the service is using lots of system resources or has become unresponsive, the worker process can be recycled to bring the Unified Messaging service back online. Having the UM worker process recycle allows for a more highly available system and prevents the Unified Messaging service from being down for extended periods of time. The UM worker process is responsible for dealing with outages in Mailbox servers, Hub Transport servers, and domain controllers. For example, if a Mailbox server for a user is unavailable, the UM server will continue to accept calls on behalf of the user. However, the user's custom greeting won't be played. Instead, a standard greeting will be used for calls to that user. Additionally, if the Hub Transport server is unavailable, the UM server will continue to accept calls and queue the calls, depending on how you've set up the queuing limit, until the Hub Transport server is available. In a situation where all domain controllers are unavailable, the UM server will be unable to accept calls.
- **IP gateways** If you want to create redundancy to help ensure that IP gateways are always available, add multiple IP gateways in an N+1 configuration. For example, if you need two IP gateways, install and set up an additional IP gateway so that you have an IP gateway to take the place of an IP gateway that fails or must be taken offline.

For details, see Understanding Unified Messaging Availability.

Scalability

Minimum requirements for uptime may vary among organizations. But every organization wants to achieve a high level of uptime, especially for their telephony system. An organization's telephony system is frequently business-critical and must be highly available to users. One of the factors you need to consider when you deploy a UM system is the ability of the system to provide service to users when a key component, for example, a UM server or an IP gateway, becomes unavailable.

Scalability is defined as the capability to increase resources to increase the capacity of a given service. There are two types of scalability that can be used to increase the capacity of UM servers in your organization: horizontal and vertical. In Unified Messaging, when you scale vertically, you add hardware resources to a single UM server or multiple UM servers by, for example:

- Adding more hard disk space for message storage.
- Increasing the speed or number of processors.
- Increasing the amount or speed of RAM.
- Increasing the number of network adapters or the number of local area network ports in a single network adapter.

For details, see Understanding Unified Messaging Performance and Scalability.

Hardware Requirements

When selecting hardware for your Unified Messaging servers, you must consider several components, including disk storage, memory, processor, and network hardware. The hardware that you select for your Exchange Unified Messaging deployment will have an effect on performance. Because many variables affect performance, including the hardware, it's difficult to predict the effect that any particular hardware component will have.

When you're selecting the hardware components for a Unified Messaging server, consider the following definitions:

- **Minimum** This is the minimum processor and memory configuration that's suitable for specific Exchange 2010 server roles. Minimum hardware requirements must be met before you can receive help from Microsoft Customer Service and Support.
- **Maximum** This is the maximum recommended processor and memory configuration for specific Exchange 2010 server roles. Maximum is defined as the upper limit of the processor and memory configurations for Exchange 2010, based on the price and performance. Maximum is a guideline and not a support criterion. It doesn't take into account the resource requirements of third-party applications. The recommended maximum may change over time, based on price changes and technology advancements.
- **Recommended** This is the recommended processor and memory configuration for specific Exchange 2010 server roles. Recommended can be defined as the best configuration based on price and performance. The recommended configuration also provides a balance between processor and memory capacity. The goal is to match the memory configuration to the processor configuration so that the system will use the processors effectively without causing a bottleneck in memory or vice versa.

Disk Storage Requirements

Here are a few helpful guidelines for selecting a storage configuration that provides good performance and capacity for Exchange 2010. Considerations of capacity and performance are often at odds with each other when it comes to selecting a storage solution, and you must consider both before you make a purchase. Generally, you should make sure that:

- There will be enough space to store all the data. Determining your capacity needs is a relatively straightforward process.
- The solution provides acceptable disk latency and a responsive user experience. You determine this by measuring or predicting transactional input/output (I/O) delivered by the solution.
- Non-transactional I/O has both enough time to complete and enough disk throughput to meet your service-level agreements.

The goal is to balance these factors so that you can design the hardware solution for your

servers.

UM doesn't really require much storage because each message is converted and forwarded as soon as a Hub Transport server is available. However, for Unified Messaging, each UM server requires storage for the following:

- Any UM language packs that are installed along with the en-US UM language pack
- Custom audio prompts for UM dial plans and auto attendants that are stored in a system mailbox
- UM messages that are queued when Hub Transport servers are unavailable, such as:
  - Missed call notifications
  - E-mail messages when a user has been UM-enabled
  - Voice mail messages with an audio attachment
  - Fax messages with an attachment

Note:
If no Hub Transport servers are available, a Unified Messaging server will queue 100 voice messages before shutting down the Microsoft Exchange Unified Messaging service.

To determine the maximum amount of storage required to accommodate these language packs, audio prompts, and queued messages, take the maximum message size of a voice message, based on the audio codec that's used and the message length, and then multiply it by 1,000 bytes. For example, if an average voice message is approximately 30 seconds, which is usually under 100 KB in size, take that number times 100 voice mails.

Memory Requirements

When you select hardware for Exchange 2010, we recommend that you consider the maximum memory limits of the server. Different server architectures have different memory limits. We recommend that you check the following technical specifications of the server to determine the most cost-efficient maximum memory limits for your servers:

- **Memory speed** Some server architectures require slower memory modules to scale to the maximum supported amount of memory. For example, maximum server memory could be limited to 32 GB with PC3 10666 (DDR3 1333) or 128 GB using PC2 6400 (DDR2 800). Check with the manufacturer to ensure that the memory configuration target for Exchange 2010 is compatible in terms of speed.
- **Memory module size** Consider the largest memory module size that the server will support. Generally, the larger the memory module, the more expensive it is. For example, two 2 GB DDR SDRAM memory modules generally cost much less than one 4 GB DDR SDRAM memory module, and two 4 GB DDR SDRAM memory modules generally cost much less than one 8 GB DDR SDRAM memory module. Make sure the size of the maximum memory module allows you to meet your target memory requirements for Exchange 2010.
- **Total number of memory slots** Consider how many memory modules a specific server will support. The total number of slots multiplied by the maximum memory module size provides the maximum memory for the server. Remember that memory modules must sometimes be installed in pairs.

Thus, the recommended minimum of 4 GB of memory installed with a recommended maximum of 2 GB per processor which would equal 4 GB minimum. However, there are several other factors that must be considered when you determine the amount of memory needed for each Unified Messaging server. These include:

- The size of the global address list or the combined size of all address lists.
- The UM language packs that are installed and available.
- Whether Voice Mail Preview is enabled or disabled.
- The number of incoming calls.

The following table shows the minimum supported and recommended maximum memory configurations for Exchange 2010.

Number of users	Recommended memory per UM server
25,000	250 MB
50,000	500 MB
100,000	1 GB

After the required number of processors has been estimated for a specific server role, baseline memory recommendations can be applied. Exchange 2010 on the 64-bit edition of the Windows Server 2008 operating system can efficiently use more than 64 GB of memory.

With effective planning and an understanding of the basic processor and memory requirements for specific Exchange 2010 server roles, you can create a balanced and cost-effective topology.

For more information about how different memory configurations perform, see Understanding Memory Configurations and Exchange Performance.

Processor Requirements

There are significant benefits to be gained by running Exchange 2010 on multiple processors. The performance benefit depends upon the specific processor that's used. Check with your server hardware vendor to see whether the benefits of processors are Exchange-specific for a given hardware architecture.

The processor on a server should maintain a load of about 60 percent during peak working hours. This percentage level allows for periods of extreme load. If the processor usage is consistently greater than 75 percent, processor performance is considered a bottleneck.

There are several ways that server CPU can affect performance. These include:

- The processor clock speed, measured in megahertz (MHz) or gigahertz (GHz)
- The number of processors used
- The type of processors used
- Whether Voice Mail Preview is enabled or disabled

Exchange can make full use of multiple processors, so using servers with more processors improves performance. However, the relationship between the number of processors, the number of processor cores, and performance is complex. The optimum number of processors and cores is partly determined by the Exchange server roles deployed on the server and whether the Unified Messaging server role is also deployed on the same physical server as other server roles.

Network Requirements

Much of the network interface subsystem is tuned automatically. Server-based network adapters are capable of detecting the type and level of traffic that passes through the network interface, and they self-tune to reflect this information. We recommend that you ensure that the latest device drivers are maintained on the server.

Every incoming call that's received from an IP gateway will generate IP-based network traffic and consume some of your available network bandwidth. Before you deploy Unified Messaging, you should perform an analysis of the network traffic to determine current usage patterns and find any potential issues. On most networks, bandwidth demand isn't evenly distributed throughout business hours. Because all the IP-based calls are routed directly to your UM servers from the IP gateways on your network, and because this IP-based network traffic consumes some available bandwidth, you should follow these

recommendations and guidelines:

- Place your PBXs physically close to your IP gateways.
- Place your IP gateways and your UM servers on the same well-connected network or within the same physical site.
- Place your UM servers on the same well-connected network or within the same physical site as other computers that have Exchange 2010 server roles installed, including Mailbox, Hub Transport, and Client Access servers.
- End your wide area network (WAN) connections close to where your telephony equipment is located.
- In branch office scenarios or over WAN connections, use the G.723.1 codec instead of the G.711u or G.711A codec to minimize the network traffic that's passed between your IP gateways and your UM servers.

The network requirements or recommendations for UM servers are as follows:

- UM servers using gigabit (1,000 megabits per second (Mbps)) or 1 gigabit per second (Gbps) Ethernet adapters.
- UM servers connected to multiple-switched, fast Ethernet networks of gigabit Ethernet connections.
- A round trip time from the IP gateway or IP PBX of less than 300 milliseconds.

Note:

Performance-related issues may arise because your hardware, firmware, or software drivers aren't designed to work in your configuration. For more information, see the Products Designed for Microsoft Windows Web site.

1.9.1.10 Fax Advisor for Exchange 2010

Fax Advisor for Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-19*

Microsoft Exchange Server 2010 Unified Messaging (UM) relies on certified fax partner solutions for enhanced fax functionality such as outbound fax or fax routing. By default, when you install the Unified Messaging server role, the server isn't configured to allow incoming fax messages to be delivered to a UM-enabled user. Instead, the UM server redirects incoming fax calls to a certified fax partner solution. The fax partner's server receives the fax data and then sends it to the recipient's mailbox in an e-mail message with the fax included as a .tif attachment. For details, see Understanding Faxing in Unified Messaging.

The Exchange 2010 Unified Messaging server ensures that the final message delivered to the user is identical to the fax messages generated by Microsoft Exchange Server 2007 Unified Messaging. However, the fax partner solution must meet a set of requirements to interoperate with Exchange 2010 Unified Messaging.

Important:

We recommend that all customers who plan to deploy Unified Messaging obtain the assistance of a Unified Messaging specialist. A Unified Messaging specialist helps you ensure that there's a smooth transition to Exchange 2010 Unified Messaging from a legacy voice mail system. Performing a new deployment or upgrading a legacy voice mail system requires significant knowledge about PBXs and Exchange 2010 Unified Messaging. For more information about how to contact a Unified Messaging specialist, see the Microsoft Exchange Server 2007 Unified Messaging (UM) Specialists Web site.

Exchange 2010 Unified Messaging Fax Partner Program

In order to become a fax partner certified for interoperability with Exchange 2010 UM, the partner must implement the requirements contained in the Fax Partner Interoperability Specification and the fax solution must be certified by an independent certification vendor. For more information about certifying a fax product to work with Exchange 2010 Unified Messaging, submit a request to Fax Partners for Exchange 2010 Unified Messaging.

Fax Partner Solutions Certified As Interoperable with Exchange 2010 Unified Messaging

If you've already deployed Exchange 2010 Unified Messaging, and you're looking for a fax partner solution to set up incoming fax processing for your organization, see Microsoft PinPoint for available partners. These fax solution partners have been certified as interoperable with Exchange 2010. Among other services, they provide certified software solutions for Unified Messaging.

IP or Media Gateways and IP PBX Support

Correctly configuring IP gateways for your organization is a difficult deployment task that must be completed to successfully deploy Exchange 2010 Unified Messaging with incoming faxing. To help answer questions and give you the most up-to-date IP gateway configuration information, see Telephony Advisor for Exchange 2010. That topic provides IP gateway configuration notes and files that you must have to correctly configure your organization's IP gateways to work with Exchange 2010 Unified Messaging.

Interoperability testing of Exchange 2010 Unified Messaging with IP gateways is now integrated with the Microsoft Unified Communications Open Interoperability Program. For more information, see Microsoft Unified Communications Open Interoperability Program.

The Microsoft Unified Communications Open Interoperability Program qualification program for IP gateways and IP PBXs ensures that customers have a seamless setup and support experience when they're using qualified telephony gateways and IP-PBXs with Microsoft Unified Communications software.

Important:

Sending and receiving faxes using T.38 or G.711 isn't supported in an environment where Unified Messaging and Communications Server 2007 are integrated.

Deploying and Configuring Faxing

Exchange 2010 UM forwards incoming fax calls to a dedicated fax partner solution, which then establishes the fax call with the fax sender and receives the fax on behalf of the UM-enabled user. However, to allow UM-enabled users to receive fax messages in their mailbox, you must first run Exchange 2010 Unified Messaging setup and configure the Fax Partner server, and then configure the UM dial plans, UM mailbox policies, and enable UM-enabled users to receive faxes. For details, see Deploy and Configure Incoming Faxing.

1.9.1.11 Voice Mail Preview Advisor for Exchange 2010

Voice Mail Preview Advisor for Exchange 2010

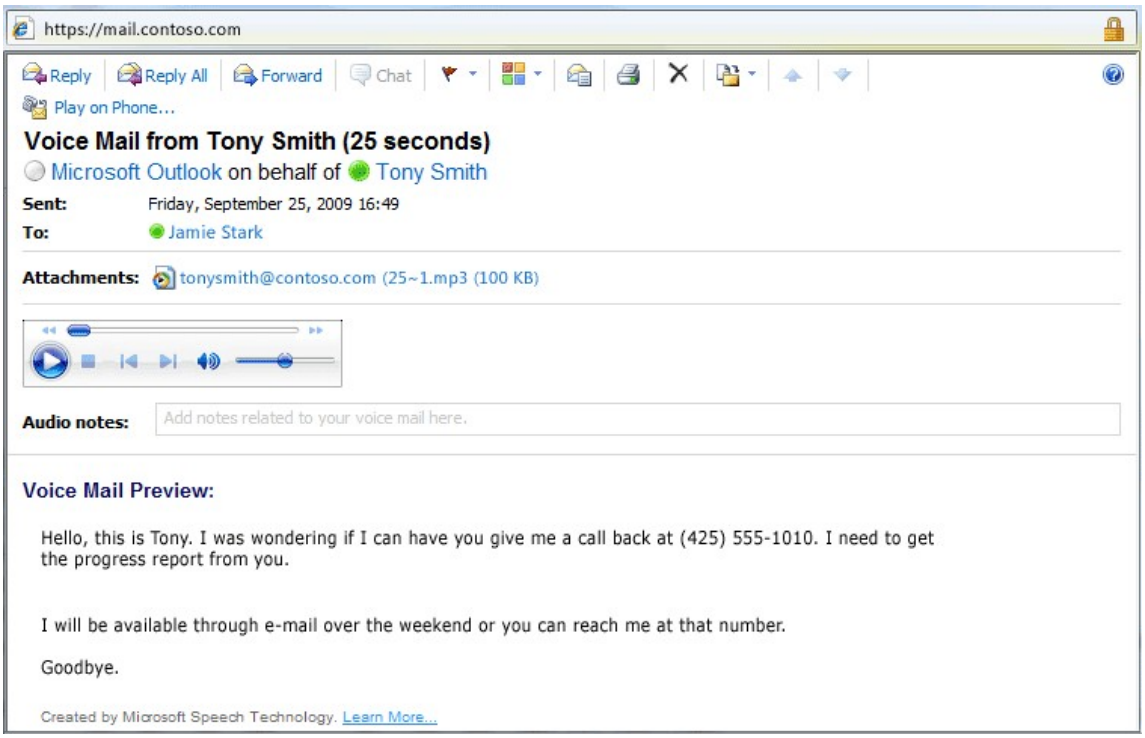
Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

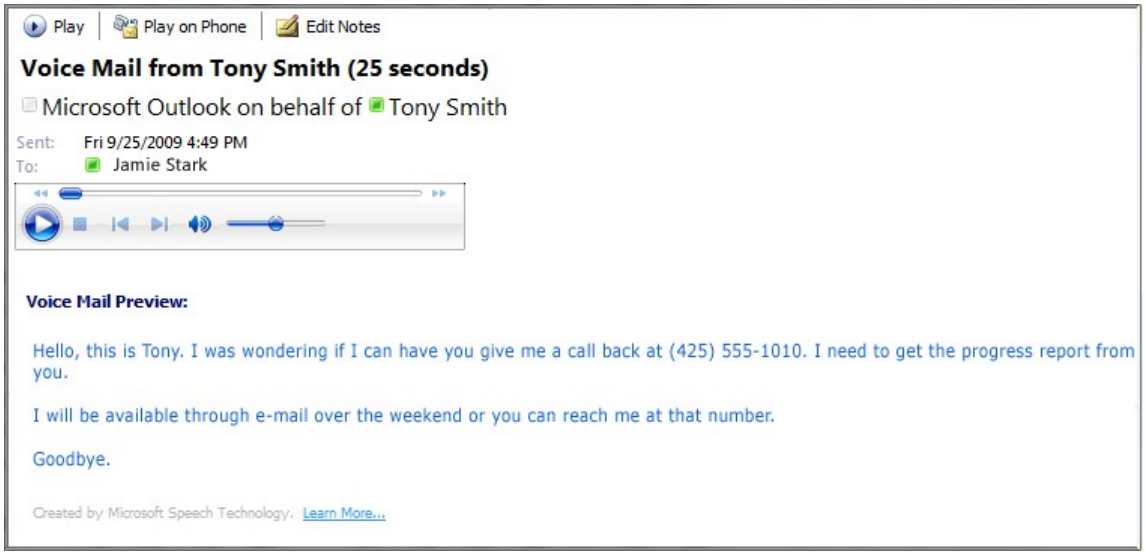
Topic Last Modified: *2012-10-30*

In Microsoft Exchange Server 2010, the Unified Messaging (UM) server role delivers a feature called Voice Mail Preview that uses automatic speech recognition (ASR) to add a text version of the voice mail audio file to voice mail messages. ASR isn't entirely accurate, especially when it's used to record audio over a phone that contains unknown voices and noises. Some organizations require consistently error-free (or near-error-free) transcripts of voice mail messages for some -- if not all -- of their users. The Voice Mail Preview Partner Program helps such organizations meet those requirements.

Voice Mail Preview uses Microsoft speech technologies to provide a text version of audio recordings. The voice mail text is displayed in e-mail messages within Microsoft Office Outlook Web App, Outlook 2010, and in other e-mail programs.

The following examples show how Voice Mail Preview is displayed in Outlook Web App and Outlook 2010:





By default, when you install the Exchange 2010 Unified Messaging server role, the server will send voice mail previews to UM-enabled users if a supported UM language pack is installed.

There are Exchange 2010 Unified Messaging Voice Mail Preview partners that offer enhanced transcription support for the Voice Mail Preview feature. These partners employ people to correct voice mail transcriptions that were created using Automatic Speech Recognition (ASR). Each Voice Mail Preview partner must meet a set of requirements to be certified to interoperate with Exchange 2010 Unified Messaging.

If you determine that the voice mail previews sent to your users aren't accurate enough, you can contact one of the certified Voice Mail Preview partners listed on the Microsoft PinPoint web page and sign up with them at an additional cost.

Overview

When an Exchange 2010 Unified Messaging server records the audio for a voice mail message, it uses ASR to create voice mail preview text from the audio file, and then submits the whole voice message to a Hub Transport server for delivery to the user. For each voice message that's created, a Unified Messaging server determines a confidence level for the voice mail preview included with the message. The voice mail system measures how well the sounds in the recording match the words, numbers, and phrases. If the system finds matches easily, the confidence level will be high. A higher level of confidence is generally associated with a higher accuracy.

The accuracy of Voice Mail Preview text is controlled by many factors, and sometimes those factors can't be controlled. However, the text is likely to be more accurate when:

- A simple voice mail is left, and the caller doesn't use slang terms, technical jargon, or unusual words or phrases.
- The caller uses a language that's easily recognized and translated by the voice mail system. Generally, voice messages left by callers who don't speak too quickly or too softly and who don't have strong accents will produce more accurate sentences and phrases.
- The voice message is free of background noise, echoes, and the audio doesn't drop out.

Most customers who deploy Exchange 2010 Unified Messaging find that the voice mail previews are accurate enough for their users. However, when ASR is applied to recordings made over the phone by unknown voices and background noises, the voice

mail preview text usually isn't completely accurate. If the level of confidence is consistently low or the voice mail previews that are received aren't very accurate, you can increase the accuracy of the Voice Mail Previews that users receive as follows:

- Sign up for a voice transcription service from a Voice Mail Preview partner. For more information about where to find a Voice Mail Preview partner, see the section "Voice Mail Preview Partners Certified for Exchange 2010 Unified Messaging" later in this topic.
- After you've signed up with a Voice Mail Preview partner, use the information provided by the partner to set it up to work with Unified Messaging. For more information, about how to configure UM for a Voice Mail Preview partner, see Configure a Voice Mail Preview Partner on a UM Mailbox Policy.

When you've signed up with a Voice Mail Preview partner, the UM server redirects voice mail messages with the audio file attached to a Voice Mail Preview partner instead of generating Voice Mail Preview text for voice messages and submitting the voice messages to a Hub Transport server. The e-mail message with the Voice Mail Preview text produced by the Voice Mail Preview partner is then submitted to the Hub Transport server for delivery to the recipient's mailbox.

Important:

We recommend that all customers who plan to deploy Unified Messaging obtain the assistance of a Unified Messaging specialist. A Unified Messaging specialist helps you ensure that there's a smooth transition to Exchange 2010 Unified Messaging from a legacy voice mail system. Performing a new deployment or upgrading a legacy voice mail system requires significant knowledge about PBXs and Exchange 2010 Unified Messaging. For more information about how to contact a Unified Messaging specialist, see the Microsoft Exchange Server 2007 Unified Messaging (UM) Specialists Web site.

Exchange 2010 Unified Messaging Voice Mail Partner Program

To become certified as a Voice Mail Preview partner that interoperates with Exchange 2010 UM, the partner must implement the requirements contained in the Voice Mail Preview Interoperability Specification, and the partner solution must be certified by an independent certification vendor. If you're interested in certifying your transcription service to work with Exchange 2010 Unified Messaging, submit a request to Voice Mail Preview Partners for Exchange 2010 Unified Messaging.

Voice Mail Preview Partners Certified for Exchange 2010 Unified Messaging

If you've already deployed Exchange 2010 Unified Messaging in your organization and you're looking for a certified Voice Mail Preview partner to provide transcription support services, see Independent Software Vendors. These software vendors have been certified as interoperable with Exchange Server 2010.

Configuring Voice Mail Preview Partners

The Exchange 2010 UM server forwards voice mail message with the audio to a dedicated Voice Mail Preview partner solution, which then takes the audio file and creates the Voice Mail Preview text. However, to allow UM-enabled users to receive the Voice Mail Preview with their voice mail message in their mailbox, you must configure a UM mailbox policy, associate users with the UM mailbox policy, and then have the UM-enabled users verify that they can receive voice mail previews in their voice mail messages in Outlook 2010 or

Outlook Web App. For more information about Voice Mail Preview with Outlook 2010 and Outlook Web App, see Outlook 2010 and Outlook Web App Features in Unified Messaging. For more information, about how to configure UM for a Voice Mail Preview partner, see Configure a Voice Mail Preview Partner on a UM Mailbox Policy.

IP or Media Gateways and IP PBX Support

Configuring IP gateways and IP PBXs for your organization is a difficult deployment task that must be completed correctly to successfully deploy Exchange 2010 Unified Messaging with a Voice Mail Preview partner. For information that can help you configure your IP gateways and IP PBXs and for the most up-to-date information about how to configure them, see Telephony Advisor for Exchange 2010.

Testing interoperability of Exchange 2010 Unified Messaging with IP gateways has been integrated with the Office Unified Communications Open Interoperability Program. For more information, see Microsoft Unified Communications Open Interoperability Program.

1.9.1.12 Telephony Advisor for Exchange 2010

Telephony Advisor for Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-13*

Unified Messaging (UM) requires that you integrate Microsoft Exchange Server 2010 with the existing telephony system for your organization. A successful deployment requires you to make a careful analysis of your existing telephony infrastructure and to perform the correct planning steps to deploy Unified Messaging.

The planning phase can be a significant challenge to Exchange administrators who have little or no experience with a telephony network. To help address this challenge, see Resources to Help with Your UM Deployment later in this topic.

To see the supported IP gateways for Unified Messaging, determine whether your PBX is supported using a specific IP gateway model or manufacturer, whether your IP PBX is supported using a direct SIP connection, or to see supported session border controllers (SBCs) for Exchange Online UM, click one of the following links:

- Supported IP Gateways
- Supported PBXs When Using an AudioCodes IP Gateway
- Supported PBXs Using a Dialogic IP Gateway
  - PBXs Supported Using a DMG1000 Series Media Gateway
  - PBXs Supported Using a DMG 2000 Series Media Gateway
  - PBXs Supported Using a DMG3000 Series Media Gateway
- Supported IP PBXs
- Supported IP PBXs Using SIP Media Gateways
- Session Border Controllers Tested with Exchange Online UM
- Exchange Unified Messaging, and Office Communications Server 2007 R2, and Lync Server 2010

Resources to Help with Your UM Deployment

It's challenging to create guidelines for deploying telephony networks. They can be very different from one another because they can include IP gateways, IP PBXs, and PBXs with different configuration settings, firmware, and requirements. This diversity makes planning and deploying Unified Messaging somewhat challenging. However, several resources are available to help you successfully deploy Unified Messaging:

- **Unified Messaging specialists** UM specialists are systems integrators who have received technical training about Exchange 2010 Unified Messaging conducted by the Exchange engineering team. To help ensure a smooth transition to Exchange 2010 Unified Messaging from legacy voice mail systems, Microsoft recommends that all customers engage a UM specialist. For contact information, visit Microsoft Exchange Server 2007 Unified Messaging (UM) Specialists.
- **PBX configuration notes** PBX configuration notes contain configuration settings and other information that's very useful when you're configuring IP gateways, IP PBXs, and PBXs to communicate with the Unified Messaging servers that are on your network. For more information, see PBX Configuration Notes Tested by Microsoft or IP Gateway Vendor Partners for Exchange 2010 Unified Messaging.

Before you engage a Unified Messaging specialist, you should be able to answer key questions that they'll ask. Having the answers to the following questions will help make the conversation between you and the UM specialist productive:

- How many existing telephone or voice mail users, or both, are in your organization?
- How many users do you intend to provide with Exchange 2010 Unified Messaging?
- Which PBX or PBXs do you intend to use for integration with Exchange 2010 Unified Messaging?
- How many PBXs does your organization have? Specify the vendors, types (circuit- or IP-based), models, and firmware versions.
- Are the PBXs networked, and are they centralized or located in multiple locations?
- What voice mail system or systems does your organization currently use? Specify the vendors, types, models, and firmware versions.
- How are the voice mail systems integrated into your PBXs (Analog, T1/E1, PRI, Digital set emulation, VoIP, other)?
- Are you currently using voice networking?
- What type of fax system or systems does your organization use, and does the fax system or systems support inbound fax routing to Exchange?
- Does your organization use automated attendants?
- Do you need support for phone-only users, that is, users who won't have e-mail access?

Supported IP Gateways

Integrating Exchange 2010 Unified Messaging with PBXs requires you to use one or more IP gateways to translate the circuit-switched protocols that are used by TDM-based PBXs to IP-based, packet-switched protocols that are used by Exchange 2010 Unified Messaging. IP gateway vendors with several models of IP gateways have been tested and are supported for Exchange 2010 Unified Messaging.

Interoperability testing of Exchange 2010 Unified Messaging with IP gateways is now integrated with the Microsoft Unified Communications Open Interoperability Program. For more information, see Microsoft Unified Communications Open Interoperability Program.

The Microsoft Unified Communications Open Interoperability Program qualification program for IP gateways and IP PBXs ensures that customers have a seamless setup and support experience when they're using qualified telephony gateways and IP-PBXs with Microsoft Unified Communications software. Only products that meet rigorous and extensive testing

requirements and conform to the specifications and test plans receive qualification.

Interoperability was verified for the following IP gateway vendors in the following years:

- AudioCodes
- Dialogic
- The following table shows the IP gateway vendor, the IP gateway model, and the protocols that are supported by each model.

Supported IP gateways for Unified Messaging

Vendor	Model	Supported protocols
AudioCodes	MediaPack 114/8 FXO	• Analog with In-Band DTMF • Analog with SMDI
AudioCodes	Mediant 1000	• Analog with In-Band DTMF • Analog with SMDI • BRI Q.SIG • T1/E1 Q.SIG • IP-to-IP
AudioCodes	Mediant 2000	• T1/E1 CAS • T1/E1 Q.SIG • IP-to-IP
Dialogic	DMG1000PBXDNIW	Digital Set Emulation
Dialogic	DMG1000LSW	• Analog with In-Band DTMF • Analog with SMDI
Dialogic	DMG2000	• T1 CAS • T1/E1 Q.SIG
Dialogic	DMG3000	• BRI Q.SIG
NET	VX1200	• T1 Q.SIG
Quintum	Tenor DX Series	• T1 Q.SIG

Supported PBXs When Using an AudioCodes IP Gateway

The following table shows the PBXs that are supported using AudioCodes IP gateways including MediaPack-114 FXO, MediaPack-118 FXO, and Mediant 2000.

PBXs Supported with an AudioCodes IP gateway

PBX manufacturer	PBX model/type	AudioCodes model "x" - replace with 4 or 8 per need "y" - replace with 1, 2, 4, 8 or 16 per need
Alcatel	OmniPCX 4400	• MediaPack 11x/FXO/AC/SIP-0 • Mediant2000/ySpans/SIP
Aastra	M1000, M2000	• Mediant2000/ySpans/SIP
Avaya	Definity G3	• MediaPack 11x/FXO/AC/SIP-0 • Mediant1000/ySpans/SIP • Mediant2000/ySpans/SIP
Avaya	Magix/Merlin	• MediaPack 11x/FXO/AC/SIP-0

Avaya	S8300	• MediaPack 11x/FXO/AC/SIP-0 • Mediant1000/ySpans/SIP • Mediant2000/ySpans/SIP
Avaya	S8700	• MediaPack 11x/FXO/AC/SIP-0 • Mediant1000/ySpans/SIP • Mediant2000/ySpans/SIP
Avaya	IP Office	• MediaPack 11x/FXO/AC/SIP-0 • Mediant2000/ySpans/SIP
Cisco	CallManager 4.x	• Mediant1000/IP-to-IP • Mediant2000/IP-to-IP
NEC	Electra Elite	• MediaPack 11x/FXO/AC/SIP-0
NEC	NEAX2400	• MediaPack 11x/FXO/AC/SIP-0 • Mediant2000/ySpans/SIP/RS232
NeXspan	S	• MediaPack 11x/FXO/AC/SIP-0
Nortel	Communication Server-1000M, 1000S, 1000E	• Mediant1000/ySpans/SIP • Mediant2000/ySpans/SIP
Nortel	Meridian 11c, 51c, 61c, 81c	• Mediant1000/ySpans/SIP • Mediant2000/ySpans/SIP
Panasonic	KX-TES824, KX-TEA308	• MediaPack 11x/FXO/AC/SIP-0
Panasonic	KX-TDA30, KX-TDA100, KX-TDA200, KX-TDA600	• MediaPack 11x/FXO/AC/SIP-0
Shortel	IP Telephony System	• MediaPack 11x/FXO/AC/SIP-0
Siemens	HiCom 150E	• MediaPack 11x/FXO/AC/SIP-0
Siemens	HiPath 3550	• MediaPack 11x/FXO/AC/SIP-0
Siemens	HiPath 4000	• MediaPack 11x/FXO/AC/SIP-0 • Mediant1000/ySpans/SIP • Mediant2000/ySpans/SIP
Tadiran Telecom	Coral Flexicom, Coral IPX	• MediaPack 11x/FXO/AC/SIP-0 • Mediant1000/ySpans/SIP • Mediant2000/ySpans/SIP

Supported PBXs Using a Dialogic IP Gateway

Each Dialogic IP gateway model supports different PBXs. The following tables show the PBX manufacturer and model and which Dialogic IP gateway can be used. Each IP gateway uses different signaling methods, densities, and protocols.

PBXs Supported Using a DMG1000 Series Media Gateway

The following table shows the PBXs that are supported with the low-density Dialogic

Media Gateway (DMG1000). However, when an analog DMG1000 is used, supplemental signaling (RS232 SMDI, MD110, MCI protocols, or Inband DTMF signaling) is required.

PBXs supported using a low-density Dialogic DMG1000 series IP gateway

PBX manufacturer	PBX model/type	DMG model and additional signaling
Aastra	Aastra MD110 (formerly Ericsson MD110)	DMG1008LSW Analog connectivity using the MD110 RS232 protocol
Alcatel	Omni PCX 4400	DMG1008LSW
Avaya	Definity G3 S8100, S8300, S8700, and S8710 (Communications Mgr SW V2.0 or later versions)	DMG1008DNIW
Intercom		DMG1008LSW Analog connectivity using SMDI serial protocol
Mitel	SX-200D, SX-200 Light, SX-2000 Light, SX-2000 S, SX-2000 VS, SX-200 ICP	DMG1008MTLDNIW
NEC	2000, 2400, 2400 IPX	DMG1008DNIW
Nortel	Meridian 1 - Option 11, 21, 21A, 51, 61, 71, and 81 Meridian SL1 - Generic X11, Release 15 or later versions Nortel Communication Server - 1000M, 1000S, 1000E with V3.0 or later versions	DMG1008DNIW
Nortel	SL 100	DMG1008LSW Analog connectivity using SMDI serial protocol
Siemens	HiCom 300E CS	DMG1008DNIW
Siemens	HiCom 300E (European)	DMG1008LSW Analog connectivity using Inband DTMF signaling
Siemens/ROLM	8000 (SW release 80003 or later versions) 9000 (All versions) 9751 (All versions of SW release 9005) 9751 (SW release 9006.4 or later versions)	DMG1008RLMDNIW

Siemens	HiPath 4000	DMG1008LSW
Toshiba	CTX (SW version AR1ME021.00)	DMG1008LSW
Others	Various	DMG1008LSW Analog connectivity using either Inband DTMF or SMDI

PBXs Supported Using a DMG 2000 Series Media Gateway

The following table shows the PBXs that are supported with the T1/E1 Dialogic Media Gateway (DMG2000). The DMG2000 gateway, which comes in single span (DMG2030DTIQ), dual span (DMG2060DTIQ), or quad span (DMG2120DTIQ) densities, supports the following protocols:

- T1 CAS
- T1 Q.SIG
- E1 Q.SIG
- T1 NI-2
- T1 5ESS
- T1 DMS100

If Channel Associated Signaling (CAS) signaling is used, supplemental signaling (RS232 SMDI, MD110, MCI protocols, or Inband DTMF signaling) is required. If Q.SIG signaling is used, the PBX must support the supplemental services that are associated with calling and called party Information and the call transfer capabilities required by Exchange 2010 Unified Messaging.

PBXs supported with the DMG2000 Media Gateway

PBX manufacturer	PBX model/type	Required software version	Protocol and additional signaling
Alcatel	Omni PCX 4400	Version 3.2.712.5	T1 Q.SIG E1 Q.SIG
Avaya	Definity G3	Version 3 or later	T1 CAS
Avaya	S8500	Manager SW V2.0 or later versions	T1 CAS T1 Q.SIG E1 Q.SIG
Ericsson	MD110	Release MX1 TSW R2A (BC13)	E1 Q.SIG
Intercom			CAS (w/ SMDI serial protocol)
NEC	2400 IMX	Release 5200 Dec. 92 1b or later versions	CAS (w/ MCI serial protocol)
NEC	2400 IPX	R17 Release 03.46.001	T1 Q.SIG
Nortel	Meridian 1 - Option 11	Release 15 or later versions, and options 19 and 46 are required	T1 Q.SIG E1 Q.SIG

Nortel	Communication Server 1000	Version 2121, Release 4	T1 Q.SIG E1 Q.SIG
Siemens	HiCom 300E CS	Release 9006.4 or later (Note: North American software load only)	T1 CAS
Siemens	HiPath 4000	V2 SMR 9 SMPO	T1 Q.SIG E1 Q.SIG
Mitel	SX-2000 S, SX-2000 VS	LW 34	T1 Q.SIG E1 Q.SIG
Mitel	3300	Version 5.1.4.8	T1 Q.SIG E1 Q.SIG

PBXs Supported Using a DMG4008BRI Series Media Gateway

The DMG4000 series Media Gateway comes with several TDM interface options. The DMG4008BRI supports 4-port/8-channel densities and supports the following protocols:

- ISDN BRI Q.SIG
- ETSI-DSS1 (Euro ISDN)
- NET 3 (Belgium)
- VN3 (France)
- 1TR6 (Germany)
- INS-64 (Japan)
- 5ESS Custom (North America - AT&T)
- National ISDN (NI1 - North America)

The following table shows the PBXs that are supported using a Dialogic 4000 Media Gateway Series (DMG4008).

PBXs supported using a DMG4008BRI Media Gateway

PBX manufacturer	PBX model/type	Required software version	Protocol and additional signaling
Siemens	HiCom 300	SA300-V3.05	BRI-Q.SIG (ECMAV2)
Siemens	HiPath 4000	S.0 B4400	BRI-Q.SIG (ECMAV2)

Supported IP PBXs

IP PBXs are also supported by Exchange 2010 Unified Messaging. The following table shows the IP PBXs that are supported using a direct SIP connection to Exchange 2010 Unified Messaging.

IP PBXs supported using a direct SIP connection

PBX manufacturer	PBX model/type	Required software version
Aastra	MX-ONE	4.0
Avaya	Aura	5.2.1 with Service Pack 5 (SP5)

Avaya	Communication Server 2100	CS2100 SE13
Cisco	Call Manager, Unified Communications Manager	5.1, 6.x, 7.0 and8.0

Supported IP PBXs Using SIP Media Gateways

IP PBXs using SIP media gateways are also supported by Exchange 2010 Unified Messaging. The following table shows the IP PBXs that are supported using IP to IP capabilities of SIP media gateways to connect to Exchange 2010 Unified Messaging.

IP PBXs supported using a SIP Media Gateway

PBX manufacturer	PBX model/type	SIP Gateway Model
Cisco	Call Manager 4.x	AudioCodes Mediant 1000/2000 (IP-to-IP enabled)

Exchange Unified Messaging, and Office Communications Server 2007 R2, and Lync Server 2010

Exchange 2010, Microsoft Office Communications Server 2007 R2, and Microsoft Lync Server 2010 can be deployed together to provide voice messaging, Instant Messaging (IM), enhanced user presence, audio-video conferencing, and an integrated e-mail and messaging experience for users in your organization. For more information, see:

- Office Communications Server 2007 Document: Enterprise Voice Planning and Deployment Guide
- Understanding Unified Messaging and Communications Server 2007 R2
- Deploy Unified Messaging and Communications Server 2007 R2
- Lync Server 2010

To find out more about the Microsoft Unified Communications Open Interoperability Program for enterprise telephony infrastructure, including finding qualified SIP PSTN gateways and IP PBXs and the process for telephony infrastructure vendors to join and participate in the program, see Microsoft Unified Communications Open Interoperability Program.

1.9.1.12.1 PBX Configuration Notes Tested by Microsoft or IP Gateway Vendor Partners for Exchange 2010 Unified Messaging

PBX Configuration Notes Tested by Microsoft or IP Gateway Vendor Partners for Exchange 2010 Unified Messaging

Unified Messaging > Understanding Unified Messaging > Telephony Advisor for Exchange 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-20*

This page provides links to configuration notes that have been created and tested by Microsoft or an IP gateway partner. When Microsoft or a partner deploys Exchange Server

2010 Unified Messaging with a new IP gateway and PBX or IP PBX configuration, the prerequisites and configuration settings are documented. This information is used to create a configuration note.

Each PBX configuration note contains information about how to deploy Exchange 2010 Unified Messaging with a specific telephony configuration, and includes the manufacturer, model, and firmware version for the IP gateways, IP PBXs, or PBXs. In addition, each PBX configuration note includes other information, such as:

- Contributors in authoring the configuration note.
- Detailed prerequisites, including the following:
  - Features that have to be enabled or disabled on the PBX.
  - Specialized hardware that has to be installed.
  - Whether an IP gateway is required.
  - Features that must be present on the IP gateway, if one is needed.
  - Specific cabling requirements between an IP gateway and a PBX.
  - A list of Unified Messaging features that may not be available with a given telephony configuration.

To find out more about the Microsoft Unified Communications Open Interoperability Program for enterprise telephony infrastructure, including finding qualified SIP PSTN gateways and IP PBXs and the process telephony infrastructure vendors can use to join and participate in the program, see Microsoft Unified Communications Open Interoperability Program.

IP Gateway, IP PBX, and PBX Configuration Notes

Microsoft is working with IP gateway partners, AudioCodes and Dialogic, to add to the list of PBXs that are tested. Because we are currently testing many combinations of telephony components, this topic is updated frequently. Please check back if you can't locate the appropriate configuration note for your deployment.

The following configuration notes are available:

- Aastra
- Alcatel
- Avaya
- Cisco
- Inter-Tel
- Intecom
- Mitel
- NEC
- NeXspan
- Nortel
- Panasonic
- Rolm
- ShoreTel
- Siemens
- Tadiran
- Toshiba

Aastra

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
Aastra MD110 (formerly Ericsson MD110)	MX1 TSW R2A (aka BC13)	Analog – Serial MD110	Dialogic	DMG1008LSW	Dialogic	Download
Aastra MD110 (formerly	MX1 TSW R2A (aka BC13)	E1 Q.SIG	Dialogic	DMG2030DTIQ	Dialogic	Download

Ericsson MD110)						
Aastra MX-ONE	4.0	Direct SIP Connection	N.A.	N.A.	Aastra	Download

Alcatel

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
OmniPCX 4400	R4.2-d2.304-4-h-il-c6s2	Analog – In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download

Avaya

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
Aura	Communication Manager 6.0.1 with SP 5.01 Session Manager 5.2.	Direct SIP Connection	N.A.	N.A.	Avaya	Download
Aura	Communication Manager 5.2.1 with SP 5 Session Manager 5.2.	Direct SIP Connection	N.A.	N.A.	Avaya	Download
CS 2100	CS 2100 SE13	Direct SIP Connection	N.A.	N.A.	Avaya	Download
CS 1000	CS 1000 E CPPM	Direct SIP Connection	N.A.	N.A.	Avaya	Download
Definity G3	R009i.05.122.4	Digital Set Emulation (DNI7434)	Dialogic	DMG1008DNIW	Dialogic	Download
Definity G3	R013i.01.1.628.7	Analog – In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download
Definity G3	R013i.01.1.628.7	T1 CAS – In-Band DTMF	AudioCodes	Mediant 2000	AudioCodes	Download
Definity G3	R013i.01.1.628.7	T1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download
Definity G3	R013i.01.1.628.7	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download
Merlin Magix	Release 1.5	Analog – In-	AudioCodes	MP-11x FXO	AudioCodes	Download

	v.6.0	Band DTMF				
S8300	G3xV11 Communication Manager 1.3	Analog – In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download
S8300	R013x.01.2.632.1	T1 CAS – In-Band DTMF	AudioCodes	Mediant 2000	AudioCodes	Download
S8300	R013x.01.2.632.1	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download
S8500	Communication Manager 3.0 (R013x00.1.346.0)	E1 Q.SIG	Dialogic	DMG2030DT IQ	Dialogic	Download
S8500	Communication Manager 3.0 (R013x00.1.346.0)	T1 CAS – In-Band DTMF	Dialogic	DMG2030DT IQ	Dialogic	Download
S8500	Communication Manager 3.0 (R013x00.1.346.0)	T1 Q.SIG	Dialogic	DMG2030DT IQ	Dialogic	Download
S8700	R011x.02.0.110.4	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download

Cisco

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
Cisco Call Manager 4.x	4.x	IP-to-IP	AudioCodes	AudioCodes	AudioCodes	Download
Cisco Call Manager 5.1	5.1.0.9921-12	Direct SIP Connection	N.A.	N.A.	Microsoft	Download
Cisco Unified Communications Manager 6.0 and 6.1	6.x	Direct SIP Connection	N.A.	N.A.	Microsoft	Download
Cisco Unified Communications Manager 7.0	7.0.2.20000-5	Direct SIP Connection	N.A.	N.A.	Microsoft	Download
Cisco Unified Communicat	8.0.3.20000-5	Direct SIP Connection	N.A.	N.A.	Microsoft	Download

ions Manager 8.0						

Inter-Tel

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
5000	Inter-Tel 5000 v2.1	T1 CAS – In-Band DTMF	AudioCodes	Mediant 2000	AudioCodes	Download
Axxess	Axxess V9.0	T1 CAS – In-Band DTMF	AudioCodes	Mediant 2000	AudioCodes	Download

Intecom

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
PointSpan M6880	40PS3.5.K.2	T1 CAS - SMDI	AudioCodes	Mediant 2000	AudioCodes	Download

Mitel

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
3300	5.1.4.8	E1 Q.SIG	Dialogic	DMG2030DTIQ	Dialogic	Download
3300	5.1.4.8	T1 Q.SIG	Dialogic	DMG2030DTIQ	Dialogic	Download
SX2000	5.0.24	Digital Set Emulation (DNISS430)	Dialogic	DMG1008MTLDNIW	Dialogic	Download
3300	7	T1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download

NEC

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
Electra Elite 192	SP034V4.5	Analog – In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download
NEAX2400IMX	version 7400	T1 CAS - serial MCI	Dialogic	DMG2030DTIQ	Dialogic	Download
NEAX2400IMX & IPX	version 7400	Digital Set Emulation (DNIDtermIII)	Dialogic	DMG1008DNIW	Dialogic	Download
NEAX2400IPX	Ver. R18.06.24.000	T1 CAS – serial MCI	AudioCodes	Mediant 2000	AudioCodes	Download

NEAX2400IPX	Ver. R18.06.24.000	Analog – serial MCI	AudioCodes	MP-11x FXO	AudioCodes	Download
NEAX2400IPX	Ver.17 Rel.03.46.001	T1 Q.SIG – serial MCI	Dialogic	DMG2030DTIQ	Dialogic	Download

NeXspan

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
S	RMS1 version R1.3 E1TA	Analog – In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download

Nortel

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
CS1000	3.0 & 4.5	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download
Meridian 81C	4.5	E1 Q.SIG	AudioCodes	Mediant 2000	AudioCodes	Download
Meridian 81C	4.5	T1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download
Option11c	Release 25	Digital Set Emulation (DNI2616)	Dialogic	DMG1008DNIW	Dialogic	Download
Option11c	Release 25	T1 Q.SIG	Dialogic	DMG2030DTIQ	Dialogic	Download
Option11c	Release 25	E1 Q.SIG	Dialogic	DMG2030DTIQ	Dialogic	Download
CS-1000M (Succession)	Release 25.40	E1 Q.SIG	Dialogic	DMG2030DTIQ	Dialogic	Download

Panasonic

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
KX-TDA200	001-001	Analog - In-Band DTMF	AudioCodes	Mediant 1000	AudioCodes	Download
KX-TDA200	3	Analog - In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download
KX-TES824	2.0.2	Analog - In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download

Rolm

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
9751	9005	Digital Set Emulation (DNIRP400)	Dialogic	DMG1008RLMDNIW	Dialogic	Download

ShoreTel

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
IP Telephony System	6.1	Analog – SMDI	AudioCodes	MP-11x FXO	AudioCodes	Download
IP Telephony System	7.5	Analog – SMDI	AudioCodes	Mediant 1000	AudioCodes	Download

Siemens

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
HiCom 150E	Rel. 2.2	Analog – In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download
HiCom 300	SA300-V3.05	BRI QSIG	Dialogic	DMG3000	Dialogic	Download
HiCom 300	9006.4SMR3	Digital Set Emulation (DNIOptiset)	Dialogic	DMG1008DNIW	Dialogic	Download
HiCom 300	9006.4SMR3	T1 CAS - In-Band DTMF	Dialogic	DMG2030DTIQ	Dialogic	Download
HiPath 3550	Rel. 3	Analog – In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download
HiPath 4000	Ver 3.0 SMR5 SMP4	Analog – In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download
HiPath 4000	SA300-V3.05	BRI QSIG	Dialogic	DMG3000	Dialogic	Download
HiPath 4000	Ver 3.0 SMR5 SMP4	T1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download
HiPath 4000	Version 2.0 SMR9 SMP0	Analog - In-Band DTMF	Dialogic	DMG1008LSW	Dialogic	Download
HiPath 4000	Version 2.0 SMR9 SMP0	T1 Q.SIG	Dialogic	DMG2030DTIQ	Dialogic	Download

Tadiran

PBX model	PBX software	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file

	release					download
Coral Flexicom	14.67.49	Analog – In-Band DTMF	AudioCodes	MP 11x FXO	AudioCodes	Download
Coral Flexicom	14.67.49	BRI QSIG	AudioCodes	Mediant 1000	AudioCodes	Download
Coral Flexicom	14.67.49	E1 CAS - In-Band DTMF	AudioCodes	Mediant 2000	AudioCodes	Download
Coral Flexicom	14.67.49	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download
Coral IPX	14.67.49	Analog – In-Band DTMF	AudioCodes	MP-11x FXO	AudioCodes	Download
Coral IPX	14.67.49	BRI QSIG	AudioCodes	Mediant 1000	AudioCodes	Download
Coral IPX	14.67.49	E1 CAS – In-Band DTMF	AudioCodes	Mediant 2000	AudioCodes	Download
Coral IPX	14.67.49	E1 QSIG	AudioCodes	Mediant 1000/2000	AudioCodes	Download

Toshiba

PBX model	PBX software release	Protocol	Gateway vendor	Gateway model	Configuration author	Configuration file download
CTX	AR1ME021.00	Analog – SMDI	Dialogic	DMG1008LSW	Dialogic	Download
CTX	AR1ME021.00	Analog – In-Band DTMF	Dialogic	DMG1008LSW	Dialogic	Download

1.9.1.13 Unified Messaging Terminology

Unified Messaging Terminology

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-10*

The following table contains the terms and definitions that are used with Microsoft Exchange Server 2010 Unified Messaging.

audio codec

A digital encoding of an analog voice signal. Most audio codecs provide compression of the data, at the cost of some loss of fidelity when the data is recovered. Audio codecs vary in their perceived sound quality, the bandwidth that is required to use them, and the system requirements that are needed to do the encoding.

Audio notes

Text-based notes that can be added to a voice mail message that has been received

in Office Outlook 2007, Outlook 2010, or Outlook Web App.

auto attendant

A software system that answers calls, plays prompts or instructions, and then collects input from the caller as touch tones or speech. Auto attendants can direct a call to telephone numbers or named users or to entities (for example, departments) that the caller specifies, without intervention from a human operator.

Automatic Speech Recognition (ASR)

A technology that enables a computer to match human speech to a predefined set of words or phrases.

call answering

The process by which a caller interacts with a voice mail system if the number they originally called isn't answered. Typically, the system will play a greeting or other prompt, and allow the caller to record a voice message.

Call Answering Rules

A form of call answering in which the user for whom the call is being answered can specify rules to determine the behavior callers experience. The user can specify conditions to be evaluated, greetings, and choices to be provided to the caller, and actions (for example, transfer or leave a message) to be taken as a result of the caller's choice.

conditional call forwarding

A set of conditions that are chosen by a user to be used when they receive an incoming call. The call is redirected based on the conditions that are set.

Dial by Name

A feature that enables a caller to spell a person’s name using the keys on a telephone (ABC=2, DEF=3, etc.).

dial plan

For Exchange Unified Messaging, this is a set of telephony-capable endpoints that share a common numbering plan. The details of the plan are determined by the telephone system to which UM is connected. In the simplest case, this can be a private branch exchange (PBX) with its extensions, each with a unique, fixed-length number.

dialing rule group

Dialing rule groups are created to enable telephone numbers to be modified before they're sent to the PBX or IP PBX for outgoing calls. Dialing rule groups may remove digits from or add digits to telephone numbers that are being used to place calls by a Unified Messaging server.

Each dialing rule group contains dialing rule entries that determine the types of in-country/region and international calls that users within a dialing rule group can make. Each dialing rule group must contain at least one dialing rule entry.

fax partner

UM fax partners provide applications or services that can accept calls handed off by UM when a fax tone is detected. The partner's product or service then receives the fax data, creates a message, and delivers it to the UM-enabled user as an e-mail with a .tif attachment. These messages will appear in the Fax search folder in Office Outlook 2007, Outlook 2010, and Outlook Web App.

hunt group

A set of extensions that are organized into a group, over which the PBX or IP PBX “hunts” to find an available extension. A hunt group is used to direct calls to identically-capable endpoints or to an application, such as voice mail.

In-Country/region number format

The In-Country/region number format specifies how a user's telephone number should be dialed by the Unified Messaging server from a different dial plan that has the same country code. This is used by an auto attendant and when an Outlook Voice Access subscriber searches and tries to call the user in the directory.

This entry consists of a number prefix and a variable number of characters (for example, 020xxxxxxx).

informational announcement

An audio message that is played when a caller first dials in to a Unified Messaging system, which may describe some interest.

International Access Code

The prefix that is used to direct a call internationally. The International Access Code is 011 in the United States and 00 in much of the rest of the world.

International Number Format

The string of digits that is used to define how to dial someone from outside a specific country.

Internet Protocol Private Branch eXchange (IP PBX)

A telephone switch that natively supports voice over IP (VoIP). An IP PBX uses VoIP-based protocols to communicate with IP-based hosts such as VoIP telephones over a packet-switched network. Some IP PBXs can also support the use of traditional analog and digital phones.

IP gateway

1. A third-party hardware device or product that connects a legacy PBX to a LAN. An IP gateway translates or converts TDM or telephony circuit-switched protocols to packet switched protocols that can be used on a VoIP-based network.
2. The Exchange Unified Messaging representation of any SIP peer with which it can communicate using VoIP protocols. It may represent a device that interfaces with a legacy PBX, or an IP PBX, or Microsoft Office Communications Server.

matched name selection method

The mechanism used to help a caller differentiate between users with names that match the touchtone or speech input.

message waiting indicator

A signal that indicates the presence of one or more unread voice messages. For voice mail systems, this is often a lamp on the phone or a stutter dial tone.

Microsoft Exchange Unified Messaging service

A service that implements Unified Messaging capabilities for UM-enabled users.

missed call notification

An e-mail message that is sent to a UM-enabled user that indicates that someone called but did not leave a voice message.

National Number Prefix

A prefix that is used to direct a call as an in-country call. In the United States, this prefix is 1. In the United Kingdom and most the rest of the world, this prefix is 0.

number mask

A set of numbers and wildcard characters that is used to determine the telephone number that the Unified Messaging server will dial. An 'X' represents a single digit (0 … 9). A '*' represents any number of such digits.

numeric extension

A string of digits that doesn't contain a '+' or a country/region code. In dial plans, extensions are required to have a specified length.

outdialing

A process in which Unified Messaging (UM) dials or transfers calls. Unified Messaging generally receives calls, but sometimes dials calls. For example, outdialing occurs when a Unified Messaging auto attendant transfers a call to a user's extension, or when a UM-enabled user uses Play on Phone from Outlook.

Outlook Voice Access

A series of voice prompts that allows authenticated callers to access their e-mail, voice mail, calendar, and contact information using a standard analog, digital, or mobile telephone. Outlook Voice Access also enables authenticated callers to navigate their personal information in their mailbox, place calls, locate users, and navigate the system prompts and menus using DTMF, also known as touchtone, or voice inputs.

Outside Line Access Code

The prefix that is used by UM (or a person using an internal extension on the PBX) to access an outside line. This prefix is typically 9.

pilot identifier

A telephone number that points to a hunt group and is the access number for calls that are routed to Unified Messaging servers. This is also sometimes called a pilot number.

PIN

A passcode that a user enters on the telephone to access their Exchange mailbox.

Play on Phone

A Unified Messaging feature that users can use to play their voice messages or play and record personalized voice mail greetings over a telephone.

Private Branch eXchange (PBX)

A private telephone network in an organization. Individual telephone numbers or extension numbers are supported, and calls are automatically routed to them. Users can call each other using extensions, even across distributed locations.

prompt

An audio message played over the telephone to explain valid options to users.

Protected Voice Mail

A UM feature that uses information rights management to encrypt the contents of voice messages and specify the operations permitted on them. Protection can be caused by caller action (marking the message as private), or by system policy.

reset

When a PIN or a password is reset, the system randomly chooses a new, temporary PIN or password. The user is required to change the temporary PIN the next time that they sign in to Outlook Voice Access.

reverse number lookup (RNL)

A method used to try to locate the name of a person, from a directory or other information store, based on a telephone number.

RTAudio codec

An advanced speech codec that is designed for real-time two-way VoIP applications such as gaming, audio conferencing, and wireless applications over IP. RTAudio is the preferred Microsoft audio codec and is the default codec for Microsoft Unified

Communications platforms.

SIP notification

A SIP notification is a SIP message sent from one SIP peer to another to advise it of a change.

SIP peer

A SIP-enabled device that provides telephony communications between an IP gateway or SIP-enabled IP PBX and a Unified Messaging server.

star out

An action a caller can perform when they are dialed in to a Unified Messaging auto attendant but they want to be able to get to Outlook Voice Access to get their e-mail and voice mail. To do this, they press the star key while the auto attendant prompts are being played.

subscriber access number

A number that is configured in a PBX and on a UM dial plan that allows users to access their Exchange mailbox using Outlook Voice Access. In some cases, this may be configured to be the same number as the pilot number (also called a pilot identifier) on the PBX or IP PBX and the UM hunt group.

system prompt

A short audio recording, installed on the Unified Messaging server, which is played to callers by the server. System prompts are used to welcome callers and to inform them of their options when they use the Unified Messaging system.

telephone user interface (TUI)

An interface that is used to navigate the menus of a Unified Messaging system using DTMF, also known touchtone, inputs.

Text-to-Speech (TTS)

Technologies for translating or converting typewritten text into speech.

UM IP gateway

(See IP gateway.) A UM IP gateway is the Exchange Unified Messaging representation of any SIP peer with which it can communicate using VoIP protocols. It may represent a device that interfaces with a legacy PBX, or an IP PBX, or Microsoft Office Communications Server.

UM worker process

A process that's created during the startup of the Microsoft Exchange Unified Messaging service. The UM service, on receiving a request to handle an incoming call, immediately redirects the request to a UM worker process, which carries out all subsequent interactions with the caller.

UM Worker Process Manager

A component that handles the creation and monitoring of all the UM worker processes that are created.

Unified Messaging

An application that consolidates a user’s voice mail and e-mail into one mailbox, so that the user only needs to check a single location for messages, regardless of type. The e-mail server is used as the platform for all types of messages, making it unnecessary to maintain separate voice mail and e-mail infrastructures.

Unified Messaging server role

A set of components and services that enable voice and e-mail messages to be stored in a user’s single mailbox. Users can also access their Exchange mailbox from a

telephone or a computer. The Unified Messaging server role is included in Exchange Server 2007 and Exchange 2010.

voice mail

A system that records and stores telephone messages in a user mailbox.

Voice Mail Preview

A feature that provides text, transcribed from the audio recording, on a voice message when it is delivered.

voice message

An electronic message with a primary content of digitized audio.

Voice over IP (VoIP)

The practice of using an IP data network to transmit voice calls.

VoIP gateway

A computer device that converts between circuit-switched telephony protocols and VoIP protocols.

voice user interface (VUI)

An interface that is used to navigate the menus of a Unified Messaging system using speech inputs.

welcome greeting

A greeting that is played when an external caller calls in to a UM auto attendant or when an Outlook Voice Access user or another caller calls a subscriber access number that is configured on a UM dial plan. The default welcome greetings can be changed by a customer to make them specific to an organization or location.

1.9.1.14 Virtualization of the Unified Messaging Role in Exchange 2010 SP1

Virtualization of the Unified Messaging Role in Exchange 2010 SP1

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-03-07*

Many organizations today rely on some degree of virtualization to run Microsoft Exchange Server 2010. Virtualization of the Unified Messaging (UM) role on the 64-bit edition of Windows Server 2008 R2 is supported starting in Microsoft Exchange Server 2010 Pack 1 (SP1).

Required hardware and software

The virtualized UM server must be running as the guest operating system under Windows Server 2008 R2 Hyper-V. Windows Server 2008 R2 Hyper-V is a powerful virtualization technology that lets organizations take advantage of the benefits of virtualization without having to buy third-party software. By deploying Exchange 2010 together with Windows Server 2008 R2 Hyper-V technology, an organization of any size can avoid the complications that can arise from dealing with third-party virtualization software vendors.

An Exchange 2010 SP1 server that is running the UM server role must be the only Exchange role within a single virtualized server or Hyper-V environment. Other Exchange

2010 server roles, such as Client Access, Edge Transport, Hub Transport, and Mailbox, are not supported in the same virtualized server as the UM server role.

We recommend that the computer that is running the virtualized UM server have at least four CPU cores, and at least 16 GB of memory. For virtualizing UM, the essential requirement is a 1-to-1 mapping of physical cores to virtual cores, and no overbooking. We recommend that the virtualized UM be configured to use at least 2 GB of RAM per core.

In this configuration, a virtualized UM server that experiences a typical mixture of user and caller interactions can handle fewer concurrent calls than a physical UM server that has the same specifications. Under a sustained load, tests show that a virtualized UM server that is configured as described can handle 40 concurrent calls if Voice Mail Preview is active for all UM users, and it can handle 65 concurrent calls if Voice Mail Preview is not in use.

UM does some media (audio) I/O and processing. For the production and consumption of this media, the UM role must be able to keep up with the demands of other endpoints or the user experience will suffer. For example, users may notice audio dropout, either directly for playback or indirectly if speech recognition accuracy is affected.

Facts to consider before deploying UM in a virtualized environment

When you deploy UM servers in both a physical and a virtualized environment, you must consider multiple factors that can affect your Exchange environment:

- The number of mailboxes that are enabled for UM
- The number of incoming calls that are processed
- Whether Voice Mail Preview is enabled for UM-enabled users
- The amount of RAM and the number of processor cores per UM server

In typical UM deployments, the ratio of UM-enabled mailboxes that are served to concurrent calls is at least 100:1. This is because the amount of time that a UM server spends in servicing requests (such as recording messages or using Outlook Voice Access) for any given user usually amounts to a few minutes per day. Therefore, a UM server role, virtualized as described, supports about 4,000 UM-enabled mailboxes if they all have Voice Mail Preview enabled, and about 6,500 mailboxes if Voice Mail Preview is not enabled.

A virtualized UM server role can handle fewer concurrent incoming calls than a physical UM server with the same specifications. Concurrent incoming calls include incoming calls such as call answering or voice mail calls, fax calls, Outlook Voice Access calls, and calls that are answered by UM auto attendants.

A virtualized UM server that is running under Hyper-V can process approximately 40 concurrent incoming calls when Voice Mail Preview is active for all UM-enabled users, and can handle 65 concurrent calls if Voice Mail Preview is not active.

Voice Mail Preview is a UM feature that provides users a text version of their voice messages. The text is generated by automatic speech recognition, and is included with the voice message when it is delivered. Voice Mail Preview is supported in 7 UM language packs (US English, Canadian English, French, Italian, Spanish, Portuguese, and Polish).

If Voice Mail Preview is used, a UM server throttles Voice Mail Previews if the UM server is too busy or is overloaded with incoming calls. Therefore, the percentage of voice messages that include a transcription may be less than 100 percent, depending on the UM configuration and the environment. To be reasonably sure that all average-length voice messages contain voice mail preview text, we recommend that you set the number of concurrent incoming calls to be processed by a virtualized UM server to about 25 instead of 40.

Administrators who must run UM in an environment in which voice mail usage is much heavier than usual should reduce these values. If users receive an average of 10 or more voice messages per day, or use Outlook Voice Access for more than five minutes per day, the ratio of UM-enabled mailboxes that are served to concurrent calls will be nearer to 30:1.

Generally, a UM server role, virtualized as described, should support about 4,000 UM-enabled mailboxes if the mailboxes all have Voice Mail Preview enabled, and about 6,500 mailboxes if Voice Mail Preview is not enabled.

More Information

The Exchange 2010 UM role provides voice mail services, and consolidates voice mail and email messages into a user's Inbox. For more information about the UM server role, see Voicemail with Unified Messaging in Exchange 2010.

An organization might have many different reasons to want to virtualize an Exchange environment. The most common reasons for most organizations are as follows:

- To consolidate underused Exchange servers onto one physical server for increased hardware utilization.
- To consolidate Exchange Client Access server (CAS) and HUB server roles into a virtualized environment together with other server roles on the same or different physical servers (especially useful for small and medium-sized organizations or for branch offices of large organizations).
- To save space, power, and cooling for the servers that are running Exchange.

Exchange can be virtualized on one or more servers. A small organization can have a single server that provides all the required Exchange roles and functionality. A large organization requires a more complex configuration in which the Exchange roles are installed on multiple servers for the CAS, Hub Transport, Edge, Mailbox, and UM roles. Each of these roles includes its own unique workload characteristics. Typically, the different server roles work most intensively with the following components:

- Mailbox: processor, memory, disk
- CAS: processor, memory
- Hub Transport: memory, disk
- UM: processor, disk

You must perform careful planning and workload balancing for all of the server roles to determine the optimum configurations. All server roles can be expanded to additional servers to provide high availability and failover for your Exchange environment.

1.9.2 Managing Unified Messaging

Managing Unified Messaging

Exchange Server 2010 > Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2008-10-21*

Managing Unified Messaging Servers

Managing Unified Messaging Users

Managing Unified Messaging Components

Managing IP Gateways

1.9.2.1 Managing Unified Messaging Servers

Managing Unified Messaging Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-18*

Install the Exchange 2010 Unified Messaging Server Role

Uninstall the Unified Messaging Server Role in Exchange 2010

View or Configure the Properties of a UM Server

Enable Unified Messaging on Exchange 2010

Disable Unified Messaging on Exchange 2010

Add a UM Server to a Dial Plan

Remove a UM Server from a Dial Plan

Install a Unified Messaging Language Pack on a UM Server

Remove a Unified Messaging Language Pack from a UM Server

Configure the Startup Mode on a UM Server

Configure the Number of Concurrent Calls on a UM Server

Start the Microsoft Exchange Unified Messaging Service

Stop the Microsoft Exchange Unified Messaging Service

View the Number of Active Calls for a UM Server

View Call Statistics for a UM Server

Update the Speech Grammar Files on a UM Server

Configure Quality of Service (QoS) for Unified Messaging

Create a Certificate for Enabling Mutual TLS in Unified Messaging

Install the Exchange 2010 Unified Messaging Server Role

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use several methods to install the Unified Messaging (UM) server role on a computer running Microsoft Exchange Server 2010. The Unified Messaging server role can be installed on a single computer that has no other Exchange 2010 server roles installed or on a computer running another Exchange 2010 server role. This topic discusses the methods you can use to install the Unified Messaging server role.

Important:

After you install the Unified Messaging server role, you must perform other tasks before the Unified Messaging server can process incoming calls. To complete the steps required to enable and configure Unified Messaging, see Deploy a New Exchange 2010 RTM UM Environment.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Use the Setup wizard to install the UM server role

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

You can use the Setup wizard on the Exchange 2010 installation DVD to install the Unified Messaging server role. For more information about how to install the Unified Messaging server role using the Setup wizard, see Install Exchange 2010 Using the Custom Installation Type.

Use the command prompt to perform an unattended installation of the UM server role

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

You can perform an unattended installation of the Unified Messaging server role at a command prompt. For more information about how to perform an unattended installation of the Unified Messaging server role, see Install Exchange 2010 in Unattended Mode.

Use Setup.com to add or remove a UM Server Role

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

You can use Setup.com to add or remove the Unified Messaging server role to an existing

Exchange 2010 server. Setup.com supports command-line switches for performing scripted or quiet installations of Exchange 2010.

Important:

After you install the Unified Messaging server role, you must restart the system to allow the Unified Messaging service to reserve the TCP ports required.

Other Tasks

After you install the Unified Messaging server role you may also want to:

- Create a UM Dial Plan
- Create a UM IP Gateway

1.9.2.1.2 Uninstall the Unified Messaging Server Role in Exchange 2010

Uninstall the Unified Messaging Server Role in Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove the Unified Messaging server role from a computer running Microsoft Exchange Server 2010. When you uninstall or remove the Unified Messaging server role from an Exchange 2010 server, the server can no longer answer and process incoming calls.

In certain situations, you may have to remove the Unified Messaging server role from an Exchange 2010 server. If the Unified Messaging server role has been installed on the same server as another Exchange 2010 server role, you can remove the Unified Messaging server role using Setup.com.

Prerequisites

You must ensure that each of the Exchange 2010 server roles meets the appropriate prerequisites and system requirements before you begin the modification or uninstall process. For more information about server roles, see Overview of Exchange 2010 Server Roles. To understand the prerequisites for all server roles, see Exchange 2010 Prerequisites. For more information about system requirements, see Exchange 2010 System Requirements.

Remove the Unified Messaging server role

To perform the following procedure you must log on by using an account that's a member of the local Administrators group on the computer you're performing the procedures on. Or, the account you use must be a member of the Delegated Setup role group.

You can either run Exchange 2010 Setup.exe or navigate to Control Panel to modify or remove the Exchange 2010 Unified Messaging server role. In Control Panel, you can either remove the specific server role or the entire installation.

1. The Exchange Server 2010 Setup wizard begins the process of changing or removing your Exchange installation on the **Exchange Maintenance Mode**

page. Click **Next** to continue.
2. On the **Server Role Selection** page, select **Unified Messaging Role**. Click **Next** to continue.
3. On the **Readiness Checks** page, view the status to determine whether the organization and server role prerequisite checks completed successfully. If the prerequisite checks didn't complete successfully, review the **Summary** page to help troubleshoot and fix any issues that are preventing Setup from completing. If the checks completed successfully, click **Uninstall** to remove the Unified Messaging server role.

4. On the **Completion** page, click **Finish**.

1.9.2.1.3 View or Configure the Properties of a UM Server

View or Configure the Properties of a UM Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After you install the Unified Messaging (UM) server role, you first need to add the Unified Messaging server to a UM dial plan to allow it to process incoming calls. You can also configure several options including the number of concurrent calls that the Unified Messaging server can answer.

Looking for other management tasks related to Unified Messaging servers? Check out Managing Unified Messaging Servers.

What Do You Want to Do?

- Use the EMC to view or configure Unified Messaging server properties
- Use the Shell to configure Unified Messaging server properties
- Use the Shell to view Unified Messaging server properties

Use the EMC to view or configure Unified Messaging server properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM servers" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Unified Messaging**.
2. In the work pane, select the Unified Messaging server that you want to configure.
3. In the action pane, click **Properties**.

4. On the **General** tab, you can view general information about the server:
   - **Version** This field displays the version of Exchange installed on the server.
   - **Edition** This field displays the Exchange Server edition. The edition is either Standard Edition or Enterprise Edition.
   - **Role(s)** This field displays the Exchange server roles installed on the server.
   - **Product ID** This field displays the product ID for the Exchange server. If

you haven't yet entered the product key for the server, the product ID displayed is **Unlicensed**. To license an unlicensed version of Exchange, see Enter Product Key.

- **Modified** This field displays the last date and time that a configuration change was made on this server.

5. On the **System Settings** tab, view the domain controller servers and global catalog servers. You can also enable an error reporting feature:
   - **Domain controller servers being used by Exchange** This read-only box displays a list of domain controller servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.

   - **Global catalog servers being used by Exchange** This read-only box displays a list of global catalog servers used by the Exchange server.

     Note:
     This box isn't available on Edge Transport servers.

   - **Automatically send fatal service error report to Microsoft** Select this check box if you want to enable the error reporting feature and automatically send an error report to Microsoft in the event of a fatal error.
     If you enable the error reporting feature, information about fatal service errors is sent to Microsoft over encrypted channels. The information is used to improve Microsoft products.
     When this feature is enabled and the issue reported has a known solution, the server receives feedback from Microsoft. This feedback contains a link to information that may help resolve the problem.

6. On the **Customer Feedback Options** tab, you can enroll the selected server into the Customer Experience Improvement Program. For more information, see Opt-in or Opt-out of the Customer Experience Improvement Program.

7. Use the **UM Settings** tab to view and configure settings for the Unified Messaging (UM) server. This tab is available only on servers that have the Unified Messaging server role installed.
   - **Associated Dial Plans** Use this box to view the UM dial plans associated with the Unified Messaging server. When you install the Unified Messaging server role on a computer running Exchange Server 2010, the server is left in an enabled state. However, for the UM server to answer and process incoming calls, you must also associate a UM dial plan with the UM server. Click **Add** to select a UM dial plan.
     An Exchange 2010 UM server can be associated with multiple UM dial plans that have different Voice over IP (VoIP) security settings at the same time. After you associate the UM server with a UM dial plan, the UM server will process incoming calls for users who are associated with the UM dial plan.
   - **Prompt languages** Use this text box to view the languages supported by the UM server. The languages listed in this box are the languages or language packs installed on the UM server.
     By default, when you install the Unified Messaging server role, the U.S. English (en-US) language is installed even if you chose to install other languages when you installed Exchange 2010, and it can't be removed. However, after you've downloaded the appropriate UM language packs, you can add language packs for UM by using the **Setup.com /AddUMLanguagePack** or run the *<UMLanguagePack>*.exe installation program after you've downloaded the UM language pack from Exchange Server 2010 UM Language Packs. For details about how to add UM languages, see Managing Unified Messaging Servers.

- **Startup mode** Use this list to specify whether the Microsoft Exchange Unified Messaging service on a Unified Messaging server will start in **TCP**, **TLS**, or **Dual** mode. If the UM server is being added to UM dial plans that have different security settings, you should select Dual mode. In Dual mode, the UM server can listen on ports 5060 and 5061 simultaneously. If you change the startup mode, you must restart the Microsoft Exchange Unified Messaging service for the change to take effect.
- **Maximum concurrent calls** Use this box to specify the number of concurrent incoming voice call connections that the UM server will accept. When you increase the number of concurrent connections on a UM server, more system resources are required than if you decrease the number of concurrent voice call connections. Decreasing this setting is especially important on low-end, slower UM servers.

  The range for this setting is from 0 through 200. The default setting is 100. There are performance counters that you can use to monitor the current number of voice calls connected to a UM server.

Use the Shell to configure Unified Messaging server properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM servers" entry in the Unified Messaging Permissions topic.

This example prevents a Unified Messaging server named `MyUMServer` from accepting new calls.

```
Set-UMServer -Identity MyUMServer -Status NoNewCalls
```

This example removes a Unified Messaging server named `MyUMServer` from all UM dial plans.

```
Set-UMServer -Identity MyUMServer -DialPlans $null
```

This example adds the Unified Messaging server named `MyUMServer` to a UM dial plan named `MyUMDialPlanName` and also sets the maximum number of incoming voice calls.

```
Set-UMServer -Identity MyUMServer -DialPlans MyUMDialPlanName -MaxCalls 50
```

This example changes the grammar generation schedule to 02:30 to 03:00 (2:30 A.M. to 3:00 A.M.) every day on a Unified Messaging server named `MyUMServer`.

```
Set-UMServer -Identity MyUMServer -GrammarGenerationSchedule 1.02:30-1.03:00, 2.0
```

For more information about syntax and parameters, see Set-UMServer.

Use the Shell to view Unified Messaging server properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM servers" entry in the Unified Messaging Permissions topic.

This example displays a list of all the Unified Messaging servers in the Active Directory forest.

```
Get-UMServer
```

This example displays a formatted list of properties for the Unified Messaging server named MyUMServer.

```
Get-UMServer -Identity MyUMServer | Format-List
```

For more information about syntax and parameters, see Get-UMServer.

Other Tasks

After configuring a Unified Messaging server, you may also want to:

- Install a Unified Messaging Language Pack on a UM Server
- Configure the Default Language on a UM Dial Plan
- Enable a User for Unified Messaging

For More Information

Understanding Unified Messaging Servers

1.9.2.1.4 Enable Unified Messaging on Exchange 2010

Enable Unified Messaging on Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable Unified Messaging (UM) in Microsoft Exchange Server 2010. You must enable the Exchange computer running the Unified Messaging server role before the Unified Messaging server can process calls for UM-enabled Exchange 2010 recipients in your Exchange organization. However, the Unified Messaging server also must be added to a UM dial plan before it can process calls for Unified Messaging.

Although, by default, the Unified Messaging server is in an enabled state after the Unified Messaging server role is installed, the Unified Messaging server also has a status parameter that can be used to enable or disable the Unified Messaging server functions. The Unified Messaging server status is controlled by the **Enable-UMServer** and **Disable-UMServer** commands.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- The Unified Messaging server status is set to disabled. For detailed steps, see Disable Unified Messaging on Exchange 2010.

Use the EMC to enable Unified Messaging on an Exchange 2010 server

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Server Configuration** > Unified Messaging.
2. In the result pane, select the Unified Messaging server to enable.
3. In the action pane, click **Enable UM Server**.

Use the Shell to enable Unified Messaging on an Exchange 2010 server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

This example enables a UM server named MyUMServer to answer incoming calls.

```
Enable-UMServer -Identity MyUMServer
```

For more information about syntax and parameters, see Enable-UMServer.

Other Tasks

After you enable Unified Messaging on an Exchange 2010 server, you may also want to:

- Add a UM Server to a Dial Plan
- Configure the Startup Mode on a UM Server

1.9.2.1.5 Disable Unified Messaging on Exchange 2010

Disable Unified Messaging on Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use disable a Unified Messaging (UM) server in Microsoft Exchange Server 2010. When you disable Unified Messaging in Exchange 2010, you prevent the Unified Messaging server from answering Unified Messaging incoming calls. You can choose to disconnect all calls immediately or else wait for existing calls to be processed before disabling the Unified Messaging server.

After you disable the Unified Messaging server, it will no longer:

- Answer any incoming calls.
- Respond to Play on Phone requests from a Client Access server.
- Be used to manage UM-enabled mailboxes.
- Be queried when a diagnostic task is used.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Use the EMC to disable Unified Messaging

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Unified Messaging**.
2. In the result pane, select the Unified Messaging server to disable.
3. In the action pane, click one of the following:
   3.a. When you select the **Disable Immediately** option, the Unified Messaging server disconnects all calls connected to the Unified Messaging server.
   3.b. When you select the **Disable After Completing Calls** option, the Unified Messaging server won't accept new calls and won't be disabled until all calls have been processed.
4. In the confirmation dialog box, click **Yes** to continue.

Use the Shell to disable Unified Messaging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

This example disables Unified Messaging on the Unified Messaging server named MyUMServer but doesn't disconnect calls that are being processed.

```
Disable-UMServer -Identity MyUMServer
```

This example disables Unified Messaging on the Unified Messaging server named MyUMServer and disconnects all calls being processed.

```
Disable-UMServer -Identity MyUMServer -Immediate $true
```

For information about syntax and parameters, see Disable-UMServer.

Other Tasks

After you disable Unified Messaging, you may also want to:

- Enable Unified Messaging on Exchange 2010
- Configure the Startup Mode on a UM Server
- Add a UM Server to a Dial Plan

1.9.2.1.6 Add a UM Server to a Dial Plan

Add a UM Server to a Dial Plan

Unified Messaging > Managing Unified Messaging > Managing Unified Messaging Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you install the Unified Messaging (UM) server, it's left in an enabled state. However, before the UM server can answer and process incoming calls, you must add the UM server to a UM dial plan. You can add a Microsoft Exchange Server 2010 UM server to one or more UM dial plans with different security settings at the same time.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

Before you perform these procedures, confirm that a UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to add a UM server to a dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Server Configuration**.
2. In the result pane, select the Unified Messaging server.
3. In the action pane, click **Properties**.
4. On the **UM Settings** > **Associated Dial Plans**, click **Add**.
5. In the **Select Dial Plan** window, select the dial plan you want to add from the list of available dial plans, and then click **OK**.
6. Click **OK** again to accept your changes.

Use the Shell to add a UM server to a dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example adds a Unified Messaging server to a dial plan named `MyUMDialPlan` and prevents the UM server from accepting new calls. It also sets the start up mode to dual mode, which enables the UM server to accept TCP and TLS requests.

```
Set-UMServer -Identity MyUMServer -DialPlans MyUMDialPlan -Status Disabled -UMSta
```

This example adds the Unified Messaging server named `MyUMServer` to two UM dial plans, named `MyUMDialPlan` and `MyUMDialPlan2`, and also sets the maximum number of incoming voice and fax calls.

```
Set-UMServer -Identity MyUMServer -DialPlans MyUMDialPlan, MyUMDialPlan2 -MaxCall
```

For more information about syntax and parameters, see Set-UMServer.

Other Tasks

After you've added a UM server to a dial plan, you may also want to:

- Install a Unified Messaging Language Pack on a UM Server
- View or Configure the Properties of a UM Server

1.9.2.1.7 Remove a UM Server from a Dial Plan

Remove a UM Server from a Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can remove an Microsoft Exchange Server 2010 Unified Messaging server from a UM dial plan. When you remove a Unified Messaging server from a UM dial plan, the Unified Messaging server will no longer answer calls or process UM calls for UM-enabled recipients.To process calls, a Unified Messaging server must be added to at least one UM dial plan. However, a Unified Messaging server can be added to multiple UM dial plans.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- The Unified Messaging server has been added to at least one UM dial plan. For detailed steps, see Add a UM Server to a Dial Plan.

Use the EMC to remove an Exchange 2010 server from a dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Unified Messaging**.
2. In the result pane, select the Unified Messaging server.
3. In the action pane, click **Properties**.
4. On the **UM Settings** tab, in the **Associated Dial Plans** section, click **Remove**.
5. In the confirmation dialog box, click **Yes** to confirm the deletion of the Exchange 2010 server from the UM dial plan.
6. Click **OK** to close the properties window.

Use the Shell to remove an Exchange 2010 server from a dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

This example removes a UM server named `MyUMServer` from the dial plan named `MyUMDialPlan`.

```
Set-UMServer -Identity MyUMServer -DialPlans MyUMDialPlan
```

For more information about syntax and parameters, see Set-UMServer.

Other Tasks

After you remove an Exchange 2010 server from a dial plan, you may also want to:

- Disable Unified Messaging on Exchange 2010
- Uninstall the Unified Messaging Server Role in Exchange 2010

1.9.2.1.8 Install a Unified Messaging Language Pack on a UM Server

Install a Unified Messaging Language Pack on a UM Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-09*

To make a language available in the list of available Unified Messaging languages on the **Settings** tab of a UM dial plan, you must first install the appropriate UM language pack. You install the language pack on a Unified Messaging server by using the language-specific self-extracting executable file or the **setup.com /AddUmLanguagePack** command. Before you can install a UM language pack, you must first download it to a local folder on the UM server. You can download UM language packs from Exchange Server 2010 SP2 UM Language Packs.

After you install the appropriate UM language pack, you can view the list of installed UM language packs by viewing the properties on the **UM Settings** tab of a Unified Messaging server. You can also configure the default language to be a language other than English (en-US) on UM dial plans and auto attendants.

Caution:

The UM language packs for Microsoft Exchange Server 2007 or Exchange 2007 Service Pack 1 (SP1), SP2, or SP3 can't be used on an Exchange 2010 Unified Messaging server. The UM language packs for Exchange Server 2010 RTM or SP1 can’t be installed on a UM server running Exchange 2010 SP2.

Looking for other management tasks related to Unified Messaging servers? Check out Managing Unified Messaging Servers.

What Do You Want to Do?

- Use the UM Language Pack Installation file to install a UM language pack
- Use setup.com to install a UM language pack

Use the UM Language Pack Installation file to install a UM language pack

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

1. From the Microsoft Download Center, download the language-specific UM language pack file into a local folder on the UM server.
2. Double-click the UMLanguagePack.*<CultureCode>.exe* file. For example, for the German UM language pack, you would download the file named UMLanguagePack.de-DE.exe.

3. In the Exchange Server 2010 Setup wizard, on the **License Agreement** page, read the terms of the agreement, select **I accept the terms in the license agreement**, and then click **Next**.

4. On the **Unified Messaging Language Pack** page, verify that the correct language is listed in the **The following Unified Messaging Language Pack (s) will be installed** window, and then click **Install**.

5. On the **Completion** page, confirm whether the UM language pack was successfully installed.
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to complete the installation of the UM language pack.

Use setup.com to install a UM language pack

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

This example installs the Japanese (ja-JP) UM language pack that's been downloaded to the D:\Exchange\UMLanguagePacks folder on a Unified Messaging server.

```
setup.com /AddUmLanguagePack:ja-JP /s:d:\Exchange\UMLanguagePacks
```

This example installs the Mexican Spanish (es-MX) and German (de-DE) UM language packs that have been downloaded to the D:\Exchange\UMLanguagePacks folder on a UM server.

```
setup.com /AddUmLanguagePack:es-MX,de-DE /s:d:\Exchange\UMLanguagePacks
```

For more information about available UM languages and the culture codes, see Understanding Unified Messaging Languages.

Other Related Tasks

After you install a Unified Messaging language pack, you may also want to:

- Configure the Default Language on a UM Dial Plan
- Add a UM Server to a Dial Plan

For More Information

Understanding Unified Messaging Languages

1.9.2.1.9 Remove a Unified Messaging Language Pack from a UM Server

Remove a Unified Messaging Language Pack from a UM Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2010, you can manage UM languages on Unified Messaging servers using the Exchange Management Console or the Exchange Management Shell. However, to remove a language from the list on a UM dial plan, you must remove the appropriate UM language pack from the Unified Messaging server by using the **Setup.com /RemoveUmLanguagePack** command. After you remove the UM language pack from the Unified Messaging server, the language won't be available when you configure a UM dial plan. You can view the UM language packs that are installed by viewing the properties of the Unified Messaging server or using the **Get-UMServer** cmdlet.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Use Setup.com to remove a UM language pack

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

At a command prompt, run the following command:

```
Setup.com /RemoveUmLanguagePack:<UmLanguagePackName> /s: d:\<MyLocalFolder>
```

In the previous command, *<UmLanguagePackName>* is the name of the UM language pack, for example, fr-FR.

Caution:

You can't use the Setup.com file that's located in the \Bin folder to remove a UM language pack after you've installed any updates for Exchange 2010. You must use the Setup.com file from the Exchange 2010 DVD or the downloaded source files. If you don't, you'll see the following error: There is a version mismatch between the running application and the installed application.

Other Tasks

After you remove a UM language pack, you may also want to:

- Configure the Default Language on a UM Dial Plan
- Configure the Language Setting on a UM Auto Attendant

1.9.2.1.10 Configure the Startup Mode on a UM Server

Configure the Startup Mode on a UM Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify the startup mode for the Microsoft Exchange Unified Messaging service on a Unified Messaging (UM) server. By default, the UM server will startup in TCP mode, but if

you are using Transport Layer Security (TLS) to encrypt Voice over IP (VoIP) traffic you must configure the UM server to use TLS or Dual mode. A UM server can be added to UM dial plans that have different security settings. If the UM server has been added to dial plans with different security settings, you should select Dual mode. If you change the startup mode, you must restart the Microsoft Exchange Unified Messaging service for the change to take effect

Important:

When Exchange Server 2010 is installed, static Windows Firewall rules are added for Exchange. If you change the TCP ports that are used by the Unified Messaging server role, you may also need to reconfigure the Windows Firewall rules to allow Unified Messaging to work correctly.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Use the EMC to configure the startup mode

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

1. In the console root, navigate to **Server Configuration** > **Unified Messaging**.
2. In the result pane, click to select the Unified Messaging server you want to set up.
3. In the action pane, click **Properties**.
4. On the **UM Settings** tab, in the **Startup Mode** drop-down list, select one of the following settings:
   - 4.a. **TCP** Use this setting if the UM server is being added to only UM dial plans that are set to **Unsecured** but won't be added to dial plans that are set to **SIP Secured** or **Secured**. In TCP mode, the UM server will only listen on TCP port 5060 for SIP requests. By default, the UM server will startup in TCP only mode.
   - 4.b. **TLS** Use this setting if the UM server is being added to UM dial plans that are set to **SIP Secured** or **Secured** but won't be added to dial plans that are set to **Unsecured**. In TLS mode, the UM server will only listen on TCP port 5061 for SIP requests.
   - 4.c. **Dual** Use this setting if the UM server is being added to UM dial plans that have different security settings. In Dual mode, the UM server can listen on ports 5060 and 5061 simultaneously.

     Note:

     If you change the startup mode, you must restart the Microsoft Exchange Unified Messaging service for the change to take effect.
5. Click **OK**.

Use the Shell to configure the startup mode

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

This example sets the startup mode for a UM server named `MyUMServer1` to Dual mode.

```
Set-UMServer -Identity MyUMServer1 -UMStartUpMode Dual
```

This example sets the startup mode for a UM server named MyUMServer1 to TCP mode.

```
Set-UMServer -Identity MyUMServer1 -UMStartUpMode TCP
```

For more information about syntax and parameters, see Set-UMServer.

Other Tasks

After you configure the startup mode, you may also want to:

- Configure VoIP Security on a UM Dial Plan
- View the Number of Active Calls for a UM Server

1.9.2.1.11 Configure the Number of Concurrent Calls on a UM Server

Configure the Number of Concurrent Calls on a UM Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You configure the number of incoming concurrent voice call connections that a Unified Messaging (UM) server accepts in Microsoft Exchange Server 2010. When you increase the number of concurrent connections on a Unified Messaging server, more system resources are required than if you decrease the number of concurrent voice call connections. Decreasing this setting is especially important on low-end, slower computers on which Unified Messaging is installed.

Note:

The range for the number of concurrent voice calls is 0 to 200. The default setting is 100.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Unified Messaging Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Unified Messaging**.
2. In the result pane, click to select the Unified Messaging server you want to set up.
3. In the action pane, click **Properties**.
4. On the **UM Settings** tab, in the **Maximum concurrent calls** text box, type the maximum number of concurrent voice calls.
5. Click **OK**.

Use the Shell to set up the number of concurrent connections on a Unified Messaging server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

This example sets the number of incoming calls that can be accepted by a UM server named MyUMServer1 to 50.

```
Set-UMServer -Identity MyUMServer1 -MaxCallsAllowed 50
```

For more information about syntax and parameters, see Set-UMServer.

Other Tasks

After you configure the number of concurrent calls, you may also want toView the Number of Active Calls for a UM Server.

1.9.2.1.12 Start the Microsoft Exchange Unified Messaging Service

Start the Microsoft Exchange Unified Messaging Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Services snap-in in Microsoft Management Console (MMC) or cmd.exe at a command prompt to start the Microsoft Exchange Unified Messaging service. By default, the Microsoft Exchange Unified Messaging service is started after the Unified Messaging server role is installed on a computer running Microsoft Exchange Server 2010. However, there may be times when you must restart the Microsoft Exchange Unified Messaging service manually, for example, when you've taken the Unified Messaging server offline and have to bring it back online.

When the Microsoft Exchange Unified Messaging service is started on a Unified Messaging server, the Unified Messaging server is available to process incoming UM calls.

Note:

The default startup time for the Microsoft Exchange Unified Messaging service is 120 seconds. You can increase this time-out value by editing the Msexchangeum.config file located in the \Program Files\Microsoft Exchange\V14\bin folder.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Use the MMC Services snap-in to start the Microsoft Exchange Unified Messaging service

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

1. Click **Start**, and then click **Control Panel**.
2. In **Control Panel**, double-click **Administrative Tools**.
3. In **Administrative Tools**, double-click **Services**.
4. In the **Services** result pane, right-click **Microsoft Exchange Unified Messaging**, and then click **Start**.

Use a command prompt to start the Microsoft Exchange Unified Messaging service

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type the following command, and then press **ENTER**.

```
net start MSExchangeUM
```

Other Tasks

After you start the Microsoft Exchange Unified Messaging service, you may also want to:

- Configure the Startup Mode on a UM Server
- Stop the Microsoft Exchange Unified Messaging Service

1.9.2.1.13 Stop the Microsoft Exchange Unified Messaging Service

Stop the Microsoft Exchange Unified Messaging Service

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can stop the Microsoft Exchange Unified Messaging service using the Services snap-in in Microsoft Management Console (MMC) or at a command prompt. There may be times when you need to stop this service, for example, when you must take the Unified Messaging server offline. When you stop the Microsoft Exchange Unified Messaging service, the Unified Messaging server won't be able to accept and process incoming calls.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Use the MMC Services snap-in to stop the Microsoft Exchange Unified Messaging service

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

1. Click **Start**, and then click **Control Panel**.
2. In **Control Panel**, double-click **Administrative Tools**.
3. In **Administrative Tools**, double-click **Services**.
4. In the **Services** details pane, right-click **Microsoft Exchange Unified Messaging**, and then click **Stop**.

Use a command prompt to stop the Microsoft Exchange Unified Messaging service

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type the following command, and then press **ENTER**.

```
net stop MSExchangeUM
```

Other Tasks

After you stop the Microsoft Exchange Unified Messaging service, you may also want to:

- Start the Microsoft Exchange Unified Messaging Service
- Configure the Startup Mode on a UM Server

1.9.2.1.14 View the Number of Active Calls for a UM Server

View the Number of Active Calls for a UM Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can view the number of active Unified Messaging (UM) calls being processed. You can view the number of active calls for a UM dial plan, a Unified Messaging server, or all calls for a UM IP gateway. If you use the **Get-UMActiveCalls** cmdlet to view the number of active calls for dial plans or IP gateways, the cmdlet uses Active Directory to determine which Unified Messaging servers must be contacted.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Use the Performance console to view the number of active calls

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

1. Click **Start**, click **Programs**, click **Administrative Tools**, and then click **Performance**.
2. In the **Performance** console, right-click the details pane, and then select **Add Counters** from the menu. You can also press CTRL+I to open the **Add Counters** window.
3. In the **Add Counters** window, in the **Performance object** list, select **MSExchangeUMGeneral**.
4. In **Select Counters from list**, select **Current Calls**, click **Add**, and then click **Close**.
5. In the **Performance** console, in the details pane, select the **Current Calls**

counter to display the number of current calls.

Use the Shell to view the number of active calls for a Unified Messaging server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

This example displays the details of all active calls on the local Unified Messaging server.

```
Get-UMActiveCalls
```

This example displays the details of all active calls on a Unified Messaging server named MyUMServer.

```
Get-UMActiveCalls -Server MyUMServer
```

This example displays the details of all active calls being processed by a UM IP gateway named MyUMIPGateway.

```
Get-UMActiveCalls -IPGateway MyUMIPGateway
```

This example displays a list of active calls associated with the UM dial plan named MyUMDialPlan.

```
Get-UMActiveCalls -DialPlan MyUMDialPlan
```

Note:

When a Unified Messaging server is process cycling, the **Get-UMActiveCalls** cmdlet won't return a list of all calls for the retired process and the active process. It returns the active calls only for the new process.

For more information about syntax and parameters, see Get-UMActiveCalls.

Other Tasks

After you view the number of active calls for a Unified Messaging server, you may also want to:

- Testing Unified Messaging Server Functionality
- Test Unified Messaging Server Operation

1.9.2.1.15 View Call Statistics for a UM Server

View Call Statistics for a UM Server

Unified Messaging > Managing Unified Messaging > Managing Unified Messaging Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the **Call Statistics** tool, available in Exchange Server 2010 Service Pack 1 (SP1), to provide aggregated statistical information about calls that are forwarded to or

placed by UM servers. This information is helpful for administrators who are interested in overall statistics for the Exchange 2010 Unified Messaging (UM) servers in their organization. Call statistics reports that you initiate in the EMC are displayed in the Exchange Control Panel (ECP) user interface. For more information, see New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1.

Reports can be filtered to show call statistics by month, by day, for the past 90 days, or since UM was deployed in your organization. You can then filter these results by UM dial plan and UM IP gateway within your organization.

Call statistics reports display:

- The total number of calls, organized by type of call (for example, missed calls, Outlook Voice Access calls, or fax calls).
- The average audio quality metrics for the selected month, day, or all calls placed or forwarded since UM was deployed in your organization.

For more information about the **Call Statistics** tool, see Using Unified Messaging Tools.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- A UM server has been added to a UM dial plan. For detailed steps, see Add a UM Server to a Dial Plan.

Use the EMC to view the call statistics for a UM server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM call data and summary reports" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Toolbox**, then **Call Statistics**, and then click **Open Tool** from the **Actions** menu. If you receive the error message "There is a problem with this website's security certificate", click **Continue to this website (not recommended)**.
2. In the **Outlook Web App** window, enter the correct user account (in the format Domain\user name) and password, and then click **Sign in**.
3. If this is your first time signing in to the ECP, select your language and time zone, and then click **OK**.
4. In the **Call Statistics** window, specify the following:
   4.a. **Show** Select the time period to show for incoming calls.
   4.b. **UM dial plan** Select the UM dial plan you want call statistics for.
   4.c. **UM IP gateway** Select the UM IP gateway you want call statistics for.
5. The call details will be listed in the table that's displayed in the window.

Use the Shell to view the call statistics for a UM server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM call data and summary reports" entry in the Unified Messaging Permissions topic.

This example displays the statistics for all calls received by or placed by Unified Messaging servers in an organization.

```
Get-UMCallSummaryReport -GroupBy Total
```

This example displays the statistics for all calls received by or placed by Unified Messaging servers in an organization over the last 12 months.

```
Get-UMCallSummaryReport -GroupBy Month
```

This example displays the statistics for all calls received by or placed by Unified Messaging servers in the organization over the last 90 days.

```
Get-UMCallSummaryReport -GroupBy Day
```

This example displays the statistics for calls received or placed by Unified Messaging servers for the UM dial plan MyUMDialPlan.

```
Get-UMCallSummaryReport -GroupBy Month -UMDialplan MyUMDialPlan
```

For more information about syntax and parameters, see Get-UMCallSummaryReport.

Other Tasks

After you view the call statistics for a UM server, you may also want to:

- View the Number of Active Calls for a UM Server
- View Call Logs for a UM-Enabled User
- Testing Call Flow with the Exchange 2010 UM Troubleshooting Tool
- Test-UMConnectivity

1.9.2.1.16 Update the Speech Grammar Files on a UM Server

Update the Speech Grammar Files on a UM Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can update the Automatic Speech Recognition (ASR) grammar files for Microsoft Exchange Server 2010 Unified Messaging (UM). Speech grammar files have a file name extension of .cfg and are used by Unified Messaging to enable callers to use speech inputs to perform directory lookups. A folder for each UM language is created in the <Program Files>\Microsoft\Exchange Server\V14\UnifiedMessaging\grammars folder. Each UM language-specific folder contains the grammar files for the given language that are used for Outlook Voice Access. The language-specific folders also contain the grammar files generated by the Microsoft Exchange Unified Messaging service for the global address list, custom address lists, UM dial plans, and UM auto attendants.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Use the galgrammargenerator.exe program to update the speech grammar files on a Unified Messaging server

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

This example creates a grammar file for each UM dial plan to which the specified UM server belongs.

```
Galgrammargenerator.exe -s MyUmServer
```

This example creates a grammar file for the UM-enabled users who belong to the UM dial plan named `MyUMDialPlan`.

```
Galgrammargenerator.exe -d MyUMDialPlan
```

This example creates or updates DTMF maps for users who are enabled for UM and who aren't enabled for UM.

```
Galgrammargenerator.exe -u
```

For more information about syntax and parameters, at the command prompt, type galgrammargenerator.exe -?

Other Tasks

After you update the speech grammar files on a Unified Messaging server, you may also want to:

- Enable or Disable Automatic Speech Recognition on a UM Auto Attendant
- Install a Unified Messaging Language Pack on a UM Server

1.9.2.1.17 Configure Quality of Service (QoS) for Unified Messaging

Configure Quality of Service (QoS) for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 Unified Messaging supports DiffServ through Differentiated Services Code Point (DSCP) marking. In Microsoft Windows Server 2008, TCP/IP performs DiffServ marking when you've installed the Quality of Service (QoS) Packet Scheduler. When you install the Unified Messaging server role on a computer that's running Windows Server 2008 with the QoS Packet Scheduler installed, all outgoing Unified Messaging packets will be marked with a DSCP value that's configured using Group Policy. If you're integrating Exchange Unified Messaging and Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010, you can also configure QoS using DiffServ.

Note:
Layer 3 network devices, such as routers, must also support DiffServ.

When you create a QoS policy on Windows Server 2008, it will be applied to all UDP packets that are set by the Microsoft Unified Communications Managed API v. 2.0 (UCMA). For more information about how to configure Policy-based QoS, see Policy-based Quality of Service (QoS).

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Prerequisites

The Unified Messaging server role is installed. For detailed steps, see Install the Exchange 2010 Unified Messaging Server Role.

Enable QoS for Unified Messaging

To perform the following procedures, you must log on to the Unified Messaging server by using an account that's a member of the local Administrators group on that computer.

1. Click **Start**, click **Run**, type **gpedit.msc** in the **Open** dialog box, and then click **OK**.
2. In the **Group Policy Object Editor** window, locate Computer Configuration/Policies/Administrative Templates/Network/QoS Packet Scheduler/DSCP value of conforming packets.
3. In the result pane, double-click **Controlled load service type**.
4. In the **Controlled load service type Properties** window, click **Enable**.
5. In the **DSCP value** dialog box, verify that the DSCP value **24** is selected, and then click **OK**.
6. In the result pane, double-click **Guaranteed service type**.
7. In the **Guaranteed service type Properties** window, click **Enable**.
8. In the **DSCP value** dialog box, verify that the DSCP value **40** is selected, and then click **OK**.
9. Close the **Group Policy Object Editor** window.
10. If you want to verify that the DSCP values are set correctly, performing these steps:

    Caution:
    Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

    10.a. Start Registry Editor (regedit).
    10.b. Locate the following key: **HKLM\Software\Policies\Microsoft\Windows\Psched\DiffservByteMappingConforming**
    10.c. The following default values will be set:
    SERVICETYPE_GUARANTEED (DSCP 40, 0x28)
    SERVICETYPE_CONTROLLEDLOAD (DSCP 24, 0x18)
11. Regardless of whether your environment is integrated with Office Communications Server 2007 R2 or Microsoft Lync Server 2010, configure the registry key to enable QoS marking of IP packets sent by setting the. **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RTC\Transport\QoSEnabled** key to **1**. Then restart the Communications Server 2007 server or the Lync Server 2010 server to load the QoS settings that are stored in the registry.

Enable QoS for Unified Messaging and Office Communications Server 2007 R2 or Microsoft Lync Server 2010

To perform the following procedures, you must log on to the Unified Messaging server by using an account that's a member of the local Administrators group on that computer.

1. Enable the **QoS Packet Scheduler** service on servers and clients. By default, the **QoS Packet Scheduler** service is enabled on Windows Server 2008 computers. However, by default, it isn't enabled on Windows Server 2003 computers. QoS marking isn't enabled by default in Communications Server 2007 R2 or Lync Server 2010 because Communications Server 2007 R2 and Lync Server 2010 only run on Windows Server 2008 and QoS marking depends on the **QOS Packet Scheduler** service running on both server and client computers.
2. Configure the registry key to enable QoS marking of IP packets sent to and from the Communications Server 2007 server or the Lync Server 2010 server by setting the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RTC\Transport\QoSEnabled** key to **1**. Then restart the Communications Server 2007 R2 or Lync Server 2010 server to load the QoS settings that are stored in the registry.
3. Use Group Policy to set DSCP values that mark the IP packets if you need values other than the defaults for Guaranteed service type packets (used for audio) and Controlled load service type packets (used for video). By default, the following settings are applied when you set the **QoSEnabled** DWORD value:
   - SERVICETYPE_GUARANTEED (DSCP 40, 0x28)
   - SERVICETYPE_CONTROLLEDLOAD (DSCP 24, 0x18)

For more information about QoS and Communications Server 2007 R2, see Voice QoS.

Other Tasks

After you enable Unified Messaging on an Exchange 2010 server, you may also want to:

- Configure the Startup Mode on a UM Server
- Start the Microsoft Exchange Unified Messaging Service
- Stop the Microsoft Exchange Unified Messaging Service

1.9.2.1.18 Create a Certificate for Enabling Mutual TLS in Unified Messaging

Create a Certificate for Enabling Mutual TLS in Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable Voice over IP (VoIP) security for a Unified Messaging (UM) dial plan. By default, when a UM dial plan is created, it will use Unsecured mode or no encryption. When you configure the UM dial plan to use Session Initiation Protocol secured (SIP

Secured) or Secured mode, the Unified Messaging servers that are associated with the UM dial plan will encrypt the SIP signaling traffic or the Realtime Transport Protocol (RTP) media channels and the SIP signaling traffic.

To enable a UM server to encrypt data that's sent between IP gateways and IP PBXs you must:

- Create a new self-signed or public certificate that you can use for mutual TLS.
- Associate a certificate with the UM server.
- Configure the UM dial plan as SIP Secured or Secured.
- Configure the startup mode on the UM server.
- Configure the listening port on the UM IP gateways to use TCP port 5061.
- Import the certificate on your IP gateways or IP PBXs.

Prerequisites

After you've installed the Unified Messaging server role, you'll have to create a certificate that can be used to encrypt data between a UM server and IP gateways or IP PBXs.

Use the EMC to create a new Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic. You must also log on by using an account that's a member of the local Administrators group on that computer.

1. In the console tree, click **Server Configuration**.
2. In the action pane, click **New Exchange Certificate** to open the New Exchange Certificate wizard.
3. On the **Introduction** page, enter a friendly name for your certificate.
4. On the **Domain Scope** page, don't select the **Enable wildcarding for this certificate** check box.
5. On the **Exchange Configuration page > expand Unified Messaging server**.
6. Select **Self-signed certificate** or **Public certificate**, enter the fully qualified domain name (FQDN) of your UM server in the **Fully qualified domain name (FQDN) of your UM servers** box, and then click **Next**.
7. On the **Organization and Location** page, enter information about your Exchange organization.
8. On the **Certificate Completion** page, verify that all the information you've entered is correct. If it is correct, click **New**.
9. On the **Completion** page, follow the steps that are listed there to complete your request. This page also contains the cmdlet syntax necessary to create a new certificate.

Use the Shell to create a new Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic. You must also log on by using an account that's a member of the local Administrators group on that computer.

This example creates a new Exchange certificate request for a UM server named `MyUMServer` with a friendly name of `UMCert`.

```
New-ExchangeCertificate -FriendlyName 'UMCert' -GenerateRequest -PrivateKeyExport
```

Other Tasks

After you create a certificate for Unified Messaging, you may also want to:

- Assign Services to a Certificate
- Configure the Startup Mode on a UM Server
- Configure VoIP Security on a UM Dial Plan

1.9.2.2 Managing Unified Messaging Users

Managing Unified Messaging Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-18*

Enable a User for Unified Messaging

Disable Unified Messaging for a User

View or Configure the Properties of a UM-Enabled User

View Call Logs for a UM-Enabled User

Configure the UM Mailbox Policy Assigned to a UM-Enabled User

Enable or Disable Automatic Speech Recognition for a UM-Enabled User

Enable or Disable Calls from Users Who Are Not UM-Enabled for a UM-Enabled User

Enable a UM-Enabled User to Receive Faxes

Prevent a UM-Enabled User from Receiving Faxes

Allow or Prevent Calls Without a Caller ID to Leave a Voice Message

Enable or Disable Call Answering Rules for a UM-Enabled User

Enable or Disable a Personal Operator for a UM-Enabled User

Add an Extension Number for a UM-Enabled User

Remove an Extension Number for a UM-Enabled User

Modify an Extension Number for a UM-Enabled User

Modify a SIP Address for a UM-Enabled User

Modify an E.164 Address for a UM-Enabled User

Configure a UM-Enabled User's TUI Settings

Configuring PIN Security for a UM-Enabled User

Set PIN Policies for UM-Enabled Users

Retrieve PIN Information for a UM-Enabled User

Reset a Unified Messaging PIN for a UM-Enabled User

Change the UM Dial Plan for a UM-Enabled User

1.9.2.2.1 Enable a User for Unified Messaging

Enable a User for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When you enable a user for Unified Messaging (UM), a default set of UM properties are applied to the user, and the user will be able to use the Unified Messaging features. When you enable a user for Unified Messaging, you have the option to add a Session Initiation Protocol (SIP) or E.164 address for the user. However, the user must still have an extension number configured.

You can configure the extension number automatically or manually using the Enable Unified Messaging wizard. An extension number is required for each UM-enabled user associated with a telephone extension, SIP Uniform Resource Identifier (URI), or E.164 dial plan. The extension number must be the correct number of digits, as specified in the UM dial plan for the UM mailbox policy. If the user is associated with an E.164 dial plan, you can manually configure an E.164 address for a user using the Enable Unified Messaging wizard. If you associate a user to a SIP URI or E.164 dial plan, you must manually enter an extension number and the SIP or E.164 address for the user.

Note:

You must add, remove, or modify the Exchange Unified Messaging proxy addresses (EUM addresses) for a user using the **EUM Address** menu item on the **E-mail Addresses** tab on the user's mailbox properties.

Looking for other management tasks related to UM-enabled users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

What Do You Want to Do?

- Use the EMC to enable a user for Unified Messaging
- Use the Shell to enable a user for Unified Messaging

Use the EMC to enable a user for Unified

Messaging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the user mailbox that you want to enable for Unified Messaging.
3. In the action pane, click **Enable Unified Messaging**.
4. In the Enable Unified Messaging wizard, on the **Introduction** page, complete the following fields:
   - **Unified Messaging Mailbox Policy** Use this text field to select the UM mailbox policy that you want to associate with a user's mailbox.
     UM mailbox policies define settings such as PIN policies, dialing restrictions, and message text for Unified Messaging messages sent to the user. Each UM-enabled user is required to be associated with at least one UM mailbox policy. However, the UM-enabled user can be associated with only one UM mailbox policy.
   - **Automatically generate PIN to access Outlook Voice Access** Click this button to automatically generate a PIN for the UM-enabled user. This is the default setting. If this option is selected, a PIN is automatically generated based on the PIN policies configured on the UM mailbox policy associated with the recipient. We recommend that you use this setting to help protect the user's PIN.
   - **Manually specify PIN** Click this button to manually specify a PIN that a recipient will use to access the Unified Messaging system.
     The PIN must comply with the PIN policy settings configured on the UM mailbox policy associated with this recipient. For example, if the UM mailbox policy is configured to accept only PINs that contain seven or more digits, the PIN you enter in this text box must be at least seven digits.
   - **Require user to reset PIN on first telephone logon** Select this check box to force the user to reset a Unified Messaging PIN when the user accesses the Unified Messaging system from a telephone.
     It's a security best practice to force UM-enabled users to change their PIN at their first logon to help protect against unauthorized access to their data and Inbox. This is the default setting.
5. In the Enable Unified Messaging wizard, on the **Extension Configuration** page, complete the following fields:
   - **Automatically generated mailbox extension** Click this button if you want the extension number for the user's mailbox to be automatically generated from the telephone number specified in the Active Directory directory service and used to populate the field. By default, this setting is enabled. This option will be unavailable if the user is being associated with a SIP URI or E.164 dial plan.
     For the user's extension number to populate this field, you can enter the telephone number in the **Business** field on the **Address and Phone** tab in the user properties in the EMC. You can also configure a telephone number for a user by configuring the **Telephone number** field on the **General** tab on the user account using Active Directory Users and Computers.
     If you select this option, the extension number generated automatically for the user will comply with the number of digits specified for the dial plan with which the UM mailbox policy that you selected is associated. For example, if the dial plan is

configured to use 5-digit extension numbers, the Unified Messaging server will take the last 5 digits of the user's telephone number and use those digits to populate this field. UM dial plans are typically configured to have extensions three through seven digits long.

- **Manually entered mailbox extension** Click this button if you want to manually configure the extension number for the user's mailbox.

  If you select this option, you must supply the extension number for the user. If you select this option, you must provide a valid extension number for the user and must match the number of digits specified on the dial plan. You can configure this field to contain a value range of numeric characters or digits from 1 through 20. The typical extension number is from 3 through 7 digits and is configured on the dial plan with which the UM mailbox policy is associated.

  If your existing telephony environment includes extension numbers, you must specify a number of digits that matches the number of digits in those extensions. The number of digits that you specify is the default setting after a UM mailbox policy is selected.

- **Automatically generated SIP resource identifier** Click this button if you want the SIP resource identifier or SIP address for the user's mailbox to be automatically generated. If you have deployed Microsoft Office Communications Server 2007, the user's SIP address is taken from the **msRTCSIP-PrimaryUserAddress** attribute in Active Directory. If this attribute isn't populated, the user's primary SMTP address will be used for the SIP address. By default, this setting is enabled, for example, tony.smith@contoso.com.

  This option is available only if the user that you enable for Unified Messaging is associated with a SIP URI dial plan. This option will be unavailable if you configure a user's mailbox to be associated with an E.164 dial plan.

  If you associate a user with a SIP URI dial plan, you must also manually enter a mailbox extension for the user. This extension number is used when users use Outlook Voice Access to access their Exchange 2010 mailbox. The number of digits that you configure in this field must match the number of digits configured on the SIP URI or E.164 dial plan.

  This option will not be available if the user is being associated with a telephone extension dial plan.

- **Manually entered SIP resource identifier** Click this button if you want to manually enter the SIP or E.164 address for the user. This option is available if the user that you enable for Unified Messaging is associated with either a SIP URI or E.164 dial plan. If you deployed Communications Server 2007, the user's SIP address is taken from the **msRTCSIP-PrimaryUserAddress** attribute in Active Directory. If this attribute isn't populated, the user's primary SMTP address is used for the SIP address, for example, tony.smith@contoso.com. This option isn't available if the user is associated with a telephone extension dial plan.

  If you associate the user with an E.164 dial plan, you must manually enter an E.164 address for the user. The number entered must be in the correct E.164 format, for example, +14255551234.

  If you associate the user with a SIP or E.164 dial plan, you must also manually enter a mailbox extension number for the user. This extension number is used when users use Outlook Voice Access to access their Exchange 2010 mailbox. The number of digits that you configure in this field must match the number of digits configured on the SIP URI or E.164 dial plan.

6. On the **Enable Unified Messaging** page, review your configuration settings. Click **Enable** to enable the user for Unified Messaging. Click **Back** to make configuration changes.

7. On the **Completion** page, confirm whether the user was successfully enabled for Unified Messaging:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
8. Click **Finish** to complete the Enable Unified Messaging wizard.

Use the Shell to enable a user for Unified Messaging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example enables Unified Messaging on the mailbox for tonysmith@contoso.com, sets the extension and PIN for the user, and then assigns a UM mailbox policy named MyUMMailboxPolicy to the user's mailbox.

```
Enable-UMMailbox -Identity tonysmith@contoso.com -UMMailboxPolicy MyUMMailboxPoli
```

This example enables Unified Messaging on a SIP-enabled mailbox for tonysmith@contoso.com, associates a UM mailbox policy named MyUMMailboxPolicy, and sets the extension number, SIP resource identifier, and PIN for the user.

```
Enable-UMMailbox -Identity tonysmith@contoso.com -UMMailboxPolicy MyUMMailboxPoli
```

For more information about syntax and parameters, see Enable-UMMailbox.

Other Tasks

After you have enabled a user for Unified Messaging, you may also want to:

- View or Configure the Properties of a UM Mailbox Policy
- Set PIN Policies for UM-Enabled Users

For More Information

Understanding Unified Messaging Users

1.9.2.2.2 Disable Unified Messaging for a User

Disable Unified Messaging for a User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can disable Unified Messaging (UM) for a UM-enabled user. When you disable a user

for Unified Messaging, the user is no longer able to use the UM features found in Microsoft Exchange Server 2010. If you prefer, you can keep the UM settings for the user after the user is disabled.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- The existing Exchange recipient has an Exchange mailbox.
- The existing user is currently enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.
- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to disable Unified Messaging for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the user whose mailbox you want to disable for Unified Messaging.
3. In the action pane, click **Disable Unified Messaging**.
4. In the confirmation dialog box, click **Yes** to confirm that Unified Messaging will be disabled for the user.

Use the Shell to disable Unified Messaging for a user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example disables Unified Messaging for the user tonysmith@contoso.com but keeps the UM mailbox settings.

```
Disable-UMMailbox -Identity tonysmith@contoso.com -KeepProperties False
```

For more information about syntax and parameters, see Disable-UMMailbox.

Other Tasks

After you disable Unified Messaging for a user, you may also want to:

- Enable a User for Unified Messaging
- Configure the UM Mailbox Policy Assigned to a UM-Enabled User

1.9.2.2.3 View or Configure the Properties of a UM-Enabled User

View or Configure the Properties of a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can view or configure the Unified Messaging (UM) properties for an existing user who's enabled for Unified Messaging. When you change a user's UM properties, you can control their access to various UM features. For example, you can enable or disable Automatic Speech Recognition (ASR) or associate the user's mailbox with a different UM mailbox policy.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- The existing Exchange user has been enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.
- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to view or configure a UM-enabled user's properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the work pane, select the UM-enabled user that you want to view or configure.
3. In the action pane, click **Properties**.
4. In the UM-enabled user's mailbox properties window, click the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
5. Use the **Unified Messaging Properties** page to view or change the UM properties for an existing UM-enabled user:
   - **UM Mailbox Status** This display-only field shows the status of the user's mailbox. By default, when a user is UM-enabled, the mailbox status is listed as **Not locked out**. However, if the user has input an incorrect Outlook Voice Access PIN multiple times, the status is listed as **Locked Out**.
   - **Unified Messaging Mailbox Policy** This display-only field shows the name of the UM mailbox policy associated with the UM-enabled user. You can specify the UM mailbox policy to be associated with this UM mailbox by clicking the **Browse** button.
   - **UM Extensions** This box displays the extension numbers and the Session Initiation Protocol (SIP) and E.164 addresses after the user has been enabled for Unified Messaging. If you've associated the user with a **Telephone Extension** dial plan, only the extension number configured for the user appears in this box.

     If you've associated the UM-enabled user with a SIP dial plan, an extension number and SIP address are listed. If you've associated the UM-enabled user with an E.164 dial plan, an

extension number and E.164 address are listed.

- **Enable for Automatic Speech Recognition** Select this option to specify whether users can use ASR when they sign in to their mailbox. By default, UM-enabled users can use voice commands when they use Outlook Voice Access to access their mailbox.

  Even if Outlook Voice Access users are speech-enabled, they must still use the keypad to enter their extension number, PIN, and personal options.
- **Allow UM Calls from non-users** Select this option to specify whether to allow incoming calls from unauthenticated callers through an auto attendant to be transferred to the UM-enabled user. By default, this setting is enabled. Enabling this setting allows callers from outside an organization to be transferred to a user inside an organization.

  The user's mailbox can still be accessed using directory searches. However, if an external caller tries to transfer to a user for whom this setting is disabled, the system will say, "I'm sorry, I am unable to transfer the call to this user." The caller is then transferred to the operator configured on the auto attendant.

  This setting doesn't apply to callers who've signed in to their mailbox using Outlook Voice Access and are sending a voice message to a user.
- **Allow faxes to be received** Select this option to specify whether a user is allowed to receive incoming faxes. By default, this setting is enabled. However, it can be disabled if you don't want the user to receive incoming faxes.

  This setting is also configured on dial plans. If you enable this setting for a UM-enabled user, but the dial plan is configured to disable fax receiving, the UM-enabled user is unable to receive faxes.
- **Diverted calls without a caller ID can leave a message** Select this option to specify whether, for diverted calls without a caller ID, the caller is allowed to leave a message. By default, this option is enabled. This enables the UM-enabled user to accept anonymous calls from callers.
- **Allow users to configure personal auto attendants** Select or clear this check box to allow or prevent a user from creating personal auto attendants. If this option is disabled on the UM dial plan or the UM mailbox policy, this feature isn't available to UM-enabled users associated with the UM mailbox policy. This option isn't available to UM-enabled users that have a mailbox on an Exchange UM server. The default setting is enabled.
- **Personal operator extension** Use this field to specify the operator extension number for the user. By default, an extension number isn't configured. The range for the extension number is from 1 through 20 characters. This enables incoming calls for the UM-enabled user to be forwarded to the extension number that you specify in this field.

  You can configure other types of operator extension numbers on dial plans and auto attendants. However, those extensions are generally meant for company-wide receptionists or operators. The personal operator extension setting could be used when an administrative assistant or personal assistant answers incoming calls before they're answered for a particular user.

Use the Shell to configure a UM-enabled user's properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example disables Play on Phone and missed call notifications, but enables text message (SMS) notifications.

```
Set-UMMailbox -Identity tony@contoso.com -UMEnabled $true -UMMailboxPolicy AdminP
```

This example prevents a user from accessing the calendar, but enables access to e-mail when the user is using Outlook Voice Access.

```
Set-UMMailbox -Identity tony@contoso.com -UMEnabled $true -UMMailboxPolicy AdminP
```

This example prevents a user from accessing the calendar and e-mail when the user is using Outlook Voice Access.

```
Set-UMMailbox -Identity tony@contoso.com -TUIAccessToCalendarEnabled $false -TUIA
```

For more information about syntax and parameters, see Set-UMMailbox.

Use the Shell to view a UM-enabled user's properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example displays a list of all the UM-enabled mailboxes in the Active Directory forest in a formatted list.

```
Get-UMMailbox | Format-List
```

This example displays the UM mailbox properties for tonysmith@contoso.com.

```
Get-UMMailbox -Identity tonysmith@contoso.com
```

For more information about syntax and parameters, see Get-UMMailbox.

Other Tasks

After you configure the properties for a UM-enabled user, you may also want to:

- Configuring PIN Security for a UM-Enabled User
- View or Configure the Properties of a UM Mailbox Policy

1.9.2.2.4 View Call Logs for a UM-Enabled User

View Call Logs for a UM-Enabled User

Unified Messaging > Managing Unified Messaging > Managing Unified Messaging Users >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the **User Call Logs** tool, available in Exchange Server 2010 Service Pack 1 (SP1), to display the call statistics for a UM-enabled user you specify. The report that's

generated is displayed in the Exchange Control Panel (ECP). It includes information about calls made by and received by the user, and can help you diagnose and fix issues with a user's voice mail. For more information, see New Unified Messaging Functionality and Voice Mail Features in Exchange 2010 SP1.

After you click the **Select a user** button and specify the user, the following information will be displayed about the user's calls:

- Date and time
- Duration of the call
- Type of call
- The calling number
- The called number
- The UM IP gateway
- Audio quality

You can copy the user's call statistics to the Clipboard and then paste them into another application. You can use the **Audio Quality Details** button to display more specific information about the call. For details on **User Call Logs** tool, see Using Unified Messaging Tools.

Looking for other management tasks related to Unified Messaging (UM) servers? Check out Managing Unified Messaging Servers.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The user whose call logs you want to view has been enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.
- A UM server has been added to a UM dial plan. For detailed steps, see Add a UM Server to a Dial Plan.

Use the EMC to view the call logs for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM call data and summary reports" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Toolbox**, click **User Call Logs**, and then click **Open Tool** from the **Actions** menu.
2. In the **Outlook Web App** window, enter the correct user account (in the format Domain\user name) and password, and then click **Sign in**.
3. If this is your first time signing in to the ECP, select your language and time zone, and then click **OK**.
4. In the **User Call Logs** window, click **Select a user**. In the pop-up window, select the UM-enabled user whose call logs you want to view, and then click **OK**.
5. The call details for the UM-enabled user will be listed in the table that's displayed in the window.

Use the Shell to view the call logs for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM call data and summary reports" entry in the Unified Messaging Permissions topic.

This example displays the UM call data records for the UM-enabled user Tony.

```
Get-UMCallDataRecord -Mailbox tony@contoso.com
```

For more information about syntax and parameters, see Get-UMCallDataRecord.

Other Tasks

After you view the call logs for a UM-enabled user, you may also want to:

- View the Number of Active Calls for a UM Server
- View Call Statistics for a UM Server
- Testing Call Flow with the Exchange 2010 UM Troubleshooting Tool
- Test-UMConnectivity

1.9.2.2.5 Configure the UM Mailbox Policy Assigned to a UM-Enabled User

Configure the UM Mailbox Policy Assigned to a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you enable a user for Microsoft Exchange Server 2010 Unified Messaging (UM), you must select the UM mailbox policy that will be associated with the user's mailbox. However, you can change the UM mailbox policy associated with the user's mailbox after the user has been enabled for Unified Messaging.

You create UM mailbox policies to apply a common set of policies or security settings to a collection of mailboxes of UM-enabled users. You can use UM mailbox policies to apply settings such as the following:

- PIN policies
- Dialing restrictions
- Other general UM mailbox policy properties

Note:

A default UM mailbox policy is created every time you create a UM dial plan. However, you can either delete the default UM mailbox policies or create additional UM mailbox policies based on the needs of your organization.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- The existing Exchange recipient is enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.
- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to change the UM mailbox policy assigned to a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, on the **Mailbox** page, select the UM-enabled user for whom you want to change the UM mailbox policy, and then click **Properties** in the action pane.
3. On the user **Properties** page, on the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
4. On the **Unified Messaging Properties** page, under **Unified Messaging Mailbox Policy**, click **Browse**.
5. On the **Select UM Policy** page, select the UM mailbox policy that you want to use, and then click **OK**.
6. Click **OK** to save your changes.

Use the Shell to change the UM mailbox policy assigned to a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example associates a UM-enabled user named Tony Smith with a UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailbox -Identity tonysmith@contoso.com -UMMailboxPolicy MyUMMailboxPolicy
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you change the UM mailbox policy assigned to a UM-enabled user, you may also want to:

- Configuring PIN Security for a UM-Enabled User
- View or Configure the Properties of a UM-Enabled User

1.9.2.2.6 Enable or Disable Automatic Speech Recognition for a UM-Enabled User

Enable or Disable Automatic Speech Recognition for a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure Automatic Speech Recognition (ASR) for a Microsoft Exchange Server 2010 user who's enabled for Unified Messaging. When ASR is enabled on the mailbox of an Outlook Voice Access user, the user can move through the mailbox menus using voice commands. If ASR is disabled, the user must use dual tone multi-frequency (DTMF), also known as touchtone, inputs to move through the menus.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- The existing Exchange recipient is enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.
- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to configure ASR for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the user's mailbox that you want to view.
3. In the action pane, click **Properties**.
4. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
5. On the **Unified Messaging Properties** page, select **Enable for Automatic Speech Recognition**.
6. Click **OK** to accept your changes.

Use the Shell to configure ASR for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example enables Automatic Speech Recognition (ASR) for a UM-enabled user named Tony.

```
Set-UMMailbox -Identity tony@contoso.com -AutomaticSpeechRecognitionEnabled $true
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you configure ASR for a UM-enabled user, you may also want to:

- Configure a UM-Enabled User's TUI Settings
- View or Configure the Properties of a UM-Enabled User

1.9.2.2.7 Enable or Disable Calls from Users Who Are Not UM-Enabled for a UM-Enabled User

Enable or Disable Calls from Users Who Are Not UM-Enabled for a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable calls from users who aren't enabled for Unified Messaging (UM). By default, Unified Messaging allows incoming calls from unauthenticated callers through an auto attendant to be transferred to UM-enabled users. With this option enabled, users from outside an organization can transfer calls to UM-enabled users.

If this setting has been disabled for a UM-enabled user, the user's mailbox can still be located using a directory search. However, if an external caller tries to transfer to the user, the system says, "I'm sorry, I am unable to transfer the call to this user." The caller is then transferred to the operator, if an operator has been configured on the auto attendant. If no operator has been configured on the auto attendant, the call is transferred to a dial plan operator, if one has been configured. If no operator extension has been configured on the speech-enabled auto attendant, the dual tone multi-frequency (DTMF) fallback auto attendant, or the dial plan, the system responds by saying, "Sorry. Neither the operator or the touchtone service are available."

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The user's mailbox has been UM-enabled. For detailed steps, see Enable a User for Unified Messaging.

Use the EMC to enable or disable calls from users who aren't UM-enabled to a user who is UM-enabled

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the user's mailbox.
3. In the action pane, click **Properties**.
4. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
5. On the **Unified Messaging Properties** page, do one of the following:
   - To enable calls from users who aren't UM-enabled, select the check box next to **Allow UM calls from non-users**.

- To disable calls from users who aren't UM-enabled, clear the check box next to **Allow UM calls from non-users**.

6. Click **OK** to accept your changes.

Use the Shell to enable or disable calls from users who aren't UM-enabled to a user who is UM-enabled

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example prevents Tony Smith from receiving voice mails from callers who aren't UM-enabled.

```
Set UMMailbox -Identity tony@contoso.com -AllowUMCallsFromNonUsers None
```

This example allows Tony Smith to receive voice mails from callers who aren't UM-enabled.

```
Set UMMailbox -Identity tony@contoso.com -AllowUMCallsFromNonUsers SearchEnabled
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you enable or disable calls from users who aren't UM-enabled to a user who is UM-enabled, you may also want to:

- Configure an Operator Extension on a UM Auto Attendant
- Configure an Operator Extension on a UM Dial Plan

1.9.2.2.8 Enable a UM-Enabled User to Receive Faxes

Enable a UM-Enabled User to Receive Faxes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable a Unified Messaging (UM) user to receive faxes. By default, when you enable a user for Unified Messaging, they will be able to receive faxes. Faxing can be enabled or disabled on UM dial plans, UM mailbox policies, or the UM-enabled user's mailbox. By default, although the user's mailbox allows incoming faxes, you must first enable inbound faxing on the UM mailbox policy that's associated with the UM-enabled user and enter the fax partner's URI.

For a specific user to be able to receive fax messages in their Microsoft Exchange 2010 mailbox, each Unified Messaging server that's associated with the dial plan that the user is associated with must be configured to accept incoming fax calls. In addition, the UM dial plan must also be configured to allow faxes to be sent to UM-enabled users.

Looking for other management tasks related to UM users? Check out Managing Unified

Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable a UM user to receive faxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the user mailbox that you want to modify.
3. In the action pane, click **Properties**.
4. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
5. On the **Unified Messaging Properties** page, select the check box next to **Allow the user to receive faxes**.
6. Click **OK** to save your changes.

Use the Shell to enable a UM user to receive faxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example enables Tony Smith to receive incoming faxes.

```
Set-UMMailbox -Identity tonysmith@contoso.com -FaxEnabled $true
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you enable a UM user to receive faxes, you may also want to:

- Enable or Disable Inbound Faxing on a UM Mailbox Policy
- Enable UM-Enabled Users to Receive Faxes on a UM Dial Plan
- Add an Extension Number for a UM-Enabled User

1.9.2.2.9 Prevent a UM-Enabled User from Receiving Faxes

Prevent a UM-Enabled User from Receiving Faxes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can prevent a Microsoft Exchange Server 2010 Unified Messaging (UM) user from receiving faxes. By default, when you enable a user for Unified Messaging, the user will receive faxes. However, you can prevent a user from being able to receive faxes after they've been enabled for Unified Messaging. You can also prevent multiple users from receiving faxes by disabling delivery of faxes to users who are associated with the UM dial plan.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- The existing Exchange recipient is enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.
- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The UM-enabled user is enabled for faxing. For detailed steps, see Enable a UM-Enabled User to Receive Faxes.

Use the EMC to prevent UM-enabled users from receiving faxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the UM-enabled user's mailbox that you want to modify.
3. In the action pane, click **Properties**.
4. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
5. On the **Unified Messaging Properties** page, clear the check box next to **Allow the user to receive faxes**.
6. Click **OK** to save your changes.

Use the Shell to prevent UM-enabled users from receiving faxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example prevents a UM-enabled user named Tony from receiving fax messages in his mailbox.

```
Set-UMMailbox -Identity tony@contoso.com -FaxEnabled $false
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you prevent UM-enabled users from receiving faxes, you may also want to:

- Prevent UM-Enabled Users from Receiving Faxes on a UM Dial Plan.
- Add an Extension Number for a UM-Enabled User

1.9.2.2.10 Allow or Prevent Calls Without a Caller ID to Leave a Voice Message

Allow or Prevent Calls Without a Caller ID to Leave a Voice Message

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can allow or prevent UM-enabled users to receive voice messages from anonymous callers or to prevent them from doing so. By default, when users are enabled for Unified Messaging (UM), they can receive calls that are anonymous and don't contain caller ID information.

In most cases, calls received by a Unified Messaging server contain a caller ID that can be used to determine the source of the incoming call. However, incoming calls may not include caller ID information for the following reasons:

- Your organization's telephony equipment is configured not to include caller ID information.
- The incoming call is from a mobile or external telephone.
- Callers have disabled caller ID on their telephone.

Because the **Allow diverted calls without a caller ID to leave a message** option is enabled by default, a UM-enabled user can receive a voice message even if caller ID information isn't included. If the **Allow diverted calls without a caller ID to leave a message** option is disabled, and the UM-enabled user receives a call that doesn't include a caller ID, the call will be identified as anonymous, and the UM-enabled user won't receive a voice message.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable voice messages from anonymous callers for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the user's mailbox.
3. In the action pane, click **Properties**.
4. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
5. On the **Unified Messaging Properties** page, do one of the following:
   - To enable voice messages from anonymous callers, select the **Allow diverted calls without a caller ID to leave a message** check box.
   - To disable voice messages from anonymous callers, clear the **Allow diverted calls without a caller ID to leave a message** check box.
6. Click **OK** to accept your changes.

Use the Shell to enable or disable voice messages from anonymous callers for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example allows UM-enabled users to receive voice mail from calls that don't contain caller ID information.

```
Set-UMMailbox -Identity tonysmith@contoso.com -AnonymousCallersCanLeaveMessages $
```

This example prevents UM-enabled users from receiving voice mail from calls that don't contain caller ID information.

```
Set-UMMailbox -Identity tonysmith@contoso.com -AnonymousCallersCanLeaveMessages $
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you enable or disable voice messages from anonymous callers for a UM-enabled user, you may also want to:

- Enable or Disable Call Transfers to Users on a UM Dial Plan
- Configure the Scope of Users Who Callers Can Contact on a UM Dial Plan

1.9.2.2.11 Enable or Disable Call Answering Rules for a UM-Enabled User

Enable or Disable Call Answering Rules for a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify whether you want individual users to be able to create and manage their

own call answering rules by configuring their mailbox properties. You can also allow or prevent them from creating call answering rules by allowing or preventing Call Answering Rules on a Unified Messaging (UM) dial plan or UM mailbox policy that's associated with a user.

You can enable or disable call answering rules for multiple UM-enabled users by configuring Call Answering Rules on a UM dial plan or UM mailbox policy.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The user's mailbox has been UM-enabled. For detailed steps, see Enable a User for Unified Messaging.

Use the EMC to enable or disable call answering rules for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the user's mailbox that you want to view.
3. In the action pane, click **Properties**.
4. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
5. On the **Unified Messaging Properties** page, select or clear the check box next to **Allow users to configure call answering rules**.
6. Click **OK** to accept your changes.

Use the Shell to enable or disable call answering rules for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example disables Call Answering Rules for the user tony@contoso.com.

```
Set-UMMailbox -Identity tony@contoso.com -CallAnsweringRulesEnabled $false
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you enable or disable call answering rules for a UM-enabled user, you may also want to:

- Allow or Prevent Call Answering Rules on a UM Dial Plan
- Enable or Disable Call Answering Rules on a UM Mailbox Policy

1.9.2.2.12 Enable or Disable a Personal Operator for a UM-Enabled User

Enable or Disable a Personal Operator for a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The personal operator extension setting on a mailbox that's enabled for a Unified Messaging (UM) user can be used when an administrative assistant or personal assistant will answer incoming calls for a specific user instead of a voice mail message being generated for the user. For example, when a UM-enabled user will be out of the office and wants callers to have the option to talk to a human operator or leave a voice message. By default, an extension number isn't defined.

You can enter an internal or external telephone number that has from 1 through 20 digits in the **Personal operator extension** field available on the UM-enabled user's mailbox properties. If you use an external telephone number, you must verify that you've correctly configured the appropriate outdialing rule groups and entries to enable this functionality.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- The existing Exchange recipient is enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.
- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The extension number assigned to the UM-enabled user is valid according to the UM dial plan defined.

Use the EMC to configure a personal operator for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the user's mailbox that you want to view.
3. In the action pane, click **Properties**.
4. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
5. On the **Unified Messaging Properties** page, in the **Personal operator extension** field, enter the extension number for the personal operator that will be used for this user.
6. Click **OK** to accept your changes.

Important:

After you accept the changes that you made using this procedure, you must set the AllowExtensions parameter to True using the **Set-UMDialPlan** cmdlet. For the correct syntax, see the following procedure. You can't set the AllowExtensions parameter to True using the EMC.

Use the Shell to configure a personal operator for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example allows extensions on a UM dial plan named MyUMDialPlan and enables a personal operator extension 12345 for a UM-enabled user named Tony Smith.

```
Set-UMMailbox -identity tonysmith@contoso.com -OperatorNumber 12345
Set-UMDialPlan -identity MyUMDialPlan -AllowExtensions $true
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you configure a personal operator for a UM-enabled user, you may also want to:

- Create a Dialing Rule Entry on a UM Dial Plan
- Configure Dialing Rule Groups on a UM Dial Plan

1.9.2.2.13 Add an Extension Number for a UM-Enabled User

Add an Extension Number for a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you enable a user for Unified Messaging (UM), you must define at least one extension number that Unified Messaging will use when voice mail is submitted to the user's Microsoft Exchange Server 2010 mailbox. After you enable the user for Unified Messaging, you can add extension numbers to the user's mailbox by configuring the Exchange Unified Messaging proxy address (EUM proxy address) on the user's mailbox.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- The existing Exchange recipient is enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.
- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM

Mailbox Policy.

- The extension number that will be assigned to the UM-enabled user is valid according to the UM dial plan associated with the UM-enabled user.

Use the EMC to add an extension number for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox for which you want to add an extension number.
3. In the action pane, under the mailbox name, click **Properties**.
4. In **<Mailbox User> Properties**, click the **E-Mail Addresses** tab.
5. Click the drop-down arrow located next to **Add**, and then click **EUM Address**. In **UM Address (Extension)**, in the **Address/Extension** box, type the extension number.
6. In the **Dial plan (Phone context)** box, click **Browse** to locate the dial plan for the user.
7. Click **Apply**, and then click **OK**.

Use the Shell to add an extension number for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example adds an extension number for Tony Smith, a UM-enabled user.

```
$mbx=Get-Mailbox tony.smith
$mbx.EmailAddresses +="eum:22222;phone-context=MyDialPlan.contoso.com"
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

For more information about syntax and parameters, see Set-Mailbox or Get-Mailbox.

Other Tasks

After you add an extension number, you may also want to:

- Modify an Extension Number for a UM-Enabled User
- Remove an Extension Number for a UM-Enabled User

1.9.2.2.14 Remove an Extension Number for a UM-Enabled User

Remove an Extension Number for a UM-Enabled User

Unified Messaging > Managing Unified Messaging > Managing Unified Messaging Users >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you enable a user for Unified Messaging (UM), you must define at least one extension number that Unified Messaging will use when voice mail is submitted to the user's Microsoft Exchange Server 2010 mailbox. After you enable the user for Unified Messaging, you can remove extension numbers from the user's mailbox by configuring the Exchange Unified Messaging proxy address (EUM proxy address) on the user's mailbox.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The user's mailbox has been UM-enabled. For detailed steps, see Enable a User for Unified Messaging.

Use the EMC to remove an extension number for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox for which you want to remove an extension number.
3. In the action pane, under the mailbox name, click **Properties**.
4. In **<Mailbox User> Properties**, click the **E-Mail Addresses** tab.
5. To remove an existing EUM proxy address, select the EUM proxy address, and then click  .
6. Click **Apply**, and then click **OK**.

Use the Shell to remove an extension number for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example removes the extension number 12345 from the mailbox of Tony Smith, a UM-enabled user.

```
$mbx = Get-Mailbox tony.smith
$mbx.EmailAddresses.Item(1) -="eum:12345;phone-context=MyDialPlan.contoso.com"
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

For more information about syntax and parameters, see Set-Mailbox or Get-Mailbox.

Other Tasks

After you remove the extension number, you may also want to:

- Add an Extension Number for a UM-Enabled User
- Modify an Extension Number for a UM-Enabled User

1.9.2.2.15 Modify an Extension Number for a UM-Enabled User

Modify an Extension Number for a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can modify an extension number that was assigned to a user when you enabled the user for Unified Messaging (UM). A single extension number is required when you enable a user for Unified Messaging. However, if you need to, you can change this extension number.

Looking for other management tasks related to Unified Messaging users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The user's mailbox has been UM-enabled. For detailed steps, see Enable a User for Unified Messaging.

Use the EMC to modify an extension number for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox for which you want to add a new extension number.
3. In the action pane, under the mailbox name, click **Properties**.
4. In **<Mailbox User> Properties**, click the **E-Mail Addresses** tab.
5. Select the appropriate Exchange Unified Messaging proxy address (**EUM** address), and then click **Edit**. In **UM Address (Extension)**, in the **Address/ Extension** box, type the new extension number.
6. In the **Dial plan (Phone context)** box, click **Browse** to locate a new dial plan for the user.
7. Click **Apply**, and then click **OK**.

Use the Shell to modify an extension number for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example changes the extension number to 22222 for Tony Smith, a UM-enabled user.

Note:
You must determine the position of the EUM address that you want to modify. To determine the position of the EUM address, use the **$mbx.EmailAddresses** command. The first proxy address in the list will be 0.

```
$mbx=Get-Mailbox tony.smith
$mbx.EmailAddresses.Item(0)="eum:22222;phone-context=MyDialPlan.contoso.com"
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

For more information about syntax and parameters, see Set-Mailbox or Get-Mailbox.

Other Tasks

After you modify the extension, you may also want to:

- Add an Extension Number for a UM-Enabled User
- Remove an Extension Number for a UM-Enabled User

1.9.2.2.16 Modify a SIP Address for a UM-Enabled User

Modify a SIP Address for a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you enable a user for Unified Messaging (UM), you must define at least one extension number that will be used by Unified Messaging when voice mail is submitted to the user's Microsoft Exchange Server 2010 mailbox. After you enable the user for Unified Messaging, you can modify the Session Initiation Protocol (SIP) address by configuring the Exchange Unified Messaging proxy address (EUM proxy address) on the user's mailbox.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The user's mailbox has been UM-enabled. For detailed steps, see Enable a User for Unified Messaging.

Use the EMC to modify a SIP address for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions

topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox for which you want to modify an e-mail address.
3. In the action pane, under the mailbox name, click **Properties**.
4. In **<Mailbox User> Properties**, click the **E-Mail Addresses** tab.
5. Select the appropriate **EUM** address, and then click **Edit**. In **UM Address (Extension)**, in the **Address/Extension** box, type the new SIP address.
6. In the **Dial plan (Phone context)** box, click **Browse** to locate a new dial plan for the user.
7. Click **Apply**, and then click **OK**.

Use the Shell to modify a SIP address for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example changes a SIP address for Tony Smith, a UM-enabled user.

Note:

You must determine the position of the EUM address that you want to modify. To determine the position of the EUM address, use the **$mbx.EmailAddresses** command. The first proxy address in the list will be 0.

```
$mbx=Get-Mailbox tony.smith
$mbx.EmailAddresses.Item(1)="eum:tsmith;phone-context=MyDialPlan.contoso.com"
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

For more information about syntax and parameters, see Set-Mailbox or Get-Mailbox.

Other Tasks

After you modify a SIP address, you may also want to:

- Modify an E.164 Address for a UM-Enabled User
- Modify an Extension Number for a UM-Enabled User

1.9.2.2.17 Modify an E.164 Address for a UM-Enabled User

Modify an E.164 Address for a UM-Enabled User

Unified Messaging > Managing Unified Messaging > Managing Unified Messaging Users >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you enable a user for Unified Messaging (UM), you must define at least one extension number that will be used by Unified Messaging when voice mail is submitted to the user's Microsoft Exchange Server 2010 mailbox. However, you have the option to modify an E.164 address for a user if the user is associated with an E.164 dial plan. After you enable the user for Unified Messaging, you can modify E.164 addresses for the user's mailbox by configuring the Exchange Unified Messaging proxy address (EUM proxy

address) on the user's mailbox.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The user's mailbox has been UM-enabled. For detailed steps, see Enable a User for Unified Messaging.

Use the EMC to modify an E.164 address for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox for which you want to modify an E.164 address.
3. In the action pane, under the mailbox name, click **Properties**.
4. In **<Mailbox User> Properties**, click the **E-Mail Addresses** tab.
5. Select the appropriate **EUM** address, and then click **Edit**. In **UM Address (Extension)**, in the **Address/Extension** box, type the new E.164 address.
6. In the **Dial plan (Phone context)** box, click **Browse** to locate the dial plan for the user.
7. Click **Apply**, and then click **OK**.

Use the Shell to modify an E.164 address for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example modifies an E.164 address for Tony Smith, a UM-enabled user.

Note:

You must determine the position of the EUM address that you want to modify. To determine the position of the EUM proxy address, use the **$mbx.EmailAddresses** command. The first proxy address in the list will be 0.

```
$mbx=Get-Mailbox tony.smith
$mbx.EmailAddresses.Item(1)="eum:+14255550123;phone-context=MyDialPlan.contoso.co
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

For more information about syntax and parameters, see Set-Mailbox or Get-Mailbox.

Other Tasks

After you modify the E.164 address, you may also want to:

- Modify a SIP Address for a UM-Enabled User

- Modify an Extension Number for a UM-Enabled User

1.9.2.2.18 Configure a UM-Enabled User's TUI Settings

Configure a UM-Enabled User's TUI Settings

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Telephone user interface (TUI) settings are used when the user accesses the Unified Messaging (UM) system by using Outlook Voice Access. When you modify the UM-enabled user's TUI configuration settings, you modify properties and their values on the UM-enabled user's mailbox.

The following is a list of the TUI settings that you can modify for a UM-enabled user:

- Allow subscriber access
- Allow TUI access to the calendar
- Allow TUI access to e-mail
- Allow Automatic Speech Recognition

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- The existing Exchange recipient is enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.
- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to modify a UM-enabled user's TUI settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, click the user's mailbox.
3. In the action pane, click **Properties**.
4. In the mailbox properties, click the **Mailbox Features** tab.
5. On the **Mailbox Features** tab, select **Unified Messaging**, and then click **Properties**.
6. On the **Unified Messaging Properties** page, select the appropriate option, and then click **OK**.

Important:

There are multiple TUI settings that can be modified only by using the Shell.

Use the Shell to modify a UM-enabled user's TUI settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example enables calendar and e-mail access using the TUI for a UM-enabled user named Tony Smith.

```
Set-UMMailbox -Identity tony@contoso.com TUIAccessToCal True -TUIAccessToEmail Tr
```

Note:

TUI settings for users are also available on UM dial plans. Modifying TUI settings on a UM dial plan affects all users who belong to the UM dial plan. For more information about how to modify TUI settings on a UM dial plan, see Configure TUI Settings on a UM Mailbox Policy.

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you modify a UM-enabled user's TUI settings, you may also want to Configure TUI Settings on a UM Mailbox Policy.

1.9.2.2.19 Configuring PIN Security for a UM-Enabled User

Configuring PIN Security for a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

When a subscriber or a Microsoft Exchange Server 2010 Unified Messaging (UM) user uses a telephone to connect to a Unified Messaging server, the user uses Outlook Voice Access to navigate the Unified Messaging menu system. However, before users can access the Unified Messaging system, the system prompts them to input their PIN. As the administrator, you can configure PIN settings and requirements and perform PIN management tasks. After a user has been enabled for Unified Messaging and a PIN has been generated or created, a hash that's a mathematical computation of the user's PIN is stored in the user's mailbox. The checksum for the PIN is stored in Active Directory in an attribute called **ExUMPINChecksum**.

Note:

Subscribers must use touchtone or dual tone multi-frequency (DTMF) inputs to input their PIN to access their UM-enabled mailbox. Speech recognition is not enabled for PIN input.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Contents

PIN Requirements

Managing Unified Messaging PINs

PIN Overview

A PIN is a numeric string that's used in certain systems, including Unified Messaging systems, so that a user can be authenticated and gain access. A PIN is a passcode that users enter on the telephone to access their Exchange Server mailbox. The strength of the PIN depends on its length, how well it's protected, and how difficult it's to guess.

PINs are most frequently used for automatic teller machines (ATMs). However, they are also used for Unified Messaging systems instead of alphanumeric passwords. In Exchange 2010 Unified Messaging, the PIN is entered over an analog, digital, or mobile telephone and is used to gain access to the user's mailbox that includes e-mail, voice mail, and calendaring information.

In Exchange 2010 Unified Messaging, PIN policies are defined and configured on a UM mailbox policy. Multiple UM mailbox policies can be created depending on your requirements. When you enable a user for Exchange 2010 Unified Messaging, you associate or link the user to an existing UM mailbox policy. The UM PIN policies that are configured on the UM mailbox policy should be based on the security requirements of your organization.

PIN Requirements

The following are several PIN configuration settings that you can set on a UM mailbox policy in Exchange 2010.

Minimum PIN Length

The Minimum PIN Length setting specifies the minimum number of digits that a mailbox PIN can be. The range is 4 through 24, and the default is 6. If you enter 0, users aren't required to enter a PIN.

Important:

Configuring this setting with zero isn't a recommended practice. By configuring this setting to zero, you greatly decrease the level of security for your network.

If you change the minimum password length to a higher value, existing subscribers are prompted to enter a new PIN that contains the new minimum number of digits before they can continue.

Note:

Increasing this number creates a more secure UM environment. However, setting it too high can result in users forgetting their PIN.

PIN Lifetime

The PIN Lifetime setting controls the time interval, in days, from the date subscribers last changed their PIN to the date they'll be forced to change their PIN again. The range is 0 through 999, and the default is 60 days. If 0 is entered, the PIN won't expire.

Note:

Unified Messaging won't notify users when their PIN is about to expire.

Logon Failures Before PIN Reset

The Logon Failures Before PIN Reset setting specifies the number of sequential unsuccessful logon attempts before the mailbox PIN is automatically reset. To disable this feature, set this setting to unlimited. Otherwise, it must be set to a number lower than

the Maximum Logon Attempts setting. The range is 1 through 998, and the default is 5.

Note:
To increase security for UM-enabled users, enter a number that's less than 5.

Maximum Logon Attempts

The Maximum Logon Attempts setting specifies how many PIN entry errors in successive calls subscribers can make before they're locked out of their mailbox. By default, after 5 attempts are made, the PIN is automatically reset. The range is 1 through 999, and the default is 15.

Note:
To increase security, decrease the number of failed attempts. But remember that decreasing it to a number much lower than the default may result in users being locked out unnecessarily. Unified Messaging will generate warning events that can be viewed using Event Viewer if PIN authentication fails for a UM-enabled user or the user is unsuccessful in trying to log on to the system.

Allow Common Patterns

The Allow Common Patterns setting is used to either enable or disable the use of common number patterns used in creating a PIN. By default, this setting is disabled and won't allow users to input the following number patterns in the following list:

- **Sequential numbers** PIN values that consist completely of consecutive numbers. Examples of sequential numbers for a PIN are 1234 and 65432.
- **Repeated numbers** PIN values that consist of repeated numbers. Examples of repeated numbers are 11111 and 22222.
- **Suffix of mailbox extension** PIN values that consist of the suffix of your mailbox extension. If your mailbox extension is 36697, your PIN cannot be 6697.

PIN History Count

The PIN History Count setting configures the number of different PINs a user must use before any PINs that were previously used can be reused. The range is 1 through 20, and the default is 5.

Managing Unified Messaging PINs

When planning for UM PINs, you must make sure that you choose the appropriate levels of security for your organization. You must carefully consider the UM PIN requirements and how your PIN security settings meet or exceed your organization's security policy.

Important:
It's a security best practice to implement strong PIN requirements for Unified Messaging users. This can be enforced by creating Unified Messaging PIN policies that require six or more digits for PINs and increases the level of security for your network.

After you set the PIN requirements that meet the security requirements for your organization, you must create and configure a UM mailbox policy to enforce your organizational PIN requirements. For more information about how to create and manage a UM mailbox policy, see Managing UM Mailbox Policies.

Note:
After you create the UM mailbox policy, you must associate the UM-enabled user or users with the appropriate UM mailbox policy. You can perform this task by using the **Enable-UMMailbox** Exchange Management Shell command. For more information about the Exchange Management Shell command, see the Enable-UMMailbox reference topic.

There are situations in which UM users forget their PIN or are locked out of UM access to their mailbox. In either case, it may be necessary for you to reset a UM-enabled user's

PIN. For more information about how to reset a user's PIN, see Reset a Unified Messaging PIN for a UM-Enabled User.

1.9.2.2.19.1 Set PIN Policies for UM-Enabled Users

Set PIN Policies for UM-Enabled Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can set PIN policies on a Unified Messaging (UM) mailbox policy. UM mailbox policies can be configured to increase the level of security for UM-enabled users by requiring users to comply with the predefined PIN policies for your organization.

To set PIN policies for UM users, you can either create a new UM mailbox policy or modify an existing UM mailbox policy. After a new UM mailbox policy is created, you can then configure the UM mailbox policy by configuring the following PIN settings:

- `MinPasswordLength`
- `PINLifetime`
- `LogonFailuresBeforePINReset`
- `MaxLogonAttempts`
- `AllowCommonPatterns`
- `PINHistoryCount`

It's a security best practice to implement strong PIN requirements for UM users. This can be enforced by creating UM PIN policies that require 6 or more digits for PINs and increase the level of security for your network.

When you change the PIN policy, the new PIN setting is applied to users who are currently associated with the UM mailbox policy. For example, if you modify the UM mailbox policy and change the minimum PIN length from 7 to 10 digits, the next time users log on they'll be forced to change their PIN to comply with the changed PIN requirement.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to set PIN policies for UM users

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic

1. In the console tree, navigate to **Organization Configuration** > **Unified**

Messaging.
2. In the work pane, click the **UM Mailbox Policies** tab.
3. Click the UM mailbox policy that you want to change. This is the UM mailbox policy that's associated to the UM-enabled user.
4. In the action pane, click **Properties**.
5. In the UM mailbox policy **Properties** window, click the **PIN Policies** tab.
6. On the **PIN Policies** tab, configure the PIN settings for the UM mailbox policy, and then click **OK** to accept your changes.

Use the Shell to set PIN policies for UM users

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic

This example sets the PIN settings for users associated with the UM mailbox policy `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 8 -M
```

For information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you set PIN policies for UM users, you may also want to:

- Include Text with the E-Mail Message Sent When a PIN Is Reset
- Reset a Unified Messaging PIN for a UM-Enabled User

1.9.2.2.19.2 Retrieve PIN Information for a UM-Enabled User

Retrieve PIN Information for a UM-Enabled User

Managing Unified Messaging > Managing Unified Messaging Users > Configuring PIN Security for a UM-Enabled User >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can retrieve PIN information for a user who is enabled for Microsoft Exchange Server 2010 Unified Messaging (UM). After a user has been enabled for Unified Messaging and a PIN is generated or created, the PIN is stored in the user's mailbox as a salted hash, and the checksum for the PIN is stored in an attribute called **ExUMPINChecksum** in the Active Directory directory service.

When you retrieve PIN information for a UM-enabled user, the information returned to you is calculated by using the PIN data stored in an encrypted format in the user's mailbox. This lets you view information from the user's mailbox and also indicates whether the user has been locked out of the mailbox.

Important:

When a UM-enabled user enters a PIN, the PIN data is passed in a format that isn't encrypted from an IP gateway over the IP-based network to Unified Messaging servers.

To increase the security for a user's PIN, use Internet Protocol security (IPsec) and Transport Layer Security (TLS)/Secure Realtime Transport Protocol (SRTP) to encrypt the PIN data.
After the PIN for a UM-enabled user is received by a Unified Messaging server and is passed from the Session Initiation Protocol (SIP)/RTP transport stack to the UM code, the PIN is temporarily held in a memory buffer in a form that isn't encrypted. Although this poses a small security risk, there's still the potential for an attacker to view the PIN while it isn't encrypted in the memory buffers on the Unified Messaging server.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The user's mailbox has been UM-enabled. For detailed steps, see Enable a User for Unified Messaging.

Use the EMC to retrieve PIN information for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the result pane, select the user mailbox that you want to view.
3. In the action pane, click **Properties**.
4. On the **Mailbox Features** tab, click **Unified Messaging**, and then click **Properties**.
5. In the **UM Mailbox Status** section, view the **Lockout status** for the user.

Use the Shell to retrieve PIN information for a UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example displays the user ID, whether a PIN is expired, the UM mailbox is locked out and whether Tony is a first time user.

```
Get-UMMailboxPIN -identity tony@contoso.com
```

For more information about syntax and parameters, see Get-UMMailboxPIN.

Other Tasks

After you retrieve PIN information for a UM-enabled user, you may also want to:

- Configuring PIN Security for a UM-Enabled User
- Reset a Unified Messaging PIN for a UM-Enabled User
- Managing UM Mailbox Policies

1.9.2.2.19.3 Reset a Unified Messaging PIN for a UM-Enabled User

Reset a Unified Messaging PIN for a UM-Enabled User

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When a UM-enabled user is locked out of their mailbox because they tried to sign in using an incorrect PIN multiple times or they forgot their PIN, you can use one of the following procedures to reset the user's PIN. When you reset a user's Outlook Voice Access PIN, you can configure Unified Messaging (UM) to automatically generate a PIN or you can manually specify the PIN. The new PIN is e-mailed to the user. If you prefer, you can specify additional PIN options when resetting the user's PIN. Users can also reset their UM PIN using Outlook or Outlook Web App.

Note:

To access their UM-enabled mailbox, subscribers need to use touchtone, also known as dual tone multi-frequency (DTMF), inputs. Speech recognition isn't available for PIN input.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Use the EMC to reset a Unified Messaging PIN

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the UM-enabled user's mailbox that you want to reset their PIN for.
3. In the action pane, under the mailbox name, click **Reset Unified Messaging PIN**.
4. Use the **Reset Unified Messaging PIN** windows to reset the UM-enabled user's PIN:
   - **Automatically generate PIN to access Outlook Voice Access** Use this option to automatically generate the PIN that's used by the user to gain access to their mailbox using Outlook Voice Access. By default, this setting is enabled.

     The automatically generated PIN will be sent in an e-mail message to the user's mailbox. After they receive the PIN and sign in to their mailbox, they'll be prompted to change the PIN to a PIN that's more familiar to them.
     Outlook Web App for Microsoft Exchange Server 2010 and Office Outlook 2007 let the user reset their PIN. The PIN is automatically generated based on the PIN policies that are configured on the UM mailbox policy that is associated with the user's mailbox. We recommend that you automatically generate PINs for Outlook Voice Access users.

- **Manually specify PIN** Use this option to manually specify a PIN for an Outlook Voice Access user. By default, this setting is disabled.
  If you specify a PIN for a user, the PIN will be sent in an e-mail message to the user's mailbox. After they receive the PIN and sign in to their mailbox, they can change the PIN by configuring personal options in Outlook Voice Access. However, in Outlook Web App for Exchange 2010 and Outlook 2007, there is no option to manually specify a PIN.
- **Require user to reset PIN at first logon** Use this option to require the user to reset their PIN when they first sign in to Outlook Web App. By default, this option is disabled.
  If you select the option to automatically generate a PIN for a user, you can enable this option to require users to change their PIN when they first sign in to Outlook Voice Access. This helps protect the user's PIN.

5. Click **Apply**, and then click **OK**.

Use the Shell to reset a Unified Messaging PIN

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example resets the voice mail PIN for Tony Smith to 1985848. However, this PIN must be changed when the user first signs in to Outlook Voice Access.

```
Set-UMMailboxPIN -Identity tonysmith@contoso.com -PIN 1985848 -PinExpired $true
```

Other Tasks

After you reset a Unified Messaging PIN, you may also want to:

- Retrieve PIN Information for a UM-Enabled User
- Set PIN Policies for UM-Enabled Users
- Configuring PIN Security for a UM-Enabled User

1.9.2.2.20 Change the UM Dial Plan for a UM-Enabled User

Change the UM Dial Plan for a UM-Enabled User

Unified Messaging > Managing Unified Messaging > Managing Unified Messaging Users >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

There are specific scenarios in which you may need to move a user who is enabled for Unified Messaging (UM) to a different UM dial plan or to change the dial plan that's associated with the UM-enabled user. For example, if you want to move a UM-enabled user from a Telephone Extension to a SIP URI dial plan or if you have a Microsoft Exchange Server 2010 organization that's integrated with Microsoft Office Communications Server 2007 but the Mediation Server is down, you'll have to disable the user for Unified Messaging and then enable the user for Unified Messaging on the new UM dial plan. This is because different dial-plans may have different settings and

requirements, such as different extension length, different URI type. For example, a SIP URI dial plan requires a SIP Resource Identifier to be assigned to each UM-enabled mailbox, but Telephone Extension dial plans don't. Also, each UM mailbox contains references to both the UM dial plan and UM mailbox policy. The UM mailbox policy, in turn, also contains references to the UM dial plan. If you change the primary proxy address for a UM-enabled user to point to a different dial plan, the UM mailbox is now in an inconsistent state.

Important:

Although it's possible to add a secondary EUM proxy address with a secondary dial plan for a UM-enabled user, the user can receive new voice mails on the secondary dial plan. Adding a secondary EUM proxy address is designed to support call answering scenarios only when a user has two phones, for example, a Unified Communications and a legacy PBX phone, but wants all their voice mails to be sent to the same Exchange 2010 mailbox. However, adding a secondary EUM proxy address for a UM-enabled user when you're changing the primary UM dial plan that's associated with a UM-enabled user isn't a supported configuration.

Looking for other management tasks related to UM users? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The existing Exchange recipient is enabled for Unified Messaging. For detailed steps, see Enable a User for Unified Messaging.

Change the UM Dial Plan for a UM-enabled User

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

1. Create the new dial plan that be used. For detailed steps, see Create a UM Dial Plan.

   Important:

   If you're migrating UM-enabled users without Office Communications Server 2007to an integrated Communications Server 2007 environment, you must first create a SIP URI dial plan.

2. Disable the UM-enabled user for Unified Messaging. For detailed steps, see Disable Unified Messaging for a User.
3. Enable the user for Unified Messaging on the new dial plan. For detailed steps, see Enable a User for Unified Messaging.

Important:

If you are moving users to an environment with Office Communications Server 2007, you must also include a SIP Resource Identifier for the user when you enable the user for UM. You must also select the UM mailbox policy that's associated with a SIP dial plan.

Other Tasks

After you change the UM dial plan for a UM-enabled user, you may also want to:

- View or Configure the Properties of a UM-Enabled User

- Modify a SIP Address for a UM-Enabled User

1.9.2.2.21 Disable Selected Outlook Voice Access Features for UM-Enabled Users

Disable Selected Outlook Voice Access Features for UM-Enabled Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Outlook Voice Access contains two interfaces: the telephone user interface (TUI) and the voice user interface (VUI). By default, when users dial in to Outlook Voice Access, they can access their calendar, e-mail, and personal Contacts, and search the directory. You can use the Shell to prevent users from accessing one or more of these features when they use Outlook Voice Access to access their mailbox in Microsoft Exchange Server 2010. When you modify Outlook Voice Access features on a Unified Messaging (UM) mailbox policy, your changes affect all users who are associated with the UM mailbox policy.

You can disable users' access to the following Outlook Voice Access features on a UM mailbox policy:

- Calendar
- Directory
- E-mail
- Personal contacts

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

You can also use the Shell to disable Outlook Voice Access features on the mailbox of a single UM-enabled user. When you do this, the features will be disabled only for that user. Although you can't disable all the Outlook Voice Access features that are found on a UM mailbox policy for a single user, you can disable access to their calendar and to their e-mail.

Looking for other management tasks related to UM mailboxes? Check out Managing Unified Messaging Users.

Note:
You can only use the Shell to modify the Outlook Voice Access features for UM-enabled users on a UM mailbox policy or on the mailbox of a single UM-enabled user.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- A user has been enabled for UM. For detailed steps, see Enable a User for Unified Messaging.

Use the Shell to disable selected Outlook Voice Access features for UM-enabled users on a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example prevents users associated with a UM mailbox policy named MyUMMailboxPolicy from accessing their calendar when they dial in to Outlook Voice Access.

```
Set-UMMailboxPolicy -id MyUMMailboxPolicy -AllowTUIAccessToCalendar $false
```

This example prevents users associated with the UM mailbox policy named MyUMMailboxPolicy from accessing the directory when they dial in to Outlook Voice Access.

```
Set-UMMailboxPolicy -id MyUMMailboxPolicy -AllowTUIAccessToDirectory $false
```

This example prevents users associated with the UM mailbox policy named MyUMMailboxPolicy from accessing their e-mail when they dial in to Outlook Voice Access.

```
Set-UMMailboxPolicy -id MyUMMailboxPolicy -AllowTUIAccessToEmail -$false
```

This example prevents users associated with the UM mailbox policy named MyUMMailboxPolicy from accessing personal contacts when they dial in to Outlook Voice Access.

```
Set-UMMailboxPolicy -id MyUMMailboxPolicy -AllowTUIAccessToPersonalContacts $fals
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Use the Shell to disable selected Outlook Voice Access features on the mailbox of a single UM-enabled user

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example disables access to the calendar on a UM mailbox named tony@contoso.com when the user dials in to Outlook Voice Access.

```
Set-UMMailbox -id tony@contoso.com -TUIAccessToCalendarEnabled
```

This example disables access to e-mail on a UM mailbox named tony@contoso.com when the user dials in to Outlook Voice Access.

```
Set-UMMailbox -id tony@contoso.com -TUIAccessToEmailEnabled $false
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you disable selected Outlook Voice Access features, you may also want to:

- Enable or Disable Outlook Voice Access on a UM Mailbox Policy
- Configure the UM Mailbox Policy Assigned to a UM-Enabled User
- Enable or Disable Sending Voice Messages on a UM Dial Plan
- Enable PIN-less Logons for UM-Enabled Users

1.9.2.2.22 Enable PIN-less Logons for UM-Enabled Users

Enable PIN-less Logons for UM-Enabled Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2010, you can set up Unified Messaging (UM) so that your users can log on to their voice mail without using a PIN. By default, Outlook Voice Access users are prompted to enter a PIN to log on to their mailbox and access their voice mail, e-mail, calendar, personal Contacts, the directory, and personal options.

To enable PIN-less logons, you must set the parameter *AllowPinlessVoiceMailAccess* to `$true` on the UM mailbox policy and set the parameter *PinlessAccessToVoiceMailEnabled* to `$true` on the UM mailbox. By default, both parameters are set to `$false`, which requires an Outlook Voice Access user to enter their PIN when they access their voice mail.

Setting both parameters to `$true` allows you to enable PIN-less logons for a large group of users who are associated with a UM mailbox and also enable PIN-less logons for a single UM mailbox or a subset of UM mailboxes. Even if you enable PIN-less logons for a group of UM-enabled users or a single UM-enabled user, when they access their e-mail, calendar, personal Contacts, the directory, or personal options, they'll be prompted to enter their PIN.

To enable PIN-less logons to voice mail for a user, the following conditions must be met:

- You must have run the following cmdlet on the UM mailbox policy: `Set-UMMailboxPolicy -id MyUMMailboxPolicy -AllowPinlessVoiceMailAccess $true`
- You must have run the following cmdlet on the mailbox of the UM-enabled user: `Set-UMMailbox -id tonys@contoso.com -PinlessAccessToVoiceMailEnabled $true`
- The UM-enabled user is associated with the same UM mailbox policy for which you enabled PIN-less logons.
- The UM-enabled user dials in to Outlook Voice Access from a phone number that’s been assigned to them.

Note:

You can only use the Shell to modify the PIN-less logon settings for a group of UM-enabled users on a UM mailbox policy or on a single UM-enabled user's mailbox.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Looking for other management tasks related to UM mailboxes? Check out Managing Unified Messaging Users.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- The user or users have been enabled for UM. For detailed steps, see Enable a User for Unified Messaging.

Use the Shell to enable PIN-less access to voice mail for UM-enabled users on a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example enables PIN-less voice mail access on a UM mailbox policy named MyUMMailboxPolicy for users associated with the mailbox policy who dial in to Outlook Voice Access.

```
Set-UMMailboxPolicy -id MyUMMailboxPolicy -AllowPinlessVoiceMailAccess $true
```

For information about syntax and parameters, see Set-UMMailboxPolicy.

Use the Shell to enable PIN-less access to voice mail on a UM-enabled user's mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailboxes" entry in the Unified Messaging Permissions topic.

This example enables PIN-less voice mail access for the user who dials in to Outlook Voice Access to reach the mailbox named tonys@contoso.com.

```
Set-UMMailbox -id tonys@contoso.com -PinlessAccessToVoiceMailEnabled $true
```

For more information about syntax and parameters, see Set-UMMailbox.

Other Tasks

After you enable PIN-less logons for voice mail, you may also want to:

- View or Configure the Properties of a UM-Enabled User
- Configure the UM Mailbox Policy Assigned to a UM-Enabled User
- Set PIN Policies for UM-Enabled Users

1.9.2.3 Managing Unified Messaging Components

Managing Unified Messaging Components

Exchange Server 2010 > Unified Messaging > Managing Unified Messaging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2008-10-26*

Managing UM Dial Plans

Managing UM Mailbox Policies

Managing UM IP Gateways

Managing UM Hunt Groups

Managing UM Auto Attendants

1.9.2.3.1 Managing UM Auto Attendants

Managing UM Auto Attendants

Unified Messaging > Managing Unified Messaging > Managing Unified Messaging Components >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Create a UM Auto Attendant

View or Configure the Properties of a UM Auto Attendant

Delete a UM Auto Attendant

Enable a UM Auto Attendant

Disable a UM Auto Attendant

Add an Extension Number to a UM Auto Attendant

Enable or Disable Automatic Speech Recognition on a UM Auto Attendant

Configure a UM Auto Attendant with a DTMF Fallback Auto Attendant

Enable or Disable Directory Lookups for a UM Auto Attendant

Enable a Custom Business Hours Welcome Greeting on a UM Auto Attendant

Enable a Custom Non-Business Hours Welcome Greeting on a UM Auto Attendant

Enable an Informational Announcement on a UM Auto Attendant

Enable a Custom Non-Business Hours Main Menu Prompt Greeting on a UM Auto Attendant

Enable a Custom Business Hours Main Menu Prompt Greeting on a UM Auto Attendant

1.9.2.3.1.1 Create a UM Auto Attendant

Create a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-09*

After you create a Unified Messaging (UM) auto attendant, incoming calls to an external telephone number that a human operator would ordinarily answer are answered by the auto attendant. Unlike for other Unified Messaging objects, such as UM dial plans and UM IP gateways, you aren't required to create UM auto attendants. However, auto attendants help internal and external callers locate users or departments that exist in an organization and transfer calls to them.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

What Do You Want to Do?

- Use the EMC to create a UM auto attendant
- Use the Shell to create a UM auto attendant

Use the EMC to create a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. In the action pane, click **New UM Auto Attendant**.
4. In the New UM Auto Attendant wizard, complete the following fields:
   - **Name** Use this text box to create the display name for the UM auto attendant. A UM auto attendant name is required and must be unique. However, it's used only for display purposes in the EMC and the Shell.
     If you have to change the display name of the auto attendant after it's created, you must first delete the existing UM auto attendant and then create another auto attendant that has the appropriate name. If your organization uses multiple UM auto attendants, we recommend that you use meaningful names for your UM auto attendants. The maximum length of a UM auto attendant name is 64 characters, and it can include spaces. Although you can include spaces in the name of a new UM auto attendant, the name cannot include spaces if you integrate Unified Messaging with Office Communications Server 2007 R2 or Microsoft Lync Server. Therefore, if you created an auto attendant that has spaces in the display name, and if you are integrating with Office Communications Server 2007 R2 or Microsoft Lync Server, you must first delete that auto attendant and then create another by using a display name that does not include spaces.
   - **Select associated dial plan** Click **Browse** to select the UM dial plan to associate with this UM auto attendant. Selecting and associating a UM dial plan with the auto attendant is required. A UM auto attendant can be associated with only one UM dial plan.
   - **Pilot identifier list** Use this field to enter the extension numbers or pilot numbers that callers will use to reach the auto attendant. Type an extension number or pilot identifier in the box, and then click **Add** to add the number to the list. The number of digits in the extension number or pilot identifier that you provide doesn't have to match the number of digits for an extension number configured on the associated UM dial plan. This is because direct calls are allowed to UM auto attendants.
     The number of extension numbers or pilot identifiers entered is unlimited. However, you may create the new auto attendant without an extension number listed. An extension number or pilot identifier isn't required.
     You can edit or remove an existing extension number or pilot identifier. To edit an existing extension number or pilot identifier, click **Edit**. To remove an existing extension number or pilot identifier from the list, click **Remove**.

- **Create auto attendant as enabled** Select this option to enable the auto attendant to answer incoming calls when you complete the New UM Auto Attendant wizard. By default, a new auto attendant is created as disabled.
  If you decide to create the UM auto attendant as disabled, you can use the EMC action pane or the Shell to enable the auto attendant after you finish the wizard.
- **Create auto attendant as speech-enabled** Select this check box to speech-enable the UM auto attendant. By speech-enabling the auto attendant, callers can respond to the system or custom prompts used by the UM auto attendant using touchtone or voice inputs. By default, the auto attendant won't be speech-enabled when it's created.
  For callers to use a speech-enabled auto attendant, you must install the appropriate Unified Messaging language pack that contains Automatic Speech Recognition (ASR) support and configure the properties of the auto attendant to use this language.

5. On the **Completion** page, confirm whether the UM auto attendant was successfully created:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to complete the New UM Auto Attendant wizard.

Use the Shell to create a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example creates a UM auto attendant named `MyUMAutoAttendant` that can accept incoming calls but isn't speech-enabled.

```
New-UMAutoAttendant -Name MyUMAutoAttendant -UMDialPlan MyUMDialPlan -PilotIdenti
```

This example creates a speech-enabled UM auto attendant named `MyUMAutoAttendant`.

```
New-UMAutoAttendant -Name MyUMAutoAttendant -UMDialPlan MyUMDialPlan -PilotIdenti
```

For more information about syntax and parameters, see New-UMAutoAttendant.

Other Tasks

After you create an auto attendant, you may also want to:

- Enable Business Hours Key Mappings on a UM Auto Attendant
- Enable Non-Business Hours Key Mappings on a UM Auto Attendant

For More Information

Understanding Unified Messaging Auto Attendants

View or Configure the Properties of a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After you create a Unified Messaging auto attendant, you can view or configure a variety of settings. For example, you can add, remove, and edit extension numbers associated with the auto attendant. You can also enable or disable Automatic Speech Recognition (ASR) for the auto attendant and change the greetings used for business and non-business hours.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

What Do You Want to Do?

- Use the EMC to view or configure UM auto attendant properties
- Use the Shell to configure UM auto attendant properties
- Use the Shell to view UM auto attendant properties

Use the EMC to view or configure UM auto attendant properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab, and then select the UM auto attendant that you want to configure.
3. In the action pane, click **Properties**.
4. Use the **General** tab to view display-only information about the UM auto attendant and to perform management tasks on a UM auto attendant, as follows:
   - **Status** This box shows whether the UM auto attendant is enabled or disabled. To enable or disable the auto attendant, close the **General** tab and use the action pane commands to enable or disable the auto attendant.
   - **Associated dial plan** This box displays the UM dial plan associated with the auto attendant. After you create an auto attendant, the dial plan associated with the auto attendant can't be changed. If you need to associate an auto attendant with a different dial plan, you must delete the dial plan and then associate the auto attendant with the correct dial plan after you re-create it.

- **Modified** This box shows the last date and time the auto attendant settings were modified.
- **Pilot identifier list** Use this box to enter the extension numbers or pilot numbers that, when it's called, leads callers to the auto attendant. By default, no extension numbers are configured when you create an auto attendant.

  The number of digits in the extension number or pilot numbers you provide must match the number of digits for an extension number configured on the UM dial plan associated with the UM auto attendant. You can also add a Session Initiation Protocol (SIP) address to this box. A SIP address is used by some IP Private Branch eXchanges (PBXs).

  However, you can create the new auto attendant without listing an extension number or pilot number. An extension number isn't required. To add an extension, type the number in this box, and then click **Add**. You can associate more than one number with an auto attendant. You can also edit or remove an existing extension number. To edit an existing extension number, click the **Edit** button. To remove an existing extension number from the list, click the **Remove** button.
- **Auto attendant is speech-enabled** Use this option to enable callers to respond verbally to auto attendant prompts to navigate the menu system. By default, when an auto attendant is created, it isn't speech-enabled.

  If you decide to create the UM auto attendant but not to speech-enable it, you can use the EMC or the Shell to speech-enable it after you finish using the New UM Auto Attendant wizard. You can then view the properties of the auto attendant and enable this option.
- **Use this DTMF fallback auto attendant** Select this check box to enable the UM auto attendant to use a dual tone multi-frequency (DTMF) fallback auto attendant. A DTMF fallback auto attendant can be used only if the **Auto attendant is speech-enabled** option is selected. You must first create a DTMF fallback auto attendant, and then click the **Browse** button to locate the appropriate DTMF auto attendant.

  A DTMF fallback auto attendant is used when the UM speech-enabled auto attendant can't understand or recognize the speech inputs from the caller. If the DTMF auto attendant is used, the caller is required to use DTMF inputs to navigate the menu system, spell a user's name, or use a custom menu prompt. A caller won't be able to use voice commands to navigate this auto attendant.

  If you don't configure a DTMF fallback auto attendant, we recommend that you configure an operator extension number on the auto attendant. If you don't configure an operator extension number, when callers use a speech-enabled auto attendant and the system doesn't recognize their voice inputs, they won't be able to navigate the system or be transferred to an operator for help.

  Although not required, we recommend that you configure the DTMF fallback auto attendant to have the same configuration as the speech-enabled auto attendant. The DTMF fallback auto attendant shouldn't be speech-enabled.
- **Auto attendant is enabled for directory lookups** Select this check box to enable the UM auto attendant to look up names in the directory for callers. This setting is enabled by default. If this setting is disabled, callers won't be able to search the directory for a specific person using touchtone or voice commands.

5. Use the **Greetings** tab on the auto attendant's **Properties** sheet to manage recorded greetings for the current UM auto attendant. You can select default

greetings or previously recorded custom greetings for business hours and non-business hours. You can configure the following:

- **Business hours greeting** This is the initial greeting played when a caller calls the auto attendant during your organization's business hours. By default, it's a system prompt that says, "Welcome to the Exchange auto attendant." This greeting plays during your organization's business hours. The business and non-business hours are configured on the auto attendant **Times** tab.

  You may want to customize this greeting to represent your company, for example, "Thank you for calling Woodgrove Bank." You can configure a customized business hours greeting by clicking **Modify** to select a previously recorded custom greeting file. You can select the following:

  Use default greeting Use this option to enable the default business hours greeting to be played to callers. By default, this option is enabled.

  Use custom greeting file Use this option when you want to enable a custom business hours greeting file to be played to callers. Click **Browse** to locate a custom business hours greeting file that was previously recorded.
- **Non-Business hours greeting** This is the initial greeting played when a caller calls the auto attendant during your organization's non-business hours. By default, no business or non-business hours are configured. Therefore, there is no default non-business hours greeting. You can configure the business and non-business hours on the auto attendant **Times** tab.

  You may want to customize this greeting to represent your company, for example, "Thank you for calling Woodgrove Bank but we are now closed." You can configure a customized business hours greeting by clicking **Modify** to select a previously recorded custom greeting file.

  This is the initial greeting played when a caller calls the auto attendant during your organization's non-business hours. There's no default non-business hours greeting because, by default, there are no business or non-business hours configured. However, you may want to provide a customized non-business hours greeting specific to your company, for example, "You have reached Contoso, Ltd. after business hours. Our business hours are from 8:00 A.M. until 5:00 P.M., Monday through Friday." You can select the following:

  Use default greeting Use this option to enable the default non-business hours greeting to be played to callers when a business hours schedule has been configured on the auto attendant. By default, this option is enabled.

  Use custom greeting file Use this option when you want to enable a custom non-business hours greeting file to be played to callers. Click **Browse** to locate a custom non-business hours greeting file that was previously recorded.
- **Informational announcement** When enabled, this optional recording plays immediately after the business or non-business hours greeting. An informational announcement may state the organization's hours of operation, for example, "Our business hours are 8:30 A.M. to 5:30 P.M., Monday through Friday and 8:30 A.M. to 1:00 P.M. on Saturday." An informational announcement can also provide information required for compliance with company policy, for example, "Calls may be monitored for training purposes." If it's important that callers hear the whole informational announcement, it can be marked as uninterruptible.

  By default, there's no informational announcement configured on UM dial plans or auto attendants. Use the following options to enable an informational announcement and use a custom

audio file specific to your organization. The recordings must already have been recorded as .wav files. You can select the following:

Disable announcement Use this option to disable an informational announcement. By default, this option is configured.

Informational announcement file Use this option when you want to enable an informational announcement to be played to callers. Click **Browse** to locate a custom informational announcement file previously recorded.

Allow informational announcement to be interrupted Use this option to enable the informational announcement to be interrupted by the caller. This should be enabled if you have long informational announcements. Callers may become frustrated if the informational announcement is long and they can't interrupt the informational announcement to access the options provided by the UM dial plan or auto attendant.

- **Business hours main menu prompt** The business hours main menu prompt for an auto attendant is the list of options callers hear during business hours defined on the **Times** tab. For example, "For technical support, press or say 1. For corporate offices and administration, press or say 2. For sales, press or say 3."

  To enable a business hours main menu prompt, you must perform the following steps:

- Specify a custom menu prompt audio file. To use a custom business hours menu prompt, click **Modify** to select the default prompt or to specify a previously recorded prompt.
- Configure the appropriate business hours using the **Business hours** option on the **Times** tab.
- Enable business hours key mappings and configure key mappings on the **Key Mapping** tab for the auto attendant.

  By default, if you enabled and defined business hours key mappings on the **Key Mapping** tab on the UM auto attendant, the Unified Messaging Text-to-Speech (TTS) engine will synthesize a business hours main menu prompt. Alternatively, you can create a customized audio file that can be used for the business hours main menu prompt for a speech-enabled auto attendant that would say, for example, "For sales, say 1. For technical support, say 2. For administration, say 3. To reach an operator, press zero." You can select the following:

  Use default greeting Use this option to enable the default business hours main menu prompt to be played to callers when a business hours schedule has been configured on the auto attendant. By default, this option is enabled.

  Use custom greeting file Use this option when you want to enable a custom business hours main menu prompt file to be played to callers. Click **Browse** to locate a previously recorded custom business hours greeting file. The recordings must already have been recorded as .wav files.

- **Non-Business hours main menu prompt** The non-business hours main menu prompt for an auto attendant is the list of options callers hear during the non-business hours defined on the **Times** tab. For example, "Your call is very important to us. However, you have reached Woodgrove Bank after normal business hours. If you want to leave a message, please press or say 1 and we will return your call as soon as possible."

  To enable a non-business hours main menu prompt, you must perform the following steps:

  a. Specify a custom menu prompt audio file. To use a custom non-business hours main menu prompt, click **Modify** to select the default prompt or to specify a previously recorded prompt.

b. Configure the appropriate business hours using the **Business hours** option on the **Times** tab.
c. Enable non-business hours key mappings and configure key mappings on the **Key Mapping** tab for the auto attendant.
By default, if you enabled and defined non-business hours key mappings on the **Key Mapping** tab on the UM auto attendant, the Unified Messaging TTS engine will synthesize a non-business hours main menu prompt. Alternatively, you can create a customized audio file that can be used for the non-business hours main menu prompt for a speech-enabled auto attendant that would say, for example, "To leave a voice message for sales, say 1. To leave a voice message for technical support, say 2. To leave a voice message for administration, say 3. To reach an after hours operator, press zero." You can select the following:
Use default greeting Use this option to enable the default non-business hours main menu prompt to be played to callers when a non-business hours schedule has been configured on the auto attendant. By default, this option is enabled. The recordings must already have been recorded as .wav files.
Use custom greeting file Use this option when you want to enable a custom non-business hours main menu prompt file to be played to callers. Click **Browse** to locate a custom non-business hours greeting file that was previously recorded. The recordings must already have been recorded as .wav files.

6. Use the **Times** tab on the auto attendant **Properties** sheet to determine the organization's open business hours. During business hours, callers hear the default business hours greeting or a customized greeting and the business hours main menu prompt if the appropriate business hours key mappings are configured on the **Key Mapping** tab. You can configure the following:
   - **Business hours** Use this list to select a standard schedule, or you can click **Customize** to create your own user-defined schedule. **Always Run** is the default setting.
     If your business hours vary only slightly from one of the system-defined schedules, you can select a schedule, and then click **Customize** to refine your business hours schedule.
   - **Select time zone** Use this list to select your time zone. Consider whether the dial plan associated with the auto attendant covers more than one time zone when you set your schedule.
     By default, the time zone is configured using the local server's system time when the Unified Messaging server role was installed.
   - **Holiday Schedule** Use **Holiday Schedule** to define days, from 00:00 through 23:59 (12:00 A.M. through 11:59 P.M.), for which your organization will be closed for a holiday. Callers who reach the auto attendant during the times that you specify in the **Select Holiday** dialog box hear a custom holiday greeting audio file that you define. When you configure the holiday schedule, you must also define the **Holiday start date** and **Holiday end date**.

7. Use the **Features** tab on the auto attendant's **Properties** sheet to define the features available to callers who dial in to the UM auto attendant. For example, you can configure auto attendant features such as the language used when callers call in to the auto attendant and the ability for callers to transfer to an operator's extension number that you define on this property sheet. You can configure the following:
   - **Business name** Use this box to enter the name of the business. By default, no business name is entered. If you enter a business name in this box, a prompt with the business name will be played to callers instead of

the default greeting.

- **Business location** Use this box to enter the location of the business. By default, there is not a business location entered. If you enter the location of the business in this box, the business location will be played for callers.
- **Language** Use this list to select the language that callers hear when they reach the auto attendant. The default language is determined when you install Microsoft Exchange Server 2010. By default, when you install the Unified Messaging server role, U.S. English is used because the auto attendant uses the language setting on the UM dial plan. To have other language options available, you must install the UM language packs for the languages you want to include. For more information about how to install a UM language pack, see Install a Unified Messaging Language Pack on a UM Server.

  Although you can select a language other than the language selected on the UM dial plan associated with the auto attendant, we recommend that the language settings on the dial plan and the auto attendant match. If language settings don't match, when callers call an extension number defined on the dial plan, callers will be presented with prompts in one language, and when they dial an extension number associated with an auto attendant, they will be presented with prompts in a different language.

  The language selected in this list is used when callers call the extension number defined on the properties for the UM auto attendant.
- **Operator extension** Use this box to type the extension number used to call an operator. This extension number can also connect the caller to a human operator or a UM-enabled mailbox or can be configured to call an external telephone number. By default, an operator extension isn't included in this box.
- **Allow caller to transfer to users** Select this check box to enable callers to transfer calls to users. By default, this option is enabled, and lets users who are associated with the dial plan transfer calls to users in the same UM dial plan. After you select this check box, you can set the group of users to whom callers can transfer by selecting the appropriate option under the **Callers can contact** section on this page.

  If you disable this option and disable the **Allow callers to send voice message** option, the options under **Callers can contact** are also disabled.
- **Allow callers to send voice messages** Select this check box to enable callers to send voice messages to users. By default, this option is enabled, and lets users who are associated with the dial plan send voice messages to users in the same UM dial plan. After you select this check box, you can set the group of users to whom callers can send voice messages by selecting the appropriate option under the **Callers can contact** section on this page.

  If you disable this option and disable the **Allow caller to transfer to users** option, the options under **Callers can contact** are also disabled.

  If you disable this option, the auto attendant won't invite callers to send a voice message during a system prompt.
- **Callers can contact** Use these options to determine a grouping of users to use. By default, the **Users within dial plan** option is selected. However, you can change the grouping of users to allow callers to transfer calls or send voice messages to users who are located in the global address list (GAL) or to a specific set of users who are contained in custom address lists by choosing from the following:

  Users within dial plan Select this option to allow callers who connect to the UM auto attendant to locate and contact users who are in the dial plan associated with the UM auto attendant.

Anyone in the default global address list Select this option to allow callers who connect to the UM auto attendant to locate and contact anyone listed in the GAL. This includes all users who are mailbox-enabled.

Anyone in this address list Select this option to allow callers who connect to the UM auto attendant to locate and contact users who are in a defined custom address list. This includes all users who are mailbox-enabled.

Important:

The **All Address Lists** container is an empty container object and differs from the GAL container. If you choose the **All Address Lists** container when you browse for a custom address list, there will be no UM-enabled users for callers to contact. If you want to select all the address lists in your organization, choose the **Anyone in the default global address list** option.

- **Matched name selection method** Use this list to select the matched name selection method for the UM auto attendant. The matched name method is used when two or more users who have the same name exist in the directory. This is also called a disambiguation field. You can configure this setting on this property sheet, or you can leave the default setting on the auto attendant and configure this setting on the dial plan.

  By default, the auto attendant is set to inherit from the dial plan. However, by default, the auto attendant is unable to disambiguate between two or more users who have the same name because the default setting for the **Matched name selection method** on the dial plan is set to **None**.

  Select one of the following methods that provide the caller more information to help the caller select the correct user in the organization:

  Title Select this option to have the auto attendant include each user's title when listing matches.

  Department Select this option to have the auto attendant include each user's department when listing matches.

  Location Select this option to have the auto attendant include each user's location when listing matches.

  None Select this option to have no additional information given when listing matches.

  Prompt For Alias Select this option to have the auto attendant prompt the caller for the user's alias.

  Inherit From Dial Plan Select this option to have the auto attendant use the default setting from the dial plan associated with the auto attendant.

- **Allow transfer to operator during business hours** Select this check box to enable callers to be transferred to a human operator during business hours using the extension number that you configure in the **Operator extension** box on this property sheet. By default, this option is disabled.

  It's useful to enable this option so that when a caller is unsuccessful at using the menu prompts or directory search to locate the required person during business hours, the caller can leave a voice message or connect to a human operator. After you enable this option, you can configure the operator extension number on a UM-enabled mailbox that's monitored. The caller can leave a voice message, or a human operator who has the extension number can help the caller.

- **Allow transfer to operator after business hours** Select this check box to enable callers to be transferred to a human operator after business hours using the extension number that you configure in the **Operator extension** box on this property sheet. By default, this option is disabled.

  It's useful to enable this option so that when a caller is

unsuccessful at using the menu prompts or directory search to locate the required person after business hours, the caller can leave a voice message or connect to a human operator. After you enable this option, you can configure the operator extension number configured on a UM-enabled mailbox that's monitored. The caller can leave a voice message, or a human operator who has the extension number can help the caller.

8. Use the **Key Mapping** tab on the auto attendant's **Property** sheet to define the telephone keys that callers can press when they reach the UM auto attendant. You can define separate key mappings for business hours and non-business hours. A key mapping is defined as an entry in a table that has as many as nine entries. The 0 (zero) key is reserved for a transfer to the operator.
   For example, a key mapping used during business hours may enable a call transfer to another extension where a human operator or receptionist is available. For non-business hours, the option to transfer to another extension may not be available, or the call may be forwarded to a UM-enabled mailbox so the caller can leave a voice message. You can configure the following:
   - **Enable business hours key mapping** Select this check box to enable specific key mappings that will be used during business hours. When you enable business hours key mapping, you can add new key mappings for business hours.
   - **Enable non-business hours key mapping** Select this check box to enable specific key mappings that will be used during non-business hours. When you enable non-business hours key mapping, you can add new key mappings for non-business hours.

     For more information about configuring key mapping entries, see Configure Key Mapping Entries on a UM Auto Attendant.

9. Use the **Dialing Restrictions** tab on the UM auto attendant properties to configure dialing rules for callers who call in to a UM auto attendant. An auto attendant is the collection of voice prompts that callers hear instead of a human operator when they call in to an organization that has Exchange 2010 Unified Messaging. You can use these settings to control the extension numbers that can be reached from an auto attendant or control the telephone numbers that can be dialed by callers that have dialed into the auto attendant. You can configure the following:
   - **Allow calls to users within the same dial plan** Select this check box to allow users who call in to an auto attendant to place or transfer calls to an extension number associated with a UM-enabled user who is associated with the same dial plan as the auto attendant. By default, this setting is enabled.

     When you disable this setting, users who call in to an auto attendant can place or transfer calls to users who aren't UM-enabled or to other extension numbers not associated with a UM-enabled user. Users can't transfer calls to UM-enabled users who are associated with the same dial plan as the auto attendant. This is because the **Allow calls to extensions** setting is enabled by default.
   - **Allow calls to extensions** When this setting is disabled, users who call in to an auto attendant can't place calls to users who aren't UM-enabled or to other extension numbers not associated with a UM-enabled user. However, they can place calls or transfer calls to extension numbers associated with UM-enabled users. This is because the **Allow calls to users within the same dial plan** setting is enabled by default. The **Allow calls to extensions** setting is enabled by default.

     When this setting is enabled, users who call in to an auto attendant can place calls to users who aren't UM-enabled, to

other extension numbers not associated with a UM-enabled user, and to UM-enabled users. This is because the **Allow calls to users within the same dial plan** setting is enabled by default.
You can enable this setting in an environment where not all users have been UM-enabled. This setting is also useful when you want to allow users who call in to a telephone number configured on an auto attendant to call extension numbers not associated with a UM-enabled user.

- **Select allowed in-country/region rule groups from dial plan** Use this section to add or remove allowed in-country/region dialing rule groups. By default, there are no in-country/region dialing rule groups configured on UM auto attendants.
  In-country/region dialing rule groups are used to allow or restrict the telephone numbers within a country or region that any user who has dialed in to the UM auto attendant can dial. This helps prevent unnecessary or unauthorized telephone calls and charges.
  To add in-country/region dialing rule groups, you must first create the appropriate in-country/region dialing rule groups on the dial plan associated with the UM auto attendant, and then add the appropriate dialing rule entries on the dialing rule group. After you create the required dialing rule groups on the dial plan, you must then add the dialing rule groups to the list of dialing restrictions on the **Dialing Restrictions** tab on the UM auto attendant.
  In-country/region dialing rule groups can be used to enable a Unified Messaging server to allow or restrict access to telephone numbers within a country or region. This is applied to any user who has called in to an auto attendant.
- **Select allowed international rule groups from dial plan** Use this section to add or remove allowed international dialing rule groups. By default, there are no international dialing rule groups configured on UM auto attendants.
  International dialing rule groups are used to allow or restrict the telephone numbers outside a country or region that any user who has dialed in to the UM auto attendant can dial. This helps prevent unnecessary or unauthorized telephone calls and charges.
  To add international dialing rule groups, you must first create the appropriate international dialing rule groups on the dial plan associated with the UM auto attendant, and then add the appropriate dialing rule entries on the dialing rule group. After you create the required dialing rule groups on the dial plan, you must then add the dialing rule groups to the list of dialing restrictions on the **Dialing Restrictions** tab on the UM auto attendant.
  International dialing rule groups can be used to enable a Unified Messaging server to allow or restrict access to telephone numbers outside a country or region. This is applied to any user who has called in to an auto attendant.
  For more information about outdialing, see Understanding Outdialing.

Use the Shell to configure UM auto attendant properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging

Permissions topic.

This example configures a UM auto attendant named MySpeechEnabledAA to fall back to the MyDTMFAA auto attendant, sets the operators extension to 50100, and enables transfers to this extension number after business hours.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -DTMFFallbackAutoAttendant MyDTMF
```

This example configures a UM auto attendant named MyUMAutoAttendant that has: Business hours configured as 10:45 to 13:15 (10:45 A.M. to 1:15 P.M.) on Sunday, 09:00 to 17:00 (9:00 A.M. to 5:00 P.M.) on Monday, and 09:00 to 16:30 (9:00 A.M. to 4:30 P.M.) on Saturday; holiday times and their associated greetings configured as "New Year" on January 2, 2010; and "Building Closed for Construction" configured from April 24 through April 28, 2010.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Use the Shell to view UM auto attendant properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example returns a formatted list of all UM auto attendants in the Active Directory forest.

```
Get-UMAutoAttendant | Format-List
```

This example displays the properties of a UM auto attendant named MyUMAutoAttendant.

```
Get-UMAutoAttendant -Identity MyUMAutoAttendant
```

For more information about syntax and parameters, see Get-UMAutoAttendant.

Other Tasks

After you configure Unified Messaging auto attendant properties, you may also want to:

- Configure Key Mapping Entries on a UM Auto Attendant
- Enable a Custom Business Hours Welcome Greeting on a UM Auto Attendant

For More Information

Understanding Unified Messaging Auto Attendants

1.9.2.3.1.3 Delete a UM Auto Attendant

Delete a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can delete an existing Unified Messaging (UM) auto attendant. After you delete an existing UM auto attendant, the incoming calls that were answered by the UM auto attendant must be answered by a human operator. A UM auto attendant can't be deleted if it's associated with a UM dial plan as the default UM auto attendant.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to delete a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the UM auto attendant you want to delete.
4. In the action pane, click **Remove**.
5. In the confirmation dialog box, click **Yes** to delete the UM auto attendant.

Use the Shell to delete a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example deletes a UM auto attendant named `MyUMAutoAttendant`.

```
Remove-UMAutoAttendant -Identity MyUMAutoAttendant
```

For more information about syntax and parameters, see Remove-UMAutoAttendant.

Other Tasks

After you delete an existing UM auto attendant, you may also want to Create a UM Auto Attendant.

Enable a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. By default, when a UM auto attendant is created, the status of the UM auto attendant is set to enabled. After you create the UM auto attendant, you can control its status using the status variable. If the status of a UM auto attendant is disabled, you'll have to enable the UM auto attendant so it can answer incoming calls.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant object you want to enable.
4. In the action pane, click **Enable**.

Use the Shell to enable a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables the UM auto attendant named `MyUMAutoAttendant` to answer incoming calls.

```
Enable-UMAutoAttendant -Identity MyUMAutoAttendant
```

For more information about syntax and parameters, see Enable-UMAutoAttendant.

Other Tasks

After you enable a UM auto attendant, you may also want to:

- View or Configure the Properties of a UM Auto Attendant
- Disable a UM Auto Attendant

1.9.2.3.1.5 Disable a UM Auto Attendant

Disable a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can disable a Unified Messaging (UM) auto attendant. By default, when a UM auto attendant is created, its status is set to enabled. After you create the UM auto attendant, you can control its status by changing the status variable. For example, you might want to disable the UM auto attendant when you're recording or re-recording customized prompts and messages. If the UM auto attendant is disabled, the UM auto attendant can't answer incoming calls.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.
- The status of the UM auto attendant is set to enabled.

Use the EMC to disable a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the result pane, click the **UM Auto Attendants** tab.
3. Select the UM auto attendant you want to disable.
4. In the action pane, click **Disable**.

Use the Shell to disable a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example disables a UM auto attendant named `MyUMAutoAttendant`.

```
Disable-UMAutoAttendant -Identity MyUMAutoAttendant
```

For more information about syntax and parameters, see Disable-UMAutoAttendant.

Other Tasks

After you disable a UM auto attendant, you may also want to:

- Enable a UM Auto Attendant
- View or Configure the Properties of a UM Auto Attendant

1.9.2.3.1.6 Add an Extension Number to a UM Auto Attendant

Add an Extension Number to a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure an extension number or multiple extension numbers on a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. When you add an extension number to a UM auto attendant, that number can be used by callers to access the auto attendant. Also, you may have to add extension numbers because there is more than one extension number that callers can use to access an auto attendant. By default, no extension numbers are configured when you create an auto attendant.

Note:
An extension number for a UM auto attendant is also known as a pilot identifier or pilot number.

You can create a new auto attendant without setting up an extension number for the auto attendant. You can also associate more than one telephone or extension number with a single auto attendant. You can either add the extension numbers when you create the UM auto attendant or add them after you configure the auto attendant. The number of digits in the extension number you configured on the UM auto attendant must match the number of digits for an extension number that's configured on the UM dial plan associated with the UM auto attendant.

Note:
You can also add a Session Initiation Protocol (SIP) address instead of adding an extension number. A SIP address is used by some IP Private Branch eXchanges (PBXs).

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- A UM auto attendant has been created. For detailed steps, see Create a UM

Auto Attendant.

Use the EMC to configure an extension number on a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to modify, and then, in the action pane, click **Properties**.
4. On the **General** tab, under **Extension number to associate**, enter the number you want to associate with this auto attendant, and then click **Add**.
5. Click **OK** to save your changes.

Use the Shell to configure an extension number on a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example configures a UM auto attendant named `MyUMAutoAttendant` with multiple extension numbers.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -PilotIdentifierList "12345, 7200
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you configure an extension number on a UM auto attendant, you may also want to:

- Enable Dialing Restrictions on a UM Auto Attendant
- Configure an Operator Extension on a UM Auto Attendant

1.9.2.3.1.7 Enable or Disable Automatic Speech Recognition on a UM Auto Attendant

Enable or Disable Automatic Speech Recognition on a UM Auto Attendant

Managing Unified Messaging > Managing Unified Messaging Components > Managing UM Auto Attendants >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable your Microsoft Exchange Server 2010 Unified Messaging (UM) auto attendant for Automatic Speech Recognition (ASR). After you speech-enable a UM auto attendant, callers can respond verbally to auto attendant prompts and move through the

menu system of the auto attendant. By default, an auto attendant isn't speech-enabled when you create it. After you speech-enable the auto attendant, callers can use only voice commands to navigate the auto attendant menu system, and touchtone inputs can't be used.

Although it isn't required, we recommend that you configure a dual tone multi-frequency (DTMF) fallback auto attendant for each speech-enabled auto attendant so callers can use touchtone inputs if the speech-enabled auto attendant doesn't recognize or understand the words they say. If a DTMF fallback auto attendant is configured, callers can use DTMF inputs, also known as touchtone inputs, to navigate the auto attendant menu system, spell a user's name, or use a custom menu prompt. We don't recommend that you speech-enable a DTMF fallback auto attendant.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to speech-enable a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to modify, and then, in the action pane, click **Properties**.
4. On the **General** tab, select **Auto attendant is speech-enabled**.
5. Click **OK** to save your changes.

Use the Shell to speech-enable a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables ASR on a UM auto attendant named `MySpeechEnabled AA`.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -SpeechEnabled $true
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you speech-enable a UM auto attendant, you may also want to:

- Install a Unified Messaging Language Pack on a UM Server
- Update the Speech Grammar Files on a UM Server

- Enable or Disable Automatic Speech Recognition for a UM-Enabled User

1.9.2.3.1.8 Configure a UM Auto Attendant with a DTMF Fallback Auto Attendant

Configure a UM Auto Attendant with a DTMF Fallback Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure a speech-enabled Unified Messaging (UM) auto attendant that has a dual tone multi-frequency (DTMF) fallback auto attendant in Microsoft Exchange Server 2010. A DTMF fallback auto attendant is used when the UM speech-enabled auto attendant can't understand or recognize the speech inputs provided by a caller. If a DTMF fallback auto attendant has been configured, the caller has to use DTMF inputs, also known as touchtone inputs, to navigate the auto attendant menu system, spell a user's name, or use a custom menu prompt. If a DTMF fallback auto attendant hasn't been configured, and the maximum number of speech inputs has been exceeded because the system didn't understand what the caller said, the system will respond with this prompt: "Sorry, I couldn't help. Please call back later."

By default, an auto attendant isn't speech-enabled when you create it. After you speech-enable the auto attendant, callers can use only voice commands to navigate the auto attendant menu system, and touchtone inputs can't be used. Although it isn't required, we recommend that you configure a DTMF fallback auto attendant for each speech-enabled auto attendant so callers can use touchtone inputs if the speech-enabled auto attendant doesn't recognize or understand the words they say. We also recommend that you don't speech-enable a DTMF fallback auto attendant.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- A UM speech-enabled auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.
- A UM DTMF fallback auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to configure a speech-enabled auto attendant with a DTMF fallback auto attendant

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to modify, and then, in the action pane, click **Properties**.
4. On the **General** tab, make sure the check box next to **Auto attendant is speech-enabled** is selected.
5. Select the check box next to **Use this DTMF fallback auto attendant**, and then click **Browse**.
6. On the **Select Auto Attendant** page, select the auto attendant you want to use as a DTMF fallback auto attendant, and then click **OK**.
7. Click **OK** to save your changes.

Use the Shell to configure a speech-enabled auto attendant with a DTMF fallback auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example configures a UM auto attendant named MySpeechEnabledAA to use a DTMF fallback auto attendant named MyDTMFAA.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -DTMFFallbackAutoAttendant MyDTMF
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you configure a speech-enabled auto attendant with a DTMF fallback auto attendant, you may also want to:

- Enable Business Hours Key Mappings on a UM Auto Attendant
- Configure Business Hours for a UM Auto Attendant
- Enable or Disable Automatic Speech Recognition on a UM Auto Attendant

1.9.2.3.1.9 Enable or Disable Directory Lookups for a UM Auto Attendant

Enable or Disable Directory Lookups for a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable directory lookups so that callers who call in to a Unified Messaging (UM) auto attendant can look up names in the directory. This setting is enabled by default. If this setting is disabled, callers won't be able to search the directory for a specific person

using touchtone or voice commands.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable or disable directory lookups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Auto Attendants** tab, select the UM auto attendant.
3. In the action pane, click **Properties**.
4. In the auto attendant **Properties** window, click the **General** tab, and then select or clear the **Auto attendant is enabled for directory lookups** check box.
5. Click **OK** to accept your changes.

Use the Shell to enable or disable directory lookups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example disables directory lookups on a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -NameLookupEnabled $false
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable or disable directory lookups on a UM auto attendant, you may also want to:

- Enable Dialing Restrictions on a UM Auto Attendant
- Configure the Scope of Users that Callers Can Contact on a UM Auto Attendant

Enable a Custom Business Hours Welcome Greeting on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable a custom business hours greeting for a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. The business hours welcome greeting is the first thing callers hear when a UM auto attendant answers their call during business hours

You'll probably want to customize the greetings, informational announcements, and menu prompts used with UM dial plans and auto attendants. After the Unified Messaging server role is installed on the Exchange 2010 server, you can enable the UM dial plans and auto attendants to use these custom .wav audio files.

If you want to include the name of your organization or business as part of the default welcome greeting, you can enter the name in the Business Name field on the UM auto attendant. For details, see Configure a Business Name on a UM Auto Attendant.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable a custom business hours greeting for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to change and then, in the action pane, click **Properties**.
4. On the **Greeting** tab, under **Business hours greeting**, click **Modify**.
5. On the **Business Hours Greeting** page, select from these options:
   - **Use default greeting**
   - **Use custom greeting file**
6. If you select the **Use custom greeting file** option, click **Browse**, locate the greeting file you've already created, and then click **OK**.
7. Click **OK** to save your changes.

Use the Shell to enable a custom business hours greeting for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables the business hours welcome greeting that uses a custom greeting named `welcomegreetingfile.wav` for the UM auto attendant `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursWelcomeGreetingEnab
```

This example configures a UM auto attendant named `MyUMAutoAttendant` that has business hours configured to be 10:45 to 13:15 (Sunday), 09:00 to 17:00 (Monday), and 09:00 to 16:30 (Saturday) and holiday times and their associated greetings configured to be "`New Year`" on January 2, 2010, and "`Building Closed for Construction`" from April 24, 2010 through April 28, 2010.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.
```

This example configures a UM auto attendant named `MyAutoAttendant` and enables business hours key mappings so that when callers press 1, they are forwarded to another UM auto attendant named `SalesAutoAttendant`. When they press 2, they are forwarded to extension number 12345 for `Support`, and when they press 3, they are sent to another auto attendant that plays an audio file.

```
Set-UMAutoAttendant -Identity MyAutoAttendant - BusinessHoursKeyMappingEnabled $t
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable a custom business hours welcome greeting for a UM auto attendant, you may also want to:

- Enable a Custom Business Hours Main Menu Prompt Greeting on a UM Auto Attendant
- Enable a Custom Non-Business Hours Welcome Greeting on a UM Auto Attendant
- Configure Key Mapping Entries on a UM Auto Attendant

1.9.2.3.1.11 Enable a Custom Non-Business Hours Welcome Greeting on a UM Auto Attendant

Enable a Custom Non-Business Hours Welcome Greeting on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable a custom non-business hours greeting for a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. The non-business hours welcome greeting is the first thing callers hear when a UM auto attendant answers their call during non-business hours.

Unified Messaging includes a default system prompt for use during non-business hours.

Although the default system prompt mustn't be replaced or changed, you may want to provide an alternative greeting. You can create a custom welcome greeting in the .wav file format that can be used when callers call in to a UM auto attendant during non-business hours. For example, "You have reached Woodgrove Bank after hours."

If you want to include the name of your organization or business as part of the default welcome greeting, you can enter the name in the Business Name field on the UM auto attendant. For details, see Configure a Business Name on a UM Auto Attendant.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable a custom non-business hours greeting for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to change, and then, in the action pane, click **Properties**.
4. On the **Greetings** tab, under **Non-business hours greeting**, click **Modify**.
5. On the **Non-Business Hours Greeting** page, select from these options:
   - **Use default greeting**
   - **Use custom greeting file**
6. If you select the **Use custom greeting file** option, click **Browse**, locate the greeting file you've already created, and then click **OK**.
7. Click **OK** to save your changes.

Use the Shell to enable a custom non-business hours greeting for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables the non-business hours welcome greeting that uses a custom greeting named `welcomegreetingfile.wav` for the UM auto attendant `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AfterHoursWelcomeGreetingEnabled
```

This example configures a UM auto attendant named `MyUMAutoAttendant` that has

business hours configured to be 10:45 to 13:15 (Sunday), 09:00 to 17:00 (Monday), and 09:00 to 16:30 (Saturday) and holiday times and their associated greetings configured to be "New Year" on January 2, 2010, and "Building Closed for Construction" from April 24, 2010 through April 28, 2010.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.
```

This example configures a UM auto attendant named MyAutoAttendant and enables business hours key mappings so that when callers press 1, they are forwarded to another UM auto attendant named SalesAutoAttendant. When they press 2, they are forwarded to extension number 12345 for Support, and when they press 3, they are sent to another auto attendant that plays an audio file.

```
Set-UMAutoAttendant -Identity MyAutoAttendant - BusinessHoursKeyMappingEnabled $t
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable a custom non-business hours greeting for a UM auto attendant, you may also want to:

- Enable a Custom Business Hours Welcome Greeting on a UM Auto Attendant
- Enable a Custom Non-Business Hours Welcome Greeting on a UM Auto Attendant
- Configure Key Mapping Entries on a UM Auto Attendant

1.9.2.3.1.12 Enable an Informational Announcement on a UM Auto Attendant

Enable an Informational Announcement on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable an informational announcement for a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. When an informational announcement is enabled, it will play immediately after the business or non-business hours greeting. By default, an informational announcement isn't configured. To enable an informational announcement, create a .wav file to be used as the informational announcement, and then configure the auto attendant to use this .wav file.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable an informational announcement for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to change, and then, in the action pane, click **Properties**.
4. On the **Greeting** tab, under **Informational announcement**, click **Modify**.
5. On the **Informational announcement** page, select from the following options:
   - **Disable announcement**
   - **Informational announcement file**
6. If you select the **Informational announcement file** option, click **Browse**, locate the informational announcement file you've already created, and then click **OK**.
7. Click **OK** to save your changes.

Use the Shell to enable an informational announcement for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables an informational announcement that uses the MyInfoAnnouncement.wav file on a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -InfoAnnouncementEnabled $true -I
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable an informational announcement for a UM auto attendant, you may also want to:

- Enable a Custom Business Hours Welcome Greeting on a UM Auto Attendant
- Enable a Custom Non-Business Hours Welcome Greeting on a UM Auto Attendant

1.9.2.3.1.13 Enable a Custom Non-Business Hours Main Menu Prompt Greeting on a UM Auto Attendant

Enable a Custom Non-Business Hours Main Menu Prompt Greeting on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable a custom non-business hours main menu prompt greeting for a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. After you create a UM auto attendant, a default system prompt will be used for the non-business hours main menu prompt greeting heard by callers after the non-business hours welcome greeting is played. Although the system prompts mustn't be replaced or changed, you will probably want to customize the greetings and menu prompts used with UM auto attendants. Frequently, in addition to configuring a customized non-business hours welcome greeting, you will also want to create and configure a custom non-business hours main menu prompt greeting. After you configure a custom non-business hours main menu prompt greeting, you must enable key mappings on the UM auto attendant for non-business hours.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable a custom non-business hours main menu prompt greeting for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to change, and then, in the action pane, click **Properties**.
4. On the **Greetings** tab, under **Main Menu Prompt**, under **Non-Business hours main menu prompt**, click **Modify**.
5. On the **Non-Business Hours Main Menu Prompt** page, select from these options:
   - **Use default greeting**
   - **Use custom greeting file**
6. If you select the **Use custom greeting file** option, click **Browse**, locate the custom non-business hours main menu prompt file you've already created, and then click **OK**.
7. Click **OK** to save your changes.

Use the Shell to enable a custom non-business hours main menu prompt greeting for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example configures a UM auto attendant named `MyUMAutoAttendant` that has business hours configured to be 10:45 to 13:15 (Sunday), 09:00 to 17:00 (Monday), and 09:00 to 16:30 (Saturday) and holiday times and their associated greetings configured to be "`New Year`" on January 2, 2010, and "`Building Closed for Construction`" from April 24, 2010 through April 28, 2010.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.
```

This example configures a UM auto attendant named `MyAutoAttendant` and enables business hours key mappings so that when callers press 1, they are forwarded to another UM auto attendant named `SalesAutoAttendant`. When they press 2, they are forwarded to extension number 12345 for `Support`, and when they press 3, they are sent to another auto attendant that plays an audio file.

```
Set-UMAutoAttendant -Identity MyAutoAttendant - BusinessHoursKeyMappingEnabled $t
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable a custom non-business hours main menu prompt greeting for a UM auto attendant, you may also want to:

- Enable a Custom Business Hours Main Menu Prompt Greeting on a UM Auto Attendant
- Enable a Custom Business Hours Welcome Greeting on a UM Auto Attendant
- Enable a Custom Non-Business Hours Welcome Greeting on a UM Auto Attendant
- Configure Key Mapping Entries on a UM Auto Attendant

1.9.2.3.1.14 Enable a Custom Business Hours Main Menu Prompt Greeting on a UM Auto Attendant

Enable a Custom Business Hours Main Menu Prompt Greeting on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable a custom business hours main menu prompt greeting for a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. After you create a UM auto attendant, a default system prompt will be used for the business hours main menu prompt greeting that's heard by callers after the business hours welcome greeting is played. Although the system prompts mustn't be replaced or changed, you will probably want to customize the greetings and menu prompts used with UM auto attendants. Frequently, in addition to configuring a customized business hours welcome greeting, you will want to create and configure a custom business hours main menu prompt greeting. After you configure a custom business hours main menu prompt greeting, you must enable key mappings on the UM auto attendant for business hours.

If you only want to include the name of your organization or business as part of the default welcome greeting, you can enter the name in the Business Name field on the UM auto attendant. For details, see Configure a Business Name on a UM Auto Attendant.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable a custom business hours main menu prompt greeting for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to change, and then, in the action pane, click **Properties**.
4. On the **Greetings** tab, under **Main Menu Prompt**, under **Business hours main menu prompt**, click **Modify**.
5. On the **Business Hours Main Menu Prompt** page, select from these options:
   - **Use default greeting**
   - **Use custom greeting file**
6. If you select the **Use custom greeting file** option, click **Browse**, locate the custom business hours main menu prompt file you've already created, and then click **OK**.
7. Click **OK** to save your changes.

Use the Shell to enable a custom business hours main menu prompt greeting for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables a business hours main menu prompt and uses a custom prompt named `businesshoursprompts.wav` on the UM auto attendant `MyUMAutoAttendant`.

```
Command Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursMainMenuCus
```

This example configures a UM auto attendant named `MyUMAutoAttendant` that has business hours configured to be 10:45 to 13:15 (Sunday), 09:00 to 17:00 (Monday), and 09:00 to 16:30 (Saturday) and holiday times and their associated greetings configured to be "`New Year`" on January 2, 2010, and "`Building Closed for Construction`" from April 24, 2010 through April 28, 2010.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.
```

This example configures a UM auto attendant named `MyAutoAttendant` and enables business hours key mappings so that when callers press 1, they are forwarded to another UM auto attendant named `SalesAutoAttendant`. When they press 2, they are forwarded to extension number 12345 for `Support`, and when they press 3, they are sent to another auto attendant that plays an audio file.

```
Set-UMAutoAttendant -Identity MyAutoAttendant - BusinessHoursKeyMappingEnabled $t
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable a custom business hours main menu prompt greeting for a UM auto attendant, you may also want to:

- Enable a Custom Non-Business Hours Main Menu Prompt Greeting on a UM Auto Attendant
- Enable a Custom Business Hours Welcome Greeting on a UM Auto Attendant
- Enable Business Hours Key Mappings on a UM Auto Attendant

1.9.2.3.1.15 Configure Business Hours for a UM Auto Attendant

Configure Business Hours for a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure business hours for a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. When you configure business hours on a UM auto attendant, you define the hours of the day that your organization is open and the business hours greetings and menu prompts callers will hear when they call an extension number that's configured on the auto attendant. If a caller reaches the auto attendant during hours that are outside the business hours you defined, the caller will hear the non-business hours prompts and greetings.

Several default schedule options are available in the EMC. For example, most businesses are open from 8:00 A.M. to 5:00 P.M., Monday through Friday. Sometimes the default options won't fit your needs and you'll want to customize the schedule. If your business hours vary from one of the schedules defined by the system, you can define a customized schedule for the auto attendant.

By default, the **Always Run** setting is selected. If you leave the **Always Run** setting selected, the UM auto attendant will play the business hours prompts and greetings regardless of the time of day callers dial in to the auto attendant.

Note:

When you set the schedule for business and non-business hours on a UM auto attendant, make sure the time zone is configured correctly.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to specify business hours for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to modify, and then, in the action pane, click **Properties**.
4. On the **Times** tab, under **Schedule Times**, under **Business hours**, select from the available options or select **Use Custom Schedule**.
5. If you select **Use Custom Schedule**, click **Customize**.
6. On the **Schedule** page, select the hours you want to use as your business hours for each day of the week, and then click **OK**.
7. Click **OK** again to save your changes.

Use the Shell to specify business hours for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example sets the business hours for a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you specify business hours for a UM auto attendant, you may also want to:

- Enable a Custom Business Hours Welcome Greeting on a UM Auto Attendant
- Enable Business Hours Key Mappings on a UM Auto Attendant

Configure the Time Zone on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

By default, the Unified Messaging (UM) auto attendant uses the time zone of the Unified Messaging server on which it's created. However, there are situations where you may have to change the time zone for a UM auto attendant to a different time zone. For example, if you've two UM dial plans hosted on the same Unified Messaging server, and each dial plan represents a different time zone, you must configure one auto attendant to have the same time zone as the Unified Messaging server and the other auto attendant to have a time zone that differs from the Unified Messaging server.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to configure the time zone

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Auto Attendants** tab, select the UM auto attendant.
3. In the action pane, click **Properties**.
4. In the auto attendant **Properties** window, click the **Times** tab, and then use the **Select time zone** list to select the time zone for the auto attendant.
5. Click **OK** to accept your changes.

Use the Shell to configure the time zone

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example sets the time zone to the Pacific time zone on a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -TimeZoneName Pacific
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you configure the time zone, you may also want to:

- Configure Business Hours for a UM Auto Attendant
- Enable a Custom Business Hours Main Menu Prompt Greeting on a UM Auto Attendant

1.9.2.3.1.17 Configure a Holiday Schedule for a UM Auto Attendant

Configure a Holiday Schedule for a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can define the dates and times your organization will be closed for holidays and other occasions. Between the start dates and the end dates you specify, callers who reach the Unified Messaging (UM) auto attendant will hear a holiday greeting you specify when you configure the holiday schedule. After the caller hears the holiday greeting you've specified, the non-business hours greeting and menu prompts will be played for the caller.

You can also create a holiday schedule within an existing holiday schedule. When you create multiple holiday schedules, Unified Messaging lets you overlap your scheduled holiday times. For example, you can define a holiday schedule from December 15th through December 31st when your organization will be closed for construction, and you can define another holiday schedule from December 24th through December 26th. When callers call in to the auto attendant from December 15th through December 23rd and from December 27th through December 31st, they'll be presented with the holiday greeting that you've specified for this schedule. For example, "We are currently closed for construction." When callers call in to the auto attendant from December 24th through December 26th, they'll be presented with another holiday greeting, such as "We are currently closed for business so that our employees can enjoy the holidays with their families."

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to specify a holiday schedule for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified**

Messaging.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to modify, and then, in the action pane, click **Properties**.
4. On the **Times** tab, under **Holiday Schedule**, click **Add**.
5. On the **Select Holiday** page, configure the following:
   - **Holiday name** Enter a name for your holiday schedule.
   - **Holiday greeting file** Browse to the .wav file you want to use as your greeting. This is a required field.
   - **Holiday start date** Use this list to select the date you want the holiday to start. The holiday schedule will start at midnight on the date specified in this list.
   - **Holiday end date** Use this list to select the date you want the holiday to end. The holiday schedule will end at 11:59 P.M. on the date specified in this list.
6. After you've configured your holiday schedule, click **OK** twice to save your changes.

Use the Shell to specify a holiday schedule for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example configures a UM auto attendant named `MyUMAutoAttendant` that has business hours configured to be 10:45 to 13:15 (Sunday), 09:00 to 17:00 (Monday), and 09:00 to 16:30 (Saturday) and holiday times and their associated greetings configured to be "New Year" on January 2, 2010, and "Building Closed for Construction" from April 24, 2010 through April 28, 2010.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you specify a holiday schedule for a UM auto attendant, you may also want to:

- Configure Business Hours for a UM Auto Attendant
- Enable an Informational Announcement on a UM Auto Attendant

1.9.2.3.1.18 Configure a Business Name on a UM Auto Attendant

Configure a Business Name on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enter the name of the business. By default, no business name is entered. If you

enter a business name in this box, a prompt with the business name will be played to callers instead of the default greeting for the Unified Messaging (UM) auto attendant.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to configure a business name

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Auto Attendants** tab, select the UM auto attendant.
3. In the action pane, click **Properties**.
4. In the auto attendant **Properties** window, click the **Features** tab, and then in the **Business name** text box, type the name of the business.
5. Click **OK** to accept your changes.

Use the Shell to configure a business name

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example sets the business name on a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessName "Northwind Traders"
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you configure a business name on a UM Auto Attendant, you may also want to:

- Configure a Business Location on a UM Auto Attendant
- Configure Business Hours for a UM Auto Attendant
- Enable a Custom Business Hours Main Menu Prompt Greeting on a UM Auto Attendant

Configure a Business Location on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify the location of a business on a UM auto attendant so that the location will be played for callers. By default, no business location is entered.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to configure a business location

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Auto Attendants** tab, select the UM auto attendant.
3. In the action pane, click **Properties**.
4. In the auto attendant **Properties** window, click the **Features** tab, and then in the **Business location** text box, type the location of the business.
5. Click **OK** to accept your changes.

Use the Shell to configure a business location

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example sets the business location on a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessLocation 'Redmond'
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you configure the business location on a UM auto attendant, you may also want to:

- Configure a Business Name on a UM Auto Attendant
- Configure Business Hours for a UM Auto Attendant
- Enable a Custom Business Hours Main Menu Prompt Greeting on a UM Auto Attendant

1.9.2.3.1.20 Configure the Language Setting on a UM Auto Attendant

Configure the Language Setting on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the language setting on a Unified Messaging (UM) auto attendant. The language setting available on a UM auto attendant enables you to configure the default prompt language on the auto attendant. When you're using the default system prompts for the auto attendant, this is the language that the caller will hear when the auto attendant answers the incoming call. This language setting affects only the default system prompts that are provided after the Unified Messaging server role is installed. However, this setting doesn't affect custom prompts that are configured on an auto attendant. The languages that are available are based on the Unified Messaging language packs that are installed on the Unified Messaging server.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to configure the default language setting

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **Auto Attendants** tab.
3. Click to select the UM auto attendant.
4. In the action pane, click **Properties**.
5. In the auto attendant **Properties** window, click the **Features** tab.
6. On the **Features** tab, in the **Language** list, select the language you want.

Use the Shell to configure the default

language setting

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example sets the default language on the UM auto attendant MyUMAutoAttendant to English (Great Britain).

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -Language en-GB
```

This example sets the default language on the UM auto attendant MyUMAutoAttendant to German.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -Language de-DE
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you configure the default language setting, you may also want to:

- Install a Unified Messaging Language Pack on a UM Server
- Configure the Default Language on a UM Dial Plan

1.9.2.3.1.21 Configure an Operator Extension on a UM Auto Attendant

Configure an Operator Extension on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify an operator extension number for a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. If you configure an operator extension number on a UM auto attendant, you let callers press 0 to reach an operator if they can't navigate the auto attendant menus or don't know which option to use from an auto attendant menu.

If you've created a speech-enabled auto attendant and configured an operator extension on the speech-enabled auto attendant, when a caller says "Operator", the auto attendant will forward the call to the number that's configured on the speech-enabled auto attendant. If the speech-enabled auto attendant is configured to use a dual tone multi-frequency (DTMF) fallback auto attendant but isn't configured to have an operator extension number, the operator extension number on the DTMF fallback auto attendant will be dialed.

At a minimum, we recommend that you configure either the auto attendant or the dial plan associated with the auto attendant to have an operator extension number to help callers find the user they're trying to reach.

Looking for other management tasks related to UM auto attendants? Check out Managing

UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to specify an operator extension for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to modify, and then, in the action pane, click **Properties**.
4. On the **Features** tab, enter a number for the operator extension in the **Operator extension** field.
5. Click **OK** to save your changes.

Use the Shell to specify an operator extension for a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example configures a UM auto attendant named MySpeechEnabledAA with an operator extension of 50100.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -OperatorExtension 50100
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you configure an operator extension number on a UM auto attendant, you may also want to:

- Enable or Disable Operator Transfers After Business Hours on a UM Auto Attendant
- Enable or Disable Operator Transfers During Business Hours on a UM Auto Attendant

Enable or Disable Call Transfers to Users from a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable callers to transfer calls to users. By default, this option is enabled, and lets callers be transferred to users in the Unified Messaging (UM) dial plan that's associated with the UM auto attendant. When this option is enabled, callers can be transferred to UM-enabled users.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable or disable call transfers to users from a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Auto Attendants** tab, select the UM auto attendant.
3. In the action pane, click **Properties**.
4. In the auto attendant **Properties** window, click the **Features** tab, and then select or clear the **Allow callers to transfer to users** check box.
5. If you select this check box, you can set the group of users to whom callers can transfer by selecting the appropriate option under the **Callers can contact** section on this page.

   Note:

   If you disable this option and disable the **Allow callers to send voice message** option, the options under **Callers can contact** are also disabled.

6. Click **OK** to accept your changes.

Use the Shell to enable or disable call transfers to users from a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example disables call transfers on a UM auto attendant named MyUMAutoAttendant.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AllowDialPlanSubscribers $false
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you to have enabled or disabled call transfers from a UM auto attendant, you may also want to:

- Enable or Disable Voice Messages to Be Sent from a UM Auto Attendant
- Enable or Disable Call Transfers to Users on a UM Dial Plan

1.9.2.3.1.23 Enable or Disable Voice Messages to Be Sent from a UM Auto Attendant

Enable or Disable Voice Messages to Be Sent from a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable callers to send voice messages to users from a Unified Messaging (UM) auto attendant, or prevent them from doing so. By default, this option is enabled and lets callers send voice messages to users in the UM dial plan that's associated with the UM auto attendant. If you disable this option, the auto attendant won't invite callers to send a voice message during a system prompt.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable callers to send voice messages or prevent them from doing so

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified**

Messaging.
2. In the work pane, on the **UM Auto Attendants** tab, select the UM auto attendant.
3. In the action pane, click **Properties**.
4. In the auto attendant **Properties** window, click the **Features** tab, and then select or clear the **Allow callers to send voice messages** check box.
5. If you select this check box, you can set the group of users to whom callers can send voice messages by selecting the appropriate option under the **Callers can contact** section on this page.

Note:
If you disable this option and disable the **Allow caller to transfer to users** option, the options under **Callers can contact** are also disabled.

1. Click **OK** to accept your changes.

Use the Shell to enable callers to send voice messages or prevent them from doing so

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example prevents callers who call in to a UM auto attendant named `MyUMAutoAttendant` from sending voice messages.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -SendVoiceMsgEnabled $false
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable callers to send voice messages on a UM auto attendant or prevent them from doing so, you may want to:

- Enable or Disable Call Transfers to Users from a UM Auto Attendant
- Configure the Scope of Users that Callers Can Contact on a UM Auto Attendant

1.9.2.3.1.24 Configure the Scope of Users that Callers Can Contact on a UM Auto Attendant

Configure the Scope of Users that Callers Can Contact on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify the grouping of users that callers can contact when calling into a Unified Messaging (UM) auto attendant. By default, callers can contact users within the same dial plan that's associated with the UM auto attendant. However, you can change the

grouping of users to allow callers to transfer calls or send voice messages to users who are located in the global address list (GAL) or to a specific set of users who are contained in custom address lists.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to configure the scope of users that callers can contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Auto Attendants** tab, select the UM auto attendant.
3. In the action pane, click **Properties**.
4. In the auto attendant **Properties** window, click the **Features** tab and then, under **Callers can contact**, choose from the following options:
   Users within dial plan Select this option to allow callers who connect to the UM auto attendant to locate and contact users who are in the dial plan associated with the UM auto attendant.
   Anyone in the default global address list Select this option to allow callers who connect to the UM auto attendant to locate and contact anyone listed in the GAL. This includes all users who are mailbox-enabled.
   Anyone in this address list Select this option to allow callers who connect to the UM auto attendant to locate and contact users who are in a defined custom address list. This includes all users who are mailbox-enabled.

   Important:

   The **All Address Lists** container is an empty container object and differs from the GAL container. If you choose the **All Address Lists** container when you browse for a custom address list, there will be no UM-enabled users for callers to contact. If you want to select all the address lists in your organization, choose the **Anyone in the default global address list** option.
5. Click **OK** to accept your changes.

Use the Shell to configure the scope of users that callers can contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example sets the scope of the users that callers can contact to all users in the Global Address List on a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -ContactScope GlobalAddressList
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you configure the scope of users that callers can contact on a UM Auto Attendant, you may also want to:

- Enable Dialing Restrictions on a UM Auto Attendant
- Enable or Disable Directory Lookups for a UM Auto Attendant

1.9.2.3.1.25 Configure the Matched Name Selection Method on a UM Auto Attendant

Configure the Matched Name Selection Method on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the matched name selection method setting on the auto attendant's **Features** tab, or you can leave the default setting on the auto attendant and then configure this setting on the dial plan associated with the auto attendant. By default, an auto attendant can't disambiguate between two or more users who have the same name because the default setting for the matched name selection method on the dial plan is set to **None**.

Note:

For the matched name selection method to work correctly, you must populate the title, department, and location boxes on the recipients in your Microsoft Exchange organization.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created.
- A UM auto attendant has been created.

Use the EMC to configure the matched name selection method on a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.

2. In the work pane, on the **UM Auto Attendants** tab, select the UM auto attendant you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, on the **Features** tab, under **Matched name selection method**, select one of the following values:
   - **Title** The auto attendant will include each user's title when it lists matches.
   - **Department** The auto attendant will include each user's department when it lists matches.
   - **Location** The auto attendant will include each user's location when it lists matches.
   - **None** The auto attendant won't include any additional information when it lists matches.
   - **Prompt For Alias** The auto attendant will prompt the caller for the user's alias.
   - **Inherit from dial plan** The auto attendant will use the default setting from the dial plan associated with the auto attendant.
4. Click **OK** to save your changes.

Use the Shell to configure the matched name selection method on a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example sets the matched name selection method to Prompt for Alias for a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -MatchedNameSelectionMethod Promp
```

This example sets the matched name selection method to the title of the users, enables name lookups, and enables callers that dial into the auto attendant to press * to be presented with the Outlook Voice Access welcome greeting for a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -MatchedNameSelectionMethod Title
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you configure the matched name selection method setting on the auto attendant, you may also want to Configure the Matched Name Selection Method on a UM Dial Plan.

1.9.2.3.1.26 Enable or Disable Operator Transfers After Business Hours on a UM Auto Attendant

Enable or Disable Operator Transfers After Business Hours on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable users to transfer calls to an operator during non-business hours in Microsoft Exchange Server 2010 Unified Messaging (UM). You can also disable operator transfers during non-business hours. You enable users to transfer calls during non-business hours by configuring an operator extension number on a UM auto attendant, selecting the **Allow transfer to operator after business hours** setting, and configuring business hours on the **Times** tab on the UM auto attendant.

At a minimum, we recommend that you configure either the UM auto attendant or the UM dial plan associated with the auto attendant to have an operator extension number. This will help callers find the user they're trying to reach or navigate the menu system.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable callers to transfer calls to an operator after business hours

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the UM auto attendant you want to change and then, in the action pane, click **Properties**.
4. On the **Features** tab, next to **Operator extension**, enter a number for your auto attendant operator.
5. Select the check box next to **Allow transfer to operator after business hours**.
6. Click **OK** to save your changes.

Use the EMC to prevent callers from transferring calls to an operator after business hours

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the UM auto attendant that you want to modify and then, in the action pane, click **Properties**.
4. Clear the check box next to **Allow transfer to operator after business hours**.
5. Click **OK** to save your changes.

Use the Shell to enable or disable operator transfers after business hours

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables callers to transfer calls to an operator after business hours.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -OperatorExtension 50100 -AfterHo
```

This example prevents callers from transferring calls to an operator after business hours.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -AfterHoursTransferToOperatorEnab
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable or disable operator transfers after business hours, you may also want to:

- Configure an Operator Extension on a UM Auto Attendant
- Enable or Disable Operator Transfers During Business Hours on a UM Auto Attendant

1.9.2.3.1.27 Enable or Disable Operator Transfers During Business Hours on a UM Auto Attendant

Enable or Disable Operator Transfers During Business Hours on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable users to transfer calls to an operator during business hours in Microsoft Exchange Server 2010 Unified Messaging (UM), or prevent them from doing so. You enable users to transfer calls during business hours by setting up an operator extension number on a UM auto attendant and selecting the **Allow transfer to operator during business hours** setting.

At a minimum, we recommend that you configure either the UM auto attendant or the UM dial plan associated with the auto attendant to have an operator extension number. This will help callers find the user they're trying to reach or navigate the menu system.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

Also, before you perform these procedures, confirm the following:

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable callers to transfer calls to an operator during business hours

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the UM auto attendant you want to change and then, in the action pane, click **Properties**.
4. On the **Features** tab, next to **Operator extension**, enter a number for your auto attendant operator.
5. Select **Allow transfer to operator during business hours**.
6. Click **OK** to save your changes.

Use the EMC to prevent callers from transferring calls to an operator during business hours

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the UM auto attendant you want to change, and then, in the action pane, click **Properties**.
4. Clear the check box next to **Allow transfer to operator during business hours**.
5. Click **OK** to save your changes.

Use the Shell to enable or prevent operator transfers during business hours

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables callers to transfer calls to an operator during business hours.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -OperatorExtension 50100 -Busines
```

This example prevents callers from transferring calls to an operator during business hours.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -BusinessHoursTransferToOperatorE
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable or disable operator transfers during business hours, you may also want to:

- Configure an Operator Extension on a UM Auto Attendant
- Enable or Disable Operator Transfers After Business Hours on a UM Auto Attendant

1.9.2.3.1.28 Enable Business Hours Key Mappings on a UM Auto Attendant

Enable Business Hours Key Mappings on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable business hours key mappings for a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. After you create a UM auto attendant, a default system prompt will be used for the business hours main menu prompt greeting callers hear after the business hours welcome greeting is played. The default business hours main menu prompt says, "Welcome to the Microsoft Exchange Auto Attendant." Because no key mappings are defined by default, no menu options are available to callers, and they hear only the default main menu prompt.

When you configure key mappings, you define the options and the operations that will be performed if a caller speaks a phrase while they're using a speech-enabled auto attendant or the caller presses the key on the keypad of the telephone while they're using an auto attendant that isn't speech-enabled.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable business hours key mappings on a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to change, and then, in the action pane,

click **Properties**.
4. On the **Key Mapping** tab, select **Enable business hours key mapping**, and then click **Add**.
5. On the **Key Mapping Entry** page, in the **Name** field, type a name for the key mapping entry.
6. In **If the user does one of the following**, select one of these options:
   - **Presses this key**
   - **Presses no key (Time-out)**
   - **Or the user says this phrase**
7. In **This Action will occur**, select from these options:
   - **Play the following audio file**
   - **Transfer to extension**
   - **Run auto attendant**
8. Click **OK** to create the key mapping entry.
9. Click **OK** to save your changes.

Use the Shell to enable business hours key mappings on a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example configures a UM auto attendant named `MyAutoAttendant` and enables business hours key mappings so that when callers press 1, they're forwarded to another UM auto attendant named `SalesAutoAttendant`. When they press 2, they're forwarded to extension number 12345 for Support, and when they press 3, they're sent to another auto attendant that plays an audio file.

```
Set-UMAutoAttendant -Identity MyAutoAttendant - BusinessHoursKeyMappingEnabled $t
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable business hours key mappings on a UM auto attendant, you may also want to:

- Enable Non-Business Hours Key Mappings on a UM Auto Attendant
- Configure Key Mapping Entries on a UM Auto Attendant

1.9.2.3.1.29 Enable Non-Business Hours Key Mappings on a UM Auto Attendant

Enable Non-Business Hours Key Mappings on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable non-business hours key mappings for a Unified Messaging (UM) auto

attendant in Microsoft Exchange Server 2010. After you create a UM auto attendant, a default system prompt will be used for the non-business hours main menu prompt greeting that callers hear after the non-business hours welcome greeting is played. The default non-business hours main menu prompt says, "Welcome to the Microsoft Exchange After Hours Auto Attendant." Because no key mappings are defined by default, no menu options are available to callers and they hear only the default non-business hours main menu prompt.

When you configure key mappings, you define the options and the operations that will be performed if callers speak a phrase while they're using a speech-enabled auto attendant or callers press the key on the keypad of the telephone while they're using an auto attendant that isn't speech-enabled.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the EMC to enable non-business hours key mappings on a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the auto attendant you want to change, and then, in the action pane, click **Properties**.
4. On the **Key Mapping** tab, select **Enable non-business hours key mapping**, and then click **Add**.
5. On the **Key Mapping Entry** page, in the **Name** field, type a name for the key mapping entry.
6. In **If the user does one of the following**, select one of these options:
   - **Presses this key**
   - **Presses no key (Time-out)**
   - **Or the user says this phrase**
7. In **This Action will occur**, select one of these options:
   - **Play the following audio file**
   - **Transfer to extension**
   - **Run auto attendant**
8. Click **OK** to create the key mapping entry.
9. Click **OK** to save your changes.

Use the Shell to enable non-business hours key mappings on a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example configures a UM auto attendant named `MyAutoAttendant` and enables non-business hours key mappings so that when callers say "After Hours" they will be forwarded to extension number 12345, and if they say "Directions" they will be forwarded to extension number 23456.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AfterHoursKeyMappingEnabled $tru
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable non-business hours key mappings on a UM auto attendant, you may also want to:

- Enable Business Hours Key Mappings on a UM Auto Attendant
- Configure Key Mapping Entries on a UM Auto Attendant

1.9.2.3.1.30 Configure Key Mapping Entries on a UM Auto Attendant

Configure Key Mapping Entries on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the **Key Mapping Entry** dialog box to configure single or multiple key mappings for business or non-business hours main menu prompts for Unified Messaging (UM) auto attendants. You can define the operation that will be performed when the key on the telephone keypad is pressed, for example, transferring the call to an extension number or another auto attendant.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Use the EMC to configure UM auto attendant key mappings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

Use the **Key Mapping Entry** dialog box to configure key mappings for a UM auto attendant. You can configure the following:

- **Description** Use this field to type the name of the key mapping entry. The key mapping name is used for display purposes only. This is a required field, and you must provide a display name for the key mapping entry.
  Because you may want to specify multiple key mappings, we recommend that you use meaningful names for your key mappings. The maximum length of the

name for the key mapping is 64 characters, and it can include spaces. However, it can't include any of the following characters: " / \ [ ] : ; | = , + * ? < >.

- **If the user does one of the following:**
  - **Press this key** Use this button to enable a key mapping. The key mapping is the number key that a caller presses to have the auto attendant perform a specific operation, for example, forwarding the caller to another auto attendant or to an operator. By default, no entries are defined.

    Use the text box to type the numeric key (from 1 through 9) that the caller must press. Zero (0) is reserved for the auto attendant operator.
  - **Presses no key (time-out)** Use this button to enable callers to be transferred to an extension number or to another auto attendant if they don't press a key on the telephone keypad. For example, "Please stay on the line and your call will be answered by the next available representative." By default, this option is disabled. The default setting is 5 seconds.

    If you enable this option, a blank key mapping will be created.
- **Or the user says this phrase** Use this field with speech-enabled auto attendants. This option enables you to define words or phrases that can be spoken by a caller. After the caller says the word or phrase, then the auto attendant will perform an action that you specify.
- **This action will occur** Use one of the following actions to define the action that you want the auto attendant to perform for the caller.
  - **Play the following audio file** Select this check box to enable an audio file to play when callers press the key specified in the **Key pressed** setting. By default, this setting is disabled. If you enable this option, specify an audio file:

    Click **Browse** to locate the audio file that you want to play. If you enable this option, the audio file that you specify here will be played to the caller after the business hours or non-business main menu prompt plays.
  - **Perform this additional action** Use one of the following actions to define additional actions that you want the auto attendant to perform for the caller.

    Transfer to extension Select this check box to enable calls to be transferred to an extension number or another auto attendant. If you enable this option, specify an extension or auto attendant.Use the text box to type the extension where the call will be transferred. This field allows only numeric characters. It can't include any of the following characters: " / \ [ ] : ; | = , + * ? < >.

    Run auto attendant Click this button to transfer the call to an auto attendant. Click **Browse** to locate the auto attendant that you want to use. Before you enable this option, you must first create and configure the auto attendant. This option is used when you create a parent/child structure of UM auto attendants.

    Leave voice mail for Click this option to enable a caller to leave a voice mail message for a UM-enabled mailbox that's on the same dial plan as the UM auto attendant that you're configuring. When a caller chooses this option from an auto attendant menu, they'll be prompted to leave a voice mail for the UM-mailbox that was selected. Click **Browse** to locate the UM-enabled mailbox.

    Announce business location Click this option to enable a caller to choose an auto attendant menu option and hear the location of the business that's configured on the UM auto attendant. To enable this to work correctly, you must first enter the business location in the **Business location** box on the **Features** tab on the UM auto attendant.

    Announce business hours Click this option to enable a caller to choose an auto attendant menu option and hear the hours of

operation for the business that's configured on the UM auto attendant. To enable this to work correctly, you must first configure the business hours in the **Business hours** drop down list on the **Times** tab on the UM auto attendant. You can optionally choose preconfigured business times using the drop down or click the **Customize** button and configure other business times. It's also important to correctly configure the time zone using the **Select time zone** drop down for the auto attendant.

Use the Shell to configure UM auto attendant key mappings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables business hours key mappings so that:

- When callers press 1, they will be forwarded to another UM auto attendant named `SalesAutoAttendant`.
- When they press 2, they will be forwarded to extension number 12345 for Support.
- When they press 3, they will be sent to another auto attendant that will play an audio file.

```
Set-UMAutoAttendant -id MyAutoAttendant -BusinessHoursKeyMappingEnabled $true -Bu
```

This example sets key mappings defined in a comma-separated value (.csv) file. You must first create the .csv file with the following headings and the correct entry: <key>,<description>,[<extension>],[<autoattendant name>],[<promptfilenamepath>], [<asrphrase1;asrphrase2>],[<leavevoicemailfor>],[<transfertomailbox>]. The values in brackets are optional. After creating the .csv file, import the .csv file using the **Import-csv** cmdlet.

```
$o = Import-csv -path "C:\UMFiles\AutoAttendants\keymappings.csv"
Set-UMAutoAttendant MyAutoAttendant -BusinessHoursKeyMapping $o
```

This example exports key mappings from an existing UM auto attendant into a .csv file, and then imports the same key mappings into another UM auto attendant. You could also export the key mappings to a .csv file, edit or modify the key mappings in the .csv file, and then import those key mappings into another UM auto attendant.

```
$aa = Get-UMAutoAttendant -id MyAutoAttendant
$aa1 = Get-UMAutoAttendant -id MyAutoAttendant2
$aa.BusinessHoursKeyMapping | Export-csv -path "C:\UMFiles\AutoAttendants\keymapp
$aa1.BusinessHoursKeyMapping = (Import-csv -path "C:\UMFiles\AutoAttendants\keyma
```

Other Tasks

After you configure UM auto attendant key mappings, you may also want to:

- Enable Business Hours Key Mappings on a UM Auto Attendant
- Configure Business Hours for a UM Auto Attendant
- Enable Non-Business Hours Key Mappings on a UM Auto Attendant

Enable Dialing Restrictions on a UM Auto Attendant

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable dialing restrictions on a Unified Messaging (UM) auto attendant in Microsoft Exchange Server 2010. Dialing restrictions are used to enable dialing rules that can be used to prohibit users who call into a UM auto attendant from making certain types of telephone calls that are known as outdialing. Outdialing is the process that happens when a Unified Messaging server places an outgoing call for users after they've called into a subscriber access number on a UM dial plan or into a UM auto attendant.

When you enable dialing restrictions, the following settings must be configured correctly:

- **Dialing group rules** Dialing group rules determine the types of calls users within a dial group can make.
- **Dialing rule entries** Dialing rule entries define the number that is dialed by the UM-enabled user and the actual number that will be dialed by the Private Branch eXchange (PBX) or IP PBX.
- **Dialing restrictions** Dialing restrictions determine the restrictions that will be applied to prevent users from incurring unnecessary telephone charges or from dialing long distance calls.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.
- A UM dialing rule group has been created. For detailed steps, see Configure Dialing Rule Groups on a UM Dial Plan.

Use the EMC to enable dialing restrictions on a UM auto attendant for in-country/region rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the UM auto attendant you want to change, and then, in the action pane, click **Properties**.
4. On the UM auto attendant **Properties** page, on the **Dialing Restrictions** tab, under **Select allowed in-country/region rule groups from dial plan**, click **Add**.
5. On the **Select Allowed In-Country/Region Groups** page, select the dialing rule group that is enabled on the UM dial plan, and then click **OK**.

6. Click **OK** to save your changes.

Use the EMC to enable dialing restrictions on a UM auto attendant for international rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Auto Attendants** tab.
3. Select the UM auto attendant you want to modify, and then, in the action pane, click **Properties**.
4. On the UM auto attendant **Properties** page, on the **Dialing Restrictions** tab, under **Select allowed international rule groups from dial plan**, click **Add**.
5. On the **Select Allowed International Groups** page, select the dialing rule group that is enabled on the UM dial plan, and then click **OK**.
6. Click **OK** to save your changes.

Use the Shell to enable in-country/region and international dialing restrictions on a UM auto attendant

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables the InCountry/RegionGroup1, InCountry/RegionGroup2. InternationalGroup1, and InternationalGroup2 dialing restrictions on a UM auto attendant named `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AllowedInCountryOrRegionGroups I
```

For more information about syntax and parameters, see Set-UMAutoAttendant.

Other Tasks

After you enable dialing restrictions on a UM auto attendant, you may also want to:

- Configure Dialing Rule Groups on a UM Dial Plan
- Create a Dialing Rule Entry on a UM Dial Plan

1.9.2.3.2 Managing UM Dial Plans

Managing UM Dial Plans

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-18*

Create a UM Dial Plan

View or Configure the Properties of a UM Dial Plan

Delete a UM Dial Plan

Prevent UM-Enabled Users from Receiving Faxes on a UM Dial Plan

Enable UM-Enabled Users to Receive Faxes on a UM Dial Plan

Allow or Prevent Call Answering Rules on a UM Dial Plan

Configure VoIP Security on a UM Dial Plan

Enable a Custom Welcome Greeting on a UM Dial Plan

Enable an Informational Announcement on a UM Dial Plan

Configure a Subscriber Access Number on a UM Dial Plan

Configure Dial Codes on a UM Dial Plan

Enable or Disable Sending Voice Messages on a UM Dial Plan

Enable or Disable Call Transfers to Users on a UM Dial Plan

Configure the Scope of Users Who Callers Can Contact on a UM Dial Plan

Configure the Matched Name Selection Method on a UM Dial Plan

Configure the Dial by Name Primary Method on a Unified Messaging Dial Plan

Configure the Dial by Name Secondary Method on a UM Dial Plan

Configure the Audio Codec on a UM Dial Plan

Configure an Operator Extension on a UM Dial Plan

Configure the Number of Logon Failures Before Users Are Disconnected on a UM Dial Plan

Configure the Maximum Call Duration on a UM Dial Plan

Configure the Maximum Recording Duration on a UM Dial Plan

Configure the Recording Idle Time-Out Value on a UM Dial Plan

Configure the Input Failures Before Disconnect on a UM Dial Plan

Configure the Default Language on a UM Dial Plan

Configure Dialing Rule Groups on a UM Dial Plan

Create a Dialing Rule Entry on a UM Dial Plan

Enable Dialing Restrictions on a UM Dial Plan

Enable Custom Prompt Recording Using the Telephone User Interface

Import and Export Custom Prompts for Unified Messaging

1.9.2.3.2.1 Create a UM Dial Plan

Create a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-10*

A Unified Messaging (UM) dial plan is created by using an organization-wide scope. This dial plan contains configuration information related to your telephony network. It also establishes a link from the telephone extension number of a Microsoft Exchange Server 2010 recipient in Active Directory to a UM-enabled mailbox.

When you create a UM dial plan, you can configure the number of digits in the extension numbers, the Uniform Resource Identifier (URI) type, and the Voice over IP (VoIP) security setting. Every time that you create a UM dial plan, a UM mailbox policy is also created. The UM mailbox policy is named *<DialPlanName>* Default Policy.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

What Do You Want to Do?

- Use the EMC to create a UM dial plan
- Use the Shell to create a UM dial plan

Use the EMC to create a UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the action pane, click **New UM Dial Plan**.
3. In the New UM Dial Plan wizard, complete the following fields:
   - **Name** Type the name of the dial plan. A UM dial plan name is required and must be unique. However, it's used only for display in the EMC and the Shell. If you have to change the display name of the dial plan after it's been created, you must first delete the existing UM dial plan and then create another dial plan that has the appropriate name. If your organization uses multiple UM dial plans, we recommend that you use meaningful names for your UM dial plans. The maximum length of a UM dial plan name is 64 characters. The name can't include any of the following characters:

     ```
     " / \ [ ] : ; | = , + * ? < >
     ```

     Although you can include spaces in the name of a new UM dial plan, the name cannot include spaces if you integrate Unified Messaging with Office Communications Server 2007 R2 or Microsoft Lync Server. Therefore, if you created a dial plan that has spaces in the display name, and if you are integrating with

Office Communications Server 2007 R2 or Microsoft Lync Server, you must first delete that dial plan, and then create another by using a display name that does not include spaces.

Important:

Although the field for the name of the dial plan can accept 64 characters, the name of the dial plan can't be longer than 49 characters. If you try to create a dial plan name that contains more than 49 characters, you will receive an error message. The message will say that the dial plan name couldn't be created because a default UM mailbox policy name couldn't be generated because the UM dial plan name is too long. This happens because when you create a dial plan, a default UM mailbox policy is also created that has the name *<DialPlanName>* Default Policy. Therefore, the name of the UM mailbox policy is 15 characters longer than the name of the dial plan. The *name* parameter for both the UM dial plan and UM mailbox policy can be 64 characters. However, if the name of the dial plan is longer than 49 characters, the name of the default UM mailbox policy will be longer than 64 characters, and this isn't allowed by the system.

- **Number of digits in extension numbers** Enter the number of digits for the dial plan. The number of digits for extension numbers is based on the telephony dial plan created on a Private Branch eXchange (PBX). For example, if a user associated with a telephony dial plan dials a four-digit extension to call another user in the same telephony dial plan, you select 4 as the number of digits in the extension.

  This is a required field that has a value range from 1 through 20. The typical extension length is from 3 through 7. If your existing telephony environment includes extension numbers, you must specify a number of digits that matches the number of digits in those extensions.

  When you create a Session Initiation Protocol (SIP) or an E.164 dial plan and associate a UM-enabled user with the dial plan, you must still input an extension number to be used by the user. This number is used by Outlook Voice Access users when they access their Exchange 2010 mailbox.
- **URI Type** Use this drop-down list to select the URI type for the UM dial plan. A URI is a string of characters that identifies or names a resource. The main purpose of this identification is to enable VoIP devices to communicate with other devices over a network using specific protocols. URIs are defined in schemes that define a specific syntax, format, and the protocols for the call.

  You can select one of the following URI types for the dial plan:

  Telephone extension This is the most common URI type. The calling and called party information from the IP gateway or IP PBX will be listed in one of the following formats: Tel:512345 or 512345@*<IP address>*. This is the default URI type for dial plans.

  SIP URI Use this URI type if you need a SIP URI dial plan when an IP PBX supports SIP routing or if you're integrating Microsoft Office Communications Server 2007 and Exchange Unified Messaging. The calling and called party information from the IP gateway or IP PBX will be listed as a SIP address in the following format: sip:*<username>*@*<domain* or *IP address>*:Port.

  E.164 E.164 is an international numbering plan for public telephone systems in which each assigned number contains a country/region code, a national destination code, and a subscriber number. The calling and called party information sent from the IP gateway is listed in the following format: Tel:+14255550123.

Note:
After you create a dial plan, you will be unable to change the URI type without deleting the dial plan, and then re-creating the dial plan to include the correct URI type.

- **VoIP Security** Use this drop-down list to select the VoIP security setting for the UM dial plan. By default, when you create a UM dial plan, it communicates in unsecured mode. A Unified Messaging server can operate in any mode configured on a dial plan because the Unified Messaging server is configured to listen on TCP port 5060 for unsecured requests and on TCP port 5061 for secured requests at the same time.
  You can select one of the following security settings for the dial plan:
  Unsecured By default, when you create a UM dial plan, it communicates in unsecured mode, and the Unified Messaging servers associated with the UM dial plan send and receive data from IP gateways, IP PBXs, and other Exchange 2010 computers using no encryption. In unsecured mode, both the Realtime Transport Protocol (RTP) media channel and SIP signaling information aren't encrypted.
  SIP secured When you select **SIP secured**, only the SIP signaling traffic is encrypted, and the RTP media channels still use TCP, which isn't encrypted. Mutual Transport Layer Security (TLS) is used to encrypt the SIP signaling traffic.
  Secured When you select **Secured**, both the SIP signaling traffic and the RTP media channels are encrypted. An encrypted signaling media channel that uses Secure Realtime Transport Protocol (SRTP) also uses mutual TLS to encrypt the VoIP data.
- **Country/Region code** Use this field to type the country/region code number used for outgoing calls. This number will precede the telephone number dialed. This field accepts from 1 through 4 digits. For example, in the United States, the country/region code is 1. In the United Kingdom, it's 44.

4. On the **Set UM Servers** page, click **Add**, and then, on the **Select UM Server** page, select the UM server that you want to add to the UM dial plan.

5. On the **Completion** page, confirm whether the dial plan was successfully created:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to complete the New UM Dial Plan wizard.

Use the Shell to create a UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example creates a new UM dial plan named `MyUMDialPlan` that uses four-digit extension numbers.

```
New-UMDialplan -Name MyUMDialPlan -NumberofDigits 4
```

This example creates a new UM dial plan named `MyUMDialPlan` that uses five-digit extension numbers and supports SIP URIs:

```
New-UMDialplan -Name MyUMDialPlan -UriType SIPName -NumberofDigits 5
```

For more information about syntax and parameters, see New-UMDialplan.

Other Tasks

After you enable a user for Unified Messaging, you may also want to:

- Add a UM Server to a Dial Plan
- Create a UM Auto Attendant

For More Information

Understanding Unified Messaging Dial Plans

Understanding Unified Messaging VoIP Security

1.9.2.3.2.2 View or Configure the Properties of a UM Dial Plan

View or Configure the Properties of a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

After you create a Unified Messaging (UM) dial plan, you can view and configure a variety of settings. For example, you can configure the level of Voice over IP (VoIP) security, the audio codec, and dialing restrictions. The settings that you configure on the UM dial plan affect all users who are associated with the dial plan through a UM mailbox policy.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

What Do You Want to Do?

- Use the EMC to view or configure UM dial plan properties
- Use the Shell to configure UM dial plan properties
- Use the Shell to view UM dial plan properties

Use the EMC to view or configure UM dial plan properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Dial Plans** tab, and then select the UM dial plan that you want to configure.
3. In the action pane, click **Properties**.

4. Use the **General** tab to view specific dial plan settings or enable or disable

features for UM-enabled users:

- **Associated UM servers** This section displays the Unified Messaging servers associated with a dial plan. The Unified Messaging servers listed in this section process incoming calls for users who are associated with the dial plan. Unified Messaging servers can be associated with single or multiple dial plans. You must use the **UM Server Settings** properties tab in the Unified Messaging server's properties to add a Unified Messaging server to a dial plan.
- **Associated UM IP gateways** This section displays the UM IP gateways associated with a dial plan. The UM IP gateways listed in this section process incoming calls for users who are associated with the dial plan. A UM hunt group establishes a link between a UM dial plan and a UM IP gateway and can also be associated with a dial plan by first being associated with a UM IP gateway. You can associate a UM IP gateway with a dial plan when you create a UM hunt group.
- **URI type** A Uniform Resource Identifier (URI) is a string of characters that identifies or names a resource. The main purpose of this identification is to enable VoIP devices to communicate with other devices over a network using specific protocols. URIs are defined in schemes that define a specific syntax and format and the protocols for the call. After you create a UM dial plan, you won't be able to change the URI type without deleting the dial plan, and then re-creating the dial plan to include the correct URI type. You can select one of the following URI types for the dial plan:

  Telephone extension This is the most common URI type. The calling and called party information from the IP gateway or IP Private Branch eXchange (PBX) is listed in one of the following formats: Tel:512345 or 512345@<*IP address*>. This is the default URI type for dial plans.

  SIP URI Use this URI type if you must have a Session Initiation Protocol (SIP) URI dial plan such as an IP PBX that supports SIP routing or if you're integrating Microsoft Office Communications Server 2007 and Microsoft Exchange Server 2010 Unified Messaging. The calling and called party information from the IP gateway or IP PBX is listed as a SIP address in the following format: sip:<*username*>@<*domain* or *IP address*>:Port.

  E.164 E.164 is an international numbering plan for public telephone systems in which each assigned number contains a country code, a national destination code, and a subscriber number. The calling and called party information sent from the IP gateway is listed in the following format: Tel:+14255550123.
- **Number of digits in the extension** This is the number of digits in the extension numbers for users who are associated with this dial plan. For example, if a user associated with a dial plan dials a 4-digit extension to call another user in the same dial plan, select 4 as the number of digits in the extension.

  The number of digits for extension numbers is based on the telephony dial plan created on a PBX. This is a required field that has a value range from 1 through 20. The typical extension length is from 3 through 7 digits. If your existing telephony environment includes extension numbers, you must specify a number of digits that matches the number of digits in those extensions when you create the UM dial plan.
- **Modified** This field shows the last date and time the dial plan settings were modified.
- **Allow users to receive faxes** Select this check box to allow fax messages to be received by users who are associated with the dial plan. If you don't select this check box, all users who are associated with the dial plan won't be able to receive fax messages in their Inbox. By default, this setting is enabled.
- **Allow user to configure call answering rules** Select this check box to

allow users associated with the dial plan through a UM mailbox policy to be able to create and configure call answering rules. When this setting is selected, UM-enabled users can create rules or actions and apply conditions to an incoming call to their phone number. They can transfer the call, have the caller leave a voice mail, or allow the caller to locate them at a different phone number.

- **VoIP security** Use this drop-down list to select the VoIP security setting for the UM dial plan. You can select one of the following security settings for the dial plan:

  Unsecured By default, when you create a UM dial plan, it communicates in an unsecured mode, and the Unified Messaging servers associated with the UM dial plan send and receive data from IP gateways, IP PBXs, and other Exchange 2010 computers using no encryption. In unsecured mode, both the Realtime Transport Protocol (RTP) media channel and SIP signaling information aren't encrypted.

  SIP secured When you select **SIP secured**, only the SIP signaling traffic is encrypted, and the RTP media channels still use TCP, which isn't encrypted. Mutual Transport Layer Security (TLS) is used to encrypt the SIP signaling traffic.

  Secured When you select **Secured**, both the SIP signaling traffic and the RTP media channels are encrypted. A secure signaling media channel that uses Secure Realtime Transport Protocol (SRTP) also uses mutual TLS to encrypt the VoIP data. A Unified Messaging server can operate in any mode configured on a dial plan because the Unified Messaging server is configured to listen on TCP port 5060 for unsecured requests and TCP port 5061 for secured requests at the same time.

5. Use the **Subscriber Access** tab of the UM dial plan that you have selected to configure subscriber access settings for the UM dial plan. A subscriber is an internal business user or network user who is enabled for Exchange 2010 Unified Messaging. Outlook Voice Access enables subscribers to access their individual mailboxes to retrieve e-mail, voice messages, contacts, and calendaring information using a telephone. You can view or configure the following:

   - **Welcome greeting** This display-only field shows the name of the sound file that will be used for the welcome greeting. Click **Modify** to specify the audio (.wav) file to use for the welcome greeting. If you don't specify an audio file, callers will hear a default welcome greeting that says, "Welcome, you are connected to Microsoft Exchange."

     The welcome greeting is used when Outlook Voice Access users or another caller calls the subscriber access number. This audio file is the default greeting for a specific UM dial plan. However, you may want to change this greeting and provide another welcome greeting specific to your company, such as, "Welcome to Outlook Voice Access for Contoso, Ltd."

     If you decide to customize this greeting, you must first record the customized greeting, save it as a *.wav file, and then configure the dial plan to use this customized greeting. The file name and path must not exceed 255 characters.

     You can configure a customized business hours greeting by clicking **Modify** to select a previously recorded custom greeting file. You can select one of the following:

     Use default greeting Use this option to enable the default welcome greeting to be played to callers. By default, this option is enabled.

     Use custom greeting file Use this option when you want to enable a custom welcome greeting file to be played to callers. Click **Browse** to locate a custom welcome greeting file that was

previously recorded.

- **Informational announcement** When enabled, this optional recording plays immediately after the business or non-business hours greeting. An informational announcement may state the organization's hours of operation, for example, "Our business hours are 8:30 A.M. to 5:30 P.M., Monday through Friday and 8:30 A.M. to 1:00 P.M. on Saturday." An informational announcement can also provide information that's required for compliance with company policy, for example, "Calls may be monitored for training purposes." If it's important that callers hear the whole informational announcement, it can be marked as uninterruptible.

  By default, there's no informational announcement configured on UM dial plans or auto attendants. Use the following options to enable an informational announcement and use a custom audio file specific to your organization. The recordings must have already been recorded as .wav files. You can select the following:

  Disable announcement Use this option to disable an informational announcement. By default, this option is enabled.

  Informational announcement file Use this option when you want to enable an informational announcement to be played to callers. Click **Browse** to locate a custom informational announcement file that was previously recorded.

  Allow informational announcement to be interrupted Use this option to enable the informational announcement to be interrupted by the caller. This should be enabled if you have long informational announcements. Callers may become frustrated if the informational announcement is long and they can't interrupt the informational announcement to access the options provided by the UM dial plan or auto attendant.
- **Enter the telephone number to associate** Use this field to add a telephone number or extension that a user will call to access the Unified Messaging system using Outlook Voice Access. In most cases, you enter an extension number or an external telephone number. However, because this field accepts alphanumeric characters, a SIP URI can be used if you're using an IP PBX.

  By default, when a dial plan is created, no subscriber access numbers are configured. To enable subscriber access, you must configure at least one telephone number. The number of alphanumeric characters can't exceed 20.

  When you configure this number on the dial plan, this number will be displayed in the Microsoft Office Outlook 2007 and Outlook Web App for Exchange 2010 voice mail options.

6. Use the **Dial Codes** tab to configure the dial codes for a UM dial plan. Several dial code settings can be configured on the dial plan. These include incoming and outgoing calling options. You can configure the following:
   - **Outside line access code** Use this field to type the number or numbers used to access an outside telephone number for outgoing external calls. This number will precede the telephone number dialed. This is also called a trunk access code. This field accepts from 1 through 16 digits. For many organizations, this number is 9. By default, this field isn't populated.

     Frequently, this setting is used in telephony environments where a PBX is located onsite or maintained in an organization. It may not have to be configured if your organization's telephony environment is maintained by an external business or vendor.
   - **International access code** Use this field to type the number code used to access international telephone numbers for outgoing calls. This number will precede the telephone number dialed. By default, this field isn't populated. This field accepts from 1 through 4 digits. For example, the international

access code for the United States is 011. For Europe, it's 00.

- **National number prefix** Use this field to type the number code used to dial telephone numbers that are out of an area code but within the country/region. This number will precede the telephone number dialed. By default, this field isn't populated. This field accepts from 1 through 4 digits. For example, 0 is used in Europe, and 1 is used in North America.
- **Country/Region code** Use this field to type the country/region code number used for outgoing calls. This number will precede the telephone number dialed. By default, this field isn't populated. This field accepts from 1 through 4 digits. For example, in the United States, the country/region code is 1. In the United Kingdom, it's 44.
- **In-country/region number format** Use this field to specify how a user's telephone number should be dialed by the Unified Messaging server in a different dial plan, which has the same country code. This is used by an auto attendant and when an Outlook Voice Access subscriber searches and tries to call the user in the directory.

  This entry consists of a number prefix and a variable number of characters (for example, 020*xxxxxxx*).

  To determine the telephone number, Unified Messaging will append the last *x* digits from the telephone number specified in the directory to the prefix specified.
- **International number format** Use this field to specify how a user's telephone number should be dialed by the Unified Messaging server in a different dial plan, which has a different country code. This is used by an auto attendant and when an Outlook Voice Access subscriber searches and tries to call the user in the directory.

  This entry consists of a number prefix and a variable number of characters (for example, 4420*xxxxxxx*).

  To determine the telephone number, Unified Messaging will append the last *x* digits from the telephone number specified in the directory to the prefix specified.

7. Use the **Features** tab to configure the UM dial plan features. Several features can be configured on the UM dial plan. These include transferring calls and sending voice messages. You can configure the following:
   - **Allow callers to transfer to users** Select this check box to enable callers to transfer calls to users. By default, this option is enabled. This lets users associated with the dial plan transfer calls to users in the same UM dial plan. After you select this check box, you can set the group of users to whom callers can transfer by selecting the appropriate option under the **Callers can contact** section on this page.

     If you disable this option and disable the **Allow callers to send voice message** setting, the options under **Callers can contact** will also be disabled.
   - **Allow callers to send voice messages** Select this check box to enable callers to send voice messages to users. By default, this option is enabled. This lets users who are associated with the dial plan send voice messages to users in the same UM dial plan. After you select this check box, you can set the group of users to whom callers can send voice messages by selecting the appropriate option under the **Callers can contact** section on this page.

     If you disable this option and disable the **Allow callers to transfer users** setting, the options under **Callers can contact** will also be disabled.

     If you disable this option, the auto attendant won't invite callers to send a voice message during a system prompt.
   - **Callers can contact** Use these options to determine a grouping of users to use. By default, the **Users within this dial plan** option is selected. However, you can change the grouping of users to allow callers to transfer calls or send voice messages to users located in the global address list

(GAL) or to a specific set of users contained in a custom address list by choosing from the following:

Users within this dial plan Use this option to allow callers who connect to the UM auto attendant to locate and contact users who are within the dial plan associated with the UM auto attendant.

Anyone in the default global address list Use this option to allow callers who connect to the UM auto attendant to locate and contact anyone who is listed in the GAL. This includes all users who are mailbox-enabled.

Only this extension Use this option to allow callers to connect to an extension number that you specified in the field for this option. This field accepts only numeric digits. The number of digits that you define in this field must match the number of digits configured on the dial plan associated with the auto attendant.

Only this auto attendant Use this list to allow callers to connect to a UM auto attendant and then connect to another auto attendant. You must create this auto attendant to allow callers to be transferred to another auto attendant that's specified.

Anyone in this address list Use this option to allow callers who connect to the UM auto attendant to locate and contact users who are within a defined custom address list. This includes all users who are mailbox-enabled.

Important:

The **All Address Lists** container is an empty container object and differs from the GAL container. If you choose the **All Address Lists** container when you browse for a custom address list, there will be no UM-enabled users for callers to contact. If you want to select all the address lists in your organization, choose the **Anyone in the default global address list** option.

- **Matched name selection method** Use this field to select the method the dial plan uses to differentiate between users who have similar names. When a caller is prompted to enter letters to find a particular user in the organization, sometimes more than one name matches the caller's input. By default, all UM auto attendants associated with this dial plan inherit this setting. However, you can change this setting on each UM auto attendant created.

  Select one of the following methods for providing callers with more information to help them locate the correct user in the organization:

- **None** No additional information is given when matches are listed. By default, this method is selected.
- **Title** The auto attendant includes each user's title when matches are listed.
- **Department** The auto attendant includes each user's department when matches are listed.
- **Location** The auto attendant includes each user's location when matches are listed.
- **Prompt For Alias** The auto attendant prompts the caller for the user's alias.

8. Use the **Settings** tab to configure dial plan settings for Unified Messaging. When you configure settings on this tab, you can control how internal and external callers locate users in the system, the number of logon failures allowed when internal users try to access their voice mail, and the default language that the dial plan uses. You can configure the following:
   - **Dial by name primary method** Use this list to select the primary way that

callers can locate a user when they dial in to the system.

By default, **Last name, First name** is selected. This means that when users are searching for a user in the directory, they will enter the user's last name first and then the first name.

When a subscriber or a UM-enabled user uses the subscriber access number to access the Unified Messaging system, they can access the menu that enables them to spell the name or alias to locate a user in the system. The option selected is the default method used by UM-enabled users.

You must select one of the supported methods to be able to use the dial-by-name primary method. The following methods are supported:

Last First (default)
First Last
SMTP Address

- **Dial by name secondary method** Use this list to select the secondary way that callers can locate a user when they dial in to the system.

  By default, **SMTP address** is selected. This means that when users search for a user in the directory, they will enter the user's e-mail alias or SMTP address.

  When subscribers or UM-enabled users use the subscriber access number to access the Unified Messaging system, they can access the menu that enables them to spell the name or alias to locate a user in the system.

  You aren't required to select one of the four methods that are supported. However, if you don't select a secondary method, callers are given only one method to use to spell a user's name in the system. The following options are available:

  Last First
  First Last
  SMTP address (default)
  None

- **Audio codec** Use this list to select the audio codec that will be used by the dial plan. When a caller places a call to a user who is associated with the dial plan, Unified Messaging uses the audio codec that you select from this list to record voice messages that will be sent to UM-enabled users. The following audio codecs are supported:

  MP3 (default)
  WMA (Windows Media Audio)
  G711 (Pulse Code Modulation (PCM) Linear)
  GSM (Group System Mobile 06.10)

  By default, the MP3 format is selected. The MP3 format is a common audio file format that's used to greatly reduce the size of the audio file and is most commonly used by personal audio devices or MP3 players. MP3 is a cross-platform type of audio codec and is used for compatibility with many mobile phone and devices and various computer operating systems.

  WMA is used because it's highly compressed and has high quality format properties. G.711 PCM Linear is a telephone quality audio codec format that's the least compressed and has the lowest quality format. GSM 06.10 is an audio codec format that's used by mobile phone vendors and is the standard for digital mobile phone services.

  If you're concerned about users' disk quotas, select WMA as the audio codec. Voice files saved in .wma format are approximately half the size of the same voice recording made using one of the other audio codecs.

- **Operator extension** Use this text box to enter the telephone number or an extension number for the dial plan's operator.

  You can configure this setting to transfer calls to an auto

attendant if one is configured, to a human operator, to external telephone numbers, or to extension numbers.
When a caller who is using the telephone keypad presses 0, or says "reception" or "operator," or the number of **Input retries** threshold is exceeded, the caller is transferred to the telephone number that you specify in this text box.
This telephone number can be a number external to the organization or an internal telephone extension number. For example, if the extension number for the receptionist or operator is 81964 and your organization has only one dial plan, enter 81964.
By default, this setting is blank. If you don't enter a number in this text box, the ability to transfer calls to the operator is disabled and callers are politely disconnected because there's no one to answer the call.
We recommend that you populate this text box with a telephone number that transfers callers to an operator if they can't locate a specific user in the directory.

- **Logon failures before disconnect** Use this text box to enter the number of sequential unsuccessful logon attempts allowed before a caller is disconnected.
  The value of this setting can be from 1 through 20. Setting this value too low can frustrate users. For most organizations, this value should be set to the default of three attempts.
- **Maximum call duration (min)** Use this text box to enter the maximum number of minutes that an incoming call can be connected to the system without being transferred to a valid extension number before the call is ended. For most organizations, this value should be set to the default of 30 minutes.
  This setting applies to all kinds of calls. This includes incoming subscriber access calls, voice calls internal to your organization, and voice calls external to your organization.
  The value of this setting can be from 10 through 120. Setting this value too low can cause incoming calls to be disconnected before they are completed. For example, if your organization receives many large fax messages, you may want to consider increasing this value from the default so that all the pages for fax messages are received.
- **Maximum recording duration (min)** Use this text box to enter the maximum number of minutes allowed for each voice recording when a caller leaves a voice mail message. For most organizations, this value should be set to the default of 20 minutes.
  The value of this setting can be from 1 through 100. Setting this value too low can cause long voice messages to be disconnected before they are completed. Setting this value too high lets users save lengthy voice messages in their Inboxes. This setting is important if you have implemented strict disk quotas for users. This value must be less than the value set for the **Maximum call duration (min)** setting.
- **Recording idle time-out (sec)** Use this text box to enter the number of seconds of silence that the system allows when a voice message is being recorded before the call is ended. For most organizations, this value should be set to the default of 5 seconds.
  The value of this setting can be from 2 through 10. Setting this value too low can cause the system to disconnect callers before they are finished leaving their voice messages. Setting this value too high allows lengthy silences in voice messages.
- **Input failures before disconnect** Use this text box to configure the number of times that callers can enter incorrect data before they are disconnected. For most organizations, this value should be set to the

default of three attempts. This is an important setting for speech-enabled UM dial plans.

Examples of incorrect data include when a caller requests an extension number that isn't found in the system, the system can't locate the user's extension number to transfer the call, or the caller presses a menu option that isn't valid.

The value of this setting can be from 1 through 20. Setting this value too low may prematurely disconnect the caller.

- **Default language** Use this list to specify the default language used by callers. When a caller places a call to a user who is associated with a dial plan, this is the default language that the voice recorded operator uses. The system prompts that callers hear are also played in the default language. The language that is chosen on the UM dial plan is used to read e-mail, voice mail and calendar items; say the user's name if a personal greeting hasn't been recorded; transcribe a voice message using the Voice Mail Preview feature; enable Automatic Speech Recognition (ASR) to work correctly.

  By default, if you install U.S. English with Exchange 2010, only one language is listed in this list. To have other language options available, you must install the UM language pack for each language you want to include. For more information about how to install a UM language pack, see Install a Unified Messaging Language Pack on a UM Server.

  Adding other languages lets subscribers use a language other than U.S. English. For example, if a subscriber calls in to the Unified Messaging system using the subscriber access number from a desk telephone, the subscriber is greeted with a prerecorded operator's voice in English. Even if the same user selects a different language in Outlook Web App, such as French, the menus are still read in U.S. English. For the user to be able to hear the prerecorded operator menus in French, you must install the appropriate language.

9. Use the **Dialing Rule Groups** tab on the UM dial plan to specify dialing rule groups for in-country/region and international calls placed by UM-enabled users. Each dialing rule entry defined on the dialing rule group determines the types of calls that users within a specific dialing rule group can make. After you use the **Dialing Rule Groups** tab to configure a dialing rule group, you must configure the UM mailbox policy to use the appropriate dialing rule group. After you configure the UM mailbox to use a dialing rule group, the dialing restrictions configured apply to all UM-enabled users who are associated with the UM mailbox policy. For example, you can configure a dialing rule group that doesn't require users who are associated with the dial plan to dial an outside line access code when they place a call to an in-country/region telephone number. You can configure the following:
   - **In-Country/Region Rule Groups** Use this text box to add, remove, or edit in-country/region dialing rule groups used by UM mailbox policies.
   - **International Rule Groups** Use this text box to add, remove, or edit international dialing rule groups used by UM mailbox policies.
   - **Dialing Rule Entry** Use this dialog box to define the telephone numbers and number masks for in-country/region and international calls that will be made by UM-enabled users. Each dialing rule entry determines the types of calls that users within a dialing rule group can make. However, you must correctly configure the dialing rule entry with a number mask and a dial number. After you use the **Dialing Rule Entry** window to configure a dialing rule entry, you must configure the UM dial plan, mailbox policy, or auto attendant to use the appropriate dialing rule group. You can configure the following:

     Name Use this list to select a name of an existing dialing rule entry. Or, if you want to create a dialing rule entry, type the

name of the dialing rule entry. This is the display name for the dialing rule entry that will be displayed in the EMC. This field can contain only text characters. The display name for the dialing rule entry can contain up to 32 characters.

Number Mask Use this text box to define the number mask for the dialing rule entry. A number mask is used to define the telephone number format that a Unified Messaging server uses to determine what outgoing telephone number it will dial for a user. When an outgoing call is made to a number matched by the number mask on the dialing rule entry, the Unified Messaging server substitutes the digits matched into the dialed number. It then uses the digit string from this match to make the outgoing call. An example of a valid number mask is 91425*xxxxxxx*. This field can contain only numbers and the character *x*.

Dialed Number Use this text box to define the dialed number for the dialing rule entry. The dialed number is used to determine the actual dial string sent to the IP gateway. This number can be different from the number obtained by Unified Messaging for the outgoing call. However, your PBX can also be configured to omit the area code for local calls and can be configured for private voice numbering plans. Any wildcard characters (*x*) in the dial string are substituted with the digits from the original number that were matched by the number mask on the dialing rule entry. An example of a valid dialed number is 9*xxxxxxx*. This field can contain only numbers and the character *x*.

Comment Use this text box to input a comment or description for the dialing rule entry that you're adding or modifying. By default, this text box is blank.

Important:

If you've integrated Exchange Unified Messaging and Office Communications Server, you'll probably find it unnecessary to configure dialing rules or dialing rule groups in Exchange Unified Messaging. Office Communications Server is designed to perform call routing and number translation for users in your organization, and will also do this when the calls are made by Exchange Unified Messaging on behalf of users.

10. Use the **Dialing Restrictions** tab on the UM dial plan properties to configure dialing rule entries for callers who call in to a subscriber access number configured on a UM dial plan. You can restrict the type of calls placed by callers when an unauthenticated user or an Outlook Voice Access user calls in to a subscriber access number configured on a dial plan by configuring dialing rule groups and dialing restrictions. You can configure the following:
    - **Allow calls to users within the same dial plan** Select this check box to let users who call in to a subscriber access number configured on a dial plan place or transfer calls to an extension number associated with a UM-enabled user who is within the same dial plan. By default, this setting is enabled.

      When you disable this setting, users who call in to the subscriber access number won't be able to place or transfer calls to any users who aren't UM-enabled, to other extension numbers, or to UM-enabled users who are associated with the same dial plan. This is because the **Allow calls to extensions** setting is disabled by default.
    - **Allow calls to extensions** When this setting is disabled, users who call in to a subscriber access number on the dial plan can't place calls to users who aren't UM-enabled or to other extension numbers not associated with

a UM-enabled user. However, they can place a call or transfer a call to extension numbers associated with UM-enabled users. This is because the **Allow calls to users within the same dial plan** setting is enabled by default. The **Allow calls to extensions** setting is disabled by default.

When this setting is enabled, users who call in to a subscriber access number configured on the dial plan can place calls to users who aren't UM-enabled, to other extension numbers not associated with a UM-enabled user, and to UM-enabled users. This is because the **Allow calls to users within the same dial plan** setting is enabled by default.

You can enable this setting in an environment where not all users have been UM-enabled. This setting is also useful when you want to allow users who call in to a subscriber access number configured on a dial plan to call extension numbers that aren't associated.

- **Select allowed in-country/region rule groups from dial plan** Use this section to add or remove allowed in-country/region dialing rule groups. By default, there are no in-country/region dialing rule groups configured on UM dial plans.

  In-country/region dialing rule groups are used to allow or restrict the telephone numbers within a country or region that any user who has dialed in to the subscriber access number can dial. This helps prevent unnecessary or unauthorized telephone calls and charges.

  To add in-country/region dialing rule groups, you must first create the appropriate in-country/region dialing rule groups on the dial plan, and then add the appropriate dialing rule entries on the dialing rule groups. After you create the required dialing rule groups on the dial plan, you must then add the dialing rule groups to the list of dialing restrictions on the **Dialing Restrictions** tab on the dial plan.

  In-country/region dialing rule groups can be used to enable a Unified Messaging server to allow or restrict access to telephone numbers within a country or region. This is applied to all users who have called in to a subscriber access number.
- **Select allowed international rule groups from dial plan** Use this section to add or remove allowed international dialing rule groups. By default, there are no international dialing rule groups configured on UM dial plans.

  International dialing rule groups are used to allow or restrict the telephone numbers outside a country or region that any user who has dialed in to the subscriber access number can dial. This helps prevent unnecessary or unauthorized telephone calls and charges.

  To add international dialing rule groups, you must first create the appropriate international dialing rule groups on the dial plan, and then add the appropriate dialing rule entries on the dialing rule groups. After you create the required dialing rule groups on the dial plan, you must then add the dialing rule groups to the list of dialing restrictions on the **Dialing Restrictions** tab on the dial plan.

  International dialing rule groups can be used to enable a Unified Messaging server to allow or restrict access to telephone numbers outside a country or region. This is applied to all users who have called in to a subscriber access number

Use the Shell to configure UM dial plan properties

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example configures a UM dial plan named MyDialPlan to use 9 for the outside line access code.

```
Set-UMDialplan -Identity MyDialPlan -OutsideLineAccessCode 9
```

This example configures a UM dial plan named MyDialPlan to use a welcome greeting.

```
Set-UMDialplan -Identity MyDialPlan -WelcomeGreetingEnabled $true -WelcomeGreetin
```

This example configures a UM dial plan named MyDialPlan with dialing rules.

```
$csv=import-csv "C:\MyInCountryGroups.csv"
Set-UMDialPlan -Identity MyDialPlan -ConfiguredInCountryGroups $csv
Set-UMDialPlan -Identity MyDialPlan -AllowedInCountryGroups "local, long distance
```

For more information about syntax and parameters, see Set-UMDialplan.

Use the Shell to view UM dial plan properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example displays a list of all the UM dial plans in the Active Directory forest.

```
Get-UMDialplan
```

This example displays a formatted list of properties for a UM dial plan named MyUMDialPlan.

```
Get-UMDialplan -Identity MyUMDialPlan | Format-List
```

For more information about syntax and parameters, see Get-UMDialplan.

Other Tasks

After you have configured a UM dial plan, you may also want to Add a UM Server to a Dial Plan.

For More Information

Understanding Unified Messaging Dial Plans.

1.9.2.3.2.3 Delete a UM Dial Plan

Delete a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can delete an existing Unified Messaging (UM) dial plan in Microsoft Exchange Server 2010. When you delete the UM dial plan, the UM dial plan will no longer be available to other UM objects such as Unified Messaging servers, UM IP gateways, UM mailbox policies, and UM hunt groups. You won't be able to delete a UM dial plan if it's referenced by or associated with other UM objects such as UM mailbox policies, UM auto attendants, UM IP gateways, UM hunt groups, or Unified Messaging servers.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to delete an existing UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Dial Plans** tab.
3. Click to highlight the UM dial plan you want to delete.
4. In the action pane, click **Remove**.
5. In the confirmation dialog box, click **Yes**.

Use the Shell to delete an existing UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example deletes a UM dial plan named `MyUMDialPlan`.

```
RemoveUMDialplan -identity MyUMDialPlan
```

For more information about syntax and parameters, see Remove-UMDialplan.

Other Tasks

After you delete an existing UM dial plan, you may also want toView or Configure the Properties of a UM Dial Plan.

Prevent UM-Enabled Users from Receiving Faxes on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can prevent UM-enabled users who are associated with a Unified Messaging (UM) dial plan from receiving fax messages. By default, users who are enabled for Unified Messaging and are associated with a UM dial plan can receive fax messages. However, there may be times when you want to prevent users who are associated with a specific UM dial plan from receiving faxes.

You can prevent UM-enabled users from receiving faxes by configuring the UM dial plan, the UM mailbox policy, or by configuring the UM-enabled user's mailbox. If you disable incoming fax message delivery on a UM dial plan, all users who are associated with the dial plan will be prevented from receiving fax messages. Enabling or disabling faxing on a UM dial plan takes precedence over the settings for an individual UM-enabled user.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to prevent users who are associated with a dial plan from receiving faxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. On the **UM Dial Plans** tab, select the UM dial plan for which you want to prevent UM-enabled users from receiving faxes, and then click **Properties** in the action pane.
3. On the dial plan Properties page, on the **General** tab, clear the check box next to **Allow users to receive faxes**.
4. Click **OK** to save your changes.

Use the Shell to prevent users who are associated with a dial plan from receiving faxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example prevents UM-enabled users associated with the UM dial plan named MyUMDialPlan from receiving faxes.

```
Set-UMDialPlan -Identity MyUMDialPlan -FaxEnabled $false
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you prevent users who are associated with a dial plan from receiving faxes, you may also want to:

- Enable or Disable Inbound Faxing on a UM Mailbox Policy
- Enable a UM-Enabled User to Receive Faxes
- Prevent a UM-Enabled User from Receiving Faxes

1.9.2.3.2.5 Enable UM-Enabled Users to Receive Faxes on a UM Dial Plan

Enable UM-Enabled Users to Receive Faxes on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable all users who are associated with a Unified Messaging (UM) dial plan to receive fax messages in their Microsoft Exchange Server 2010 mailbox. To allow UM-enabled users to receive fax messages in their mailbox, each Unified Messaging server that's associated with the dial plan must be configured to accept incoming fax calls. You must also enable fax messages to be received by users who are associated with the dial plan However, there may be times when these default settings have changed and UM-enabled users can't receive fax messages.

If you prevent fax messages from being received on a dial plan, all users who are associated with the dial plan won't be able to receive fax messages, even if you configure an individual user's properties to allow them to receive fax messages. Enabling or disabling faxing on a UM dial plan takes precedence over the settings for an individual UM-enabled user.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to enable faxes to be received by users who are associated

with a dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. On the **UM Dial Plans** tab, select the UM dial plan for which you want to allow users associated with the dial plan to receive fax messages, and then, in the action pane, click **Properties**.
3. On the dial plan **Properties** page, on the **General** tab, select the check box next to **Allow users to receive faxes**.
4. Click **OK** to save your changes.

Use the Shell to enable faxes to be received by users who are associated with a dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example enables UM-enabled users who are associated with the UM dial plan named `MyUMDialPlan` to receive incoming faxes.

```
Set-UMDialPlan -Identity MyUMDialPlan -FaxEnabled $true
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you enable faxes to be received by users who are associated with a dial plan, you may also want to:

- Prevent a UM-Enabled User from Receiving Faxes
- Prevent UM-Enabled Users from Receiving Faxes on a UM Dial Plan

1.9.2.3.2.6 Allow or Prevent Call Answering Rules on a UM Dial Plan

Allow or Prevent Call Answering Rules on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can allow users associated with a Unified Messaging (UM) dial plan to create and configure call answering rules, or prevent them from doing so. When this setting is enabled, UM-enabled users can create rules or actions and apply conditions to an incoming call to their phone number. They can transfer the call, have the caller leave a

voice message, or allow the caller to locate them at a different phone number.

You can also allow users to create and configure call answering rules, or prevent them from doing so, by configuring the UM mailbox policy associated with the user or on the user's mailbox.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to allow or prevent users from configuring call answering rules

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **General** tab.
4. Under **Allow users to configure call answering rules**, clear or select the check box.
5. Click **OK** to save your changes.

Use the Shell to allow or prevent users from configuring call answering rules

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example allows users who are associated with a UM dial plan named `MyUMDialPlan` to configure call answering rules.

```
Set-UMDialPlan -identity MyUMDialPlan -CallAnsweringRulesEnabled $true
```

This example prevents users who are associated with a UM dial plan named `MyUMDialPlan` from configuring call answering rules.

```
Set-UMDialPlan -identity MyUMDialPlan -CallAnsweringRulesEnabled $false
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you've allowed users to configure call answering rules on a UM dial plan or prevented them from doing so, you may also want to:

- Enable or Disable Call Answering Rules for a UM-Enabled User
- Enable or Disable Call Answering Rules on a UM Mailbox Policy

1.9.2.3.2.7 Configure VoIP Security on a UM Dial Plan

Configure VoIP Security on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable Voice over IP (VoIP) security for a Unified Messaging (UM) dial plan. By default, when a UM dial plan is created, it will use unsecured mode or no encryption. A Unified Messaging server can be associated with a single or multiple UM dial plans and can be associated with dial plans that have different VoIP security settings.

When you configure the UM dial plan to use Session Initiation Protocol (SIP) secured or secured mode, the Unified Messaging servers that are associated with the UM dial plan will encrypt the SIP signaling traffic or the Realtime Transport Protocol (RTP) media channels and the SIP signaling traffic.

Important:

When Microsoft Exchange Server 2010 is installed, static Windows Firewall rules are added for Exchange. If you change the TCP ports that are used by the Unified Messaging server role, you may also need to reconfigure the Windows Firewall rules to allow Unified Messaging to work correctly.

- Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure VoIP security on a UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Dial Plans** tab, select the UM dial plan that you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **General** tab.
4. Click the drop-down list next to **VoIP security**, and then select one of the following options:
   - SIP secured
   - Unsecured (default)
   - Secured

Click **OK** to save your changes.

Use the Shell to configure VoIP security on a UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example configures a UM dial plan named `MySecureDialPlan` to encrypt both SIP and RTP traffic.

```
Set-UMDialPlan -identity MySecureDialPlan -VoIPSecurity Secured
```

This example configures a UM dial plan named `MySecureDialPlan` to encrypt SIP but not encrypt RTP traffic.

```
Set-UMDialPlan -identity MySecureDialPlan -VoIPSecurity SIPsecured
```

This example configures a UM dial plan named `MySecureDialPlan` to not encrypt SIP and RTP traffic.

```
Set-UMDialPlan -identity MySecureDialPlan -VoIPSecurity Unsecured
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you configure VoIP security on a UM dial plan, you may also want to:

- Connect a Unified Messaging Server to a Supported IP Gateway
- Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server
- Add a UM Server to a Dial Plan

For More Information

Import and Export Certificates

1.9.2.3.2.8 Enable a Custom Welcome Greeting on a UM Dial Plan

Enable a Custom Welcome Greeting on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable a custom welcome greeting on a Microsoft Exchange Server 2010 Unified Messaging (UM) dial plan. By default, each dial plan uses a system prompt or .wav file for its default welcome greeting. However, you can create a custom .wav file or custom prompt to use for the welcome greeting, and then enable the welcome greeting to be played to callers, including Outlook Voice Access users who dial in to a subscriber access number.

However, you might want to change this default welcome greeting and instead provide an alternative welcome greeting that's specific to your company, such as, "Welcome to

Outlook Voice Access for Woodgrove Bank." To do this, you record the customized welcome greeting and save it as a .wav file. Then you configure the dial plan to use the customized welcome greeting.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to enable a custom welcome greeting

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan that you want to manage.
3. In the action pane, click **Properties**.
4. On the dial plan **Properties** page, on the **Subscriber Access** tab, under **Welcome greeting**, click **Modify**.
5. On the **Welcome Greeting** page, under **Welcome greeting**, click **Use custom greeting file**, and then click **Browse** to locate the file that you want to use for your custom welcome greeting file.
6. Click **OK** to save your changes.

Use the Shell to enable a custom welcome greeting

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example enables a welcome greeting that uses the C:\UMPrompts\welcome.wav file on a UM dial plan named `MyUMDialPlan`.

```
Set-UMDialPlan -Identity MyUMDialPlan -WelcomeGreetingEnabled $true -WelcomeGreet
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you enable a custom welcome greeting, you may also want to:

- Enable an Informational Announcement on a UM Dial Plan
- Configure a Subscriber Access Number on a UM Dial Plan
- Enable Custom Prompt Recording Using the Telephone User Interface

Enable an Informational Announcement on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable an informational announcement on a Microsoft Exchange Server 2010 Unified Messaging (UM) dial plan. By default, an informational announcement isn't played to callers, including Outlook Voice Access users who dial in to a subscriber access number. If you want an informational announcement to be played, you must create a .wav file to use for the informational announcement after you create a dial plan, and then enable the informational announcement on the dial plan.

You can use an informational announcement for general announcements that change more frequently than the welcome greeting does, or for announcements required by corporate compliance policies. When it's important that the whole informational announcement be heard, you can configure it to be uninterruptible. This prevents a caller from pressing a key or speaking a command to interrupt and stop the informational announcement.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to enable an informational announcement

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. On the **UM Dial Plans** tab, select the UM dial plan that you want to manage, and then click **Properties** in the action pane.
3. On the dial plan Properties page, under the **Subscriber Access** tab, under **Informational announcement**, click **Modify**.
4. On the **Informational Announcement** page, under **Informational announcement**, click **Informational announcement file**, click **Browse**, and then navigate to the .wav file that you want to use for your informational announcement.
5. (Optional) If you want to let your users interrupt the informational announcement, select the check box next to **Allow informational announcement to be interrupted**.
6. Click **OK** to save your changes.

Use the Shell to enable an informational announcement

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example enables an informational announcement that uses the informational.wav information announcement file on a UM dial plan named MyUMDialPlan.

```
Set-UMDialPlan -Identity MyUMDialPlan -InfoAnnouncementEnabled $true-InfoAnnounce
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you enable an informational announcement, you may also want to:

- Enable a Custom Welcome Greeting on a UM Dial Plan
- Enable an Informational Announcement on a UM Auto Attendant

1.9.2.3.2.10 Configure a Subscriber Access Number on a UM Dial Plan

Configure a Subscriber Access Number on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A subscriber access number lets a user who is enabled for Unified Messaging (UM) access a mailbox in Microsoft Exchange Server 2010 using Outlook Voice Access. When you configure a subscriber access number on a dial plan, UM-enabled users can call in to the subscriber access number, log on to their Exchange 2010 mailbox, and access their e-mail, voice mail, calendar, and personal contact information.

By default, when you create a UM dial plan, a subscriber access number isn't configured. To configure a subscriber access number, you first need to create the dial plan and then configure a subscriber access number on the dial plan's **Subscriber Access** tab. Although a subscriber access number isn't required, you need to configure at least one subscriber access number to enable a UM-enabled user to use Outlook Voice Access to access to their Exchange 2010 mailbox. You can also configure multiple subscriber access numbers for a single dial plan.

For more information about the menu options available for Outlook Voice Access users, see the Quick Reference Guide for Outlook Voice Access, which is available from the Microsoft Download Center.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure a subscriber access number

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **Subscriber Access** tab.
4. Under **Associated Subscriber Access Numbers**, enter the subscriber access number in the box labeled **Enter the telephone number to associate**, and then click **Add**.
5. Click **OK** to save your changes.

Use the Shell to configure a subscriber access number

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the subscriber access number to 4255550100 for a UM dial plan named `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -AccessTelephoneNumbers 4255550100
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you configure a subscriber access number, you may also want to:

- Configure the Dial by Name Primary Method on a Unified Messaging Dial Plan
- Configure the Dial by Name Secondary Method on a UM Dial Plan

1.9.2.3.2.11 Configure Dial Codes on a UM Dial Plan

Configure Dial Codes on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure dial codes for a Unified Messaging (UM) dial plan in Microsoft Exchange Server 2010. You can configure dial codes, national number prefixes, and in-country/region and international number formats used by a Unified Messaging server to dial incoming and outgoing calls for users who are enabled for Unified Messaging. In most

cases, you'll configure a dial plan with the dial codes and national number prefix currently configured on your telephony network.

Dial codes, national number prefixes, and formats are used by a Unified Messaging server to determine the correct number to dial for an outgoing call that's placed by a UM-enabled user. On the **Dial Codes** tab, you can also configure the Unified Messaging servers associated with the dial plan to match the incoming call number format for both in-country/region and international numbers. When you configure the in-country/region and international number formats, you can restrict incoming calls for users associated with a dial plan.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure dial codes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. On the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, on the **Dial Codes** tab, under **Outgoing Configuration**, configure these options:
   - Outside line access code
   - International access code
   - National number prefix
   - Country/Region code
4. Under **Incoming Configuration**, configure the following:
   - In-country/region number format
   - International number format
5. Click **OK** to save your changes.

Use the Shell to configure dial codes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example configures a UM dial plan named `MyUMDialPlan` with an In-Country or Region Number format and an International Number format and the following dial codes.

- 9 for the Outside Line Access Code
- 011 for the International Access Code
- 1 for the National Number Prefix
- 1 for the Country or Region code

```
Set-UMDialPlan -Identity MyUMDialPlan -OutsideLineAccessCode 9 -InternationalAcce
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you configure dial codes, you may also want to:

- Configure Dialing Rule Groups on a UM Dial Plan
- Create a Dialing Rule Entry on a UM Dial Plan

1.9.2.3.2.12 Enable or Disable Sending Voice Messages on a UM Dial Plan

Enable or Disable Sending Voice Messages on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable users who are enabled for Unified Messaging (UM) to send voice messages to other UM-enabled users who are associated with the same dial plan, or prevent them from doing so.

By default, this option is enabled. If you disable this setting and disable the **Allow callers to transfer users** setting, the options under **Callers can contact** will also be disabled. If you disable this option, an auto attendant associated with the UM dial plan won't invite callers to send a voice message when a system prompt is played.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to enable or prevent UM-enabled users from sending voice messages to users in the same dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan that you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **Settings** tab.
4. Under **Allow callers to send voice messages**, clear or select the check box. If you select this option, under **Callers can contact**, specify who users can transfer calls to.
5. Click **OK** to save your changes.

Use the Shell to enable or prevent UM-enabled users from sending voice messages to users in the same dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example prevents UM-enabled users associated with the UM dial plan named `MyUMDialPlan` from sending voice messages to users associated with the same dial plan.

```
Set-UMDialPlan -identity MyUMDialPlan -SendVoiceMsgEnabled $false
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you've enabled or prevented users from sending voice messages to other UM-enabled users associated with the same UM dial plan, you may also want to:

- Enable or Disable Call Transfers to Users on a UM Dial Plan
- Configure the Scope of Users Who Callers Can Contact on a UM Dial Plan

1.9.2.3.2.13 Enable or Disable Call Transfers to Users on a UM Dial Plan

Enable or Disable Call Transfers to Users on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable call transfer to a user who's associated with a Unified Messaging (UM) dial plan. By default, this option is enabled, and lets users associated with the dial plan transfer calls to users in the same UM dial plan. After you select this check box, you can set the group of users to whom callers can transfer by selecting the option you want under the **Callers can contact** section on this page. If you disable the **Allow callers to transfer to users** option and disable the **Allow callers to send voice messages** setting, the options under **Callers can contact** will also be disabled.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to enable or disable call

transfer to users

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **Settings** tab.
4. Under **Allow callers to transfer to users**, clear or select the check box. If you select this option, under **Callers can contact**, specify the people to whom users can transfer calls.
5. Click **OK** to save your changes.

Use the Shell to enable or disable call transfer to users

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example prevents users from transferring calls for a UM dial plan named `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -AllowDialPlanSubscribers $false>
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you've enabled or disabled call transfer to users, you may also want to:

- Enable or Disable Sending Voice Messages on a UM Dial Plan
- Configure the Scope of Users that Callers Can Contact on a UM Auto Attendant
- Enable or Disable Call Transfers to Users from a UM Auto Attendant

1.9.2.3.2.14 Configure the Scope of Users Who Callers Can Contact on a UM Dial Plan

Configure the Scope of Users Who Callers Can Contact on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify which users will be able to receive transferred calls or voice messages from users who call in to a subscriber access number. By default, the **Users within this dial plan** option is selected. You can change this setting to allow callers to transfer calls or send voice messages to users located in the global address list, to a specific extension

number, to a UM auto attendant, or to a specific set of users contained in a custom address list.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure the scope of users who callers can contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **Features** tab.
4. Under **Callers can contact**, select one of the following options:
   - 4.a. **Users within this dial plan** Use this option to allow callers who call in to a subscriber access number to locate and contact users who are within the dial plan associated with the UM auto attendant.
   - 4.b. **Anyone in the default global address list** Use this option to allow callers who call in to a subscriber access number to locate and contact anyone who's listed in the global address list. This includes all users who are mailbox-enabled.
   - 4.c. **Only this extension** Use this option to allow callers to connect to an extension number that you specify. You can only use numeric digits for the extension. The number of digits that you define in this field must match the number of digits in the extension numbers that are configured on the UM dial plan.
   - 4.d. **Only this auto attendant** Use this option to allow callers who call in to a subscriber access number to connect to a specific auto attendant. You must create the auto attendant before you specify it here. This allows callers to be transferred to another auto attendant. The auto attendant you choose here can be a speech-enabled or non speech-enabled auto attendant.
   - 4.e. **Anyone in address list** Use this option to allow callers who call in to a subscriber access number to locate and contact users who are in a defined custom address list. This includes all users who are mailbox-enabled.
5. Click **OK** to save your changes.

Use the Shell to configure the scope of users who callers can contact

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the scope of the users who callers can contact for a UM dial plan named `MyUMDialPlan` to the global address list.

```
Set-UMDialPlan -Identity MyUMDialPlan -ContactScope 'GlobalAddressList' -UMAutoAt
```

This example sets the scope of the users who callers can contact for a UM dial plan named `MyUMDialPlan` to a custom address list named `MyAddressList`.

```
Set-UMDialPlan -Identity MyUMDialPlan -ContactScope MyAddressList -AllowDialPlanS
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you've configured the scope of users who callers can contact, you may also want to:

- Enable or Disable Call Transfers to Users on a UM Dial Plan
- Enable or Disable Sending Voice Messages on a UM Dial Plan

1.9.2.3.2.15 Configure the Matched Name Selection Method on a UM Dial Plan

Configure the Matched Name Selection Method on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the matched name selection method for a Unified Messaging (UM) dial plan in Microsoft Exchange Server 2010. The matched name selection method is used by Unified Messaging to differentiate between users who have the same or similar names. When a caller or an Outlook Voice Access user is prompted to enter letters to find a particular user, sometimes more than one name matches the caller's input. You can use one of the available methods for providing the caller with more information to help them locate the user they're trying to reach.

You can set the matched name selection method on UM dial plans and UM auto attendants. When a UM auto attendant is created, it inherits the matched name selection method from the dial plan associated with the auto attendant. By default, the matched name selection method isn't configured for dial plans.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure the matched name selection method on a UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Dial Plans** tab.
3. Select the dial plan you want to modify, and then, in the action pane, click **Properties**.
4. On the **Features** tab, under **Matched name selection method**, select from one of the following:
   - **Title** The dial plan operator or auto attendant will include each user's title when matches are listed.
   - **Department** The dial plan operator or auto attendant will include each user's department when matches are listed.
   - **Location** The dial plan operator or auto attendant will include each user's location when matches are listed.
   - **None** No additional information will be given when matches are listed. By default, this method is selected.
   - **Prompt For Alias** The dial plan operator or auto attendant will prompt the caller for the user's e-mail alias.
5. Click **OK** to save your changes.

Use the Shell to configure the matched name selection method on a UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the matched name selection method to prompt for the user's alias on a UM dial plan named `MyDialPlan`.

```
Set-UMDialplan -Identity MyDialPlan -MatchedNameSelectionMethod PromptForAlias
```

This example sets the matched name selection method to Department on a UM dial plan named `MyDialPlan`.

```
Set-UMDialplan -Identity MyDialPlan -MatchedNameSelectionMethod Department
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you configure the matched name selection method on a UM dial plan, you may also want to:

- Configure the Matched Name Selection Method on a UM Auto Attendant
- View or Configure the Properties of a UM Dial Plan

1.9.2.3.2.16 Configure the Dial by Name Primary Method on a Unified Messaging Dial Plan

Configure the Dial by Name Primary Method on a Unified Messaging Dial Plan

Managing Unified Messaging > Managing Unified Messaging Components > Managing UM Dial Plans >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you create a dial plan, you can configure the primary and secondary dial by name methods. These dial by name methods are used by callers use to look up names when they want to locate and contact a user when they call into an Outlook Voice Access number or when they call into a UM auto attendant that's associated with the dial plan. Callers can use either touchtone inputs or voice inputs to locate a UM-enabled user.

Note:

None isn't an available option for the dial by name primary method. When **None** is selected for the dial by name secondary method, only the dial by name primary method will be available to callers.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to change the primary dial by name method

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, on the **Settings** tab, select from the following options in the drop-down list next to **Dial by name primary method**:
   - Last First (default)
   - First Last
   - SMTP Address
4. Click **OK** to save your changes.

Use the Shell to change the primary dial by name method

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the primary dial by name method to `FirstLast`. This enables callers who call the Outlook Voice Access number or a UM auto attendant associated with the dial plan to search for a UM-enabled user by their first and then last name.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNamePrimary FirstLast
```

This example sets the primary dial by name method to `LastFirst`. This enables callers who call the Outlook Voice Access number or a UM auto attendant associated with the dial

plan to search for a UM-enabled user by their last and then first name.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNamePrimary LastFirst
```

This example sets the primary dial by name method to SMTP address. This enables callers who call the Outlook Voice Access number or a UM auto attendant associated with the dial plan to search for a UM-enabled user by their SMTP address.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNamePrimary SMTPAddress
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you've configured the dial by name primary method, you may also want to:

- Configure the Dial by Name Secondary Method on a UM Dial Plan
- Configure the Matched Name Selection Method on a UM Dial Plan

1.9.2.3.2.17 Configure the Dial by Name Secondary Method on a UM Dial Plan

Configure the Dial by Name Secondary Method on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you create a dial plan, you can configure the primary and secondary dial by name methods. These dial by name methods are used by callers use to look up names when they want to locate and contact a user when they call into an Outlook Voice Access number or when they call into a UM auto attendant that's associated with the dial plan. Callers can use either touchtone inputs or voice inputs to locate a UM-enabled user.

Note:

If **None** is selected as the dial by name secondary method, only the dial by name primary method will be available to callers who want to locate users.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to change the secondary dial by name method

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, on the **Settings** tab, select from the following options in the drop-down list next to **Dial by name secondary method**:
   - Last First
   - First Last
   - SMTP address (default)
   - None
4. Click **OK** to save your changes.

Use the Shell to change the secondary dial by name method

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the secondary dial by name method to `FirstLast`. This enables callers who call the Outlook Voice Access number or a UM auto attendant associated with the dial plan to search for a UM-enabled user by their first and then last name.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNameSecondary FirstLast
```

This example sets the secondary dial by name method to `LastFirst`. This enables callers who call the Outlook Voice Access number or a UM auto attendant associated with the dial plan to search for a UM-enabled user by their last and then first name.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNameSecondary LastFirst
```

This example sets the secondary dial by name method to `SMTP address`. This enables callers who call the Outlook Voice Access number or a UM auto attendant associated with the dial plan to search for a UM-enabled user by their SMTP address.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNameSecondary SMTPAddress
```

This example sets the secondary dial by name method to `None` and the dial by name primary method to SMTP address. This enables callers who call the Outlook Voice Access number or a UM auto attendant associated with the dial plan to search for a UM-enabled user by their SMTP address only.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNamePrimary SMTPAddress -DialByNameS
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you've configured the dial by name secondary method, you may also want to:

- Configure the Dial by Name Primary Method on a Unified Messaging Dial Plan
- Configure the Matched Name Selection Method on a UM Dial Plan

Configure the Audio Codec on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Unified Messaging (UM) servers can use one of four codecs for creating voice messages: MP3, Windows Media Audio (WMA), Group System Mobile (GSM) 06.10, and G.711 Pulse Code Modulation Linear. By default, when you create a UM dial plan, the UM dial plan uses the MP3 audio codec. However, after the UM dial plan is created, you can configure the UM dial plan to use the WMA, GSM 06.10 or G.711 PCM Linear audio codecs.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to change the audio codec on a Unified Messaging dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to modify.
3. In the action pane, click **Properties**.
4. On the dial plan **Properties** page, click the **Settings** tab.
5. On the **Settings** tab, use the **Audio codec** list to select the audio codec you want.
6. Click **OK** to accept your changes.

Use the Shell to change the audio codec on a Unified Messaging dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the audio codec on a UM dial plan named `MyUMDialPlan` to G.711.

```
Set-UMDialPlan -Identity MyUMDialPlan -AudioCodec G711
```

This example sets the audio codec on a UM dial plan named `MyUMDialPlan` to WMA.

```
Set-UMDialPlan -Identity MyUMDialPlan -AudioCodec Wma
```

For more information about syntax and parameters, see Set-UMDialplan.

1.9.2.3.2.19 Configure an Operator Extension on a UM Dial Plan

Configure an Operator Extension on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure an extension number for a Unified Messaging (UM) dial plan. You can set it to transfer calls to a UM auto attendant, if one is configured, a human operator, external telephone numbers, or extension numbers. When you configure an operator extension number on a UM dial plan, a caller can connect to the dial plan operator by doing one of the following:

- Pressing the zero (0) key
- Saying "Reception"
- Saying "Operator"

Note:
If the caller exceeds the maximum number of touchtone or voice input retries, they're transferred to the operator extension number, if you've defined an operator extension number and enabled business hours operator transfers.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure an operator extension

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to modify.
3. In the action pane, click **Properties**.
4. On the dial plan **Properties** page, click the **Settings** tab.
5. On the **Settings** tab, in the **Operator extension** text box, type the telephone number for the operator.
6. Click **OK** to accept your changes.

Use the Shell to configure an operator extension

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example configures an operator extension of 12345 on a UM dial plan named MyUMDialPlan.

```
Set-UMDialPlan -Identity MyUMDialPlan -OperatorExtension 12345
```

For more information about syntax and parameters, see Set-UMDialplan reference topic.

Other Tasks

After you configure an operator extension, you may also want to:

- View or Configure the Properties of a UM Dial Plan
- Configure an Operator Extension on a UM Auto Attendant

1.9.2.3.2.20 Configure the Number of Logon Failures Before Users Are Disconnected on a UM Dial Plan

Configure the Number of Logon Failures Before Users Are Disconnected on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify the number of sequential unsuccessful sign-in attempts that are allowed before a caller is disconnected. The value of this setting can be from 1 through 20. Setting this value too low can frustrate users. For most organizations, this value should be set to the default of three attempts.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure the number of sign-in failures before users are disconnected

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **Settings** tab.
4. Under **Logon failures before disconnect**, enter the number of sequential

unsuccessful sign-in attempts that are allowed before a caller is disconnected.

5. Click **OK** to save your changes.

Use the Shell to configure the number of sign-in failures before users are disconnected

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the number of sign-in failures before users are disconnected to 5 for a UM dial plan named `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -LogonFailuresBeforeDisconnect 5
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you've configured the number of sign-in failures before users are disconnected on a dial plan, you may also want to:

- Configure the Input Failures Before Disconnect on a UM Dial Plan
- Configure the Recording Idle Time-Out Value on a UM Dial Plan

1.9.2.3.2.21 Configure the Maximum Call Duration on a UM Dial Plan

Configure the Maximum Call Duration on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify the maximum number of minutes that an incoming call can be connected to the system without being transferred to a valid extension number before the call is ended. For most organizations, this value should be set to the default: 30 minutes. This setting applies to all calls, including incoming subscriber access calls, voice calls internal to your organization, and voice and fax calls placed from outside your organization.

This value can be set to a number from 10 through 120. Setting this value too low can cause incoming calls to be disconnected before they're completed. For example, if your organization receives many large fax messages, you may want to consider increasing this value from the default so that all the pages of fax messages are received.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure the maximum call duration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **Settings** tab.
4. Under **Maximum call duration (min)**, specify the maximum number of minutes that an incoming call can be connected to the system without being transferred to a valid extension before the call is ended.
5. Click **OK** to save your changes.

Use the Shell to configure the maximum call duration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the maximum call duration to 10 minutes on a UM dial plan named `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -MaxCallDuration 10
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you configure the maximum call duration on a UM dial plan, you may also want to:

- Configure the Maximum Recording Duration on a UM Dial Plan
- Configure the Number of Logon Failures Before Users Are Disconnected on a UM Dial Plan

1.9.2.3.2.22 Configure the Maximum Recording Duration on a UM Dial Plan

Configure the Maximum Recording Duration on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify the maximum number of minutes allowed for each voice recording when a caller leaves a voice mail message. This value can be set from 1 through 100. For most organizations, this value should be set to the default of 20 minutes. Setting this value too low can cause long voice messages to be disconnected before they're completed. Setting this value too high lets users save lengthy voice messages in their Inboxes.

This setting is important if you've implemented strict disk quotas for users. It must be set to a lower value than the one set for **Maximum call duration (min)**.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure the maximum recording duration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **Settings** tab.
4. Under **Maximum recording time duration (min)**, specify the maximum number of minutes allowed for each voice recording when a caller leaves a voice mail message.
5. Click **OK** to save your changes.

Use the Shell to configure the maximum recording duration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the maximum recording duration to 10 minutes for a UM dial plan named `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -MaxRecordingDuration 10
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you've configured the maximum recording duration on a UM dial plan, you may also want to:

- Configure the Number of Logon Failures Before Users Are Disconnected on a UM Dial Plan

- Configure the Maximum Call Duration on a UM Dial Plan
- Configure the Recording Idle Time-Out Value on a UM Dial Plan

1.9.2.3.2.23 Configure the Recording Idle Time-Out Value on a UM Dial Plan

Configure the Recording Idle Time-Out Value on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify the number of seconds of silence that the system allows when a voice message is being recorded before the call is ended. For most organizations, this value should be set to the default: 5 seconds.

This value can be set from 2 through 10. Setting this value too low can cause the system to disconnect callers before they've finished leaving their voice messages. Setting this value too high allows lengthy silences in voice messages.

Looking for other management tasks related to Unified Messaging (UM) dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure the recording idle time-out value

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **Settings** tab.
4. Under **Recording idle time-out (sec)**, enter the number of seconds of silence that the system allows when a voice message is being recorded before the call is ended.
5. Click **OK** to save your changes.

Use the Shell to configure the recording idle time-out value

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the recording idle time-out value to 10 for a UM dial plan named MyUMDialPlan.

```
Set-UMDialPlan -identity MyUMDialPlan -RecordingIdleTimeout 10
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you've configured the recording idle time-out value, you may also want to:

- Configure the Maximum Recording Duration on a UM Dial Plan
- Configure the Maximum Call Duration on a UM Dial Plan

1.9.2.3.2.24 Configure the Input Failures Before Disconnect on a UM Dial Plan

Configure the Input Failures Before Disconnect on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the number of times that users who call in to a subscriber access number can enter incorrect data before they're disconnected. This setting applies to both Outlook Voice Access users and unauthenticated callers who use directory search.

The following are examples of types of data that are considered incorrect:

- A caller requests an extension number that isn't found in the system
- The system can't locate the user's extension number to transfer the call
- A caller presses a menu option that isn't valid.

The value of this setting can be from 1 through 20. For most organizations, this value should be set to the default of three attempts. Setting this value too low may prematurely disconnect callers.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure the input failures before disconnect

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to manage, and then click **Properties** in the action pane.
3. On the dial plan **Properties** page, click the **Settings** tab.
4. Under **Input failures before disconnect**, enter the number of times that callers can enter incorrect data before they're disconnected.
5. Click **OK** to save your changes.

Use the Shell to configure the input failures before disconnect

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the input failures before disconnect to 5 on a UM dial plan named `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -InputFailuresBeforeDisconnect 5
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you configure the input failures before disconnect, you may also want to:

- Configure the Number of Logon Failures Before Users Are Disconnected on a UM Dial Plan
- Configure the Maximum Call Duration on a UM Dial Plan

1.9.2.3.2.25 Configure the Default Language on a UM Dial Plan

Configure the Default Language on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure a Unified Messaging (UM) dial plan with a default language. Each dial plan and auto attendant you create will use English (en-US) as the default language. The English (en-US) language pack is installed by default on all versions of Microsoft Exchange Server 2010 and can't be removed.

If you want to select another language, such as German (de-DE), you must first download the German UM language pack .exe file from Exchange Server 2010 SP2 UM Language Packs and install the UM language pack on the UM server using the executable (UMLanguagePack.de-de.exe) installation file. After you've installed the UM language pack, you can set the default language to a language other than English (en-US) on UM dial plans and UM auto attendants.

Looking for other management tasks related to UM dial plans? Check out Managing UM

Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure the default language on a UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Dial Plans** tab, select the UM dial plan you want to modify.
3. In the action pane, click **Properties**.
4. On the dial plan **Properties** page, click the **Settings** tab.
5. On the **Settings** tab, in the **Language Settings** section, in the **Default language** option list, select the language you want to use.
6. Click **OK** to accept your changes.

Use the Shell to configure the default language on a UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example sets the default language on a UM dial plan named `MyUMDialPlan` to German.

```
Set-UMDialPlan -Identity MyUMDialPlan -DefaultLanguage de-DE
```

This example sets the default language on a UM dial plan named `MyUMDialPlan` to Japanese.

```
Set-UMDialPlan -Identity MyUMDialPlan -DefaultLanguage ja-JP
```

This example sets the default language on a UM dial plan named `MyUMDialPlan` to Australian English.

```
Set-UMDialPlan -Identity MyUMDialPlan -DefaultLanguage en-AU
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you configure the default language on a UM dial plan, you may also want to:

- View or Configure the Properties of a UM Dial Plan
- Install a Unified Messaging Language Pack on a UM Server
- Remove a Unified Messaging Language Pack from a UM Server

1.9.2.3.2.26 Configure Dialing Rule Groups on a UM Dial Plan

Configure Dialing Rule Groups on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure dialing rule groups for a Unified Messaging (UM) dial plan in Microsoft Exchange Server 2010. Dialing rule groups specify settings for in-country/region and international calls that will be placed by UM-enabled users from inside your organization. After you create a dialing rule group, you must add a dialing group entry. Each dialing rule entry that's defined in the dialing rule group determines the types of calls, in-country/region or international, that users within a specific dialing rule group can make when they place outgoing calls. By default, UM-enabled users aren't allowed to dial external telephone numbers from inside the organization. However, they're allowed to dial UM-enabled users who are associated with the same dial plan.

After you create the UM dial plan with an in-country/region or international dialing rule group and configure the dialing rule entries, you must add the dialing rule group to the dialing restrictions on the UM mailbox policy associated with the UM dial plan. When you add the dialing rule group to the dialing restrictions on the UM mailbox policy, the settings you use will apply to all UM-enabled users associated with the UM mailbox policy. For more information about how to create dialing rule entries, see Create a Dialing Rule Entry on a UM Dial Plan.

Important:

If you've integrated Exchange Unified Messaging and Office Communications Server, you'll probably find it unnecessary to configure dialing rules or dialing rule groups in Exchange Unified Messaging. Office Communications Server is designed to perform call routing and number translation for users in your organization, and will also do this when the calls are made by Exchange Unified Messaging on behalf of users.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure in-country/region dialing rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Dial Plans** tab.
3. Select the dial plan you want to modify, and then, in the action pane, click **Properties**.

4. On the **Dialing Rule Groups** tab, under **In-Country/Region Rule Groups**, do one of the following:
   - Click **Add** to add a dialing rule entry. On the **Dialing Rule Entry** page, enter the number mask and the number to be dialed for the dialing rule entry. A number mask is represented by a series of Xs or asterisks and replaces the number of digits that follow the prefix for a telephone number, for example, 91425xxxxxxx, or 91425*. If a number that's dialed by a caller matches the prefix configured in the dialing rule entry, the PBX will dial the number that was specified in the **Dialed number** field.
   - Click **Edit** to change the in-country/region dialing rule entry settings.
   - Click **Remove** to delete the in-country/region dialing rule entry.
5. Click **OK** to save your changes.

Use the EMC to configure international dialing rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Dial Plans** tab.
3. Select the dial plan you want to modify, and then, in the action pane, click **Properties**.
4. On the **Dialing Rule Groups** tab, under **International Rule Groups**, do one of the following:
   - Click **Add** to add a dialing rule entry. On the **Dialing Rule Entry** page, enter the number mask and the number to be dialed for the dialing rule entry. A number mask is represented by a series of Xs or asterisks and replaces the number of digits that follow the prefix for a telephone number, for example, 91425xxxxxxx, or 91425*. If a number that's dialed by a caller matches the prefix configured in the dialing rule entry, the PBX will dial the number that was specified in the **Dialed number** field.
   - Click **Edit** to change the international dialing rule entry settings.
   - Click **Remove** to delete the international dialing rule entry.
5. Click **OK** to save your changes.

Use the Shell to configure in-country/region dialing rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example configures a UM dial plan named `MyDialPlan` with in-country or region dialing rules.

```
$csv=import-csv "C:\MyInCountryGroups.csv"
Set-UMDialPlan -Identity MyDialPlan -ConfiguredInCountryGroups $csv
Set-UMDialPlan -Identity MyDialPlan -AllowedInCountryGroups "local, long distance
```

Use the Shell to configure international dialing rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions

topic.

This example configures a UM dial plan named MyDialPlan with international dialing rules.

```
$csv=import-csv "C:\MyInternationalGroups.csv"
Set-UMDialPlan -Identity MyDialPlan -ConfiguredInternationalGroups $csv
Set-UMDialPlan -Identity MyDialPlan -AllowedInternationalGroups "local, long dist
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you configure dialing rule groups, you may also want to:

- Create a Dialing Rule Entry on a UM Dial Plan
- Enable Dialing Restrictions on a UM Mailbox Policy.

1.9.2.3.2.27 Create a Dialing Rule Entry on a UM Dial Plan

Create a Dialing Rule Entry on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can create a dialing rule entry for a dialing rule group on a Unified Messaging (UM) dial plan in Microsoft Exchange Server 2010. After you create an in-country/region or international dialing rule group on a UM dial plan, you must create a dialing rule entry for the dialing rule group.

A dialing rule entry defines the telephone numbers and number masks for in-country/region and international calls that can be made by UM-enabled users associated with a UM mailbox policy. Each dialing rule determines the types of calls users within a dialing rule group can make. However, you must correctly configure the dialing rule entry with a valid number mask and a dial number. After you create a dialing rule group and define the appropriate dialing rule entries on the **Dialing Group Rules** tab, you must add the appropriate dialing rule groups from the UM dial plan to a UM mailbox policy on the **Dialing Restrictions** tab.

Important:

If you've integrated Exchange Unified Messaging and Office Communications Server, you'll probably find it unnecessary to configure dialing rules or dialing rule groups in Exchange Unified Messaging. Office Communications Server is designed to perform call routing and number translation for users in your organization, and will also do this when the calls are made by Exchange Unified Messaging on behalf of users.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

Use the EMC to configure a dialing rule entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. On the **UM Dial Plans** tab, select the UM dial plan you want to manage.
3. In the action pane, click **Properties**.
4. On the dial plan **Properties** page, under the **Dialing Rule Groups** tab, under **In-Country/Region Rule Groups** or **International Rule Groups**, click the **Add** button.
5. On the **Dialing Rule Entry** page for the **In-Country/Region Rule Groups** or **International Rule Groups**, enter the following information:
   - **Name** Use this list to select the name of an existing dialing rule group or, if you want to create a dialing rule group, type the name of the dialing rule group. This box can contain only text characters. The display name for the dialing rule entry can contain up to 32 characters.
   - **Number mask** Use this box to define the number mask for the dialing rule. A number mask defines the telephone number format that a Unified Messaging server will use to determine what outgoing telephone number it will dial for a user. An example of a valid number mask is 91425xxxxxxx. This box can contain only numbers and the letter "x."
   - **Dialed number** Use this box to define the dialed number for the dialing rule. The dialed number is used to determine the actual dial string that's sent to the IP gateway. This number can be different from the number that's obtained by Unified Messaging for the outgoing call. However, your Private Branch eXchange (PBX) can also be configured to omit the area code for local calls and can be configured for private voice numbering plans. Any wildcard (x) characters included in the dial string replace the digits from the original number that were matched by the number mask on the dialing rule. An example of a valid dialed number is 9xxxxxxx. This box can contain only numbers and the letter "x."
   - **Comment** Use this box to enter a comment or description for the dialing rule that you are adding or modifying. By default, this box is blank.
6. Click **OK** to save your changes.

Use the Shell to configure a dialing rule entry

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example configures a dialing rule entry for an in-country/region rule group.

```
Set-UMDialPlan -Identity MyUMDialPlan -ConfiguredInCountryOrRegionGroups <name, a
```

This example configures a dialing rule entry for an international rule group.

```
Set-UMDialPlan -Identity MyUMDialPlan -ConfiguredInternationalGroups <name, allow
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you configure a dialing rule entry, you may also want to:

- Delete a UM Dial Plan
- Managing UM Auto Attendants
- Configure Business Hours for a UM Auto Attendant

1.9.2.3.2.28 Enable Dialing Restrictions on a UM Dial Plan

Enable Dialing Restrictions on a UM Dial Plan

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable dialing restrictions on a Unified Messaging (UM) dial plan in Microsoft Exchange Server 2010. Dialing restrictions are used to configure dialing rules that can be used to prohibit users who call in to a subscriber access number configured on a UM dial plan from making certain types of telephone calls. Dialing restrictions are also used when you want to allow users to place calls to in-country/region or international telephone numbers.

When you configure dialing restrictions and outdialing on a UM dial plan, the dialing restrictions that you configure will apply to all UM-enabled or Outlook Voice Access users associated with the UM dial plan and to anonymous callers when they call in to a subscriber access number configured on the UM dial plan.

For outdialing to work, the following settings must be configured correctly:

- **Dialing group rules** Dialing group rules determine the types of calls users within a dialing group can make. Dialing group rules include:
- **Dialing rule entries** Dialing rule entries define the number that is dialed by the user and the actual number that will be dialed by the Private Branch eXchange (PBX) or IP PBX.
- **Dialing restrictions** Dialing restrictions determine the restrictions that will be applied to prevent users from incurring unauthorized telephone charges or from dialing long distance calls.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.
- A UM dialing rule group has been created. For detailed steps, see Configure Dialing Rule Groups on a UM Dial Plan.

Use the EMC to enable dialing restrictions on a UM dial plan for in-country/region rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Dial Plans** tab.
3. Select the UM dial plan you want to change, and then, in the action pane, click **Properties**.
4. On the UM dial plan **Properties** page, on the **Dialing Restrictions** tab, under **Select allowed in-country/region rule groups from dial plan**, click **Add**.
5. On the **Select Allowed In-Country/Region Groups** page, select the dialing rule group configured on the UM dial plan, and then click **OK**.
6. Click **OK** to save your changes.

Use the EMC to enable dialing restrictions on a UM dial plan for international rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Dial Plans** tab.
3. Select the UM dial plan you want to change, and then, in the action pane, click **Properties**.
4. On the UM dial plan **Properties** page, on the **Dialing Restrictions** tab, under **Select allowed international rule groups from dial plan**, click **Add**.
5. On the **Select Allowed International Groups** page, select the dialing rule group configured on the UM dial plan, and then click **OK**.
6. Click **OK** to save your changes.

Use the Shell to enable in-country/region and international dialing restrictions on a UM dial plan

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables the InCountry/RegionGroup1, InCountry/RegionGroup2, InternationalGroup1, and InternationalGroup2 dialing restrictions on a UM dial plan named `MyUMDialPlan`.

```
Set-UMDialPlan -Identity MyUMDialPlan -AllowedInCountryOrRegionGroups InCountry/R
```

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you enable dialing restrictions on a UM dial plan, you may also want to:

- Create a Dialing Rule Entry on a UM Dial Plan
- Configure Dialing Rule Groups on a UM Dial Plan

1.9.2.3.2.29 Enable Custom Prompt Recording Using the Telephone User Interface

Enable Custom Prompt Recording Using the Telephone User Interface

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the Shell to record custom prompts and greetings for Unified Messaging (UM) dial plans and auto attendants using the telephone user interface (TUI). This can be useful when you can't create and edit a custom prompt or a greeting by using a computer, when you don't have access to a Unified Messaging server, or when there's an emergency such as an organization closure because of severe weather.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the Shell to enable a custom prompt or greeting recording using the TUI

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM dial plans" entry in the Unified Messaging Permissions topic.

This example enables you to manage custom prompt recording using the telephone user interface. You can record custom prompts and greetings by using the TUI if you follow these steps:

1. Create a domain user account that cannot log on interactively.
2. Delegate the Exchange Organization Administrator role to the domain user account.
3. Create an Exchange mailbox for the domain user.
4. Enable the domain user's mailbox for Unified Messaging.

Important:
Allow only those administrators who are managing prompts and greetings

access to the extension number and PIN for the domain user account. Use this domain user account only for managing prompts over the telephone.

5. Create a .wav file to be used for the custom greeting for the UM dial plan or auto attendant. Save the .wav file and upload it to a Unified Messaging server.
6. Run the following cmdlet:

```
Set-UMDialPlan -identity MyUMDialPlan -TUIPromptEditingEnabled $true
```

Note:
You must log on using the account that you'll use so that the mailbox is set up. If you don't first log on to the user's mailbox, you must log off and log back on to the system before you can hear the correct prompts and greetings when you use the TUI.

Perform TUI prompt provisioning on a UM auto attendant

1. Call the phone number that's been configured on the UM auto attendant.
2. While the welcome greeting for the auto attendant is being played, press the # key, then press the * key.
3. You'll be prompted to enter an extension number. Enter the extension number of the UM-enabled user who has permission to perform TUI prompt provisioning.
4. You'll be prompted for a PIN. Enter the user's PIN.

Perform TUI prompt provisioning on a UM dial plan

1. Call a pilot or subscriber access number you use to log on to Outlook Voice Access.
2. While the welcome greeting is being played, press the # and * keys.
3. If you're calling from a phone that's being used by a UM-enabled user, you'll be prompted for a PIN. Instead of entering the PIN, press the * key. You'll be prompted for an extension number.
4. If you're calling from a phone that's not used by a UM-enabled user, you'll automatically be prompted for an extension number. Enter the extension number of the UM-enabled user who has permission to perform TUI prompt provisioning.
5. You'll be prompted for a PIN. Enter the user's PIN.

For more information about syntax and parameters, see Set-UMDialplan.

Other Tasks

After you enable a custom prompt or greeting recording using the TUI, you may also want to:

- Enable a Custom Welcome Greeting on a UM Dial Plan
- Enable a Custom Business Hours Welcome Greeting on a UM Auto Attendant

1.9.2.3.2.30 Import and Export Custom Prompts for Unified Messaging

Import and Export Custom Prompts for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can import custom prompts into a system mailbox or export custom prompts from system mailboxes that are used with Unified Messaging (UM) dial plans and auto attendants in Microsoft Exchange Server 2010. Custom prompts are audio files used by Unified Messaging and include the following:

- UM dial plans: Customized welcome greetings and informational announcements.
- UM auto attendants: Customized after hours welcome greetings and menus, informational announcements, business hours and non-business hours welcome greetings and menus, and key mappings.

Custom prompts can be imported and exported by using the new cmdlet **Import-UMPrompt** and **Export-UMPrompt** cmdlets. The Microsoft Exchange Server 2007 Unified Messaging cmdlet **Copy-UMCustomPrompt** isn't supported in Exchange 2010 Unified Messaging for copying custom prompts.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.

Use the Shell to import custom prompts for UM dial plans and auto attendants

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM prompts" entry in the Unified Messaging Permissions topic.

This example imports the welcome greeting file welcomegreeting.wav from d:\UMPrompts into the UM dial plan `MyUMDialPlan`.

```
[byte[]]$c = Get-content -Path "d:\UMPrompts\welcomegreeting.wav" -Encoding Byte
Import-UMPrompt -UMDialPlan MyUMDialPlan -PromptFileName "welcomegreeting.wav" -P
```

This example imports the welcome greeting file welcomegreeting.wav from d:\UMPrompts into the UM auto attendant `MyUMAutoAttendant`.

```
[byte[]]$c = Get-content -Path "d:\UMPrompts\welcomegreeting.wav" -Encoding Byte
Import-UMPrompt -UMAutoAttendant MyUMAutoAttendant -PromptFileName "welcomegreeti
```

For more information about syntax and parameters, see Import-UMPrompt.

Use the Shell to export custom prompts from UM dial plans and auto attendants

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM prompts" entry in the Unified Messaging Permissions topic.

This example exports the welcome greeting for the UM dial plan MyUMDialPlan and saves it as the file welcomegreeting.mp3.

```
$prompt = Export-UMPrompt -PromptFileName "customgreeting.mp3" -UMDialPlan MyUMDi
set-content -Path "d:\DialPlanPrompts\welcomegreeting.mp3" -Value $prompt.AudioDa
```

This example exports the business hours welcome greeting used for the UM auto attendant MYUMAutoAttendant and saves it as the file BusinessHoursWelcomeGreeting.mp3.

```
$prompt = Export-UMPrompt -BusinessHoursWelcomeGreeting -UMAutoAttendant MyUMAuto
set-content -Path "d:\UMPrompts\BusinessHoursWelcomeGreeting.mp3" -Value $prompt.
```

For more information about syntax and parameters, see Export-UMPrompt.

Other Tasks

After you import and export custom prompts for UM dial plans and auto attendants, you may also want to:

- View or Configure the Properties of a UM Dial Plan
- View or Configure the Properties of a UM Auto Attendant
- Enable Custom Prompt Recording Using the Telephone User Interface

1.9.2.3.2.31 Import Custom Prompts from Exchange 2007 to Exchange 2010

Import Custom Prompts from Exchange 2007 to Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the MigrateUMCustomPrompts.ps1 script to migrate a copy of all Microsoft Exchange Server 2007 Unified Messaging (UM) custom prompts to Exchange 2010 Unified Messaging. This includes all custom prompts in all Exchange 2007 UM dial plans and UM auto attendants. By default, the MigrateUMCustomPrompts.ps1 script is located in the *<Program Files>\Microsoft\Exchange Server\V14\Scripts* folder on a UM server running Microsoft Exchange Server 2010 Service Pack 1 (SP1).

System mailboxes are created when you install Exchange 2010 to support features such as message approval, and are also used in Exchange 2010 Unified Messaging to store dial plan and auto attendant custom prompts and Unified Messaging reports. You can import custom prompts from Exchange 2007 Unified Messaging into an Exchange 2010 system mailbox that's used with Unified Messaging dial plans and auto attendants in Exchange 2010. Custom prompts are audio files that are used by Unified Messaging, and include the following:

- UM dial plans: Customized welcome greetings and informational announcements.
- UM auto attendants: Customized after-hours welcome greetings and menus, informational announcements, business hours and non-business hours welcome greetings and menus, and key mappings.

Custom prompts can also be imported individually by using the cmdlet **Import-UMPrompt**. The Exchange 2007 Unified Messaging cmdlet **Copy-UMCustomPrompt** isn't supported for copying custom prompts in Exchange 2010 Unified Messaging.

Note:
The MigrateUMCustomPrompts.ps1 script is included with Exchange 2010 SP1. It must be run on an Exchange 2010 Unified Messaging server that has SP1 installed in the same organization with your Exchange 2007 UM servers.

Looking for other management tasks related to UM dial plans? Check out Managing UM Dial Plans.

Looking for other management tasks related to UM auto attendants? Check out Managing UM Auto Attendants.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM auto attendant has been created. For detailed steps, see Create a UM Auto Attendant.
- A custom prompt publishing point exists for the UM dial plans and UM auto attendants for the Exchange 2007 Unified Messaging servers.
- Custom prompts for UM dial plans and UM auto attendants have been created and saved in the custom prompt publishing point.

Use the MigrateUMCustomPrompts.ps1 script to migrate a copy of all custom prompts for UM dial plans and auto attendants

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM prompts" entry in the Unified Messaging Permissions topic.

1. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010** > **Exchange Management Shell**.
2. In the Shell, at the prompt, type the path to the script. For example, type **cd "D:\Program Files\Microsoft\Exchange Server\V14\Scripts"**, and then press Enter.
3. At the Shell prompt, type **".\MigrateUMCustomPrompt"**, and then press Enter.

For more information about syntax and parameters, see Import-UMPrompt.

Other Tasks

After you import custom prompts for UM dial plans and auto attendants, you may also want to:

- View or Configure the Properties of a UM Dial Plan
- View or Configure the Properties of a UM Auto Attendant
- Enable Custom Prompt Recording Using the Telephone User Interface
- Upgrade from Exchange 2007 SP3 to Exchange 2010 RTM Unified Messaging
- Import and Export Custom Prompts for Unified Messaging

1.9.2.3.3 Managing UM Mailbox Policies

Managing UM Mailbox Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-18*

Create a UM Mailbox Policy

View or Configure the Properties of a UM Mailbox Policy

Delete a UM Mailbox Policy

Configure the Maximum Greeting Duration on a UM Mailbox Policy

Enable or Disable Missed Call Notifications on a UM Mailbox Policy

Enable or Disable Message Waiting Indicator on a UM Mailbox Policy

Enable or Disable Inbound Faxing on a UM Mailbox Policy

Enable or Disable Voice Mail Preview on a UM Mailbox Policy

Enable or Disable Outlook Voice Access on a UM Mailbox Policy

Enable or Disable Play on Phone on a UM Mailbox Policy

Enable or Disable Call Answering Rules on a UM Mailbox Policy

Include Text with the E-Mail Message Sent When a Mailbox Is UM-Enabled

Include Text with the E-Mail Message Sent When a PIN Is Reset

Include Text with the E-Mail Message Sent When a Voice Message Is Received

Include Text with the E-Mail Message Sent When a Fax Message Is Received

Configure the Minimum PIN Length on a UM Mailbox Policy

Configure the PIN Lifetime on a UM Mailbox Policy

Configure the Number of Previous PINs to Disallow on a UM Mailbox Policy

Enable or Disable Common PIN Patterns on a UM Mailbox Policy

Configure the Number of Incorrect PIN Entries Before a PIN Is Reset on a UM Mailbox Policy

Configure the Number of Incorrect PIN Entries Before a Mailbox Is Locked Out on a UM Mailbox Policy

Enable Dialing Restrictions on a UM Mailbox Policy

Configure Protected Voice Mail from Unauthenticated Callers on a UM Mailbox Policy

Configure Protected Voice Mail from Authenticated Callers on a UM Mailbox Policy

Enable or Disable Multimedia Playback of Protected Voice Messages on a UM Mailbox Policy

Specify the Text to Display for E-Mail Clients that Don't Support Windows Rights Management on a UM Mailbox Policy

Configure TUI Settings on a UM Mailbox Policy

Configure a Voice Mail Preview Partner on a UM Mailbox Policy

Set the Voice Mail Preview Partner Address on a UM Mailbox Policy

Set the Voice Mail Preview Partner ID on a UM Mailbox Policy

Set the Maximum Message Duration for a Voice Mail Preview Partner on a UM Mailbox Policy

Set the Maximum Delivery Delay for a Voice Mail Preview Partner on a UM Mailbox Policy

1.9.2.3.3.1 Create a UM Mailbox Policy

Create a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can create a Unified Messaging (UM) mailbox policy to apply a common set of UM policy settings, such as PIN policy settings or dialing restrictions, to a collection of UM-enabled mailboxes. UM mailbox policies link a UM-enabled user with a UM dial plan and apply a common set of policies or security settings to a collection of UM-enabled mailboxes. UM mailbox policies are useful for applying and standardizing UM configuration settings for UM-enabled users.

By default, when a UM dial plan is created, a UM mailbox policy is also created. However, there are other times that you may have to create additional UM mailbox policies or modify existing UM mailbox policies after you deploy Unified Messaging in your Microsoft Exchange Server 2010 organization.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

What Do You Want to Do?

- Use the EMC to create a UM mailbox policy
- Use the Shell to create a UM mailbox policy

Use the EMC to create a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Mailbox Policies** tab.
3. In the action pane, click **New UM Mailbox Policy**.
4. In the New UM Mailbox Policy wizard, complete the following fields:
   - **Name** Use this text box to specify a unique name for the UM mailbox policy. This is a display name that appears in the EMC. If you must change the display name of the UM mailbox policy after it's been created, you must first delete the existing UM mailbox policy, and then create another UM mailbox policy that has the appropriate name. To delete the UM mailbox policy, there must not be any UM-enabled users who are associated with the UM mailbox policy.

     The UM mailbox policy name is required, but it is used for display purposes only. Because your organization may use multiple UM mailbox policies, we recommend that you use meaningful names for your UM mailbox policies. The maximum length of a UM mailbox policy name is 64 characters, and it can include spaces. However, it cannot include any of the following characters: " / \ [ ] : ; | = , + * ? < >.
   - **Select associated dial plan** Click **Browse** to select the UM dial plan that will be associated with the UM mailbox policy. You must associate a UM mailbox policy with at least one UM dial plan. A single UM mailbox policy must be associated with at least one UM dial plan. However, you can also associate multiple UM mailbox policies with a single dial plan.
5. On the **Completion** page, confirm whether the UM mailbox policy was successfully created:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to complete the New UM Mailbox Policy wizard.

Use the Shell to create a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example creates a UM mailbox policy named `MyUMMailboxPolicy` associated with a UM dial plan named `MyUMDialPlan`.

```
New-UMMailboxPolicy -Name MyUMMailboxPolicy -UMDialPlan MyUMDialPlan
```

For more information about syntax and parameters, see New-UMMailboxPolicy.

Other Tasks

After you have created a Unified Messaging Mailbox Policy, you may also want to:

- Configuring PIN Security for a UM-Enabled User
- Configure a UM-Enabled User's TUI Settings
- Enable a User for Unified Messaging

For More Information

Understanding Unified Messaging Mailbox Policies

1.9.2.3.3.2 View or Configure the Properties of a UM Mailbox Policy

View or Configure the Properties of a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After you create a Unified Messaging (UM) mailbox policy, you can view and configure a variety of settings. For example, you can configure Unified Messaging features like Voice Mail Preview or Play on Phone and other security-related options such as Protected Voice Mail and PIN policy settings.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

What Do You Want to Do?

- Use the EMC to view or configure UM mailbox policy properties
- Use the Shell to configure UM mailbox policy properties
- Use the Shell to view UM mailbox policy properties

Use the EMC to view or configure UM mailbox policy properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Mailbox Policies** tab, and then select the UM mailbox policy that you want to configure.
3. In the action pane, click **Properties**.
4. Use the **General** tab to view and configure settings for a UM mailbox policy. For example, you can view the dial plans associated with the UM mailbox policy or disable missed call notifications for users who are associated with a specific UM mailbox policy.

When you modify the settings on a UM mailbox policy, the settings are applied to all users who are associated with the UM mailbox policy. UM mailbox policies let you apply a common set of settings to a collection or group of mailboxes. You must create a UM mailbox policy before you can enable users for Unified Messaging. You can view or configure the following:

- **Associated UM dial plan** Displays the name of the dial plan associated with the UM mailbox policy. This is the name of the dial plan displayed in the Shell.

  When a new UM mailbox policy is created, it must be associated with a dial plan. After the UM mailbox policy is created and associated with a dial plan, the settings defined on the mailbox policy are applied to the users who are associated with the dial plan. By default, when you create a UM dial plan using the Shell, it will also create a UM mailbox policy.

  A UM mailbox policy can't be changed after it's associated with a dial plan.
- **Modified** Displays the date of the last modification or change made to the UM mailbox policy.
- **Maximum greeting duration (minutes)** Use this text box to enter the maximum number of minutes that users who are associated with the UM mailbox policy can use when they record their voice mail greeting. You can modify this setting after the UM mailbox policy is created. Only numeric characters are allowed. The valid range for the greeting is from 1 through 10 minutes. The default setting is 5 minutes.
- **Allow missed call notifications** Select this check box to enable or disable missed call notifications for users associated with the UM mailbox policy.

  A missed call notification is an e-mail message sent to a user's mailbox when the user doesn't answer an incoming call. This is a different e-mail message than the e-mail message that contains the voice mail message left for a user.

  Typically, when a user misses an incoming call, the user receives two e-mail messages: an e-mail message that contains the voice mail message and a missed call notification message.

  By default, missed call notifications are enabled when a UM mailbox policy is created.
- **Allow Message Waiting Indicator** Select this check box to enable or disable Message Waiting Indicator for users associated with the UM mailbox policy. Message Waiting Indicator is a feature found in most legacy voice mail systems. In its most common form, it lights a lamp on the voice mail subscriber’s phone to indicate the presence of a new voice mail. Message Waiting Indicator can also be a text message sent to the UM-enabled user's mobile phone. If this option is disabled on the UM IP gateway, this feature isn't available to UM-enabled users associated with the UM mailbox policy. This option isn't available to UM-enabled users who have a mailbox on a Microsoft Exchange 2007 server. The default setting is enabled.
- **Allow inbound faxes** Select this check box to enable or disable inbound faxes for users associated with the UM mailbox policy. By default, when you enable users for Unified Messaging, they can receive faxes. However, there may be situations when users can't receive faxes, because the ability to receive faxes has been disabled on their mailbox. If this option is disabled on the UM dial plan, UM-enabled users associated with the UM mailbox policy won't be able to receive faxes. The default setting is disabled.

  After you have enabled the **Allow inbound faxes** setting, you will need to specify the URI for the partner fax server. If the Unified Messaging mailbox policy is associated with UM servers that use TCP and TLS, you will need to enter URIs for both TCP and TLS.
- **Allow Voice Mail Preview** Select this check box to enable or disable the Voice Mail Preview feature for users associated with the UM mailbox policy.

Enabling this setting allows users to receive the text of a voice mail in the message body of an e-mail or text message. If this option is disabled on the UM dial plan, this feature won't be available to UM-enabled users associated with the UM mailbox policy. This option isn't available to UM-enabled users who have a mailbox on an Exchange 2007 Unified Messaging server. The default setting is enabled.

- **Allow Outlook Voice Access** Select this check box to enable or disable access to Outlook Voice Access for UM-enabled users who are associated with this UM mailbox policy. Outlook Voice Access is a feature used by UM-enabled users to access their Exchange 2007 or Exchange 2010 mailbox over a phone. By default, this setting is enabled.
- **Allow Play on Phone** Select this check box to enable or disable the Play on Phone feature for users associated with the UM mailbox policy. This option is enabled by default and allows users to play their voice mail messages over a phone. The phone can be any phone, including an office or mobile phone. This option isn't available to UM-enabled users who have a mailbox on an Outlook 2007 Unified Messaging server.
- **Allow users to configure call answering rules** Select this check box to allow users who are associated with the UM mailbox policy to create call answering rules. If this option is disabled on the UM dial plan, this feature won't be available to UM-enabled users associated with the UM mailbox policy. This option isn't available to UM-enabled users who have a mailbox on an Exchange 2007 Unified Messaging server. The default setting is enabled.

5. Use the **Message Text** tab to configure message text settings for users who are associated with a UM mailbox policy. For example, you can specify the e-mail message text sent to users after they reset their UM PIN. You can configure the following:
   - **Text sent when a UM Mailbox is enabled** The text entered in this text box appears in the e-mail message sent to users when they are enabled for Unified Messaging. When a recipient's mailbox is enabled for Unified Messaging, an e-mail message that welcomes the user to Unified Messaging is sent to the user. This text box is limited to 512 characters. By default, no text is defined in this text box.

     This welcome message contains welcome text and the PIN information that the user will use to access the Unified Messaging system. The text entered in this text box is included at the bottom of this welcome message. You can use this text box to include information such as the Unified Messaging technical support telephone numbers or subscriber access numbers.

     If text isn't entered in this text box, the default text generated by the Unified Messaging system is included in the e-mail message.

     The text that you provide in this text box can be plain. It can also contain simple HTML formatting tags if you want to emphasize text or add hyperlinks to other content.

     Example 1 If you have any questions or suggestions about voice mail service, please call the help desk at extension 4200.

     Example 2 If you have any questions or suggestions about voice mail service, please call the help desk at extension 4200 or visit our Web site at .
   - **Text sent when a PIN is reset** The text entered in this text box is included in the e-mail message sent to UM-enabled users when their UM PIN is reset.

     A PIN is reset by the Unified Messaging system if the number of failed logon attempts exceeds 10 (by default) or if users reset their PIN using the Unified Messaging features included with

Microsoft Office Outlook 2007, Exchange 2010, Outlook Web App, or Outlook Voice Access from a telephone. You can use this text box to include information such as security notices or other security-related information in the e-mail message.
If text isn't entered in this text box, the default text generated by the Unified Messaging system is included in the e-mail message.
This text box is limited to 512 characters. By default, no text is defined in this text box.
The text that you provide in this text box can be plain. It can also contain simple HTML formatting tags if you want to emphasize text or add hyperlinks to other content.
Example 1 If you have any questions or suggestions about voice mail service, please call the help desk at extension 4200.
Example 2 If you have any questions or suggestions about voice mail service, please call the help desk at extension 4200 or visit our Web site at .

- **Text included with a voice message** The text entered in this text box is included in the e-mail message sent to users when they receive a voice mail message from an incoming caller. For example, this text can include disclaimers that contain information about forwarding voice mail messages or system security policies that describe the correct way to handle voice mail messages in your organization.
  If text isn't entered in this text box, the default text generated by the system is included in the e-mail message. This text box is limited to 512 characters. By default, no text is defined in this text box.
  The text that you provide in this text box can be plain. It can also contain simple HTML formatting tags if you want to emphasize text or add hyperlinks to other content.
  Example 1 If you have any questions or suggestions about voice mail service, please call the help desk at extension 4200.
  Example 2 If you have any questions or suggestions about voice mail service, please call the help desk at extension 4200 or visit our Web site at .
- **Text included with a fax message** The text entered in this text box is included in the e-mail message sent to users when they receive an incoming fax message in their Inbox. You can use this text box to include disclaimers that contain information about forwarding fax messages or other system security policies about the correct way to handle fax messages in your organization.
  If text isn't entered in this text box, the default text generated by the system is included in the e-mail message. This text box is limited to 512 characters. By default, no text is defined in this text box.

6. Use the **PIN Policies** tab to configure PIN settings for users who are associated with a UM mailbox policy. Unified Messaging PINs enable users to access their Inboxes by using a telephone. By configuring settings on this page, you can specify the minimum number of digits for a UM PIN or the number of failed logon attempts before users are locked out of their UM mailbox.
   Make sure that you plan carefully for the UM PIN policies that you implement in your environment. If you don't plan and implement the appropriate UM PIN policies, you may introduce security threats and mistakenly allow unauthorized access to your network. You can configure the following:
   - **Minimum PIN length** Use this text box to specify the minimum number of digits that a UM user's PIN can contain. The default setting is six digits. The

range is from 4 through 24 numeric digits. This setting can't be disabled.

Increasing the number of digits required for a PIN increases the level of security for your Unified Messaging system. Decreasing the number of digits required for a PIN reduces the level of security for your network. The fewer the digits that are required in a PIN, the easier it is for a potential attacker to guess a user's PIN.

If this setting is set too high, users might have problems remembering their PINs. However, if the setting is too low, you risk unauthorized access to the Unified Messaging system.

- **PIN lifetime (days)** Use this text box to configure the number of days until the UM-enabled user's PIN expires. After the PIN expires, the user must create a new UM PIN. For most organizations, this value should be set to the default of 60 days.

  The value of this setting can be from 0 through 999. If it's set to 0, PINs never expire. Setting this value too low can frustrate users because they are required to create and memorize new PINS too frequently.
- **Number of previous PINs to disallow** Use this setting to set the number of unique PINs that users must use before they can reuse an old PIN. For most organizations, this value should be set to the default of 5, the number of PINs that the system will remember. PIN history can't be disabled.

  You can set this value from 1 through 20. Setting this value too high can frustrate users because it can be difficult to memorize many PINs. Setting it too low may introduce a security threat to your network.
- **Allow common patterns in PIN** Use this setting to set PIN complexity requirements for Unified Messaging. These complexity requirements are enforced on PIN changes or when new PINs are created.

  If this option is disabled, sequential and repeated numbers and the suffix of the mailbox extension will be rejected. If this option is enabled, only the suffix of the mailbox extension will be rejected.

  As a security best practice, we recommend that you disable this setting. If this setting is disabled, user PINs can't contain the following:

  Sequential numbers, such as 123456 or 456789.

  Repeated numbers, such as 111111 or 8888888.

  Suffix of the mailbox extension.
- **Number of incorrect PIN entries before PIN is automatically reset** Use this text box to enter the number of sequential unsuccessful or failed logon attempts that can occur before the Unified Messaging system automatically resets a user's PIN. For most organizations, this value should be set to the default of 5 attempts.

  The value of this setting can be from 0 through 999. If it's set to 0, this setting is disabled and the system won't automatically reset users' PINs. Setting this value too low can frustrate users; setting it too high gives malicious users more attempts to determine the PIN.

  This setting must be set to a number lower than the number configured in the **Number of incorrect PIN entries before UM mailbox is locked out** setting. This setting is designed to help prevent a brute force attack on user PINs.
- **Number of incorrect PIN entries before UM mailbox is locked out** Use this text box to enter the maximum number of sequential unsuccessful or failed logon attempts before users are locked out of their mailbox.

  For example, if a user tries to log on to the mailbox unsuccessfully five times, based on the **Failed logon attempts before automatic PIN reset** setting, the system will reset the

user's PIN. If the user tries to use the new PIN five more times unsuccessfully, the system will again reset the PIN. If the user tries to use this new PIN five more times unsuccessfully, the user is then locked out of the mailbox. After a user is locked out, an administrator must manually reset or unlock the mailbox for the user.
This value can be set from 1 through 999. Setting this value too low can frustrate users; setting it too high gives malicious users more attempts to determine the PIN. For most organizations, this value should be set to the default of 15 attempts.
This number must be greater than the number set in the **Number of incorrect PIN entries before PIN is automatically reset** setting. This setting is designed to help prevent a brute force attack on user PINs.

7. Use the **Dialing Restrictions** tab on the UM mailbox policy properties to configure dialing rules for UM-enabled users who are associated with this UM mailbox policy. UM mailbox policies are required to enable users for Unified Messaging. They are useful for applying and standardizing Unified Messaging configuration settings for UM-enabled users. You can create UM mailbox policies to apply a common set of policies or security settings to a collection of UM-enabled mailboxes.
   You can use these settings to control the extension numbers that can be reached by UM-enabled users who are associated with the UM mailbox policy or to control the telephone numbers that can be dialed by UM-enabled users who are associated with the UM mailbox policy. You can configure the following:
   - **Allow calls to users within the same dial plan** Select this check box to allow UM-enabled users who call in to a subscriber access number configured on a dial plan and successfully log on to their mailbox to place calls or transfer to users who have extension numbers associated with another UM-enabled user within the same dial plan. By default, this setting is enabled.
     When you disable this setting, UM-enabled users who call in to a subscriber access number configured on a dial plan and successfully log on to their mailbox can place calls or transfer calls to users who aren't UM-enabled or to other extension numbers not associated with a UM-enabled user. However, they can't transfer to UM-enabled users who are within the same dial plan. This is because the **Allow calls to extensions** setting is enabled by default.
   - **Allow calls to extensions** When this setting is enabled, users who call in to a subscriber access number configured on a dial plan and successfully log on to their mailbox can place calls to users who aren't UM-enabled, to other extension numbers not associated with a UM-enabled user, and to UM-enabled users within the same dial plan. This is because the **Allow calls to users within the same dial plan** setting is enabled by default.
     When this setting is disabled, users who call in to a subscriber access number configured on a dial plan and successfully log on to their mailbox can't place calls to users who aren't UM-enabled or to other extension numbers not associated with a UM-enabled user. However, they can place calls or transfer calls to extension numbers associated with UM-enabled users. This is because the **Allow calls to users within the same dial plan** setting is enabled by default. The **Allow calls to extensions** setting is enabled by default.
     You can enable this setting in an environment where not all users have been UM-enabled. This setting is also useful when you want to allow users who call in to a subscriber access number configured on a dial plan to call extension numbers not

associated with a UM-enabled user.

- **Select allowed in-country/region rule groups from dial plan** Use this section to add or remove allowed in-country/region dialing rule groups. By default, there are no in-country/region dialing rule groups configured on UM mailbox policies.

  In-country/region dialing rule groups are used to allow or restrict the telephone numbers within a country or region that Outlook Voice Access users can dial. This helps prevent unnecessary or unauthorized telephone calls and charges.
  To add in-country/region dialing rule groups, you must first create the appropriate in-country/region dialing rule groups on the dial plan associated with the UM mailbox policy, and then add the appropriate dialing rule entries on the dialing rule group. After you create the required dialing rule groups on the dial plan, you must then add the dialing rule groups to the list of dialing restrictions on the **Dialing Restrictions** tab on the UM mailbox policy.
  In-country/region dialing rule groups can be used to enable a Unified Messaging server to allow or restrict access to telephone numbers within a country or region. This is applied to Outlook Voice Access users who have called in to a subscriber access number.
- **Select allowed international rule groups from dial plan** Use this section to add or remove allowed international dialing rule groups. By default, there are no international dialing rule groups configured on UM mailbox policies.

  To add international dialing rule groups, you must first create the appropriate international dialing rule groups on the dial plan associated with the UM mailbox policy, and then add the appropriate dialing rule entries on the dialing rule group. After you create the required dialing rule groups, you must add the dialing rule groups to the dialing restrictions on the UM mailbox policy.
  International dialing rule groups can be used to enable a Unified Messaging server to allow or restrict access to telephone numbers outside a country or region. This is applied to Outlook Voice Access users who have called in to a subscriber access number.
  International dialing rule groups are used to allow or restrict the telephone numbers outside a country or region that Outlook Voice Access users can dial. This helps prevent unnecessary or unauthorized telephone calls and charges.

8. Use the **Protected Voice Mail** tab to configure the following settings:
   - **Protect voice messages from unauthenticated callers** Select one of the following options from the drop-down list to determine whether an incoming call answered by a Unified Messaging server will protect voice messages. This setting applies to voice messages sent to UM-enabled users when they don't answer their phone. This setting also applies to voice messages sent directly to UM-enabled users when the caller uses a UM auto attendant. This option isn't available to UM-enabled users who have a mailbox on an Exchange 2007 Unified Messaging server. You can configure the following:

     None Use this setting to not have protection applied to any voice messages sent to UM-enabled users.
     Private Use this setting when you want the Unified Messaging server to apply protection only to voice messages that have been marked as private by the caller.
     All Use this setting when you want the Unified Messaging server to apply protection to all voice messages including those

not marked as private.

- **Protect voice messages from authenticated callers** Select one of the following options from the drop-down list to determine whether an incoming call answered by a Unified Messaging server will protect voice messages. This setting applies to voice messages sent to UM-enabled users when they don't answer their phone. This setting also applies when callers log on to their mailbox using Outlook Voice Access, and then create and send a voice message. This option isn't available to UM-enabled users who have a mailbox on an Exchange 2007 Unified Messaging server. You can configure the following:
  None Use this setting to not have protection applied to any voice messages sent to UM-enabled users.
  Private Use this setting when you want the Unified Messaging server to apply protection only to voice messages that have been marked as private by the caller.
  All Use this setting when you want the Unified Messaging server to apply protection to all voice messages including those not marked as private.
- **Allow multimedia playback of protected voice messages** Select this check box if you want to force users who receive protected voice messages to use the Play on Phone feature. Or, if the client software doesn't support rights management, users must use Outlook Voice Access. The Play on Phone feature only applies to clients using a version of Outlook that supports rights management. For Outlook 2007 and earlier versions that don't support rights management, and for Outlook Web App clients, Outlook Voice Access is the only way that users can listen to Protected Voice Mail.
  The default setting requires all users associated with the UM mailbox policy to use the Play on Phone feature to listen to voice messages that are protected. By doing this, it prevents other people from hearing the voice message using a media player over computer speakers or using a media player on a mobile phone to hear the voice message. Even if this is enabled, a UM-enabled user can still use Outlook Voice Access to hear the Protected Voice Mail.
  This is especially useful when UM-enabled users use public computers, laptops in public places, or their mobile phone's media player to listen to Protected Voice Mail that can contain private information. This option isn't available to UM-enabled users who have a mailbox on an Exchange 2007 Unified Messaging server.
- **Specify the text to display to voice mail recipients who have e-mail clients that don't support Windows Rights Management** Protected Voice Mail can only be accessed by e-mail clients that support Information Rights Management (IRM), or if a UM-enabled user uses Outlook Voice Access to access the Protected Voice Mail message.
  If a Protected Voice Mail is sent to an e-mail client that doesn't support IRM, the text that you include in this box will be sent to the user in an e-mail message. This information should include instructions about what to do to be able to receive the Protected Voice Mail.

Use the Shell to configure UM mailbox policy properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the PIN settings for users who are associated with a UM mailbox policy named MyUMMailboxPolicy.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 8 -M
```

This example selects the in-country or region groups and international groups from those configured on the UM dial plan associated with the UM mailbox policy. UM-enabled users associated with this UM mailbox policy will be able to place outbound calls according to the rules defined on these groups.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowDialPlanSubscribers $true -
```

This example configures the text of voice messages sent to UM-enabled users and the text included in an e-mail sent to a user who has been UM-enabled.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -UMEnabledText "You have been ena
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Use the Shell to view UM mailbox policy properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example returns a formatted list of all UM mailbox policies in the Active Directory forest.

```
Get-UMMailboxPolicy | Format-List
```

This example returns the properties and values for a UM mailbox policy named MyUMMailboxPolicy.

```
Get-UMMailboxPolicy -Identity MyUMMailboxPolicy
```

For more information about syntax and parameters, see Get-UMMailboxPolicy.

Other Tasks

After you configure settings on a UM mailbox policy, you may also want to configure PIN security. For details, see Configuring PIN Security for a UM-Enabled User.

For More Information

Understanding Unified Messaging Mailbox Policies

Understanding Outdialing

1.9.2.3.3.3 Delete a UM Mailbox Policy

Delete a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can delete or remove a Unified Messaging (UM) mailbox policy. When you delete a UM mailbox policy, the UM mailbox policy will no longer be available to be associated to the Microsoft Exchange Server 2010 recipients who are newly enabled for Unified Messaging. However, the UM mailbox policy can't be deleted if it's referenced by any UM-enabled mailboxes.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to delete a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Mailbox Policies** tab.
3. Click to highlight the UM mailbox policy you want to delete.
4. In the action pane, click **Remove**.
5. In the confirmation dialog box, click **Yes**.

Use the Shell to delete a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example deletes a UM mailbox policy named `MyUMMailboxPolicy`.

```
Remove-UMMailboxPolicy -Identity MyUMMailboxPolicy
```

For information about syntax and parameters, see the Remove-UMMailboxPolicy reference topic.

Other Tasks

After you delete a UM mailbox policy, you may also want to Create a UM Mailbox Policy.

Configure the Maximum Greeting Duration on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Maximum greeting duration setting enables you to enter the maximum number of minutes that users associated with the UM mailbox policy can use to record their voice mail greetings. This setting applies to both their standard voice mail and their Out of Office voice mail greetings. By default, the maximum greeting duration is set to 5 minutes. However, you can configure the maximum meeting duration to any setting between 1 and 10 minutes.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to change the maximum greeting duration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **General** tab, next to **Maximum greeting duration (minutes)**, enter the time, in minutes, for the maximum greeting duration for your UM users.
4. Click **OK** to save your changes.

Use the Shell to change the maximum greeting duration

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example configures the maximum greeting duration on the UM mailbox policy `MyUMMailboxPolicy` to 3 minutes.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy MaxGreetingDuration 3
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

- After you change the maximum greeting duration, you may also want to View or Configure the Properties of a UM Mailbox Policy.

1.9.2.3.3.5 Enable or Disable Missed Call Notifications on a UM Mailbox Policy

Enable or Disable Missed Call Notifications on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable missed call notifications for a Unified Messaging (UM) mailbox policy in Microsoft Exchange Server 2010. A missed call notification is an e-mail message that's sent to a user's mailbox when the user doesn't answer an incoming call. This is a different e-mail message than the e-mail message that contains the voice message that's left for a user.

When you disable missed call notifications on a UM mailbox policy, you prevent all users associated with the UM mailbox policy from receiving an e-mail message when they don't answer an incoming call. By default, missed call notifications are enabled with each UM mailbox policy that's created.

Note:

By default, a UM mailbox policy is created every time you create a UM dial plan.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable missed call notifications for a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Mailbox Policies** tab.

3. Select the UM mailbox policy that you want to change, and then, in the action pane, click **Properties**.
4. On the UM mailbox policy **Properties** page, click the **General** tab.
5. To enable missed call notifications, select the check box next to **Allow missed call notifications**.
6. To disable missed call notifications, clear the check box next to **Allow missed call notifications**.
7. Click **OK** to save your changes.

Use the Shell to enable or disable missed call notifications for a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example enables missed call notifications for a UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowMissedCallNotifications $tr
```

This example disables missed call notifications for a UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowMissedCallNotifications $fa
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you enable or disable missed call notifications for a UM mailbox policy, you may also want to:

- Enable or Disable Message Waiting Indicator on a UM Mailbox Policy
- Allow or Prevent Message Waiting Indicator on a UM IP Gateway

Enable or Disable Message Waiting Indicator on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable the Message Waiting Indicator for users associated with a Unified Messaging (UM) mailbox policy. Message Waiting Indicator is a feature found in most legacy voice mail systems. In its most common form, it lights a lamp on a voice mail subscriber's phone to indicate the presence of a new voice mail message. Message Waiting Indicator can also be a text message sent to a UM-enabled user's mobile phone. The default setting is enabled.

If this option is disabled on the UM IP gateway, this feature isn't available to UM-enabled users associated with the UM mailbox policy. This option isn't available to UM-enabled users who have a mailbox on a Microsoft Exchange Server 2007 server.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable Message Waiting Indicator

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **General** tab, select or clear the check box next to **Allow Message Waiting Indicator**.
4. Click **OK** to save your changes.

Use the Shell to enable or disable Message Waiting Indicator

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example disables the Message Waiting Indicator for users associated with the UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowMessageWaitingIndicator $fa
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you've enabled or disabled Message Waiting Indicator on a UM mailbox policy, you may also want to View or Configure the Properties of a UM Mailbox Policy.

1.9.2.3.3.7 Enable or Disable Inbound Faxing on a UM Mailbox Policy

Enable or Disable Inbound Faxing on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable inbound faxes for users associated with a Unified Messaging (UM) mailbox policy. By default, when you enable users for Unified Messaging, this option is selected but users can't receive fax messages until you specify the URI for the fax partner server and deploy a fax partner server for your organization. If the Unified Messaging mailbox policy is associated with UM servers that use TCP and TLS, you'll need to enter URIs for both TCP and TLS. If the option to allow incoming faxes is disabled on the UM dial plan, UM-enabled users associated with the UM mailbox policy won't be able to receive faxes.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable inbound faxing

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **General** tab, select or clear the check box next to **Allow inbound faxes**.
4. Click **OK** to save your changes.

Use the Shell to enable or disable inbound faxing

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example allows users who are associated with the UM mailbox policy `MyUMMailboxPolicy` to use inbound faxing.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowFax $true
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you enable or disable inbound faxing on a UM mailbox policy, you may also want to

View or Configure the Properties of a UM Mailbox Policy.

1.9.2.3.3.8 Enable or Disable Voice Mail Preview on a UM Mailbox Policy

Enable or Disable Voice Mail Preview on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable the Voice Mail Preview feature for users associated with the Unified Messaging (UM) mailbox policy. Enabling this setting allows users to receive the text of a voice mail in the message body of an e-mail or text message. If this option is disabled on the UM dial plan, Voice Mail Preview won't be available to UM-enabled users associated with the UM mailbox policy. This option isn't available to UM-enabled users who have a mailbox on a Microsoft Exchange Server 2007 Unified Messaging server. The default setting is enabled.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable Voice Mail Preview

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **General** tab, select or clear the check box next to **Allow Voice Mail Preview**.
4. Click **OK** to save your changes.

Use the Shell to enable or disable Voice Mail Preview

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example prevents users who are associated with the UM mailbox policy `MyUMMailboxPolicy` from using the Voice Mail Preview feature.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy - AllowVoiceMailPreview $false
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you enable or disable Voice Mail Preview on a UM mailbox policy, you may also want to View or Configure the Properties of a UM Mailbox Policy.

1.9.2.3.3.9 Enable or Disable Outlook Voice Access on a UM Mailbox Policy

Enable or Disable Outlook Voice Access on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable access to Outlook Voice Access for UM-enabled users who are associated with a Unified Messaging (UM) mailbox policy. Outlook Voice Access is a feature used by UM-enabled users to access their Microsoft Exchange Server 2007 or Exchange Server 2010 mailbox over a phone. By default, this setting is enabled.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable Outlook Voice Access

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **General** tab, select or clear the check box next to **Allow Outlook Voice Access**.
4. Click **OK** to save your changes.

Use the Shell to enable or disable Outlook Voice Access

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example prevents users who are associated with the UM mailbox policy MyUMMailboxPolicy from using Outlook Voice Access.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowSubscriberAccess $false
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you enable or disable Outlook Voice Access on a UM mailbox policy, you may also want to:

- View or Configure the Properties of a UM Mailbox Policy
- Enable or Disable Play on Phone on a UM Mailbox Policy

1.9.2.3.3.10 Enable or Disable Play on Phone on a UM Mailbox Policy

Enable or Disable Play on Phone on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable the Play on Phone feature for users associated with the Unified Messaging (UM) mailbox policy. This option is enabled by default and allows users to play their voice mail messages over a phone. The phone can be any phone, including an office or a mobile phone. This option isn't available to UM-enabled users who have a mailbox on a Microsoft Exchange Server 2007 server.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable Play on Phone

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox

policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **General** tab, select or clear the check box next to **Allow Play on Phone**.
4. Click **OK** to save your changes.

Use the Shell to enable or disable Play on Phone

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example disables the Play on Phone feature for users who are associated with the UM mailbox policy `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowPlayOnPhone $false
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

- After you enable or disable Play on Phone on a UM mailbox policy, you may also want to:
- View or Configure the Properties of a UM Mailbox Policy
- Enable or Disable Voice Mail Preview on a UM Mailbox Policy
- Enable or Disable Outlook Voice Access on a UM Mailbox Policy

1.9.2.3.3.11 Enable or Disable Call Answering Rules on a UM Mailbox Policy

Enable or Disable Call Answering Rules on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can allow users who are associated with a Unified Messaging (UM) mailbox policy to create call answering rules, or prevent them from doing so. If the option to create call answering rules is disabled on a UM dial plan, the Call Answering Rules feature won't be available to UM-enabled users associated with the UM mailbox policy. The default setting is enabled.

Call Answering Rules aren't available to UM-enabled users who have a mailbox on a Microsoft Exchange Server 2007 Unified Messaging server.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial

Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable call answering rules on a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **General** tab, select or clear the check box next to **Allow users to configure call answering rules**.
4. Click **OK** to save your changes.

Use the Shell to enable or disable call answering rules on a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example prevents users who are associated with the UM mailbox policy `MyUMMailboxPolicy` from creating call answering rules.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowCallAnsweringRules $false
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you enable or disable call answering rules on a UM mailbox policy, you may also want to:

- View or Configure the Properties of a UM Mailbox Policy.
- Allow or Prevent Call Answering Rules on a UM Dial Plan

1.9.2.3.3.12 Include Text with the E-Mail Message Sent When a Mailbox Is UM-Enabled

Include Text with the E-Mail Message Sent When a Mailbox Is UM-Enabled

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When a user's mailbox is enabled for Microsoft Exchange Server 2010 Unified Messaging,

an e-mail message is sent that welcomes the user to Unified Messaging. This message contains the PIN information the user will use to access the Unified Messaging system.

You can customize the text that's sent in the welcome e-mail message by adding text in the **Text sent when a UM mailbox is enabled** box on a UM mailbox policy. You can include such information as the UM technical support telephone numbers or subscriber access numbers. After you add the text, it will be included in the e-mail message sent when users associated with the UM mailbox policy are enabled for Unified Messaging.

Note:
The limit for custom text you add to the welcome message is 512 characters.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to customize the text sent when a mailbox is enabled for Unified Messaging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. On the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the mailbox policy Properties page, on the **Message Text** tab, under **Text sent when a UM mailbox is enabled**, enter the text you want to send to the user when a UM mailbox is enabled.
4. Click **OK** to save your changes.

Use the Shell to customize the text sent when a mailbox is enabled for Unified Messaging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example enables UM-enabled users who are associated with a UM mailbox policy to receive additional instructions about UM and the Outlook Voice Access number that they can use to access their mailbox over a phone.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -UMEnabledText "You've been enabl
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you customize the text sent when a mailbox is enabled for Unified Messaging, you may also want to:

- Include Text with the E-Mail Message Sent When a PIN Is Reset
- Enable a User for Unified Messaging
- Configure the UM Mailbox Policy Assigned to a UM-Enabled User

1.9.2.3.3.13 Include Text with the E-Mail Message Sent When a PIN Is Reset

Include Text with the E-Mail Message Sent When a PIN Is Reset

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can include additional text in the e-mail message that's sent to users when their Unified Messaging (UM) PIN is reset. You can customize the e-mail message sent to users when their UM PIN is reset by including custom text in the **Text sent when a PIN is reset** box on the **Message Text** tab.

By default, a PIN is reset by the Unified Messaging system if the number of failed logon attempts exceeds 5. Users can also reset their PINs using the UM features included with Microsoft Office Outlook 2007, the version of Outlook Web App that's included with Microsoft Exchange Server 2010, or by using Outlook Voice Access from a telephone. The customized text can include, for example, security-related information for UM-enabled users.

Note:

The text you enter in this box is limited to 512 characters.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to add text to the e-mail message sent to users when their PIN is reset

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. On the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the mailbox policy Properties page, on the **Message Text** tab, under **Text sent when a PIN is reset**, enter the text you want to send to users when their UM PIN is reset.
4. Click **OK** to save your changes.

Use the Shell to add text to the e-mail message sent to users when their PIN is reset

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example includes the additional text, "Do not share your PIN with other users. Doing so may result in disciplinary action", in the e-mail message sent to users who are associated with the UM mailbox policy `MyUMMailboxPolicy` when their PIN is reset.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -ResetPINText "Do not share your
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you add text to the e-mail message sent to users when their PIN is reset, you may also want to:

- Configure the Number of Incorrect PIN Entries Before a PIN Is Reset on a UM Mailbox Policy
- Reset a Unified Messaging PIN for a UM-Enabled User

1.9.2.3.3.14 Include Text with the E-Mail Message Sent When a Voice Message Is Received

Include Text with the E-Mail Message Sent When a Voice Message Is Received

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can include additional text in the e-mail message that's sent when a voice mail message is received by users who are enabled for Microsoft Exchange Server 2010 Unified Messaging (UM). By default, the text that's included with a voice message indicates only that the caller has received a voice message. However, you can create a custom message by adding text in the **Text included with a voice message** text box on a UM mailbox policy. For example, the text can include information about system security policies and describe the correct way to handle voice messages in your organization. After

you add the text, it will be included in each e-mail message that's sent when UM-enabled users associated with the UM mailbox policy receive a voice message.

Note:
The custom text that accompanies a voice message is limited to 512 characters.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to change the text included with a voice message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. On the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the mailbox policy Properties page, on the **Message Text** tab, under **Text included with a voice message**, enter the text you want to send to users when they receive a voice message.
4. Click **OK** to save your changes.

Use the Shell to change the text included with a voice message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example includes the additional text, "Do not forward voice message to users outside this organization", with voice messages sent to users who are associated with the UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailText "Do not forward vo
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you change the text included with a voice message, you may also want toInclude Text with the E-Mail Message Sent When a Fax Message Is Received.

Include Text with the E-Mail Message Sent When a Fax Message Is Received

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can include additional text in the e-mail message that's sent when a fax message is received by users who are enabled for Microsoft Exchange Server 2010 Unified Messaging (UM) and are fax-enabled, and when the UM mailbox policy has been configured correctly to use a fax partner provider. By default, the text included when a UM-enabled user receives a fax message indicates only that the caller has received a fax message. However, you can create a custom message by adding text in the **Text included with a fax message** text box on a UM mailbox policy. For example, the text can include information about system security policies and describe the correct way to handle fax messages in your organization. After you add the text, it will be included in each e-mail message that's sent when UM-enabled users who are associated with the UM mailbox policy receive a fax message.

Note:

The custom text that accompanies a fax message is limited to 512 characters.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to change the text included with a fax message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. On the **UM Mailbox Policies** tab, select the UM mailbox policy that you want to manage, and then click **Properties** in the action pane.
3. On the mailbox policy Properties page, on the **Message Text** tab, under **Text included with a fax message**, enter the text that you want to send to users when they receive a fax message.
4. Click **OK** to save your changes.

Use the Shell to change the text included with a fax message

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging

Permissions topic.

This example enables UM-enabled users who are associated with a UM mailbox policy to receive additional instructions on how to open a fax message that they've received in their mailbox.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -FaxMessageText "To open this fax
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you change the text included with a fax message, you may also want to:

- Enable or Disable Inbound Faxing on a UM Mailbox Policy
- Enable UM-Enabled Users to Receive Faxes on a UM Dial Plan

1.9.2.3.3.16 Configure the Minimum PIN Length on a UM Mailbox Policy

Configure the Minimum PIN Length on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the minimum PIN length for your mail-enabled recipients in Microsoft Exchange Server 2010 who are enabled for Unified Messaging (UM). The PIN settings that you configure on a UM mailbox policy will apply to all UM-enabled users associated with the UM mailbox policy.

Outlook Voice Access is used by UM-enabled users so that they can access their voice mail, e-mail, calendar, and personal contact information located in their Exchange 2010 mailbox. However, before they can access their mailbox, they must enter a PIN so they can be authenticated by the system.

Note:

If you make a change to the minimum PIN length value, existing subscribers will be prompted to enter a new PIN that contains the new minimum number of digits before they can continue.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to configure the minimum

PIN length

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Mailbox Policies** tab.
3. Select the UM mailbox policy you want to manage, and then, in the action pane, click **Properties**.
4. On the UM mailbox policy **Properties** page, on the **PIN Policies** tab, next to **Minimum PIN length**, enter a value between 4 and 24.
5. Click **OK** to save your changes

Use the Shell to configure the minimum PIN length

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the minimum PIN length to 8 digits for UM-enabled users who are associated with the UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -MinPINLength 8
```

This example sets the minimum PIN length to 8 digits and sets the number of times a sign-in can fail before the user's PIN is reset to 3. This applies to UM-enabled users who are associated with the UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3 -M
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you configure the matched name selection method on a UM dial plan, you may also want to:

- Enable or Disable Common PIN Patterns on a UM Mailbox Policy
- Configure the PIN Lifetime on a UM Mailbox Policy
- Set PIN Policies for UM-Enabled Users

1.9.2.3.3.17 Configure the PIN Lifetime on a UM Mailbox Policy

Configure the PIN Lifetime on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the PIN lifetime for users who are enabled for Unified Messaging (UM). The PIN lifetime is the maximum time that an Outlook Voice Access PIN will be valid for your UM-enabled recipients in Microsoft Exchange Server 2010. The PIN lifetime setting is configured on a UM mailbox policy and applies to all UM-enabled users associated with the UM mailbox policy.

Several PIN-related settings can be configured on a UM mailbox policy. The PIN lifetime setting controls the time interval, in days, from the date Outlook Voice Access users last changed their PIN to the date they'll be forced to change their PIN again. The range is 0 through 999, and the default is 60 days. If you enter 0, the user's PIN won't expire. But we don't recommend that you configure this setting to 0. By configuring this setting to 0, you greatly reduce the security of your network.

Important:

Unified Messaging doesn't notify users when their PIN is about to expire.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to configure the PIN lifetime

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then, in the action pane, click **Properties**.
3. On the UM mailbox policy **Properties** page, click the **PIN Policies** tab.
4. On the **PIN Policies** tab, next to **PIN lifetime (days)**, enter a value between 0 and 999.
5. Click **OK** to save your changes.

Use the Shell to configure the PIN lifetime

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the number of days that a PIN can be used for UM-enabled users who are associated with a UM mailbox policy named `MyUMMailboxPolicy` to 30.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -PINLifetime 30
```

This example configures the following PIN related settings for UM-enabled users who are associated with a UM mailbox policy named `MyUMMailboxPolicy`:

- Sets the number of logon failures before the user's PIN is reset to 3
- Sets the maximum number logon attempts to 5
- Sets the minimum PIN length to 9 digits.
- Sets the PIN to expire in 40 days.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3
-MaxLogonAttempts 5 -MinPINLength 9 -PINLifetime 40
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you configure the number of logon failures before a mailbox is locked out, you may also want to:

- Configure the Number of Previous PINs to Disallow on a UM Mailbox Policy
- Configure the Minimum PIN Length on a UM Mailbox Policy
- Set PIN Policies for UM-Enabled Users

1.9.2.3.3.18 Configure the Number of Previous PINs to Disallow on a UM Mailbox Policy

Configure the Number of Previous PINs to Disallow on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When Outlook Voice Access users dial in to a subscriber access number, they're prompted to enter their PIN so that the Unified Messaging (UM) system in Microsoft Exchange Server 2010 can authenticate them. After they're authenticated, they can access the voice mail, e-mail, calendaring, and personal contact information in their Exchange 2007 mailbox from any telephone.

Several PIN-related settings can be configured on a UM mailbox policy. The **Number of previous PINs to disallow** setting specifies the number of unique PINs users need to use before they can reuse an old PIN. You can set the value of this setting between 1 and 20. For most organizations, this value should be set to the default, 5 PINs.Setting this value too high can frustrate users because it can be difficult for users to create and memorize many PINs. Setting it too low may introduce a security threat to your network.

Important:

The PIN history can't be disabled.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to change the number of

previous PINs to disallow

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, click the **PIN Policies** tab.
4. On the **PIN Policies** tab, next to **Number of previous PINs to disallow**, enter a value between 1 and 20.
5. Click **OK** to save your changes.

Use the Shell to change the number of previous PINs to disallow

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the PIN history on the UM mailbox policy `MyUMMailboxPolicy` to 10.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -PINHistoryCount 10
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you change the number of previous PINs to disallow, you may also want to:

- Configure the Number of Incorrect PIN Entries Before a PIN Is Reset on a UM Mailbox Policy
- Enable or Disable Common PIN Patterns on a UM Mailbox Policy

1.9.2.3.3.19 Enable or Disable Common PIN Patterns on a UM Mailbox Policy

Enable or Disable Common PIN Patterns on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable common Unified Messaging (UM) PIN patterns for Outlook Voice Access users in Microsoft Exchange Server 2010. If you enable or disable the common PIN patterns setting on a UM mailbox policy, the setting will apply to all UM-enabled users associated with the UM mailbox policy. By default, UM-enabled users can't use common patterns when they create a PIN.

You can configure several PIN-related settings on a UM mailbox policy. The **Allow**

Common Patterns setting is used to allow or prevent the use of common number patterns when users create a PIN. By default, this setting is disabled and prevents users from using the following number patterns:

- **Sequential numbers** These are PIN values that include only consecutive numbers. Examples of consecutive numbers for a PIN are 1234 and 65432.
- **Repeated numbers** These are PIN values that include only repeated numbers. Examples of repeated numbers are 11111 and 22222.
- **Suffix of mailbox extension** These are PIN values that include the suffix of a user's mailbox extension. For example, if a user's mailbox extension is 36697, the user's PIN cannot be 3669712.

Note:
If the **Allow Common Patterns** setting is enabled, only the suffix of the mailbox extension will be rejected.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable common PIN patterns

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to Organization Configuration node > Unified Messaging.
2. On the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, click the **PIN Policies** tab.
4. On the **PIN Policies** tab, select the check box **Allow common patterns in PIN** to enable common PIN patterns. Unselecting the check box prevents users from using common patterns in their Outlook Voice Access PINs.
5. Click **OK** to save your changes.

Use the Shell to enable or disable common PIN patterns

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example enables user's associated with the UM mailbox policy named `MyUMMailboxPolicy` to use PINs that contain common patterns.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowCommonPatterns $true
```

This example prevents user's associated with the UM mailbox policy named `MyUMMailboxPolicy` from using PINs that contain common patterns.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowCommonPatterns $false
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you enable or disable common PIN patterns, you may also want to:

- Configuring PIN Security for a UM-Enabled User
- Set PIN Policies for UM-Enabled Users

1.9.2.3.3.20 Configure the Number of Incorrect PIN Entries Before a PIN Is Reset on a UM Mailbox Policy

Configure the Number of Incorrect PIN Entries Before a PIN Is Reset on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the number of logon failures allowed before the PIN is reset for an Outlook Voice Access user. You can configure the number of logon failures allowed before a PIN is reset from 1 through 998. The default is 5. The number of logon failures allowed before a PIN is reset is configured on a Unified Messaging (UM) mailbox policy and applies to all UM-enabled users associated with the UM mailbox policy.

Note:

You can increase security by configuring the **Number of incorrect PIN entries before PIN is automatically reset** setting to a number less than 5. You decrease security if you configure it to a number more than 5.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to configure the number of logon failures before a PIN is reset

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox

policy you want to manage, and then, in the action pane, click **Properties**.
3. On the UM mailbox policy **Properties** page, click the **PIN Policies** tab.
4. On the **PIN Policies** tab, under **Failed Logons** next to **Number of incorrect PIN entries before PIN is automatically reset**, enter a value between 1 and 998.
5. Click **OK** to save your changes.

Use the Shell to configure the number of logon failures before a PIN is reset

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the number of logon failures before the user's PIN is reset to 3 for UM-enabled users who are associated with a UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3
```

This example sets the number of logon failures before the user's PIN is reset to 3, the maximum number logon attempts to 5 and a minimum PIN length to 9 for UM-enabled users who are associated with a UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3
-MaxLogonAttempts 5 -MinPINLength 9
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you configure the number of logon failures before a PIN is reset, you may also want to:

- Configure the Number of Previous PINs to Disallow on a UM Mailbox Policy
- Configure the PIN Lifetime on a UM Mailbox Policy
- Configure the Minimum PIN Length on a UM Mailbox Policy
- Set PIN Policies for UM-Enabled Users

1.9.2.3.3.21 Configure the Number of Incorrect PIN Entries Before a Mailbox Is Locked Out on a UM Mailbox Policy

Configure the Number of Incorrect PIN Entries Before a Mailbox Is Locked Out on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the number of logon failures allowed before Outlook Voice Access users are locked out of their mailbox in Microsoft Exchange Server 2010. The number of logon failures allowed before a mailbox is locked out is configured on a Unified Messaging (UM) mailbox policy and applies to all UM-enabled users associated with the UM mailbox policy.

To increase security, decrease the maximum number of failed attempts. However, remember that if you decrease it to a number much lower than the default, users may be locked out unnecessarily. Unified Messaging will generate warning events you can view using Event Viewer if PIN authentication fails for UM-enabled users or if users are unsuccessful when they try to log on to the system.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to configure the number of logon failures before a mailbox is locked out

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then, in the action pane, click **Properties**.
3. On the UM mailbox policy **Properties** page, click the **PIN Policies** tab.
4. On the **PIN Policies** tab, under **Failed Logons**, next to **Number of incorrect PIN entries before UM mailbox is locked out**, enter a value between 1 and 998.
5. Click **OK** to save your changes.

Use the Shell to configure the number of logon failures before a mailbox is locked out

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the maximum number logon attempts to 10 for UM-enabled users who are associated with a UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -MaxLogonAttempts 10
```

This example sets the number of logon failures before the user's PIN is reset to 3, the maximum number logon attempts to 5 and a minimum PIN length to 9 for UM-enabled users who are associated with a UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3
-MaxLogonAttempts 5 -MinPINLength 9
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you configure the number of logon failures before a mailbox is locked out, you may also want to:

- Configure the Number of Previous PINs to Disallow on a UM Mailbox Policy
- Configure the PIN Lifetime on a UM Mailbox Policy
- Configure the Minimum PIN Length on a UM Mailbox Policy
- Set PIN Policies for UM-Enabled Users

1.9.2.3.3.22 Enable Dialing Restrictions on a UM Mailbox Policy

Enable Dialing Restrictions on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use the EMC and the Shell to enable dialing restrictions on a Unified Messaging (UM) mailbox policy in Microsoft Exchange Server 2010. A dialing restriction is used to configure dialing rules that can be used to prohibit users associated with a UM mailbox policy from making certain types of telephone calls.

Dialing restrictions are used when you configure outdialing for UM-enabled users and can be used when you want to enable users to place calls to in-country/region or international telephone numbers. When you configure a setting on a UM mailbox policy, that setting will apply to all UM-enabled users associated with the UM mailbox policy.

Outdialing enables UM-enabled users to initiate calls from inside an organization that has Unified Messaging. For outdialing to work correctly, certain settings must be configured correctly. These settings include:

- **Dialing group rules** Dialing group rules determine the types of calls users within a dial group can make.
- **Dialing rule entries** Dialing rule entries define the number dialed by the UM-enabled user and the actual number that will be dialed by the Private Branch eXchange (PBX) or IP PBX.
- **Dialing restrictions** Dialing restrictions determine the restrictions applied to prevent users from incurring unnecessary telephone charges or from dialing long distance calls.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.
- A UM dialing rule group has been created. For detailed steps, see Configure Dialing Rule Groups on a UM Dial Plan.

Use the EMC to enable dialing restrictions on a UM mailbox policy for in-country/region rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Mailbox Policies** tab.
3. Select the UM mailbox policy you want to change, and then, in the action pane, click **Properties**.
4. On the UM mailbox policy **Properties** page, on the **Dialing Restrictions** tab, under **Select allowed in-country/region rule groups from dial plan**, click **Add**.
5. On the **Select Allowed In-Country/Region Groups** page, select the dialing rule group that's configured on the UM dial plan, and then click **OK**.
6. Click **OK** to save your changes.

Use the EMC to enable dialing restrictions on a UM mailbox policy for international rule groups

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM Mailbox Policies** tab.
3. Select the UM mailbox policy you want to change, and then, in the action pane, click **Properties**.
4. On the UM mailbox policy **Properties** page, on the **Dialing Restrictions** tab, under **Select allowed international rule groups from dial plan**, click **Add**.
5. On the **Select Allowed International Groups** page, select the dialing rule group that's configured on the UM dial plan, and then click **OK**.
6. Click **OK** to save your changes.

Use the Shell to enable in-country/region and international dialing restrictions on a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM auto attendants" entry in the Unified Messaging Permissions topic.

This example enables the InCountry/RegionGroup1, InCountry/RegionGroup2, InternationalGroup1, and InternationalGroup2 dialing restrictions on a UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowedInCountryOrRegionGroups I
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you to enable dialing restrictions on a UM mailbox policy, you may also want to:

- Configure Dialing Rule Groups on a UM Dial Plan
- Create a Dialing Rule Entry on a UM Dial Plan

1.9.2.3.3.23 Configure Protected Voice Mail from Unauthenticated Callers on a UM Mailbox Policy

Configure Protected Voice Mail from Unauthenticated Callers on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can determine whether an incoming call answered by a Unified Messaging server will protect voice mail messages. Protected Voice Mail is encrypted. When a voice mail message is protected:

- The message is marked as Private in Microsoft Office Outlook and in Outlook Web App.
- The voice message can only be opened by the intended recipient of the voice message.
- The recipient can reply to the voice message, but can't forward it to someone who wasn't included on the original voice message.

This setting applies to voice messages sent to UM-enabled users when they don't answer their phone. This setting also applies to voice messages sent directly to UM-enabled users when the caller uses a UM auto attendant. This option isn't available to UM-enabled users who have a mailbox on a Microsoft Exchange Server 2007 Unified Messaging server.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to configure Protected Voice Mail from unauthenticated callers

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **Protected Voice Mail** tab, next to **Protect voice messages from unauthenticated callers**, select **None**, **Private**, or **All**. You can configure the following:
   None Use this setting if you don't want protection applied to any voice messages sent to UM-enabled users.
   Private Use this setting when you want the Unified Messaging server to apply protection only to voice messages that have been marked as private by the caller.
   All Use this setting when you want the Unified Messaging server to apply protection to all voice messages, including those not marked as private.
4. Click **OK** to save your changes.

Use the Shell to configure Protected Voice Mail from unauthenticated callers

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example protects all voice messages from all unauthenticated callers on the UM mailbox policy `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -ProtectUnauthenticatedVoiceMail
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you've configured Protected Voice Mail from unauthenticated callers on a UM mailbox policy, you may also want to View or Configure the Properties of a UM Mailbox Policy.

1.9.2.3.3.24 Configure Protected Voice Mail from Authenticated Callers on a UM Mailbox Policy

Configure Protected Voice Mail from Authenticated Callers on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can determine whether an incoming call answered by a Unified Messaging server will protect voice mail messages. Protected Voice Mail is encrypted. When a voice mail message is protected:

- The message is marked as Private in Microsoft Office Outlook and in Outlook Web App.
- The voice message can only be opened by the intended recipient of the voice message.
- The recipient can reply to the voice message, but can't forward it to someone who wasn't included on the original voice message.

This setting applies to voice messages sent to UM-enabled users when they don't answer their phone. This setting also applies when callers sign in to their mailbox using Outlook Voice Access, and then create and send a voice message. This option isn't available to UM-enabled users who have a mailbox on a Microsoft Exchange Server 2007 Unified Messaging server.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to configure Protected Voice Mail from authenticated callers

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **Protected Voice Mail** tab, next to **Protect voice messages from authenticated callers**, select **None**, **Private**, or **All**.
   None Use this setting if you don't want protection applied to any voice messages sent to UM-enabled users.
   Private Use this setting when you want the Unified Messaging server to apply protection only to voice messages that have been marked as private by the caller.
   All Use this setting when you want the Unified Messaging server to apply protection to all voice messages, including those not marked as private.
4. Click **OK** to save your changes.

Use the Shell to configure Protected Voice Mail from authenticated callers

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example protects voice messages from all authenticated callers on the UM mailbox policy `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy ProtectAuthenticatedVoiceMail -Al
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you've configured Protected Voice Mail from authenticated callers on a UM mailbox policy, you may also want to View or Configure the Properties of a UM Mailbox Policy.

1.9.2.3.3.25 Enable or Disable Multimedia Playback of Protected Voice Messages on a UM Mailbox Policy

Enable or Disable Multimedia Playback of Protected Voice Messages on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can force users who receive protected voice messages to use the Play on Phone feature to listen to their messages. Or, if the client software doesn't support rights management, users must use Outlook Voice Access.

To listen to voice mail messages, UM-enabled users can use the Play on Phone feature or use multimedia software on a computer or mobile phone. Multimedia playback allows a UM-enabled user to use a media player over computer speakers or use a media player on a mobile phone to hear the voice message.

Note:

Protected voice mail is available only on clients that are using a version of Outlook that supports rights management. If the client software doesn't support rights management, users must use Outlook Voice Access to listen to their calls

By default, the value of the **RequireProtectedPlayOnPhone** property on a UM mailbox policy is set to false. This means that UM-enabled users that are associated with that UM mailbox policy can listen to protected voice mails by:

- Placing a call into Microsoft Exchange Server 2010 Unified Messaging and using Outlook Voice Access.
- Using the built-in media player or the Play on Phone button in Outlook 2010.
- Using the built-in media player or the Play on Phone button in Outlook Web App.

If this value is set to true, multimedia playback of protected voice mail isn't allowed. UM-enabled users associated with a UM mailbox policy on which this value is set to true can only listen to protected voice mails by:

- Placing a call into Exchange 2010 Unified Messaging and using Outlook Voice Access.
- Using the Play on Phone button in Outlook 2010.
- Using the Play on Phone button in Outlook Web App.

This setting is especially useful when UM-enabled users use public computers, laptops in public places, or their mobile phone's media player to listen to Protected Voice Mail that can contain private information.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to enable or disable multimedia playback of protected voice messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **Protected Voice Mail** tab, select or clear the **Allow multimedia playback of protected voice messages** check box.
4. Click **OK** to save your changes.

Use the Shell to enable or disable multimedia playback of protected voice messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example allows users who are associated with the UM mailbox policy `MyUMMailboxPolicy` to play back protected voice messages using a media player.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -RequireProtectedPlayOnPhone $fal
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you've enabled or disabled multimedia playback of protected voice messages on a UM mailbox policy, you may also want to View or Configure the Properties of a UM Mailbox Policy.

1.9.2.3.3.26 Specify the Text to Display for E-Mail Clients that Don't Support Windows Rights Management on a UM Mailbox Policy

Specify the Text to Display for E-Mail Clients that Don't Support Windows Rights Management on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can specify the text that will be sent to a called party when they receive a protected voice message but their e-mail client doesn't support Active Directory Rights Management Services (AD RMS), shown in the user interface as Windows Rights Management, and they're not using Outlook Voice Access to access the message. This text is set on the UM mailbox policy.

Protected Voice Mail can only be accessed by e-mail clients that support Windows Rights Management or when a Unified Messaging–enabled user uses Outlook Voice Access to access a protected voice message.

Protected Voice Mail is encrypted. When a voice message is protected:

- The message is marked as Private in Microsoft Office Outlook and in Outlook Web App.
- The voice message can only be opened by the intended recipient of the voice message.
- The recipient can reply to the voice message, but can't forward it to someone who wasn't included on the original voice message.

If a protected voice message is sent to someone whose e-mail client doesn't support Windows Rights Management and isn't accessing the message using Outlook Voice Access, an e-mail message will be sent to them that includes the text you specify. This text should include instructions about what the called party should do to be able to receive the protected voice message.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the EMC to specify the text to display for e-mail clients that don't support Windows Rights Management

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, on the **UM Mailbox Policies** tab, select the UM mailbox policy you want to manage, and then click **Properties** in the action pane.
3. On the UM mailbox policy **Properties** page, on the **Protected Voice Mail** tab, next to **Specify the text to display to voice mail recipients who have e-mail clients that don't support Windows Rights Management**, type the text that you want to display.
4. Click **OK** to save your changes.

Use the Shell to specify the text to display for e-mail clients that don't support

Windows Rights Management

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example specifies the text to display to users associated with the UM mailbox policy named `MyUMMailboxPolicy` who have e-mail clients that don't support Windows Rights Management.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -ProtectedVoiceMailText "Your e-m
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you specify the text to display for e-mail clients that don't support Active Directory Rights Management Services (AD RMS) on a UM mailbox policy, you may also want to:

- View or Configure the Properties of a UM Mailbox Policy
- Configure Protected Voice Mail from Unauthenticated Callers on a UM Mailbox Policy
- Configure Protected Voice Mail from Authenticated Callers on a UM Mailbox Policy

Configure TUI Settings on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Outlook Voice Access contains two interfaces: the telephone user interface (TUI) and a voice user interface (VUI). You can configure a UM-enabled user's TUI settings when the user accesses a mailbox using the Unified Messaging (UM) system in Microsoft Exchange Server 2010. When you modify a UM-enabled user's TUI settings on a UM mailbox policy, the changes affect all users who are associated with the UM mailbox policy. You can modify the following TUI settings on a UM mailbox policy including:

- PIN-less access to voice mail
- Voice responses to other messages
- TUI access to their calendar
- TUI access to the directory
- TUI access to their e-mail
- TUI access to their personal Contacts

Note:

You can only use the Shell to modify the Outlook Voice Access TUI settings for UM-enabled users.

Looking for other management tasks related to UM mailbox policies? Check out Managing

UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the Shell to modify TUI settings on a UM mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets TUI related settings on a UM mailbox policy named `MyUMMailboxPolicy`.

```
Set-UMMailbox -identity MyUMMailboxPolicy -AllowSubscriberAccess $true -AllowTUIA
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you modify TUI settings on a UM mailbox policy, you may also want to:

- Configure the UM Mailbox Policy Assigned to a UM-Enabled User
- Configure a Subscriber Access Number on a UM Dial Plan
- Enable or Disable Sending Voice Messages on a UM Dial Plan

1.9.2.3.3.28 Configure a Voice Mail Preview Partner on a UM Mailbox Policy

Configure a Voice Mail Preview Partner on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can configure a Voice Mail Preview partner on a Unified Messaging (UM) mailbox policy. After you've configured Voice Mail Preview partner settings, such as the Voice Mail Preview partner ID and Voice Mail Preview partner address, on a UM mailbox policy the settings you configure will apply to all UM-enabled users who are associated with that mailbox policy.

You must use the Exchange Management Shell to configure a Voice Mail Preview partner. You must be logged on to an Exchange server, or to a computer on which the Exchange system management tools have been installed. From the Start menu, choose **Exchange Management Shell** and then **Run as Administrator**.

For more information about the Voice Mail Preview partner program, see Voice Mail Preview Advisor for Exchange 2010.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the Shell to Configure a Voice Mail Preview Partner

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

Step 1: Sign Up with a Partner Service

To find the list of certified partners and detailed instructions for how to sign up, see Voice Mail Preview Advisor for Exchange 2010. After you've signed up, the Voice Mail Preview partner will provide you a partner ID and the SMTP address to use to forward the voice messages.

In Step 2, you'll apply the Partner ID and SMTP address you acquired in Step 1 to the required UM mailbox policies.

Step 2: Set the Voice Mail Preview Partner Address and ID

This example sets the Voice Mail Preview partner address to exumvmp@fabrikam.com and the Voice Mail Preview partner ID to CON123-2010 on a UM mailbox policy named *MyUMMailboxPolicy*.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailPreviewPartnerAddress e
-VoiceMailPreviewPartnerAssignedID CON123-2010
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Step 3: Optional - Configure Advanced Voice Mail Preview Partner Settings

If the partner requires custom settings, you may want to set two additional parameters for a Voice Mail Preview partner as follows:

- *VoiceMailPreviewPartnerMaxMessageDuration*
- *VoiceMailPreviewPartnerMaxDeliveryDelay*

This example sets the maximum message duration to 300 seconds (5 minutes) and the maximum delivery delay to 600 seconds (10 minutes) on a UM mailbox policy named *MyUMMailboxPolicy*.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailPreviewPartnerMaxMessag
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Step 4: Assign a UM-Enabled User to the UM Mailbox Policy for a Voice Mail Preview Partner

If you want to configure the Voice Mail Preview partner service for some, but not all, UM-

enabled users in a UM dial plan, you must create a new UM mailbox policy and configure the partner settings. When you've finished, you can apply the new policy to selected UM-enabled users. For more information about how to assign a UM-enabled user to a UM mailbox policy, see the following topics:

- Configure the UM Mailbox Policy Assigned to a UM-Enabled User
- Set-UMMailbox

For more information about Voice Mail Preview, see Voice Mail Preview for End Users.

Other Tasks

After you configure a Voice Mail Preview partner on a UM mailbox policy, you may also want to Enable or Disable Voice Mail Preview on a UM Mailbox Policy.

Set the Voice Mail Preview Partner Address on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can set a Voice Mail Preview partner address on a Unified Messaging (UM) mailbox policy. After you've set the Voice Mail Preview partner address on a UM mailbox policy, the setting will apply to all UM-enabled users who are associated with that mailbox policy.

You must use the Exchange Management Shell to set a Voice Mail Preview partner address. You must be logged on to an Exchange server, or to a computer on which the Exchange system management tools have been installed. From the Start menu, choose **Exchange Management Shell** and then **Run as Administrator**.

For more information about the Voice Mail Preview partner program, see Voice Mail Preview Advisor for Exchange 2010.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the Shell to Set the Voice Mail Preview Partner Address on a UM Mailbox Policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the Voice Mail Preview partner address to exumvmp@fabrikam.com on a UM mailbox policy named *MyUMMailboxPolicy*.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailPreviewPartnerAddress e
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you set the Voice Mail Preview partner address on a UM mailbox policy, you may also want to:

- Set the Voice Mail Preview Partner ID on a UM Mailbox Policy
- Set the Maximum Message Duration for a Voice Mail Preview Partner on a UM Mailbox Policy
- Set the Maximum Delivery Delay for a Voice Mail Preview Partner on a UM Mailbox Policy

Set the Voice Mail Preview Partner ID on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can set a Voice Mail Preview partner ID on a Unified Messaging (UM) mailbox policy. After you've set the Voice Mail Preview partner ID on a UM mailbox policy, the setting will apply to all UM-enabled users who are associated with that mailbox policy.

You must use the Exchange Management Shell to set the Voice Mail Preview partner ID. You must be logged on to an Exchange server, or to a computer on which the Exchange system management tools have been installed. From the Start menu, choose **Exchange Management Shell** and then **Run as Administrator**.

For more information about the Voice Mail Preview partner program, see Voice Mail Preview Advisor for Exchange 2010.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the Shell to Set the Voice Mail Preview Partner ID on a UM Mailbox

Policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the Voice Mail Preview partner ID to CON123-2010 on a UM mailbox policy named *MyUMMailboxPolicy*.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy
-VoiceMailPreviewPartnerAssignedID CON123-2010
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you set the Voice Mail Preview partner ID on a UM mailbox policy, you may also want to:

- Set the Voice Mail Preview Partner Address on a UM Mailbox Policy
- Set the Maximum Message Duration for a Voice Mail Preview Partner on a UM Mailbox Policy
- Set the Maximum Delivery Delay for a Voice Mail Preview Partner on a UM Mailbox Policy

Set the Maximum Message Duration for a Voice Mail Preview Partner on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can set the message duration for a Voice Mail Preview partner on a Unified Messaging (UM) mailbox policy. After you've set the maximum message duration, the setting will apply to all UM-enabled users who are associated with that mailbox policy.

You must use the Exchange Management Shell to set the maximum message duration for a Voice Mail Preview partner. You must be logged on to an Exchange server, or to a computer on which the Exchange system management tools have been installed. From the Start menu, choose **Exchange Management Shell** and then **Run as Administrator**.

For more information about the Voice Mail Preview partner program, see Voice Mail Preview Advisor for Exchange 2010.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the Shell to Set the Maximum Message Duration for a Voice Mail Preview Partner

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the maximum message duration for a Voice Mail Preview partner to 300 seconds (5 minutes) on a UM mailbox policy named *MyUMMailboxPolicy*.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailPreviewPartnerMaxMessag
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you set the maximum message duration for a Voice Mail Preview partner, you may also want to:

- Set the Voice Mail Preview Partner Address on a UM Mailbox Policy
- Set the Voice Mail Preview Partner ID on a UM Mailbox Policy
- Set the Maximum Delivery Delay for a Voice Mail Preview Partner on a UM Mailbox Policy

Set the Maximum Delivery Delay for a Voice Mail Preview Partner on a UM Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can set the maximum delivery delay for a Voice Mail Preview partner on a Unified Messaging (UM) mailbox policy. After you've set the maximum delivery delay, the setting will apply to all UM-enabled users who are associated with that UM mailbox policy.

You must use the Exchange Management Shell to set the maximum delivery delay for a Voice Mail Preview partner. You must be logged on to an Exchange server, or to a computer on which the Exchange system management tools have been installed. From the Start menu, choose **Exchange Management Shell** and then **Run as Administrator**.

For more information about the Voice Mail Preview partner program, see Voice Mail Preview Advisor for Exchange 2010.

Looking for other management tasks related to UM mailbox policies? Check out Managing UM Mailbox Policies.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the Shell to Set the Maximum Delivery Delay for a Voice Mail Preview Partner

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM mailbox policies" entry in the Unified Messaging Permissions topic.

This example sets the maximum delivery delay to 600 seconds (10 minutes) on a UM mailbox policy named *MyUMMailboxPolicy*.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy - VoiceMailPreviewPartnerMaxDeliv
```

For more information about syntax and parameters, see Set-UMMailboxPolicy.

Other Tasks

After you set the maximum delivery delay for a Voice Mail Preview partner, you may also want to:

- Set the Maximum Message Duration for a Voice Mail Preview Partner on a UM Mailbox Policy
- Set the Voice Mail Preview Partner ID on a UM Mailbox Policy
- Set the Voice Mail Preview Partner Address on a UM Mailbox Policy

1.9.2.3.4 Managing UM IP Gateways

Managing UM IP Gateways

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-18*

Create a UM IP Gateway

View or Configure the Properties of a UM IP Gateway

Delete a UM IP Gateway

Enable a UM IP Gateway

Disable a UM IP Gateway

Configure the IP Address on a UM IP Gateway

Configure a Fully Qualified Domain Name for a UM IP Gateway

Enable or Disable Outgoing Calls on a UM IP Gateway

Allow or Prevent Message Waiting Indicator on a UM IP Gateway

Configure the TCP Listening Port on a UM IP Gateway

1.9.2.3.4.1 Create a UM IP Gateway

Create a UM IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

A Unified Messaging (UM) IP gateway establishes a logical link between the IP gateway device, a UM IP gateway, and single or multiple UM hunt groups. When you create a new UM IP gateway, you enable Unified Messaging servers to connect to a new IP gateway or an IP Private Branch eXchange (PBX) enabled for Session Initiation Protocol (SIP). Immediately after you create a UM IP gateway, you should create a new UM hunt group and then associate the UM hunt group with the UM IP gateway. You can associate the UM IP gateway with one or more UM dial plans by creating one or more UM hunt groups.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

What Do You Want to Do?

- Use the EMC to create a UM IP gateway
- Use the Shell to create a UM IP gateway

Use the EMC to create a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. In the action pane, click **New UM IP Gateway**.
4. In the New UM IP Gateway wizard, complete the following fields:
   - **Name** Use this text box to specify a unique name for the UM IP gateway. This is a display name that appears in the EMC. If you have to change the display name of the UM IP gateway after it's been created, you must first

delete the existing UM IP gateway, and then create another UM IP gateway that has the appropriate name. The UM IP gateway name is required, but it's used for display purposes only. When you're using the **Get-UMIPGateway** cmdlet, you can't enter the IP address that's configured on the UM IP gateway. You must use the name of the UM IP gateway. The name that's specified on the Identity parameter with the **Get-UMIPGateway** cmdlet can be the same as or different from the host name of the UM IP gateway. For example, **Get-UMIPGateway** *MyUMIPGateway*.

Because your organization may use multiple UM IP gateways, we recommend that you use meaningful names for your UM IP gateways. The maximum length of a UM IP gateway name is 64 characters, and it can include spaces.

- **IP address** You can configure a UM IP gateway with either an IP address or an FQDN. Use this field to specify the IP address configured on the IP gateway or SIP-enabled IP PBX.

  Although you can enter alphabetical and numeric characters in this text box, IPv4 addresses that are correctly formatted are required. IPv6 addresses aren't supported even though they can be entered into this field.
- **Fully qualified domain name (FQDN)** You can configure a UM IP gateway with either an IP address or an FQDN. Use this text box to enter the FQDN for the UM IP gateway or SIP-enabled IP PBX. This text box accepts only FQDNs that are valid and formatted correctly.

  If you want to use mutual Transport Layer Security (mutual TLS) between a UM IP gateway and a dial plan operating in either SIP secured or Secured mode, you must configure the UM IP gateway with an FQDN. You must also configure it to listen on port 5061 and verify that any IP gateways or IP PBXs have also been configured to listen for mutual TLS requests on port 5061. To configure a UM IP gateway, run the following command: **Set-UMIPGateway -identity MyUMIPGateway -Port 5061**.
  If you use an FQDN, you must also make sure that you have correctly configured a DNS host record for the IP gateway so that the host name will be correctly resolved to an IP address. Also if you use an FQDN instead of an IP address, and the DNS configuration for the UM IP gateway is changed, you must disable and then enable the UM IP gateway to make sure that configuration information for the UM IP gateway is updated correctly in Active Directory.
- **Dial plan** Click the **Browse** button to select the UM dial plan that you want to associate with the UM IP gateway. When you select a UM dial plan to associate with a UM IP gateway, a default UM hunt group is also created and associated with the UM dial plan that you selected. If you don't select a UM dial plan, you must manually create a UM hunt group and then associate that UM hunt group with the UM IP gateway that you create.

5. On the **Completion** page, confirm whether the UM IP gateway was successfully created:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to complete the New UM IP Gateway wizard.

Use the Shell to create a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging

Permissions topic.

This example creates a UM IP gateway named MyUMIPGateway that enables a Unified Messaging server to start accepting calls from an IP gateway that has an IP address of 10.10.10.1.

```
New-UMIPGateway -Name MyUMIPGateway -Address 10.10.10.1
```

This example creates a UM IP gateway named MyUMIPGateway that enables a Unified Messaging server to start accepting calls from an IP gateway that has an FQDN of MyUMIPGateway.contoso.com and listens on port 5061.

```
New-UMIPGateway -Name MyUMIPGateway -Address "MyUMIPGateway.contoso.com" -Port 50
```

For more information about syntax and parameters, see New-UMIPGateway.

Other Tasks

After you create a UM IP gateway, you may also want to:

- Create a UM Hunt Group
- Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server
- Configure an IP Gateway to Communicate with a PBX

For More Information

Understanding Unified Messaging IP Gateways

1.9.2.3.4.2 View or Configure the Properties of a UM IP Gateway

View or Configure the Properties of a UM IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After you create a Unified Messaging (UM) IP gateway, you can view or configure a variety of settings. For example, you can configure the IP address or a fully qualified domain name (FQDN), configure outgoing call settings, and enable or disable the Message Waiting Indicator. When you're using the **Get-UMIPGateway** cmdlet, you can't enter the IP address that's configured on the UM IP gateway. You must use the name of the UM IP gateway. The name that's specified on the Identity parameter with the **Get-UMIPGateway** cmdlet can be the same as or different from the host name of the UM IP gateway. For example, **Get-UMIPGateway** *MyUMIPGateway*.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.

What Do You Want to Do?

Use the EMC to view or configure UM IP gateway properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab, and then select the UM IP gateway that you want to configure.
3. In the action pane, click **Properties**.
4. Use the **General** tab to view and configure settings for the UM IP gateway. For example, you can configure the IP address that points to an IP gateway or Private Branch eXchange (PBX) enabled for Session Initiation Protocol (SIP) on your network. You can also change the display name of the UM IP gateway that was configured when the UM IP gateway was created. You can view or configure the following settings:
   - **Status** This display-only field shows the status of the UM IP gateway.
   - **Modified** This display-only field shows the date that the UM IP gateway was last modified.
   - **IP address** You can configure a UM IP gateway with either an IP address or an FQDN. Use this field to specify the IP address configured on the IP gateway or SIP-enabled IP PBX.

     Although you can enter alphabetical and numeric characters in this text box, IPv4 addresses that are correctly formatted are required. IPv6 addresses aren't supported even though they can be entered into this field.
   - **Fully qualified domain name (FQDN)** You can configure a UM IP gateway with either an IP address or an FQDN. Use this text box to enter the FQDN for the UM IP gateway or SIP-enabled IP PBX. This text box accepts only FQDNs that are valid and formatted correctly.

     If you want to use mutual Transport Layer Security (mutual TLS) between a UM IP gateway and a dial plan operating in either SIP secured or Secured mode, you must configure the UM IP gateway with an FQDN. You must also configure it to listen on port 5061 and verify that any IP gateways or IP PBXs have also been configured to listen for mutual TLS requests on port 5061. To configure a UM IP gateway, run the following command: **Set-UMIPGateway -identity MyUMIPGateway -Port 5061**.
     If you use an FQDN, you must also make sure that you have correctly configured a DNS host record for the IP gateway so that the host name will be correctly resolved to an IP address. Also if you use an FQDN instead of an IP address, and the DNS configuration for the UM IP gateway is changed, you must disable and then enable the UM IP gateway to make sure that configuration information for the UM IP gateway is updated correctly in Active Directory.
   - **Allow outgoing calls through this UM IP gateway** Select this check box to allow the UM IP gateway to accept and process outgoing calls. This setting doesn't affect call transfers or incoming calls from an IP gateway.

By default, when the UM IP gateway is created, this setting is enabled. If you disable this setting, users associated with the dial plan won't be able to make outgoing calls through the IP gateway defined in the **Address** field.

- **Allow Message Waiting Indicator** Select this check box to allow voice mail notifications to be sent to users for calls taken by the UM IP gateway. This setting allows the UM IP gateway to receive and send SIP NOTIFY messages for users. The default setting is enabled by default and allows for message waiting notifications to be sent to users.

  Message Waiting Indicator is a feature found in most legacy voice mail systems. In its most common form, it lights a lamp on the voice mail subscriber's phone to indicate the presence of a new voice message.

  Message Waiting Indicator can refer to any mechanism that indicates the existence of a new message. The voice mail message could be a new or unheard voice message. The indication that a new voice message has arrived can be found in the Inbox in clients such as Outlook and Outlook Web App. It can take the form of a Short Messaging Service (SMS) or text message sent to a registered mobile phone, an outbound call made from an Exchange Unified Messaging server to a preconfigured number to play the new item, or a lighted desktop phone lamp for a user.

Use the Shell to configure UM IP gateway properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example modifies the IP address of a UM IP gateway named `MyUMIPGateway`.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.1
```

This example prevents the UM IP gateway from accepting incoming calls and prevents outgoing calls.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.1 -Status 2 -OutcallsAl
```

This example enables the UM IP gateway to function as an IP gateway simulator and can be used with the **Test-UMConnectivity** cmdlet.

```
Set-UMIPGateway -Identity MyUMIPGateway -Simulator $true
```

Important:

There is a period of latency before all changes that you make to the configuration of a UM IP gateway replicate to all Unified Messaging servers in the same UM dial plan as the UM IP gateway.

For more information about syntax and parameters, see Set-UMIPGateway.

Use the Shell to view UM IP gateway properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging

Permissions topic.

This example displays a formatted list of all the UM IP gateways in the Active Directory forest.

```
Get-UMIPGateway |Format-List
```

This example displays the properties for a UM IP gateway named MyUMIPGateway.

```
Get-UMIPGateway -Identity MyUMIPGateway
```

This example displays all the UM IP gateways including IP gateway simulators in the Active Directory forest.

```
Get-UMIPGateway -IncludeSimulator $true
```

For more information about syntax and parameters, see Get-UMIPGateway.

Other Tasks

After you configure UM IP gateway properties, you may also want to:

- Create a UM Hunt Group
- Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server
- Configure an IP Gateway to Communicate with a PBX

For More Information

Understanding Unified Messaging IP Gateways

1.9.2.3.4.3 Delete a UM IP Gateway

Delete a UM IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can delete a Unified Messaging (UM) IP gateway. When you delete the UM IP gateway, Unified Messaging servers are no longer able to accept incoming calls from the IP gateway or SIP-enabled IP PBX associated with the UM IP gateway.

Important:

Deleting a UM IP gateway should be performed only when you fully understand the implications of disabling communication with an IP gateway or a Session Initiation Protocol (SIP)–enabled IP Private Branch eXchange (PBX).

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP

Gateway.

Use the EMC to delete a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the result pane, click the **UM IP Gateways** tab.
3. In the work pane, click the UM IP gateway that you want to delete.
4. In the action pane, click **Remove**.
5. In the confirmation dialog box, click **Yes**.

Use the Shell to delete a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example removes or deletes the UM IP gateway named `MyUMIPGateway`.

```
Remove-UMIPGateway -Identity MyUMIPGateway
```

For more information about syntax and parameters, see Remove-UMIPGateway.

Other Tasks

After you delete a UM IP gateway, you may also want to:

- View or Configure the Properties of a UM IP Gateway
- Delete a UM Hunt Group

1.9.2.3.4.4 Enable a UM IP Gateway

Enable a UM IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can to enable a Unified Messaging (UM) IP gateway. By default, when a UM IP gateway is created, the status of the UM IP gateway is set to enabled. After you create the UM IP gateway, you can control the operation and functionality of the UM IP gateway by setting its status variable.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial

Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.

Use the EMC to enable a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

1. In the console tree, click **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. Select the UM IP gateway that you want to enable.
4. In the action pane, click **Enable**.

Use the Shell to enable a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example enables a UM IP gateway named `MyUMIPGateway`.

```
Enable-UMIPGateway -Identity MyUMIPGateway
```

For more information about syntax and parameters, see Enable-UMIPGateway.

Other Tasks

After you enable a UM IP gateway, you may also want to:

- View or Configure the Properties of a UM IP Gateway
- Disable a UM IP Gateway

1.9.2.3.4.5 Disable a UM IP Gateway

Disable a UM IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can disable a Unified Messaging (UM) IP gateway. By default, when you create a UM IP gateway, the status of the UM IP gateway is enabled. However, after the UM IP gateway is created, you can disable the operation of the UM IP gateway by setting its status variable to disabled. After you disable the UM IP gateway, the IP gateway device with which it's associated no longer processes Unified Messaging incoming calls.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.
- The UM IP gateway status has been enabled. For detailed steps, see Enable a UM IP Gateway.

Use the EMC to disable a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the result pane, click the **UM IP Gateways** tab.
3. In the work pane, select a UM IP gateway that you want to disable.
4. In the action pane, click **Disable immediately**.
5. In the confirmation dialog box, click **Yes** to confirm.

Use the Shell to disable a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example disables a UM IP gateway named `MyUMIPGateway` and stops it from accepting incoming calls from the IP gateway.

```
Disable-UMIPGateway -Identity MyUMIPGateway
```

This example disables a UM IP gateway named `MyUMIPGateway` and disconnects all current calls immediately.

```
Disable-UMIPGateway -Identity MyUMIPGateway -Immediate $true
```

For more information about syntax and parameters, see Disable-UMIPGateway.

Other Tasks

After you disable a UM IP gateway, you may also want to:

- Enable a UM IP Gateway
- Configure the IP Address on a UM IP Gateway
- Configure a Fully Qualified Domain Name for a UM IP Gateway

1.9.2.3.4.6 Configure the IP Address on a UM IP Gateway

Configure the IP Address on a UM IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you create a Unified Messaging (UM) IP gateway, you must define the IP address or the fully qualified domain name (FQDN) configured on the IP gateway or Session Initiation Protocol (SIP)-enabled IP Private Branch eXchange (PBX) that you're using. However, you can change the IP address after the UM IP gateway is created. The IP address configured on the UM IP gateway is the IP address configured on the network or LAN interface of the IP gateway or SIP-enabled IP PBX. If you create a UM IP gateway with an IP address and you view the properties of the UM IP gateway using the **Get-UMIPgateway** cmdlet, you can't use the IP address, you must use the name of the UM IP gateway. For example, **Get-UMIPGateway** *MyUMIPGateway*.

You can only configure a UM IP gateway with an IPv4 IP address. The **IP Address** field can accept an IPv6 address. However, IPv6 isn't supported.

Important:

If you create a UM IP gateway using an FQDN, and the DNS configuration for the UM IP gateway is changed, you must disable and then enable the UM IP gateway to make sure that the UM IP gateway's configuration information is updated correctly in the Active Directory directory service.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.

Use the EMC to configure the IP address on a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. Select the UM IP gateway that you want to modify, and then in the action pane, click **Properties**.
4. On the UM IP gateway **Properties** page, under **IP Address**, enter the IP address for the IP gateway or IP PBX.

   Note:

   If you use an FQDN instead of an IP address on the UM IP gateway, verify that the correct DNS records have been created.

5. Click **OK** to save your changes.

Use the Shell to configure the IP address on a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example configures a UM IP gateway named `MyUMIPGateway` with an IP address of

10.10.10.1.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.1
```

This example configures a UM IP gateway named MyUMIPGateway with an IP address of 10.10.10.10 and listens for SIP requests on TCP port 5061.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.10 -Port 5061
```

For more information about syntax and parameters, see Set-UMIPGateway.

Other Tasks

After you've changed the IP address on a UM IP gateway, you may also want to:

- View or Configure the Properties of a UM IP Gateway
- Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server
- Connect a Unified Messaging Server to a Supported IP Gateway

1.9.2.3.4.7 Configure a Fully Qualified Domain Name for a UM IP Gateway

Configure a Fully Qualified Domain Name for a UM IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure a Unified Messaging (UM) IP gateway with either an IP address or an FQDN. You can enter the FQDN for the UM IP gateway or SIP-enabled IP PBX. When you create a UM IP gateway, you must define the IP address or the fully qualified domain name (FQDN) configured on the IP gateway or Session Initiation Protocol (SIP)-enabled IP Private Branch eXchange (PBX) that you're using. However, you can change the IP address or FQDN after the UM IP gateway is created.

If you want to use mutual Transport Layer Security (mutual TLS) between a UM IP gateway and a dial plan operating in either SIP secured or Secured mode, you must configure the UM IP gateway with an FQDN. You must also configure it to listen on port 5061 and verify that any IP gateways or IP PBXs have also been configured to listen for mutual TLS requests on port 5061. To configure a UM IP gateway, run the following command: `Set-UMIPGateway -identity MyUMIPGateway -Port 5061`.

Important:

If you create a UM IP gateway using an FQDN, and the DNS configuration for the UM IP gateway is changed, you must disable and then enable the UM IP gateway to make sure that the UM IP gateway's configuration information is updated correctly in the Active Directory directory service.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.

Use the EMC to configure a FQDN

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. Select the UM IP gateway that you want to modify, and then in the action pane, click **Properties**.
4. On the UM IP gateway **Properties** page, under **Fully qualified domain name (FQDN)**, enter the FQDN for the IP gateway or IP PBX.

   Note:
   If you use an FQDN instead of an IP address on the UM IP gateway, verify that the correct DNS records have been created.

5. Click **OK** to save your changes.

Use the Shell to configure a FQDN

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example configures a UM IP gateway named `MyUMIPGateway` with a FQDN of Contoso.com.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address Contoso.com
```

This example configures a UM IP gateway named `MyUMIPGateway` with FQDN of Contoso.com and listens for SIP requests on TCP port 5061.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address Contoso.com -Port 5061
```

For more information about syntax and parameters, see Set-UMIPGateway.

Other Tasks

After you configured a FQDN on a UM IP gateway, you may also want to:

- View or Configure the Properties of a UM IP Gateway
- Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server
- Connect a Unified Messaging Server to a Supported IP Gateway

1.9.2.3.4.8 Enable or Disable Outgoing Calls on a UM IP Gateway

Enable or Disable Outgoing Calls on a UM IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable or disable outgoing calls for a Unified Messaging (UM) IP gateway in Microsoft Exchange Server 2010 Unified Messaging. When you select the **Allow outgoing calls through this UM IP gateway** check box on the properties for the UM IP gateway, you configure the UM IP gateway to accept and send outgoing calls to an IP gateway. If you clear the check box, you prevent the UM IP gateway from sending outgoing calls to an IP gateway. Although the **Allow outgoing calls through this UM IP gateway** setting controls whether the IP gateway is able to initiate outgoing calls for users, it doesn't affect call transfers or incoming calls from an IP gateway.

Outdialing is the term used to describe a situation in which a user in one UM dial plan initiates a call to another UM-enabled user in another dial plan or to an external telephone number

To allow outdialing for UM-enabled users, you must:

- Verify that the UM IP gateway allows outgoing calls.
- Create dialing rule groups by creating dialing rule entries on the UM dial plan associated with the UM IP gateway.
- Add the correct dialing rule groups to the list of dialing restrictions on the **Dialing Restrictions** tab on the UM dial plan and on the UM mailbox policy.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.

Use the EMC to enable or disable outgoing calls for a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. Select the UM IP gateway that you want to modify, click **Properties** in the action pane, and then do one of the following:
   - To enable outgoing calls on a UM IP gateway, on the **UM IP Gateway Properties** page, select the check box next to **Allow outgoing calls through this UM IP gateway**.
   - To disable outgoing calls on a UM IP gateway, on the **UM IP Gateway Properties** page, clear the check box next to **Allow outgoing calls through this UM IP gateway**.
4. Click **OK** to save your changes.

Use the Shell to enable or disable

outgoing calls for a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example enables outgoing calls on a UM IP gateway.

```
Set-UMIPGateway -Identity MyUMIPGateway -OutcallsAllowed $true
```

This example disables outgoing calls on a UM IP gateway.

```
Set-UMIPGateway -Identity MyUMIPGateway -OutcallsAllowed $false
```

For more information about syntax and parameters, see Set-UMIPGateway.

Other Tasks

After you enable or disable outgoing calls for a UM IP gateway, you may also want to:

- Enable Dialing Restrictions on a UM Dial Plan
- Enable Dialing Restrictions on a UM Mailbox Policy

1.9.2.3.4.9 Allow or Prevent Message Waiting Indicator on a UM IP Gatew ay

Allow or Prevent Message Waiting Indicator on a UM IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can allow voice mail notifications to be sent to users for calls received by a Unified Messaging (UM) IP gateway. If you enable this setting, the UM IP gateway will be able to receive and send SIP NOTIFY messages for users. Message Waiting Indicator is enabled by default and allows message waiting notifications to be sent to users.

Message waiting indicator is a feature found in most legacy voice mail systems. In its most common form, it lights a lamp on the called party's phone to indicate the presence of a new voice message. Message waiting indicator can refer to any mechanism that indicates the existence of a new voice message or an unheard voice message.

The indication that a new voice message has arrived can be found in the Inbox in clients such as Outlook and Outlook Web App. It can take the form of a text (SMS) message sent to a registered mobile phone, an outgoing call made from an Exchange Unified Messaging server to number that's been configured for playing new messages, or it can be a lighted lamp on a user's desktop phone.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.

Use the EMC to allow or prevent Message Waiting Indicator from displaying

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. Select the UM IP gateway that you want to modify and then, in the action pane, click **Properties**.
4. On the UM IP gateway **Properties** page, select or clear the **Allow Message Waiting Indicator** button.
5. Click **OK** to save your changes.

Use the Shell to allow or prevent Message Waiting Indicator from displaying

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example prevents the message waiting indicator from displaying for users who are associated with the UM IP gateway named `MyUMIPGateway` with an IP address of 10.10.10.1.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.1 -MessageWaitingIndica
```

For more information about syntax and parameters, see Set-UMIPGateway.

Other Tasks

After you've allowed or prevented the message waiting indicator from displaying on a UM IP gateway, you may also want to:

- View or Configure the Properties of a UM IP Gateway
- Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server
- Connect a Unified Messaging Server to a Supported IP Gateway

1.9.2.3.4.10 Configure the TCP Listening Port on a UM IP Gateway

Configure the TCP Listening Port on a UM IP Gateway

Managing Unified Messaging > Managing Unified Messaging Components > Managing UM IP Gateways >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure the TCP port that's used to listen for SIP requests on a Unified Messaging (UM) IP gateway. By default, when you create a UM IP gateway, the TCP SIP listening port number is set to 5060. The TCP SIP listening port can't be configured when you create a UM IP gateway or changed by using the EMC. You must configure the TCP SIP listening port number using the **Set-UMIPGateway** cmdlet.

You may have to configure the TCP listening port to 5061 if you want to:

- Set the VoIP security setting on a UM dial plan to SIP Secured.
- Set the VoIP security setting on a UM dial plan to Secured.
- Integrate Microsoft Exchange Server 2010 with Microsoft Office Communications Server.
- Use mutual Transport Layer Security (mutual TLS) to encrypt network data between a UM server and other Exchange servers, IP gateways, or IP PBXs.

If you want to use mutual TLS between a UM IP gateway and a dial plan operating in either SIP Secured or Secured mode, when you create the UM IP gateway you must configure it with an FQDN and then use the Exchange Management Shell to configure the UM IP gateway to listen on TCP port 5061. You must also verify that any IP gateways or IP PBXs have also been configured to listen for mutual TLS requests on port 5061.

Important:

If you create a UM IP gateway using an FQDN, and the DNS configuration for the UM IP gateway is changed, you must disable and then enable the UM IP gateway to make sure that the UM IP gateway's configuration information is updated correctly in Active Directory.

Looking for other management tasks related to UM IP gateways? Check out Managing UM IP Gateways.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.

Use the Shell to configure the TCP listening port on a UM IP gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM IP gateways" entry in the Unified Messaging Permissions topic.

This example configures a UM IP gateway named `MyUMIPGateway` with an FQDN of mTLS.MyUMIPGateway.contoso.com and listens for SIP requests on TCP port 5061.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address mTLS.MYUMIPGateway.contoso.com -
```

This example configures a UM IP gateway named `MyUMIPGateway` with an FQDN of SIPSecured.MyUMIPGateway.contoso.com and listens for SIP requests on TCP port 5061.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address SIPSecured.MyUMIPGateway.contoso
```

This example configures a UM IP gateway named MyUMIPGateway with an FQDN of MyOCSUMIPGateway.contoso.com and listens for SIP requests on TCP port 5061.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address MyOCSUMIPGateway.contoso.com -Po
```

For more information about syntax and parameters, see Set-UMIPGateway.

Other Tasks

After you configure the TCP listening port for a UM IP gateway, you may also want to:

- Configure a Fully Qualified Domain Name for a UM IP Gateway
- View or Configure the Properties of a UM Dial Plan

1.9.2.3.5 Managing UM Hunt Groups

Managing UM Hunt Groups

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-08-21*

Create a UM Hunt Group

View the Properties of a UM Hunt Group

Delete a UM Hunt Group

1.9.2.3.5.1 Create a UM Hunt Group

Create a UM Hunt Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When you create a Unified Messaging (UM) hunt group, a UM Hunt Group object is created in the Active Directory directory service and is a logical representation of an existing Private Branch eXchange (PBX) or IP PBX hunt group. A UM hunt group acts as a connection or link between a UM IP gateway and a dial plan. After you create a UM hunt group, you can't change any of the settings that you defined. If you want to change the UM hunt group settings, you must delete the hunt group and then create another hunt group that has the appropriate settings.

Note:

If you associate a UM dial plan with the UM IP gateway when you create a UM IP gateway, a UM hunt group will also be created.

Looking for other management tasks related to UM hunt groups? Check out Managing UM Hunt Groups.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.

What Do You Want to Do?

- Use the EMC to create a UM hunt group
- Use the Shell to create a UM hunt group

Use the EMC to create a UM hunt group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM hunt groups" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. In the result pane, select a UM IP gateway.
4. In the action pane, click **New UM Hunt Group**.
5. In the New UM Hunt Group wizard, view or complete the following fields:
   - **Associated UM IP gateway** This display-only field shows the name of the UM IP gateway that will be associated with the UM hunt group.
   - **Name** Use this text box to create the display name for the UM hunt group. A UM hunt group name is required and must be unique, but it's used only for display purposes in the EMC and the Shell. If you have to change the display name of the hunt group after it has been created, you must first delete the existing hunt group and then create another hunt group that has the appropriate name.

     If your organization uses multiple hunt groups, we recommend that you use meaningful names for your hunt groups. The maximum length of a UM hunt group name is 64 characters, and it can include spaces. However, it can't include any of the following characters: " / \ [ ] : ; | = , + * ? < >.
   - **Dial plan** Click the **Browse** button to select the dial plan that will be associated with the UM hunt group. Associating a hunt group with a dial plan is required. A UM hunt group can be associated with only one UM IP gateway and one UM dial plan.
   - **Pilot identifier** Use this text box to specify a string that uniquely identifies the pilot identifier or pilot ID configured on the PBX or IP PBX.

     An extension number or a Session Initiated Protocol (SIP) Uniform Resource Identifier (URI) can be used in this field. Alphanumeric characters are accepted in this field. For legacy PBXs, a numeric value is used as a pilot identifier. However, some IP PBXs can use SIP URIs.
6. On the **Completion** page, confirm whether the UM hunt group was successfully created:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task

fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

7. Click **Finish** to complete the New UM Hunt Group wizard.

Use the Shell to create a UM hunt group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM hunt groups" entry in the Unified Messaging Permissions topic.

This example creates a UM hunt group named `MyUMHuntGroup` that has a pilot identifier of 12345.

```
New-UMHuntGroup -Name MyUMHuntGroup -PilotIdentifier 12345  -UMDialplan MyUMDialP
```

This example creates a UM hunt group named `MyUMHuntGroup` that has multiple pilot identifiers.

```
New-UMHuntGroup -Name MyUMHuntGroup -PilotIdentifier 5551234,55555 -UMDialplan My
```

For more information about syntax and parameters, see New-UMHuntGroup.

Other Tasks

After you configure dialing rule groups, you may also want to:

- View the Properties of a UM Hunt Group
- Create a UM Auto Attendant

1.9.2.3.5.2 View the Properties of a UM Hunt Group

View the Properties of a UM Hunt Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can view Unified Messaging (UM) hunt group properties. When you view the properties for a UM hunt group, you can view the properties associated with a single UM hunt group or all UM hunt groups associated with a single UM IP gateway. If neither parameter is specified, all UM hunt groups in the forest will be returned.

After a UM hunt group has been created, the settings configured can't be changed. If you want to change a configuration setting such as the pilot identifier on a UM hunt group, you must delete the existing UM hunt group and create a new UM hunt group that has the correct settings. When you're using the **Get-UMHuntGroup** cmdlet, you can't only enter the name of the UM hunt group. You must also include the name of the UM IP gateway that's associated with the UM hunt group. For example, **Get-UMHuntGroup** *MyUMIPGateway\MyUMHuntGroup1*.

Looking for other management tasks related to UM hunt groups? Check out Managing UM Hunt Groups.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.

Use the EMC to view the properties of a UM hunt group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM hunt groups" entry in the Unified Messaging Permissions topic.

1. In the console root, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. On the **UM IP Gateways** tab, expand the UM IP Gateway object that contains the hunt group for which you want to review properties.
4. In the work pane, review the configuration settings of the UM hunt group by reviewing the **UM Dial Plans**, **Pilot Identifier**, **Address**, and **Status** columns.

Use the Shell to view the properties of a UM hunt group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM hunt groups" entry in the Unified Messaging Permissions topic.

This example displays all the UM hunt groups in the Active Directory forest.

```
Get-UMHuntGroup
```

This example displays the details of a UM hunt group named `MyUMHuntGroup` in a formatted list.

```
Get-UMHuntGroup -identity MyUMIPGateway\MyUMHuntGroup | Format-List
```

For more information about syntax and parameters, see Get-UMHuntGroup.

Other Tasks

After you view the properties of a UM hunt group, you may also want to:

- Delete a UM Hunt Group
- Create a UM Hunt Group

1.9.2.3.5.3 Delete a UM Hunt Group

Delete a UM Hunt Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can delete an existing Unified Messaging (UM) hunt group. After you delete the UM hunt group, the UM IP gateway associated with the UM hunt group will no longer service or answer incoming calls. If the deleted UM hunt group operation leaves the UM IP gateway without any remaining configured hunt groups, the UM IP gateway can't handle or process UM calls.

Looking for other management tasks related to UM hunt groups? Check out Managing UM Hunt Groups.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.
- A UM hunt group has been created. For detailed steps, see Create a UM Hunt Group.

Use the EMC to delete an existing UM hunt group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM hunt groups" entry in the Unified Messaging Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Unified Messaging**.
2. In the work pane, click the **UM IP Gateways** tab.
3. Under the name of the UM IP gateway, select a UM hunt group.
4. In the action pane, click **Remove**.
5. In the confirmation dialog box, click **Yes** to confirm the deletion of the UM hunt group.

Use the Shell to delete an existing UM hunt group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM hunt groups" entry in the Unified Messaging Permissions topic.

This example deletes a UM hunt group named `MyUMHuntGroup`.

```
Remove-UMHuntGroup -Identity MyUMHuntGroup
```

For information about syntax and parameters, see Remove-UMHuntGroup.

Other Tasks

After you delete an existing UM hunt group, you may also want to:

- Create a UM Hunt Group
- View the Properties of a UM Hunt Group

1.9.2.4 Managing IP Gateways

Managing IP Gateways

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2008-10-26*

Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server

Connect a Unified Messaging Server to a Supported IP Gateway

Configure an IP Gateway to Communicate with a PBX

1.9.2.4.1 Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server

Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-20*

You must configure the IP gateway devices correctly when you deploy Microsoft Exchange Server 2010 Unified Messaging (UM) for your organization. To do this, you need to configure the interface of the IP gateways to communicate with the Unified Messaging server.

Important:

When you perform administrative tasks on the IP gateway using a Web browser, the HTTP requests sent over the network when you configure an IP gateway device are not encrypted. To increase the level of security for the IP gateways on your network, use Internet Protocol security (IPsec) or Secure Sockets Layer (SSL) to help protect the administrative credentials and data transmitted over the network. We also recommend that you use a strong authentication mechanism and complex administrative passwords to protect the administrative credentials for the device.

IP Gateway Interface

There are several types of ports or interfaces that you must configure to enable communication between a Private Branch eXchange (PBX), IP gateway, and Unified Messaging servers on your network. When you configure an IP gateway, you must consider whether the IP gateway device is analog, digital, or analog and digital. If the IP gateway interface that connects to a PBX is analog, you must correctly configure the appropriate settings to enable the IP gateway to communicate with your Unified Messaging servers on your network. For your Unified Messaging servers to communicate with the IP gateways on your network, you must configure the interfaces to communicate with your PBXs, and you must configure the Local Area Network (LAN) connection or

network interface for the device.

The following is a list of suggested resources that contain information that can help you correctly configure your IP gateway interfaces and the network interface:

- **IP gateway, IP PBX, and PBX documentation** The Exchange TechCenter contains configuration files and setup information you can use when you configure IP gateways, IP PBXs, and PBXs. For more information, see Telephony Advisor for Exchange Server 2007.
- **Configuring an AudioCodes-based IP gateway** You can find the latest support and configuration information at the Microsoft AudioCodes Technical Resources for Exchange 2007 and 2010 Web site to help you configure AudioCodes-based IP gateways for use with Unified Messaging.
- **Configuring a Dialogic-based IP gateway** You can find the latest support and configuration information for Dialogic-based IP gateways at the Dialogic Technical Documentation Web site.

We also recommend that all customers who plan to deploy Exchange 2010 Unified Messaging obtain the assistance of a Unified Messaging specialist. A Unified Messaging specialist helps make sure that there is a smooth transition to Exchange 2010 Unified Messaging from a legacy voice mail system. Performing a new deployment or upgrading a legacy voice mail system requires significant knowledge about PBXs and Exchange 2010 Unified Messaging. For more information about how to contact a Unified Messaging specialist, see the Microsoft Exchange Server 2007 Unified Messaging (UM) Specialists Web site.

After you configure the IP gateway IP interface, you must create and configure a UM IP gateway. For more information about how to create a UM IP gateway, see Create a UM IP Gateway.

After you install the IP gateway, you must create an UM IP gateway object to represent the IP gateway. After you create a UM IP gateway object, the Unified Messaging server associated with the UM IP gateway sends a SIP OPTIONS request to the IP gateway to make sure that the IP gateway is responsive. If the IP gateway doesn't respond to the SIP OPTIONS request from the Unified Messaging server, the Unified Messaging server will log an event with ID 1088 stating that the request failed. To resolve this issue, make sure the IP gateway is available and online and the Unified Messaging configuration is correct.

A Unified Messaging server will communicate only with IP gateways or IP PBXs that are listed as a trusted Session Initiation Protocol (SIP) peer. An event with ID 1175 will be logged when multiple DNS hosts share the same IP address. This event may occur if you've configured you DNS zones with a fully qualified domain names (FQDN) for the IP gateways on your network. Unified Messaging protects against unauthorized requests by retrieving the internal URL of the Unified Messaging Web Services Virtual Directory that is located on the server that has the Client Access role installed and then uses the URL to build the list of FQDNs for the trusted SIP peers. After two FQDNs are resolved to the same IP address, this event will be logged.

Note:

You must restart the Microsoft Exchange Unified Messaging service if an IP gateway is configured to have an FQDN and the IP gateway's DNS record is changed after the service has been started. If you don't restart the service, the Unified Messaging server won't be able to locate the IP gateway. This occurs because a Unified Messaging server maintains a cache for all IP gateways in memory, and DNS resolution is performed only when the service is restarted or when an IP gateway's configuration has changed.

For More Information

Understanding Telephony Concepts and Components

Connect a Unified Messaging Server to a Supported IP Gateway

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You must configure the IP gateways and IP PBXs on your network to communicate with the Exchange 2010 Unified Messaging servers in your Exchange organization. You must also configure your Exchange 2010 Unified Messaging servers to communicate with the IP gateways and IP Private Branch eXchanges. After you've configured IP gateways or IP PBXs on your network, you then need to configure Active Directory and the computers on which the Unified Messaging server role is installed.

Note:

After you've connected the UM server to an IP gateway or IP PBX, you must also enable users for Unified Messaging.

Steps

Here are the basic steps for connecting IP Gateways or IP PBXs to a Unified Messaging server:

Step 1: Install the Unified Messaging server role

Step 2: Create and configure a UM IP gateway

Step 3: Create a new UM hunt group (possibly)

See the following sections for information about each step.

Step 1: Install the Unified Messaging server role

If you're installing the Unified Messaging server role on an Exchange 2010 server that is separate from the server on which the Mailbox and Hub Transport server roles are installed, use **Setup.exe**. If you're installing the Unified Messaging server role on the Exchange 2010 computer that currently has the Mailbox and Hub Transport server roles installed, you can use **Add or Remove Programs** or Setup.com.

For detailed steps, see Install the Exchange 2010 Unified Messaging Server Role.

Step 2: Create and configure a UM IP gateway

When you create a UM IP gateway, you can configure the UM IP gateway object to use an IP address or a fully qualified domain name (FQDN). If you use an FQDN, you must make sure you've correctly configured a DNS host record for the IP gateway so the host name will be correctly resolved to an IP address.

A Unified Messaging server will communicate only with IP gateways or IP PBXs listed as a trusted Session Initiation Protocol (SIP) peer. In some cases, if two IP gateways are configured to use the same IP address, an event with ID 1175 will be logged. Unified

Messaging protects against unauthorized requests by retrieving the internal URL of the Unified Messaging Web Services virtual directory that is located on the server that has the Client Access role installed and then uses the URL to build the list of FQDNs for the trusted SIP peers. When two FQDNs are resolved to the same IP address, this event will be logged.

Note:

You must restart the Microsoft Exchange Unified Messaging service if an IP gateway is configured to use an FQDN and the IP gateway's DNS record is changed after the service has been started. If you don't restart the service, the UM server won't be able to locate the IP gateway. This occurs because a UM server maintains a cache for all IP gateways in memory and DNS resolution is performed only when the service is restarted or when an IP gateway's configuration has changed.

After you install the IP gateway, you must create a UM IP gateway to represent the IP gateway. After you've created a UM IP gateway object, the UM server associated with the UM IP gateway will send a SIP OPTIONS request to the IP gateway to ensure that the IP gateway is responsive. If the IP gateway doesn't respond to the SIP OPTIONS request from the Unified Messaging server, the Unified Messaging server will log an event with ID 1088 stating that the request failed. To resolve this issue, make sure that the IP gateway is available and online and that the Unified Messaging configuration is correct.

Unified Messaging supports various IP gateway vendors and other vendors of IP PBXs. Each IP gateway is designed to connect to a variety of third-party PBX systems.

For detailed information about IP gateways, see the following topics:

- Create a UM IP Gateway
- View or Configure the Properties of a UM IP Gateway
- Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server

Looking for other management tasks related to Unified Messaging? Check out Managing Unified Messaging Components.

Step 3: Create a new UM hunt group (possibly)

Depending on how you create the UM IP gateway, you may have to create a new UM hunt group. For more information about how to create a UM hunt group, see Create a UM Hunt Group.

Other Tasks

After you've connected the UM server to an IP gateway or IP PBX, you may also want to:

- Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server
- Configure an IP Gateway to Communicate with a PBX

Configure an IP Gateway to Communicate with a PBX

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-08-19*

When you configure your telephony and data networks for Microsoft Exchange Server 2010 Unified Messaging (UM), you must correctly configure the IP gateways so they communicate with the Unified Messaging servers running Exchange 2010. You must also correctly configure the IP gateways to communicate with the Private Branch eXchanges (PBXs) in your organization. You can use the information and links to configure an IP gateway to communicate with a PBX.

Note:

Exchange 2010 Unified Messaging supports only Session Initiation Protocol (SIP) over Transmission Control Protocol (TCP).

Configuring an IP Gateway

When you configure an IP gateway, you must consider whether the IP gateway device is analog, digital, or analog and digital. If the IP gateway interface that connects to a PBX is analog, you must correctly configure the appropriate settings to enable the IP gateway to communicate with a PBX. If the IP gateway interface that connects to a PBX is digital, there may be no additional configuration required to enable the digital interface to communicate with a PBX.

The following list of suggested resources contains information that can help you correctly configure your IP gateways:

- **IP gateway, IP PBX, and PBX documentation** The Exchange TechCenter contains configuration files and setup information you can use when you configure IP gateways, IP PBXs, and PBXs. For more information, see Telephony Advisor for Exchange Server 2007.
- **Configuring an AudioCodes-based IP gateway** You can find the latest support and configuration information at the Microsoft UM Specialist Resource Page to help you configure AudioCodes-based IP gateways for use with Unified Messaging.
- **Configuring a Dialogic-based IP gateway** You can find the latest support and configuration information for Dialogic-based IP gateways at the Dialogic Technical Documentation Web site.

We also recommend that all customers who plan to deploy Exchange 2010 Unified Messaging obtain the assistance of a Unified Messaging specialist. A Unified Messaging specialist will help make sure that there's a smooth upgrade to Unified Messaging from a legacy voice mail system. Performing a new deployment or upgrading a legacy voice mail system requires significant knowledge about PBXs and Exchange 2010 Unified Messaging. For more information about how to contact a Unified Messaging specialist, see the Microsoft Exchange Server 2007 Unified Messaging (UM) Specialists Web site.

Important:

When you perform administrative tasks on the IP gateway using a Web browser, the HTTP requests sent over the network when you're configuring an IP gateway device aren't encrypted. To increase the level of security for the IP gateways on your network, use Internet Protocol security (IPsec) or Secure Sockets Layer (SSL) to help protect the administrative credentials and data transmitted over the network. We also recommend that you use a strong authentication mechanism and complex administrative passwords to protect the administrative credentials for the device.

For More Information

PBX Configuration Notes Tested by Microsoft or IP Gateway Vendor Partners

Configure an IP Gateway or IP PBX for Use with a Unified Messaging Server

Connect a Unified Messaging Server to a Supported IP Gateway

Understanding Telephony Concepts and Components

1.9.3 Securing Unified Messaging Servers

Securing Unified Messaging Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

An important aspect of network security for your organization is correctly configuring security for your Microsoft Exchange Server 2010 Unified Messaging (UM) infrastructure. This includes using the security-related configuration options for your Unified Messaging servers and UM-enabled users. By increasing the level of security within your Unified Messaging environment, you increase the level of security for your whole network. This topic contains information and links to security-related topics that can help you increase the level of protection by doing the following:

- Configuring the appropriate PIN settings for users in your organization
- Enabling the security settings to help protect the Unified Messaging network data and servers in your organization
- Effectively assigning administrative permissions to manage your Unified Messaging environment

Unified Messaging Security

There are three security-related areas to consider when you deploy Unified Messaging. You can help increase the level of protection for your network if you correctly plan a Unified Messaging security strategy and then correctly configure the security settings that are available to administrators in the following areas:

- **UM-enabled user PIN security** When a subscriber or a UM-enabled user uses a telephone to connect to a computer that has the Unified Messaging server role installed, they use Outlook Voice Access to move through the Unified Messaging menu system. However, before users can access the Unified Messaging system, the system prompts them to input their PIN. As the administrator, you can configure PIN settings and requirements and perform PIN management tasks. For more information about how to configure PIN settings for UM-enabled users, see Configuring Security for Unified Messaging Users.
- **Securing Unified Messaging network traffic** There are several security methods that can help you protect the Unified Messaging servers and the network traffic in your organization. This includes traffic that's sent between your IP gateways and Unified Messaging servers and between your Unified Messaging servers and other Exchange 2010 servers in your organization. For more information about how to help secure the network traffic that's generated by Unified Messaging, see Securing Unified Messaging Network Traffic.

- **Configuring permissions for Unified Messaging** In many organizations, there are separate administrators for Microsoft Exchange, the Active Directory directory service, and the telecommunications equipment. Therefore, administrative functions must be delegated to maintain distinct boundaries between different levels of administrative permissions.

1.9.3.1 Configuring Security for Unified Messaging Users

Configuring Security for Unified Messaging Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

In Microsoft Exchange Server 2010 Unified Messaging (UM), PIN policies are defined and configured on a UM mailbox policy. Multiple UM mailbox policies can be created, depending on your requirements. When you enable a user for Unified Messaging, you associate or link the user to an existing UM mailbox policy. The UM PIN policies that are configured on the UM mailbox policy should be based on the security requirements of your organization.

Unified Messaging PIN Security

A PIN is a numeric string used in certain systems, including Unified Messaging systems, so a user can be authenticated and gain access. A PIN is a pass code users enter on the telephone to access their Exchange mailbox. The strength of the PIN depends on its length, how well it's protected, and how difficult it is to guess.

After you configure PIN settings for a UM-enabled user, you configure and manage PIN settings on the UM-enabled user's Exchange 2010 mailbox and on the UM mailbox policy associated with the UM-enabled user.

- When subscribers or a UM-enabled users use a telephone to connect to an Exchange 2010 Unified Messaging server, they use Outlook Voice Access to move through the Unified Messaging menu system. However, before users can access the Unified Messaging system, the system prompts them to input their PIN. As the administrator, you can configure PIN settings and requirements and perform PIN management tasks.

UM mailbox policies can be configured to increase the level of security for UM-enabled users by requiring users to comply with the predefined PIN policies for your organization.

When you modify a UM mailbox policy, you can change such settings as PIN policies, message text settings, and dialing restrictions for a single UM-enabled recipient or for multiple UM-enabled recipients. UM mailbox policies can be configured to increase the level of security for UM-enabled users.

You can increase the level of security for your network by correctly implementing and configuring the following PIN settings on a UM mailbox policy:

- The minimum number of digits required for a PIN
- The time, in days, a PIN is accepted by the system
- The number of times attempts to log on can fail before the user's PIN will be reset
- The maximum number of logon attempts before the user is locked out of their mailbox

- Whether to allow users to use common patterns in their PIN
- The number of past PIN entries the system should remember

For More Information

Understanding Unified Messaging Users

Understanding Unified Messaging Mailbox Policies

Configure the Number of Incorrect PIN Entries Before a Mailbox Is Locked Out on a UM Mailbox Policy

Configure the Minimum PIN Length on a UM Mailbox Policy

Configure the PIN Lifetime on a UM Mailbox Policy

Configure the Number of Previous PINs to Disallow on a UM Mailbox Policy

Configure the Number of Incorrect PIN Entries Before a PIN Is Reset on a UM Mailbox Policy

Enable or Disable Common PIN Patterns on a UM Mailbox Policy

Include Text with the E-Mail Message Sent When a PIN Is Reset

1.9.3.2 Securing Unified Messaging Network Traffic

Securing Unified Messaging Network Traffic

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-10*

An important aspect of the overall network security for your organization is configuring security correctly for Microsoft Exchange Server 2010 Unified Messaging (UM) servers. Enabling Unified Messaging servers, IP gateways, and other servers running Exchange 2010 to communicate by using Transport Layer Security (TLS) or IP security increases the level of security for your whole network. The following information and links to security-related topics can help you increase the level of protection for your network.

Securing Network Traffic

Unified Messaging can communicate with IP gateways, IP Private Branch eXchanges (PBXs), and other Exchange 2010 computers in a secured or an unsecured mode, depending on how the UM dial plan is configured and whether the appropriate certificate trusts have been established between the IP gateways and Unified Messaging servers on your network. In Unsecured mode, the Voice over IP (VoIP) and Session Initiation Protocol (SIP) traffic isn't encrypted. However, the UM dial plans and the UM server associated with the UM dial plan can be configured using the *VoIPSecurity* parameter. The *VoIPSecurity* parameter configures the dial plan to encrypt the VoIP and SIP traffic using mutual Transport Layer Security (TLS) using SIP Secured or Secured mode..

There are several things you can do to help protect your UM servers and the network traffic that is sent between your IP gateways and UM servers and between your UM servers and other Exchange 2010 servers in your organization. To understand the

components that must be used in your UM environment to help protect the network data sent and received by UM servers in your organization, you need to first understand how to do the following:

- Use IPsec to protect UM network data.
- Use TLS to protect UM network data.
- Use the different types of certificates used with Unified Messaging to implement TLS.
- Correctly configure UM servers and IP gateways to use TLS.

UM Security Components

There are various components that must be configured to help enable the Unified Messaging server to communicate in a secure manner with other Exchange 2010 servers and IP gateways. The following components help secure the data that is passed over the network:

- **IPsec** IPsec uses cryptography-based protection services, security protocols, and dynamic key management. It provides the strength and flexibility to help protect communications between private network computers, domains, sites, remote sites, extranets, and dial-up clients. It can even be used to block receipt or transmission of specific types of traffic. For more information about the security options available to help secure UM traffic, see Understanding Unified Messaging VoIP Security.
- **TLS** After you've successfully imported and exported the required trusted certificates, an IP gateway will request a certificate from the UM server, and then it will request a certificate from the IP gateway. Exchanging the trusted certificates between the IP gateway and the UM server helps secure the channel over which the IP gateway and UM server communicate by using TLS. For more information about the security options available to help secure UM traffic, see Understanding Unified Messaging VoIP Security.
- **Certificates** Digital certificates are electronic files that work like an online passport to verify the identity of a user or computer. They're used to create an encrypted channel that is used to help protect data. A certificate is basically a digital statement issued by a certification authority (CA) that vouches for the identity of the certificate holder and enables the parties to communicate in a secure manner by using encryption. They can be issued by a trusted third-party CA, for example, using Certificate Services, or they can be self-signed. For more information about the security options that are available to help secure UM traffic, see Understanding Unified Messaging VoIP Security.
- **VoIP security** Unified Messaging can communicate with IP gateways, IP PBXs, and other Exchange 2010 computers in a secured or an unsecured mode depending on how the UM dial plan is configured. By default, UM dial plans communicate in an unsecured mode. You can use the **Get-UMDialPlan** cmdlet in the Exchange Management Shell to determine the security setting for a UM dial plan. For more information about how to enable VoIP security on a UM dial plan, see Configure VoIP Security on a UM Dial Plan.

1.9.4 Troubleshooting Reference for Unified Messaging Servers

Troubleshooting Reference for Unified Messaging Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-21*

After you've installed the Unified Messaging (UM) server role on a computer running Microsoft Exchange Server 2010, you may have to test the functionality of the server. The following are two situations in which you will use the diagnostic tools and commands included with Exchange 2010:

- Troubleshooting errors and events
- Testing the Unified Messaging server to make sure that an installation was successful

The following topics will help you test and troubleshoot a Unified Messaging server:

- Enable Tracing for Unified Messaging
- Enable Diagnostic Logging on a Unified Messaging Server
- Testing Unified Messaging Server Functionality
- Testing Call Flow with the Exchange 2010 UM Troubleshooting Tool

1.9.4.1 Enable Tracing for Unified Messaging

Enable Tracing for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

There are several tracing options available for troubleshooting issues related to Microsoft Exchange Server 2010 Unified Messaging (UM). Tracing lets you troubleshoot, debug, and isolate problems on a computer. You can enable tracing, configure tracing settings, and gathering the appropriate information about an Exchange 2010 Unified Messaging server to help you diagnose problems or evaluate system performance. Although there are many tracing tools offered by Microsoft and third-party vendors that may offer more complex tracing options, Microsoft Exchange Analyzers and Network Monitor are tools that you can download to help you enable tracing on a Unified Messaging server. This topic discusses tracing tools and tracing options available for troubleshooting and diagnosing Unified Messaging issues.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Prerequisites

You can install these tools on a client computer running Microsoft .NET Framework 1.1.

For more information about Exchange Analyzers, see Overview: Microsoft Exchange Analyzers.

Use the Exchange Troubleshooting Assistant to create a network trace

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

The Exchange Troubleshooting Assistant includes several tools that can be used to troubleshoot Unified Messaging issues and gather information about different Unified Messaging services and components.

The Trace Control tool that's included in the Exchange Troubleshooting Assistant is a graphical user interface (GUI) that lets you enable and configure tracing on an Exchange 2010 Unified Messaging server. It can also be used to enable tracing on other Exchange 2010 servers in your organization. To enable tracing, select the trace type, component to trace, and any trace tags. When you're enabling tracing on a Unified Messaging server, you must enable the **MSExchangeUM** component listed under the **Components to Trace** section of the tool. Several features are available when you enable tracing using the Exchange Troubleshooting Assistant, including the following:

- Ability to display only enabled components and tags
- Ability to search components and tags
- Ability to display the current status of tracing on startup, including output file size, type, and location

The Microsoft Exchange Troubleshooting Assistant can be used to automatically determine what set of data is required to troubleshoot symptoms that you identify. It can also be used to collect configuration data, performance counters, event logs, and live tracing information from an Exchange 2010 Unified Messaging server in addition to Exchange 2010 servers in your organization running other Exchange 2010 server roles. The Exchange Troubleshooting Assistant analyzes each subsystem on a physical computer to determine individual bottlenecks and component failures. Then it aggregates the information to analyze the cause of the bottlenecks and failures. To download a copy of the Exchange Troubleshooting Assistant, see Microsoft Exchange Troubleshooting Assistant v1.1.

For more information about Exchange Analyzers, see Microsoft Exchange Analyzers

Important:

Tracing information and files can be very complex, depending on the operation and depth of tracing that has been completed. We recommend that after you enable tracing and collect the correct information, you contact Microsoft Enterprise Support.

Use Network Monitor to create a network trace

To perform the following procedures, you must log on by using an account that's a member of the local Administrators group on that computer.

You can use Network Monitor 3.3 to capture network traffic between a Unified Messaging server and an IP gateway or between Exchange 2010 servers running the Client Access, Mailbox, and Hub Transport server roles. A network monitor is a network protocol analyzer tool used to capture network data packets, which lets you analyze specific protocol information.

Network traffic to and from a Unified Messaging server may consist of the following protocols. However, there may be other protocols used, depending on the applications and devices. The following protocols can be used:

- **Session Initiation Protocol (SIP)** Used between an IP gateway, an IP Private Branch eXchange (PBX), or a Microsoft Office Communications Server 2007 front-end server and a Unified Messaging server to establish a communication session. By default, when SIP packets are sent over a network, they are not encrypted. However, you can use mutual Transport Layer Security (TLS) to encrypt the SIP packets.
- **Realtime Transport Protocol (RTP)** Used between media endpoints that send and receive audio packets such as an IP gateway, an IP-based phone, or

a Microsoft Office Communicator 2007 client and a Unified Messaging server. By default, when RTP packets are sent over a network, they are not encrypted. However, you can use mutual TLS to encrypt the SIP packets. If mutual TLS is used to protect the RTP packets, another protocol, Secure Realtime Transport Protocol (SRTP), will be used.

- **T.38** Used for the transmission of fax audio signals between a media endpoint and a Unified Messaging server.
- **SMTP** Used between a Unified Messaging server and a Hub Transport server.
- **LDAP** Used between a Unified Messaging server and an Active Directory domain controller.
- **MAPI RPC** Used between a Unified Messaging server and a Mailbox server.
- **Mutual TLS** Used between an IP gateway and a Unified Messaging server and between a Unified Messaging server and Hub Transport, Mailbox, and Client Access servers. Mutual TLS can be used with SIP, SMTP, or RTP to encrypt the protocol's content.

Note:
If mutual TLS transport is used, the Network Monitor parser will be unable to decode the packets because they are encrypted.

By default, the following parsers are available in Network Monitor 3.3 for protocols used specifically by a Unified Messaging server:

- RTP
- Session Description Protocol (SDP)
- SIP
- SMTP
- Interactive Connectivity Establishment
- To download a copy of Network Monitor 3.3, see Microsoft Network Monitor 3.3.

Other Tasks

After you enable Unified Messaging on an Exchange 2010 server, you may also want to read one or more of the following topics:

- Understanding Protocols, Ports, and Services in Unified Messaging
- Unified Messaging Voice Call Processing
- Unified Messaging Outlook Voice Access Call Processing
- Unified Messaging Auto Attendant Call Processing
- Unified Messaging Play on Phone Call Processing

1.9.4.2 Enable Diagnostic Logging on a Unified Messaging Server

Enable Diagnostic Logging on a Unified Messaging Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use EMC, Shell or a registry editing tool to enable diagnostic logging on a Microsoft Exchange Server 2010 Unified Messaging (UM) server. By default, diagnostic logging is enabled on a UM server but is set to the lowest level. However, if you're troubleshooting an issue on a UM server, you may have to increase the diagnostic logging

level to help you locate the source of the problem.

Event Viewer maintains logs about program, security, and system events on your computer. These logs include errors and events that occur on a UM server. You can use Event Viewer to view and manage the event logs, gather information about hardware and software problems, and monitor Unified Messaging errors and events. Although Event Viewer is a Microsoft Windows operating system tool and not a Microsoft Exchange tool, Event Viewer is useful when you troubleshoot problems with Unified Messaging. For more information about Unified Messaging errors and events, see Error and Event Reference for Unified Messaging Servers.

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

What Do You Want to Do?

- Use the EMC to set logging levels
- Use the Shell to set logging levels
- Use the Registry to set logging levels

Use the EMC to set logging levels

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Shell infrastructure permissions" section in the Exchange and Shell Infrastructure Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Mailbox**.
2. In the Actions pane, select **Manage Diagnostic Logging Properties**.
3. On the **Manage Diagnostic Logging Properties** wizard page, click the Exchange service for which you want to change the logging level.
4. Select the logging level, and then click **Configure**.

   Note:

   You can return to the default logging levels by selecting **Reset all services to default logging levels** and then clicking **Configure**.

5. On the **Completion** page, confirm whether the process completed successfully. A status of **Completed** indicates that the wizard completed the task successfully. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to complete the Manage Diagnostic Logging Level wizard.

Use the Shell to enable diagnostic logging on a Unified Messaging server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Shell infrastructure permissions" section in the Exchange and Shell Infrastructure Permissions topic.

This example enables diagnostic logging for the **UMCore** DWORD value.

```
Set-EventlogLevel "MyUMServer\MSExchange Unified Messaging\UMCore" -level <Lowest
```

This example enables diagnostic logging for the **UMWorkerProcess** DWORD value.

```
Set-EventlogLevel "MyUMServer\MSExchange Unified Messaging\UMWorkerProcess" -leve
```

This example enables diagnostic logging for the **UMManagement** DWORD value.

```
Set-EventlogLevel "MyUMServer\MSExchange Unified Messaging\UMManagement" -level <
```

This example enables diagnostic logging for the **UMService** DWORD value.

```
Set-EventlogLevel "MyUMServer\MSExchange Unified Messaging\UMService" -level <Low
```

This example enables diagnostic logging for the **UMClientAccess** DWORD value.

```
Set-EventlogLevel "MyUMServer\MSExchange Unified Messaging\UMClientAccess" -level
```

This example enables diagnostic logging for the **UMCallData** DWORD value.

```
Set-EventlogLevel "MyUMServer\MSExchange Unified Messaging\UMCallData" -level <Lo
```

This example lets you see the current logging level for a Unified Messaging server.

```
Get-EventlogLevel "MyUMServer\MSExchange Unified Messaging"
```

For more information about syntax and parameters, see Set-EventLogLevel.

Use Registry Editor to enable diagnostic logging on a Unified Messaging server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

1. Start Registry Editor (regedit).
2. Locate the following registry key: **HKeyLocalMachine\System \CurrentControlSet\services\MSExchange Unified Messaging\Diagnostics**
3. In the details pane, double-click the appropriate registry value, and then use the following values to configure the appropriate logging level:

Logging level	Value
Expert	7
High	5
Medium	3
Low	1
Lowest	0

Other Tasks

After you enable diagnostic logging on a Unified Messaging server, you may also want to:

- Enable Tracing for Unified Messaging
- Testing Unified Messaging Server Functionality

1.9.4.3 Testing Unified Messaging Server Functionality

Testing Unified Messaging Server Functionality

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

After you install the Unified Messaging server role on a computer running Microsoft Exchange Server 2010 and enable and configure Unified Messaging, you can use multiple diagnostic tests and a software-based telephone application to test telephony connectivity and the operation of the Unified Messaging server. This topic gives you information about the diagnostic tests for testing a Unified Messaging server.

Test-UMConnectivity

There are three diagnostic tests that can be used to test the functionality of an Exchange 2010 Unified Messaging system and a Unified Messaging server: Local, Local with a TUILogon, and Remote. The **Test-UMConnectivity** cmdlet can be used to check connectivity to Unified Messaging servers in several ways, depending on the parameters used with the cmdlet. For testing Unified Messaging functionality, you can use these tests:

- **Local** The **Test-UMConnectivity** cmdlet verifies Voice over IP (VoIP) communication with the Unified Messaging server running on the same local computer.
- **Local with TUILogon** The **Test-UMConnectivity** cmdlet tries to establish VoIP communication with the Unified Messaging server running on the same computer. If it connects, it tries to sign in to one or more UM-enabled mailboxes by sending the extension number and PIN of the mailbox. If the *–TUILogon* parameter is supplied, the following parameter values must also be supplied for the test to complete successfully. You must supply the following parameters with the appropriate information for the test mailbox:
  - *–Phone* This parameter must contain the extension number for the test mailbox.
  - *–PIN* This parameter must contain the PIN of the UM-enabled mailbox.
  - *–UMDialPlan* This parameter must contain the dial plan associated with the test mailbox.

  When you use this diagnostic test, you must create a test mailbox using the New-TestCasConnectivity.ps1 script located in the %ExchangeRoot%\Scripts folder. Mailboxes created using this script can also be used for other kinds of connectivity testing, for example, with Microsoft Exchange ActiveSync. When you create the test mailbox, you have the option to also enable the test mailbox for Unified Messaging by specifying the *-UMDialPlan* and *-UMExtension* parameters. If you created the test mailbox but didn't enable it for Unified Messaging, you can use the **Enable-UMMailbox** cmdlet or the Exchange Management Console to enable the test mailbox.
  If the *–TUILogonAll* parameter is supplied with the **Test-UMConnectivity** cmdlet, the **Test-UMConnectivity** cmdlet will try to log on to each Client Access server connectivity test mailbox created using the New-TestCasConnectivityUser.ps1 script in the current Active Directory site.
- **Remote** The **Test-UMConnectivity** cmdlet tries to connect to a remote Unified Messaging server by placing a call through an IP gateway. After it connects, it performs connectivity checks on the remote Unified Messaging server and the media paths.

Note:

If you receive the following message, you should restart the Microsoft

Exchange Unified Messaging service because it has stopped or is not responding: "The Test-UMConnectivity task encountered an error while trying to make a call. Details: Unable to establish a connection."

1.9.4.3.1 Test Unified Messaging Server Operation

Test Unified Messaging Server Operation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic explains how to use the Shell to test the operation of a computer running Microsoft Exchange Server 2010 that has the Unified Messaging (UM) server role installed. When you perform the following procedure, the Unified Messaging server initiates a diagnostic Session Initiation Protocol (SIP) call, and then returns a health state variable of the Unified Messaging server.

This diagnostic test can be run only on a local Unified Messaging server, and you can't test the operation of the Unified Messaging server using the EMC.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the Shell to test the operation of the Unified Messaging server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

This example performs connectivity and operational tests on the local Unified Messaging server, and then displays the Voice over IP (VoIP) connectivity information.

```
Test-UMConnectivity
```

This example tests the ability for a local UM server to listen for incoming unencrypted SIP requests on TCP port 5060.

```
Test-UMConnectivity -ListenPort 5060
```

This example tests the ability for a local UM server to listen for incoming encrypted SIP requests on TCP port 5061.

```
Test-UMConnectivity -ListenPort 5061
```

Note:
Use mode 1 when the -UMIPGateway parameter isn't specified.

Note:
You can set the -Timeout parameter with a value of less than 5 seconds. However, we recommend that you always configure this parameter with a value of 5 seconds or more.

For more information about syntax and parameters, see Test-UMConnectivity.

Other Tasks

After you test the operation of the Unified Messaging server and telephony components, you may also want to:

- Testing Unified Messaging Server Functionality
- Test Unified Messaging Server Operation
- Connect a Unified Messaging Server to a Supported IP Gateway

1.9.4.3.2 Test Unified Messaging Server Connectivity to IP Gateways and PBXs

Test Unified Messaging Server Connectivity to IP Gateways and PBXs

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can test the operation of a Microsoft Exchange Server 2010 Unified Messaging (UM) server and related connected telephony equipment. When you perform the following procedure, the Unified Messaging server tests the full end-to-end operation of the UM system. This includes the telephony components connected to the Unified Messaging server, including IP gateways, Private Branch eXchanges (PBXs), and cabling.

This diagnostic test can be run only on a local Unified Messaging server, and you can't test the operation of the Unified Messaging server using the EMC.

Looking for other management tasks related to UM servers? Check out Managing Unified Messaging Servers.

Prerequisites

- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM mailbox policy has been created. For detailed steps, see Create a UM Mailbox Policy.

Use the Shell to test the operation of the

Unified Messaging server and telephony components

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

This example tests the ability of the UM IP gateway to listen on TCP port 5060 for incoming SIP requests.

```
Test-UMConnectivity -ListenPort 5060 -UMIPGateway MyIPGateway
```

This example tests the ability of the local Unified Messaging server to use an unsecured TCP connection instead of a secured mutual TLS connection to place a call through a UM IP gateway named MyUMIPGateway by using the telephone number 56780.

```
Test-UMConnectivity -UMIPGateway MyUMIPGateway -Phone 56780 -Secured $false
```

This example tests the subscriber access number on a dial plan by using a SIP URI. This example can be used in an environment that includes Microsoft Office Communications Server 2007.

```
Test-UMConnectivity -UMIPGateway OCSGateway1 -Phone "sip:SIPdialplan.contoso.com@
```

Note:
You can set the -Timeout parameter with a value of less than 5 seconds. However, we recommend that you always configure this parameter with a value of 5 seconds or more. Use mode 2 when the UMIPGateway parameter is specified in the command-line syntax.

For more information about syntax and parameters, see Test-UMConnectivity.

Other Tasks

After you test the operation of the Unified Messaging server and telephony components, you may also want to:

- Testing Unified Messaging Server Functionality
- Test Unified Messaging Server Operation
- Connect a Unified Messaging Server to a Supported IP Gateway

1.9.4.4 Testing Call Flow with the Exchange 2010 UM Troubleshooting Tool

Testing Call Flow with the Exchange 2010 UM Troubleshooting Tool

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-10*

Understanding the Exchange 2010 UM Troubleshooting Tool

1.9.4.4.1 Understanding the Exchange 2010 UM Troubleshooting Tool

Understanding the Exchange 2010 UM Troubleshooting Tool

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-22*

The Microsoft Exchange 2010 Unified Messaging Troubleshooting Tool is an Exchange Management Shell cmdlet named **Test-ExchangeUMCallFlow**. You can use this tool to conduct a series of diagnostic tests for Unified Messaging (UM) in your organization. If any of the tests fail, the tool reports the reason for the failure and possible solutions to fix the problem. You can only use the UM Troubleshooting Tool on Exchange 2010 servers that have Exchange Server 2010 Service Pack 1 (SP1) installed.

The UM Troubleshooting Tool can be used to test whether voice mail is functioning correctly in both on-premises and cross-premises deployments. You can use this tool in UM deployments that include Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010, or in UM deployments that include IP gateways or IP Private Branch eXchanges (IP PBXs).

Note:

The UM Troubleshooting Tool is used for testing and troubleshooting. The **Test-UMConnectivity** cmdlet, on the other hand, should be used for monitoring. The **Test-UMConnectivity** cmdlet is used with System Center Operations Manager (SCOM) management packs that are used for monitoring Unified Messaging servers and the telephony components. The **Test-UMConnectivity** cmdlet performs local SIP tests and local logon tests to mailboxes, and can be run as an SCOM task.

To download the UM Troubleshooting Tool, see Unified Messaging Troubleshooting Tool.

Contents

Overview

The UM Troubleshooting Tool simplifies testing and troubleshooting in UM deployments. When the UM Troubleshooting Tool is run, it automatically generates a set of trace files that are stored in the C:\Users\%UserProfile%\AppData\Roaming\Microsoft Exchange 2010 UM Troubleshooting folder. The following trace files are generated by the tool:

- **UMTool_Collaboration** Includes RTC stack traces.
- **UMTool_DiagnosticLog** Lists all the tests that are run and their results.
- **UMTool_S4** Includes the S4: signaling stack traces.
- **UMTool_SIPMessageLogs** Includes the full SIP traces for the test call that's made.

The UM Troubleshooting Tool connects directly to an on-premises Session Border Controller (SBC), if one exists, or connects to an SBC in a datacenter and emulates an incoming call as if the call was coming from a PBX through an IP gateway or an IP PBX. The UM Troubleshooting tool can be used to diagnose:

- Incorrect settings in on-premises or cross-premises UM deployments in which Office Communications Server R2 or Microsoft Lync Server 2010 is deployed.
- Incorrect settings on on-premises or cross-premises telephony equipment that includes IP gateways and PBXs or IP PBXs.
- Issues with Domain Name System (DNS).
- Certificate issues when you're using SIP secured or Secured UM dial plans.
- Signaling and media issues for DTMF (also known as touchtone) and audio.

If the UM Troubleshooting Tool detects a failure in your configuration, the tool reports the reason for the error and the possible solutions for the issues that have been detected. The errors that can be reported when the UM Troubleshooting Tool is used in an on-premises deployment include the following:

- The maximum call limit has been reached.
- The user isn't enabled for Unified Messaging.
- The UM IP gateway, dial plan, or hunt group information can't be located.
- The security type doesn't match the UM dial plan.
- There are no worker processes available to process the call.
- The UM server is disabled.
- The Active Directory forest couldn't be located.
- No disk space is available.
- Invalid SIP headers were used in the request.
- A call was made to an Office Communications Server 2007 R2 server or Lync Server server.
- The UM IP gateway is disabled.
- The URI for the user who is being called isn't valid.

When the UM Troubleshooting Tool is used in a cross-premises deployment, the errors that can be reported include the following:

- The user isn't enabled for Unified Messaging.
- The UM IP gateway is disabled.
- The URI for the user is invalid.
- The security type doesn't match the UM dial plan.
- Invalid SIP headers were used in the request.
- The UM IP gateway, dial plan, or hunt group information can't be located.

The UM Troubleshooting Tool sends a sample wav file for 15 seconds. After the audio file and RTP audio stream is sent and played back, the tool reports general audio quality metrics for diagnosing audio quality issues related to network connectivity, such as jitter and average packet loss. These reports include the media stream quality to and from a UM server and contain the following:

- Network Mean Opinion Score (NMOS)
- Codec
- Latency in milliseconds (ms)
- Jitter in milliseconds (ms)

- % of packet loss
- The NMOS classification and rating that will be used to determine the audio quality will be:
- NMOS less than 2 = Poor
- NMOS greater than 2 but less than 3 = Average
- NMOS greater than 3 but less than 4 = Good
- NMOS greater than 4 but less than 5 = Excellent

The UM Troubleshooting Tool supports testing UM dial plans that use Secured, SIP Secured, and Unsecured calls. If you choose Secured or SIP Secured, the thumbprint of the certificate that's used is checked to determine whether the certificate is expired and the type of certificate that's used for TLS (Transport Layer Security) communications. The certificate is used to correctly identify and ensure the identity of the remote computer. When Secured or SIP Secured mode is selected, the UM Troubleshooting Tool verifies whether the following are true:

- The local certificate was found in the local computer store.
- The certificate being used is trusted.
- The target name specified in the certificate is valid.
- The certificate has expired.
- The remote computer trusts the certificate.
- The certificate has been revoked.
- The certificate doesn't have the required enhanced key usage.

The UM Troubleshooting Tool can be run in either Gateway or SIPClient mode, depending on whether Office Communications Server 2007 R2 or Lync Server 2010 is deployed or whether IP gateways and PBXs or IP PBXs are used with Unified Messaging servers. When either Gateway or SIPClient mode is used, the UM Troubleshooting Tool supports making calls using the following formats. The format that's used depends on the URI type of the UM dial plan:

- Telephone extension 425-555-1010
- E.164 phone numbers +1 (425) 555-1010
- SIP addresses tonysmith@contoso.com

When SIPClient mode is used, the UM Troubleshooting Tool makes a voice memo call. This is a call that doesn't ring a phone or a Unified Communications (UC) endpoint. Instead, it sends the call directly to voice mail. When the UM Troubleshooting Tool is run in SIPClient mode, it will determine:

- Which target user is being called.
- Whether the SIP call was established successfully.

Whether the SIP call was accepted by an Exchange Unified Messaging server.

- Whether the correct DTMF sequence was received.
- Whether the diagnostic .wav file was sent and received by a UM server.
- The metrics that were used when the media or audio quality stream was received.

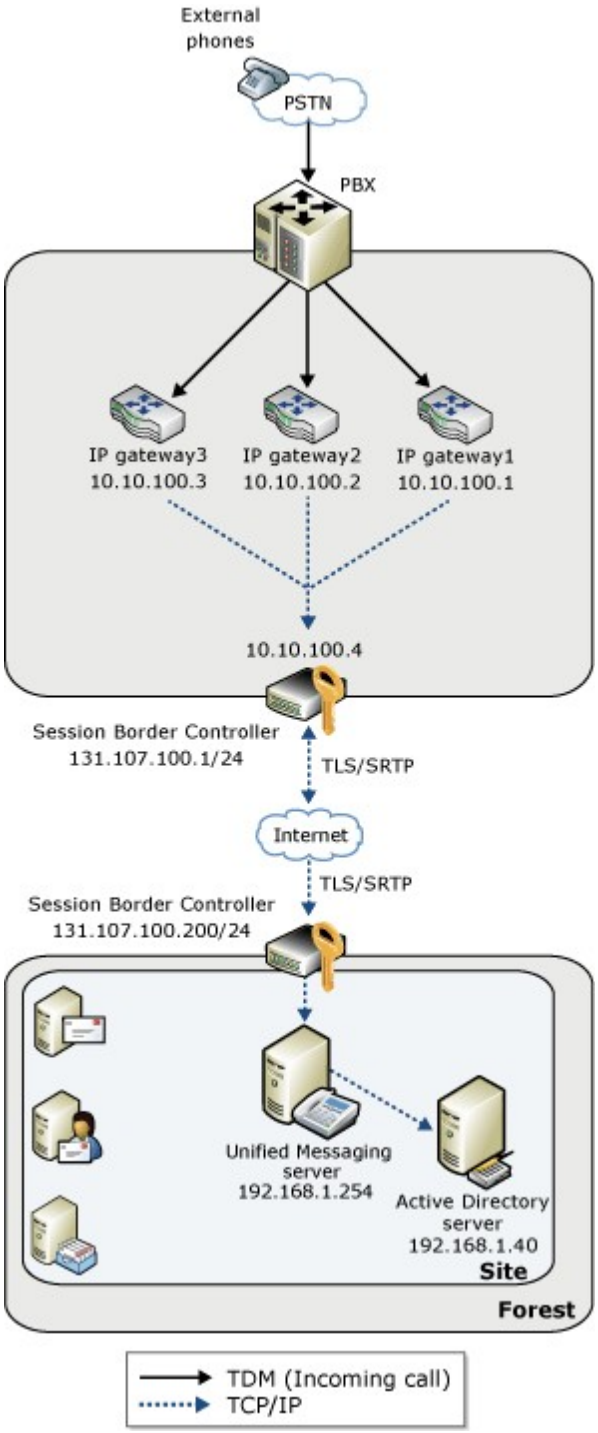
The UM Troubleshooting Tool emulates incoming calls and runs a series of diagnostic tests that help on-premises administrators and tenant administrators test call flow for call answering and identify configuration errors. Although the UM Troubleshooting Tool can be used in call answering scenarios, it can't be used to test the following types of calls:

- Outlook Voice Access calls, including calls that access voice mail, e-mail, calendar, the directory, personal Contacts, or personal options
- UM auto attendants
- Play on Phone
- Call Answering Rules
- Faxing
- Prompt provisioning

Return to top

UM Troubleshooting Architecture

Although the UM Troubleshooting Tool can help you troubleshoot, diagnose, and repair configuration issues in a cross-premises deployments, you can also used it in on-premises Unified Messaging deployments. In cross-premises deployments, the tool also validates on-site SBC configurations. The administrator can test all the Unified Messaging components that are used by Unified Messaging, including the SBCs. The following figure shows an overview of the components that can be tested in a cross premises deployment that includes on-site IP gateways and a local SBC that connects to an off-site SBC.

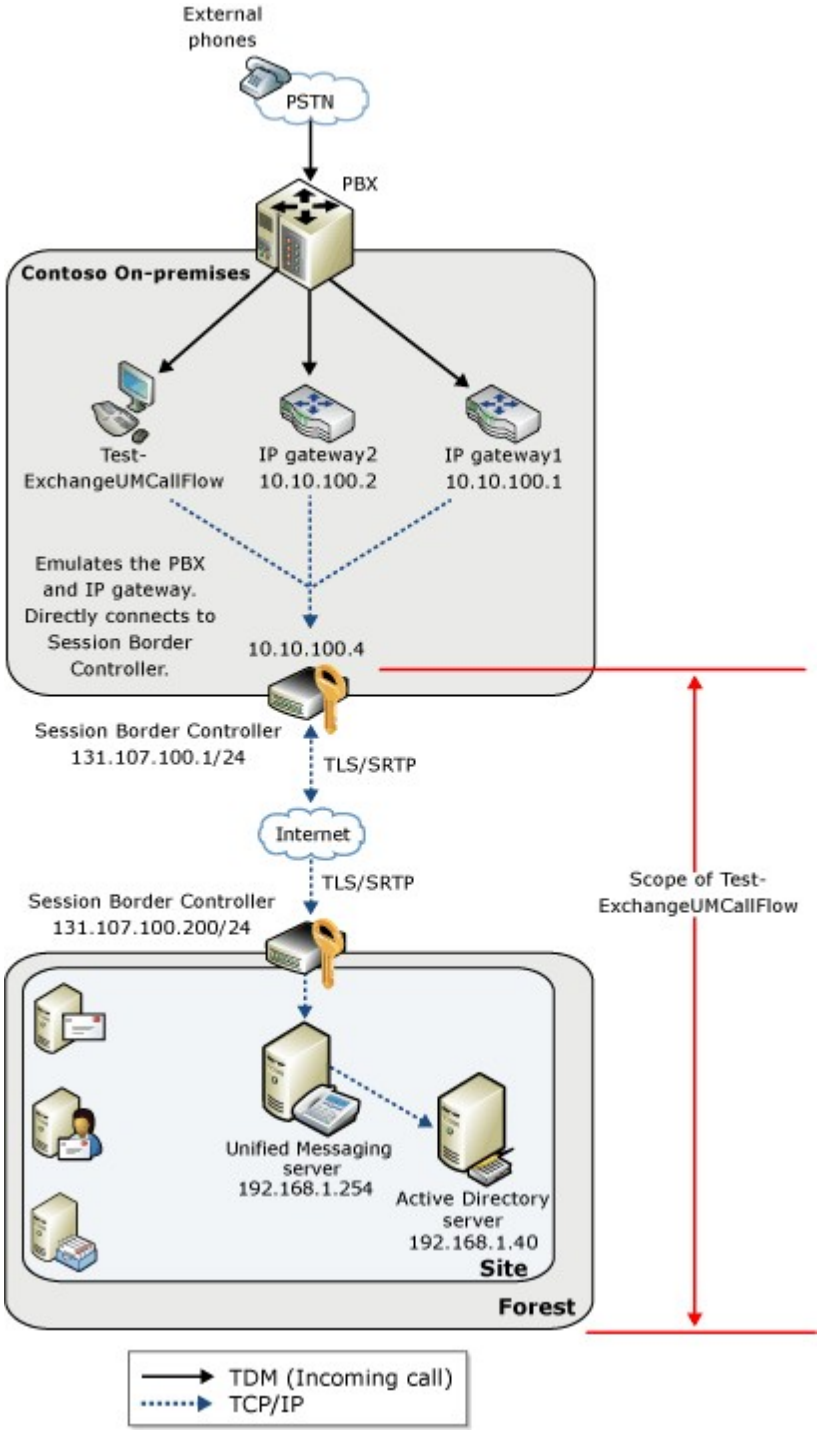


IP Gateway and IP PBX Deployments

In the following example, Gateway mode is used to test call flow in an environment that doesn't include Office Communications Server 2007 R2 or Lync Server 2010. This example tests the telephony equipment, including IP gateways, PBXs and IP PBXs, and the Unified Messaging components. This example sets the Voice over IP (VoIP) security mode to Unsecured, uses the IP address 10.1.1.1 as the next hop, and includes an extension number in the diversion information.

```
Test-ExchangeUMCallFlow -Mode Gateway -VoIPSecurity Unsecured -NextHop 10.1.1.1 -
```

The following figure shows the components that are tested when Gateway mode is used.



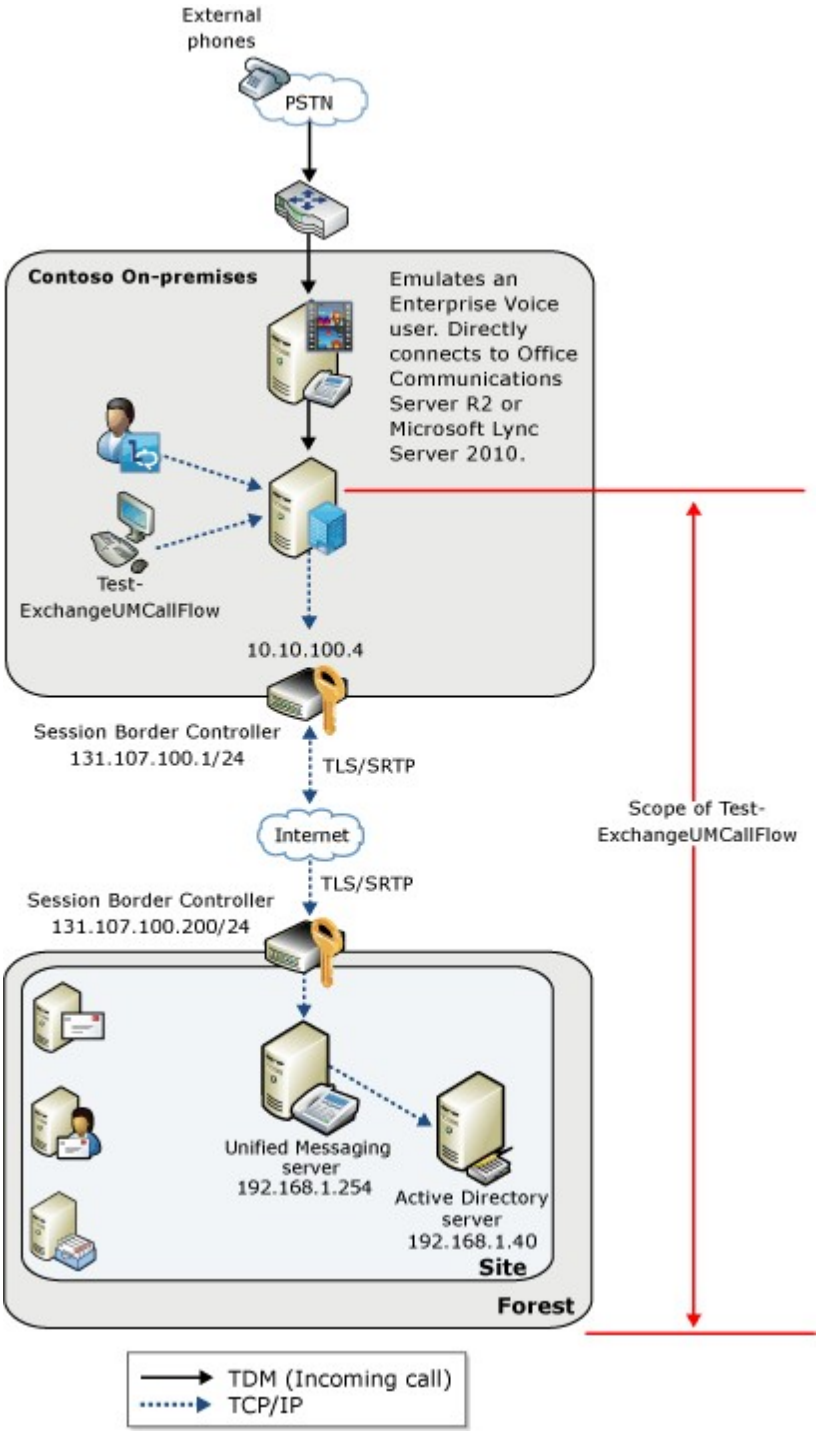
Return to top

Office Communications Server R2 and Microsoft Lync Server 2010 Deployments

The UM Troubleshooting Tool can be used in on-premises or cross-premises deployments that include Office Communications Server 2007 R2 or Microsoft Lync Server 2010 when SIPClient mode is set. The following example uses SIPClient mode and tests the call flow with a secured UM dial plan in an environment that contains Office Communications Server 2007 R2 or Lync Server 2010 servers. By default, when you run the UM Troubleshooting Tool, it uses the credentials of the user who is currently logged on to the computer. When you run the following example, you'll be prompted for the credentials you want to use when you run the UM Troubleshooting Tool. For details, see Set the Credentials to Use with the Exchange 2010 UM Troubleshooting Tool.

```
Test-ExchangeUMCallFlow -Mode SIPClient -VoIPSecurity Secured -CallingParty tony@
```

The following figure shows the components that are tested when SIPClient mode is used.



Installing the UM Troubleshooting Tool

The UM Troubleshooting Tool can be installed on a local Unified Messaging server or on another 64-bit computer running either:

- The Windows 7 or Windows Vista operating systems.
- The Windows Server 2008 or Windows Server 2008 R2 operating systems.

If you're using the UM Troubleshooting Tool on a 64-bit version of Windows 7, Windows

Vista, or the 64-bit edition of Windows Server 2008, the following components must be installed before you can install the UM Troubleshooting Tool:

- Microsoft .NET Framework 3.5 Service Pack 1 (SP1) See Microsoft .NET Framework 3.5 Service Pack 1.

  Note:
  If the tool will be run on a Windows Vista or Windows Server 2008 computer, see Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64.

- Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu) See Microsoft Knowledge Base article 968930, Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0).
- Microsoft Unified Communications Managed API 2.0 Core Runtime (UcmaRuntimeWebDownloadX64.msi) See Unified Communications Managed API 2.0, Core Runtime (64-bit).

The UM Troubleshooting Tool (**Test-ExchangeUMCallFlow** cmdlet) isn't included on the Exchange 2010 SP1 DVD or the download that only includes Exchange 2010. However you can download the UM Troubleshooting Tool from the Microsoft Download Center.

For details, see Install the Exchange 2010 UM Troubleshooting Tool.

Return to top

Cmdlet Parameters

The following table includes the parameters you can use with the **Test-ExchangeUMCallFlow** cmdlet and descriptions of those parameters. You can also use the Shell command `Get-help Test-ExchangeUMCallFlow -detailed` to find detailed information about each parameter that can be used with the **Test-ExchangeUMCallFlow** cmdlet, along with usage examples.

Parameters

Parameter	Description
CalledParty	The *CalledParty* parameter specifies the SIP URI of the Office Communications Server 2007 R2 or Lync Server 2010 user who has been enabled for Enterprise Voice. This is the user who the **Test-ExchangeUMCallFlow** cmdlet will make the voice call to, for example: `-CalledParty tonysmith@contoso.com`. Use this parameter if you're running the tool in SIPClient mode.
CallingParty	The *CallingParty* parameter specifies the SIP URI of the Office Communications Server 2007 R2 or Lync Server 2010 user who has been enabled for Enterprise Voice. This is the user who's making the incoming call, for example: `-CallingParty tonysmith@contoso.com`. Use this parameter if you're running the tool in SIPClient mode.
Diversion	The *Diversion* parameter specifies the string that should be sent as diversion information for the incoming call. This can be in the form of a Diversion or History-Info header. The diversion information that is included in the incoming call can be an

	extension number or can include additional diversion information. When you provide diversion information as a History-Info header, verify the following: • There are at least two different entries with different user parts. • The last entry contains pilot number of the user's associated UM dial plan. • The second-to-last entry includes a UM-enabled user's extension number. This entry must also include the appropriate Reason text. This text must be escaped correctly in accordance with standard URL parameter escaping rules.
Mode	The *Mode* parameter specifies whether the IP gateway, IP PBX, or Office Communications Server R2 or Lync Server 2010 mode is to be used. You can specify either Gateway mode when your UM deployment includes IP gateways or IP PBXs or SIPClient mode when your UM deployment includes Office Communications Server 2007 R2 or Lync Server 2010.
NextHop	The *NextHop* parameter specifies the IP address or fully qualified domain name (FQDN) of the next hop and can also include the TCP port of the next hop that the **Test-ExchangeUMCallFlow** cmdlet must connect to while emulating the IP gateway or IP PBX. When you include the TCP port, you must specify either port 5060 for Unsecured mode or port 5061 for Secured or SIP Secured mode. For example: `gateway.contoso.com:5061`.
CertificateThumbprint	The *CertificateThumbprint* parameter specifies the thumbprint of the certificate used for TLS. This is required if either SIP Secured or Secured mode is configured on the UM dial plan. This certificate thumbprint is the certificate that was exported from the IP gateway, IP PBX, or SBC. Also, the computer that has the UM Troubleshooting Tool installed and is being used to test for call flow must trust the certificate of authority for the next hop.
Credential	The *Credential* parameter specifies the credentials that will be used to run the cmdlet.
HuntGroup	The *HuntGroup* parameter specifies the UM hunt group associated with the IP gateway that's being emulated. This is typically an extension number. Use this parameter if you're running the tool in Gateway mode.
VoIPSecurity	The *VoIPSecurity* parameter specifies the security mode when using the cmdlet in Gateway mode. You can use one of the following VoIP security modes: • Secured (TLS/SRTP) • Unsecured (TCP/RTP) (default)

	• SIP Secured (TLS/RTP)

Return to top

1.9.4.4.2 Install the Exchange 2010 UM Troubleshooting Tool

Install the Exchange 2010 UM Troubleshooting Tool

Unified Messaging > Troubleshooting Reference for Unified Messaging Servers > Testing Call Flow with the Exchange 2010 UM Troubleshooting Tool >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Microsoft Exchange 2010 UM Troubleshooting Tool is an Exchange Management Shell cmdlet named **Test-ExchangeUMCallFlow**. You can use the cmdlet to diagnose configuration errors specific to call answering scenarios and to test whether voice mail is functioning correctly in both on-premises and cross-premises Microsoft Exchange Server 2010 Service Pack 1 (SP1) UM deployments. You can use this cmdlet in deployments with Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010 or in UM deployments with IP gateways or IP PBXs.

The UM Troubleshooting tool can be installed on a local Unified Messaging server or on another 64-bit computer.

Prerequisites

The UM Troubleshooting tool requires that the following components be installed on a computer running Windows 7, Windows Vista, or the 64-bit edition of Windows Server 2008 before the tool is installed:

- Microsoft .NET Framework 3.5 Service Pack 1 (SP1) See Microsoft .NET Framework 3.5 Service Pack 1.
- If the tool will be run on a Windows Vista or Windows Server 2008 computer See Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64.
- Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu) See Microsoft Knowledge Base article 968930, Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0).
- Microsoft Unified Communications Managed API 2.0 Core Runtime (UcmaRuntimeWebDownloadX64.msi) See Unified Communications Managed API 2.0, Core Runtime (64-bit).

Install the UM Troubleshooting Tool

1. Download the Unified Messaging Troubleshooting Tool from the Microsoft Download Center, and then double-click the MicrosoftExchange2010UMTroubleshootingTool.msi installation folder.
2. On the **Welcome to the Microsoft Exchange 2010 UM Troubleshooting Tool Setup Wizard** page, click **Next**.
3. On the **End-User License Agreement** page, review the software license terms, and if you agree, click **I accept the terms in the license agreement** and then click **Next**.
4. On the **Select Installation Folder** page, verify the path to the installation folder and click **Next**.
5. On the **Confirm Installation** page, click **Next** to start installation.

6. On the **Installation Complete** page, click **Close**.

Other Tasks

After you install the UM Troubleshooting Tool, you may also want to review:

- Set the Credentials to Use with the Exchange 2010 UM Troubleshooting Tool
- Run the Exchange 2010 UM Troubleshooting Tool on Windows 7 or Windows Vista

1.9.4.4.3 Set the Credentials to Use with the Exchange 2010 UM Troubleshooting Tool

Set the Credentials to Use with the Exchange 2010 UM Troubleshooting Tool

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Microsoft Exchange 2010 UM Troubleshooting Tool is an Exchange Management Shell cmdlet named **Test-ExchangeUMCallFlow**. You can use the cmdlet to diagnose configuration errors specific to call answering scenarios and to test whether voice mail is functioning correctly in both on-premises and cross-premises Microsoft Exchange Server 2010 Service Pack 1 (SP1) UM deployments. You can use this cmdlet in deployments with Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010 or in UM deployments with IP gateways or IP PBXs.

By default, when you're running the UM Troubleshooting Tool, it uses the credentials that are used when you log on to the computer. The credentials used are those that are specified for the calling party. You must set or specify the credentials to be used when you're running the UM Troubleshooting Tool in `SIPClient` mode. However, you don't need to set the credentials when running the UM Troubleshooting Tool in `Gateway` mode.

Prerequisites

- An Exchange 2010 server with the UM server role installed. For detailed steps, see Install the Exchange 2010 Unified Messaging Server Role.
- A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.
- A UM server has been added to a UM dial plan. For detailed steps, see Add a UM Server to a Dial Plan.
- Install the UM Troubleshooting Tool. For detailed steps, see Install the Exchange 2010 UM Troubleshooting Tool.

Important:

If you will be using the UM Troubleshooting Tool in `SIPClient` mode, there are several other Office Communications Server 2007 R2 or Microsoft Lync Server 2010 requirements and prerequisites. For more information, see Checklist: Deploy Office Communications Server 2007 R2 and Exchange 2010 Unified Messaging.

Set the credentials to use with the UM Troubleshooting Tool

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

1. Open the **Microsoft Exchange 2010 UM Troubleshooting Tool** from the **Start** menu.
2. In the **Microsoft Exchange 2010 UM Troubleshooting Tool** window, at the prompt, type the following and press **Enter**.

```
$cred=Get-Credential
```

3. In the **Windows PowerShell Credential Request** window, type the domain \user name and password and then click **OK**.
4. In the **Microsoft Exchange 2010 UM Troubleshooting Tool** window, specify the necessary cmdlet parameters to test for call flow. For example:

```
Test-ExchangeUMCallFlow -Mode SIPClient -CallingParty tonysmith@contos
```

Other Tasks

After you set the credentials for the UM Troubleshooting Tool, you may also want to:

- Run the Exchange 2010 UM Troubleshooting Tool on Windows 7 or Windows Vista
- Test-UMConnectivity

1.9.4.4.4 Run the Exchange 2010 UM Troubleshooting Tool on Windows 7 or Windows Vista

Run the Exchange 2010 UM Troubleshooting Tool on Windows 7 or Windows Vista

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

The Microsoft Exchange 2010 UM Troubleshooting Tool is an Exchange Management Shell cmdlet named **Test-ExchangeUMCallFlow**. You can use the cmdlet to diagnose configuration errors specific to call answering scenarios and to test whether voice mail is functioning correctly in both on-premises and cross-premises Microsoft Exchange Server 2010 Service Pack 1 (SP1) UM deployments. You can use this cmdlet in deployments with Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010 or in UM deployments with IP gateways or IP PBXs.

Prerequisites

- Make sure your Exchange 2010 organization meets the following requirements:
  - A UM dial plan has been created. For detailed steps, see Create a UM Dial Plan.
  - A UM mailbox policy has been created. For detailed steps, see Create a UM

Mailbox Policy.
- A UM IP gateway has been created. For detailed steps, see Create a UM IP Gateway.
- A UM server has been added to a UM dial plan. For detailed steps, see Add a UM Server to a Dial Plan.

- If you're running the UM Troubleshooting Tool on a local UM server with Exchange 2010 SP1, you may not have to install all the prerequisites listed below. They may have already been installed along with the UM server role. However, if you're installing the UM Troubleshooting Tool on a 64-bit computer other than a server that is running the UM server role, you will need to install the following components:
  - Microsoft .NET Framework 3.5 Service Pack 1 (SP1) See Microsoft .NET Framework 3.5 Service Pack 1.
  - If the tool will be run on a Windows Vista or Windows Server 2008 computer See Microsoft .NET Framework 3.5 Family Update for Windows Vista x64, and Windows Server 2008 x64.
  - Windows Remote Management (WinRM) 2.0 and Windows PowerShell V2 (Windows6.0-KB968930.msu) See Microsoft Knowledge Base article 968930, Windows Management Framework Core package (Windows PowerShell 2.0 and WinRM 2.0).
  - Microsoft Unified Communications Managed API 2.0 Core Runtime (UcmaRuntimeWebDownloadX64.msi) See Unified Communications Managed API 2.0, Core Runtime (64-bit).
- Download and install the UM Troubleshooting Tool.
  - Download Unified Messaging Troubleshooting Tool from the Microsoft Download Center.
  - Install the tool. For details, see Install the Exchange 2010 UM Troubleshooting Tool.

Important:

If you will be using the UM Troubleshooting Tool in `SIPClient` mode, there are several other Office Communications Server 2007 R2 or Microsoft Lync Server 2010 requirements and prerequisites that must be met. For more information, see Checklist: Deploy Office Communications Server 2007 R2 and Exchange 2010 Unified Messaging.

Run the UM Troubleshooting Tool on Windows 7 or Windows Vista

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "UM server" entry in the Unified Messaging Permissions topic.

1. Click **Start** > **All Programs** > **Accessories** > **Windows PowerShell**.
2. Right-click **Windows PowerShell**, and from the pop-up menu select **Run as administrator**.
3. At the PowerShell command prompt, go to the folder where the UM Troubleshooting Tool was installed and run the following.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -psconsolefi
```

4. If you're running the UM Troubleshooting Tool on Windows 7, at the PowerShell command prompt, run the following:

```
Set-ExecutionPolicy RemoteSigned
```

5. Open the **Microsoft Exchange 2010 UM Troubleshooting Tool** from the **Start** menu.
6. In the **Microsoft Exchange 2010 UM Troubleshooting Tool** window, at the prompt, type the following and press Enter.

```
$cred=Get-Credential
```

7. In the **Windows PowerShell Credential Request** window, type the domain \user name and password and click **OK**.
8. In the **Microsoft Exchange 2010 UM Troubleshooting Tool** window, specify the necessary cmdlet parameters to test for call flow. For example:

```
Test-ExchangeUMCallFlow -Mode SIPClient -CallingParty tonysmith@contos
```

Other Tasks

After you set the credentials for the UM Troubleshooting Tool, you may also want to:

- Set the Credentials to Use with the Exchange 2010 UM Troubleshooting Tool
- Install the Exchange 2010 UM Troubleshooting Tool
- Test-UMConnectivity

1.9.5 Performance Counter Reference for Unified Messaging Servers

Performance Counter Reference for Unified Messaging Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Ensuring that servers running Microsoft Exchange Server 2010 are operating reliably is a key objective for messaging operations. An important part of Exchange 2010 operations is monitoring the Exchange components to understand the health state of servers and server roles. For more information about Unified Messaging performance counters, see the following topics:

- Unified Messaging Counters
- Performance and Scalability Counters and Thresholds

1.9.6 Error and Event Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-20*

Microsoft Exchange Server 2010 Unified Messaging (UM) components, features, and services generate errors and events to enable you to effectively troubleshoot and monitor a Unified Messaging server.

Event Viewer maintains logs about program, security, and system events on your computer. You can use Event Viewer to view and manage the event logs, gather information about hardware and software problems, and monitor Microsoft Windows

security events. Although Event Viewer is a Windows operating system tool and not a Microsoft Exchange tool, Event Viewer is useful when you troubleshoot problems with Exchange. This topic describes the basic concepts related to Event Viewer.

This topic also describes the events that Unified Messaging lists in Event Viewer, explains how to use them to monitor Unified Messaging, and describes the error messages that are generated by a Unified Messaging server.

Unified Messaging Errors and Events

Unified Messaging generates errors and events in Event Viewer so that you can troubleshoot and verify the performance of Unified Messaging components, features, and services. Event Viewer tracks error events, warning events, and informational events in order of importance. The logs in Event Viewer provide an audited record of all services and processes in the Windows Server 2008 operating system.

Unified Messaging errors and events are grouped into six categories that are based on core components, processes, and services of Unified Messaging. You can also filter the errors or events that have been generated by a Unified Messaging server by category. The categories for Unified Messaging error and events include the following:

- UMCallData
- UMClientAccess
- UMCore
- UMManagement
- UMService
- UMWorkerProcess

The following is a list of the different types of Unified Messaging errors and events. They are grouped according to the administrative functionality of the errors and events that are generated by a Unified Messaging server.

- Unified Messaging Administrative Errors and Events
- Unified Messaging Auto Attendant Errors and Events
- Unified Messaging Call Answering Errors and Events
- Unified Messaging Call Transfer Errors and Events
- Unified Messaging Outdialing Errors and Events
- Unified Messaging Performance Errors and Events
- Unified Messaging Prompt Publishing Errors and Events
- Unified Messaging Speech Grammar Errors and Events
- Unified Messaging Subscriber Access Errors and Events
- Unified Messaging System Errors and Events
- Unified Messaging Active Directory Errors and Events

1.9.6.1 Unified Messaging Administrative Errors and Events

Unified Messaging Administrative Errors and Events

Exchange Server 2010 > Unified Messaging > Error and Event Reference for Unified Messaging Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates administrative events

in Event Viewer so that you can troubleshoot and verify the performance of UM administrative components, features, and services. Event Viewer tracks the following kinds of events in the following order, based on importance:

1. Error events
2. Warning events
3. Informational events

UM Administrative Errors and Events

The following table provides a list of the UM administrative events that you can use to troubleshoot and monitor Unified Messaging.

Administrative events

Event ID	Category	Event type	Logging	Value or description	Class
1015	UMManagement	Information	LogAlways	User "%1" has been successfully enabled for Unified Messaging.	Administrative
1016	UMManagement	Information	LogAlways	User "%1" has been disabled for Unified Messaging.	Administrative
1017	UMManagement	Information	LogAlways	The Unified Messaging mailbox for UM-enabled user "%1" has been successfully unlocked.	Administrative
1018	UMManagement	Information	LogAlways	The Outlook Voice Access PIN for user "%1" has been changed.	Administrative
1060	UMManagement	Information	LogAlways	A new UM dial plan named "%1" was created.	Administrative
1061	UMManagement	Information	LogAlways	A new UM IP gateway named "%1" with IP address "%2" has been created.	Administrative
1062	UMManagement	Information	LogAlways	A new Unified Messaging hunt group	Administrative

				named "%1" has been created with pilot identifier "%2" and is associated with UM dial plan "%3".	
1063	UMManagement	Information	LogAlways	The dial plan named "%1" has been removed.	Administrative
1064	UMManagement	Information	LogAlways	IP gateway "%1", which has IP address "%2", has been removed.	Administrative
1065	UMManagement	Information	LogAlways	The UM hunt group "%1" with the pilot identifier "%2" that is associated with UM dial plan "%3" has been removed.	Administrative
1066	UMManagement	Information	LogAlways	Unified Messaging server "%1" has been enabled.	Administrative
1067	UMManagement	Information	LogAlways	The UM IP gateway "%1" with IP address "%2" has been enabled.	Administrative
1068	UMManagement	Information	LogAlways	The Unified Messaging server named "%1" has been disabled.	Administrative
1069	UMManagement	Information	LogAlways	The Unified Messaging IP gateway "%1" with the IP address "%2" has been disabled.	Administrative
1070	UMManageme	Information	LogAlways	A new UM	Administrative

	nt			auto attendant named "%1" was created and associated with UM dial plan "%2".	
1071	UMManagement	Information	LogAlways	The UM auto attendant named "%1" has been enabled.	Administrative
1072	UMManagement	Information	LogAlways	The auto attendant named "%1" has been disabled.	Administrative

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.2 Unified Messaging Auto Attendant Errors and Events

Unified Messaging Auto Attendant Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates UM auto attendant events in Event Viewer so that you can troubleshoot and verify the performance of the UM auto attendant components, features, and services. Event Viewer tracks the following kinds of events in the following order based on importance:

1. Error events
2. Warning events
3. Informational events

UM Auto Attendant Errors and Events

The following table provides a list of the UM auto attendant events that you can use to troubleshoot and monitor Unified Messaging.

Auto attendant events

Event ID	Category	Event type	Logging	Value or description	Class

1128	UMService	Error	LogPeriodic	No operator extension number has been configured for the UM auto attendant named "%1", or for the dial plan to which it belongs. Therefore, incoming calls received by this UM auto attendant cannot be transferred to the operator.	Auto Attendant
1129	UMService	Warning	LogAlways	The Unified Messaging auto attendant "%1" has not been configured with a valid time zone. Incoming calls answered by the UM auto attendant will be answered according to the time zone that has been configured on the Unified Messaging server that answers the call. To resolve this error, configure a valid time zone on the UM auto attendant.	Auto Attendant
1154	UMCore	Warning	LogAlways	An error occurred while adding a custom menu speech grammar entry for "%1" in auto attendant "%	Auto Attendant

				2". Details follow: "%3"	
1156	UMCore	Warning	LogAlways	Auto attendant "%1" is configured to use "%2", a language that is not supported on this Unified Messaging server. The auto attendant will use "%3", which is the default language of the associated dial plan "%4"'.	Auto Attendant
1164	UMCore	Warning	LogAlways	A call to auto attendant "%1" was not handled. "%2"	Auto Attendant
1172	UMCallData	Information	LogAlways	Call data: "%1"	Auto Attendant

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.3 Unified Messaging Call Answering Errors and Events

Unified Messaging Call Answering Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates call answering events in Event Viewer so that you can troubleshoot and verify the performance of the call answering components, features, and services. Event Viewer tracks the following kinds of events in the following order based on importance:

1. Error events
2. Warning events
3. Informational events

Call Answering Errors and Events

The following table provides a list of the call answering events that you can use to troubleshoot and monitor Unified Messaging.

Call answering events

Event ID	Category	Event type	Logging	Value or description	Class
1004	UMCore	Information	LogAlways	A call was received with the following parameters: Calling Party: "%1", Called Party: "%2", Diversion Information: "%3", Call ID "%4".	Call Answering
1006	UMCore	Information	LogAlways	The Unified Messaging server has received a call from "%1", with user extension "%2" and a call ID of "%3".	Call Answering
1021	UMCore	Warning	LogAlways	The Unified Messaging server rejected an incoming call with the ID "%1". Reason: "%2"	Call Answering
1081	UMCore	Warning	LogAlways	The Unified Messaging server failed to receive an incoming call for user "%1" during the call with ID "%2" because a Hub Transport server is currently busy or not available. To correct this error, make sure that there is at least one Hub	Call Answering

				Transport server installed in the same Active Directory site as the Unified Messaging server and that a Hub Transport server is available.	
1082	UMService	Error	LogAlways	The Unified Messaging server was unable to submit messages to a Hub Transport server because there is no Hub Transport server available to process the request with UM header file "%1". Make sure that there is a Hub Transport server located in the same Active Directory site as the UM server. In addition, make sure that the Microsoft Exchange Transport service is started on the Hub Transport server.	Call Answering
1109	UMCore	Warning	LogAlways	The Unified Messaging server has received an inbound call that has an invalid extension "%1" for UM dial plan "%2".	Call Answering

				The call ID is "%3".	
1146	UMCore	Warning	LogAlways	The Unified Messaging server was unable to resolve the caller ID "%1" to a user in Active Directory or personal contact before attempting to submit voice mail to the Hub Transport server. The recipient of the message was "%2". More information: "%3"	Call Answering
1153	UMCore	Information	LogAlways	The Unified Messaging server received an incomplete number of digits for the extension number with ID "%1". The number of digits received was %2. This does not match the number of digits that was configured on dial plan "%3", which is %4. Because the number of digits does not match the number configured on the dial plan, the Unified Messaging server will send this call to the dial	Call Answering

				plan pilot number.	
1169	UMCore	Warning	LogAlways	The user with extension "%1" is not enabled for Unified Messaging.	Call Answering
1170	UMCallData	Information	LogAlways	Call data: %1	Call Answering

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.4 Unified Messaging Call Transfer Errors and Events

Unified Messaging Call Transfer Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-24*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates call transfer events in Event Viewer so that you can troubleshoot and verify the performance of call transfers in Unified Messaging. Event Viewer tracks the following kinds of events in the following order based on importance:

1. Error events
2. Warning events
3. Informational events

Call Transfer Errors and Events

The following table provides a list of the UM call transfer events that you can use to troubleshoot and monitor Unified Messaging.

Call transfer events

Event ID	Category	Event type	Logging	Value or description	Class
1024	UMCore	Information	LogAlways	The Unified Messaging server is transferring a call from "%1", with diversion "%2", to extension number "%3". The call ID is	Call Transfer

				"%4".	
1025	UMCore	Error	LogAlways	The voice call with ID "%1" did not transfer to "%2" because: "%3"	Call Transfer
1026	UMCore	Information	LogAlways	A call was transferred successfully from "%1", with diversion information "%2", to extension number "%3". The call ID was "%4".	Call Transfer
1073	UMManagement	Information	LogAlways	The Unified Messaging server transferred a call to "%1".	Call Transfer
1136	UMCore	Warning	LogAlways	An error occurred while transferring the call to the phone number "%1". The call ID is: "%2".	Call Transfer

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.5 Unified Messaging Outdialing Errors and Events

Unified Messaging Outdialing Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates outdialing events in Event Viewer so that you can troubleshoot and verify the performance of the outdialing feature in Exchange 2010 Unified Messaging. Event Viewer tracks the following kinds of events in the following order, based on importance:

1. Error events

2.Warning events
3.Informational events

Outdialing Errors and Events

The following table provides a list of the outdialing events that you can use to troubleshoot and monitor Unified Messaging.

Outdialing events

Event ID	Category	Event type	Logging	Value or description	Class
1005	UMCore	Information	LogAlways	The Unified Messaging server is initiating an outgoing call. The calling party is "%1", the party being called is "%2", and the call ID is "%3".	Outdialing
1075	UMCore	Information	LogAlways	The Unified Messaging server received a Play on Phone request from "%1". The calling number "%2" is dialing "%3" using the IP gateway "%4".	Outdialing
1076	UMCore	Warning	LogAlways	The Unified Messaging server received a Play on Phone request from user "%1", but the telephone number "%2" cannot be dialed as specified. To correct this issue, make sure that you have properly configured the dialing rules on the UM dial plan and the dial	Outdialing

				restrictions on the UM mailbox policy that is associated with the user. Diagnostic information: "%3".	
1085	UMCore	Warning	LogAlways	The Unified Messaging server attempted to translate "%1" into a number that can be dialed. "%2". Check the following warning messages: "%3".	Outdialing
1087	UMCore	Warning	LogAlways	An outgoing call to "%1" could not be established. The selected outgoing IP gateway "%2" returned the error: "%3". The caller ID for this call was "%4". For help troubleshooting the SIP response error code that was specified in the event description, contact the vendors who support your IP gateway and IP PBX hardware. You can also run diagnostic tests on your IP gateway or IP PBX hardware to make sure that the	Outdialing

				devices are operating correctly. More information: "%5"	
1173	UMCallData	Information	LogAlways	Call data: "%1"	Outdialing

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.6 Unified Messaging Performance Errors and Events

Unified Messaging Performance Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates events related to performance in Event Viewer so that you can troubleshoot and verify the performance of UM components, features, and services. Event Viewer tracks the following types of events in the following order:

1. Error events
2. Warning events
3. Informational events

UM Performance Errors and Events

The following table provides a list of performance-related events that you can use to troubleshoot and monitor Unified Messaging.

Unified Messaging performance-related events

Event ID	Category	Event type	Logging	Value or description	Class
1054	UMService	Information	LogAlways	The Unified Messaging Worker Process was terminated because its startup time exceeded the configured maximum, %1 seconds.	Performance

1089	UMService	Warning	LogPeriodic	SIP IP gateway %1 did not respond within %2 seconds to the Session Initiation Protocol (SIP) option request that was sent by the Unified Messaging server. Make sure that the IP gateway has no performance bottleneck. Also, make sure that there are no network connectivity issues between the IP gateway and the Unified Messaging server.	Performance

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.7 Unified Messaging Prompt Publishing Errors and Events

Unified Messaging Prompt Publishing Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates prompt publishing events in Event Viewer so that you can troubleshoot and verify the performance of the prompt publishing feature in Exchange 2010 Unified Messaging. Event Viewer tracks the following kinds of events in the following order based on importance:

1. Error events
2. Warning events
3. Informational events

Prompt Publishing Errors and Events

The following table provides a list of the prompt publishing events that you can use to troubleshoot and monitor Unified Messaging.

Prompt publishing events

Event ID	Category	Event type	Logging	Value or description	Class
1094	UMManagement	Information	LogAlways	The user "%1" modified a custom prompt for UM dial plan "%2". The custom prompt file name is "%3" and the custom prompt publishing point is "%4".	Prompt Publishing
1095	UMManagement	Warning	LogAlways	User "%1" attempted to modify a custom prompt for dial plan "%2". The operation failed. Make sure that the UM administrator is a member of the local Administrators group, has been delegated the Exchange Organization Administrator role, and has at least read and write permissions to the UM prompt publishing point shared folder. More information: "%3"	Prompt Publishing
1096	UMCore	Information	LogAlways	The Unified Messaging server updated the	Prompt Publishing

				custom prompt cache for UM dial plan "%1". The name of the file that was updated is "%2".	
1097	UMManagement	Warning	LogAlways	The custom prompts that are associated with UM dial plan "%1" could not be removed. More information: %2	Prompt Publishing
1098	UMManagement	Information	LogAlways	User "%1" has modified a custom prompt for UM auto attendant "%2". The custom prompt file name was "%3" and the custom prompt publishing point was "%4".	Prompt Publishing
1099	UMManagement	Warning	LogAlways	User "%1" attempted to modify a custom prompt for auto attendant "%2". The operation failed. Make sure that the UM administrator is a member of the local Administrators group and has been delegated the Exchange Organization Administrator	Prompt Publishing

				role, and has at least read and write permissions to the UM prompt publishing point shared folder. More information: "%3"	
1100	UMCore	Information	LogAlways	The Unified Messaging server updated the custom prompt cache for UM auto attendant "%1". The name of the file that was updated is "%2".	Prompt Publishing
1101	UMManagement	Warning	LogAlways	The Unified Messaging server could not delete the custom prompt files associated with UM auto attendant "%1" from the prompt publishing point. No user action is required. To avoid this warning being logged in the future, make sure that the appropriate permissions have been configured on the prompt publishing point shared folder. More information: "%2".	Prompt Publishing
1160	UMCore	Warning	LogPeriodic	The Unified Messaging server could not find a local	Prompt Publishing

				copy of the following custom prompt files for UM auto attendant "%1": "%2". If these custom prompt files were added recently, you must allow time for prompt distribution.	
1161	UMCore	Warning	LogPeriodic	The following custom prompt files were not found for UM dial plan "%1": "%2". If new custom prompt files were published recently, you must allow time for them to be copied to all Unified Messaging servers in the dial plan.	Prompt Publishing

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.8 Unified Messaging Speech Grammar Errors and Events

Unified Messaging Speech Grammar Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates speech grammar generation events in Event Viewer so that you can troubleshoot and verify the performance of speech grammar generation in Exchange 2010 Unified Messaging. Event Viewer tracks the following kinds of events in the following order based on importance:

1. Error events
2. Warning events
3. Informational events

Speech Grammar Errors and Events

The following table provides a list of the speech grammar events that you can use to troubleshoot and monitor Unified Messaging.

Speech grammar events

Event ID	Category	Event type	Logging	Value or description	Class
1086	UMCore	Warning	LogAlways	Automatic Speech Recognition (ASR) has been enabled on the UM auto attendant "%1". However, the speech grammar file "%2" cannot be found. Until this problem is corrected, ASR will be disabled for this auto attendant.	Speech Grammar
1102	UMCore	Warning	LogAlways	Automatic Speech Recognition (ASR) has been enabled for personal contacts, but the speech grammar file "%1" for personal contacts cannot be found. Until this problem is corrected, ASR will be disabled for contacts.	Speech Grammar
1130	UMCore	Warning	LogAlways	The Unified Messaging server encountered an error when generating or updating a	Speech Grammar

				grammar file. Error details: "%1"	
1131	UMWorkerProcess	Information	LogAlways	The Unified Messaging Worker Process has started grammar generation for Automatic Speech Recognition. The log file is "%1".	Speech Grammar
1132	UMWorkerProcess	Information	LogAlways	The Unified Messaging Worker Process has completed the scheduled speech grammar generation.	Speech Grammar
1137	UMCore	Warning	LogAlways	The Microsoft Exchange Unified Messaging service or the galgrammargenerator.exe command failed to update the msExchUMDtmfMap Active Directory attribute for UM-enabled recipients. More information: "%1"	Speech Grammar
1139	UMCore	Information	LogAlways	The speech grammar generation log file will be written to"'%1".	Speech Grammar
1140	UMCore	Information	LogAlways	"%1". The grammar file is named "%2".	Speech Grammar
1141	UMCore	Information	LogAlways	The Unified Messaging	Speech Grammar

				server has created a grammar file named "%1". The grammar file was then compiled into a file named "%2".	
1157	UMCore	Warning	LogAlways	The Unified Messaging server encountered an error in the speech grammar filter list at line "%1", character "%2". The error is "%3". Generation of the speech grammar files on the Unified Messaging server has been canceled.	Speech Grammar
1158	UMCore	Warning	LogAlways	The Unified Messaging server encountered an error while processing the speech grammar filter list that is used for Automatic Speech Recognition (ASR). Generation of the speech grammar files on the Unified Messaging server has been canceled. "%1"	Speech Grammar
1162	UMWorkerProcess	Information	LogAlways	The following dial plans were added to the server: "%1","%2". The	Speech Grammar

				Unified Messaging Worker Process has started grammar generation for these dial plans.	
1163	UMWorkerProcess	Information	LogAlways	The Unified Messaging Worker Process has finished updating the speech grammar files for UM dial plans that are associated with the Unified Messaging server.	Speech Grammar

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.9 Unified Messaging Subscriber Access Errors and Events

Unified Messaging Subscriber Access Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates subscriber access events in Event Viewer so that you can troubleshoot and verify the performance of the subscriber access components and services. Event Viewer tracks the following kinds of events in the following order based on importance:

1. Error events
2. Warning events
3. Informational events

Subscriber Access Errors and Events

The following table provides a list of the subscriber access events that you can use to troubleshoot and monitor Unified Messaging.

Subscriber access events

Event ID	Category	Event type	Logging	Value or description	Class
1012	UMCore	Warning	LogAlways	User "%1" is locked out of their mailbox because they have entered an incorrect PIN "%2" consecutive times. The PIN must be reset before the user can log on to the mailbox from the telephone again.	Subscriber Access
1013	UMCore	Warning	LogAlways	User "%1" was disconnected by the Unified Messaging server because the user failed to log on "%2" consecutive times. The user did not enter the correct PIN.	Subscriber Access
1019	UMCore	Warning	LogAlways	User "%1" was unable to log on to their mailbox using Outlook Voice Access because the checksum for the user's PIN is not valid. The user will not be able to log on to the system until their PIN is reset.	Subscriber Access
1036	UMCore	Information	LogAlways	The Unified Messaging server successfully authenticated user "%1".	Subscriber Access

				The call ID is "%2".	
1080	UMCore	Warning	LogAlways	The Unified Messaging (UM) server failed to process messages for user "%1" during the call with ID "%2" because the user has exceeded their mailbox quota.	Subscriber Access
1134	UMCore	Warning	LogAlways	The Unified Messaging server detected corrupt user configuration data for user "%1". This data contains information such as whether the user has previously logged on to their mailbox or has set their Out of Office status, and also contains any personalized voice mail greetings the user has recorded. The Unified Messaging server will use default configuration data for the user.	Subscriber Access
1135	UMCore	Error	LogAlways	The Microsoft Exchange Unified Messaging service detected a corrupted PIN	Subscriber Access

				for user "%1". The user's UM configuration data contains information such as the user's current PIN and the number of consecutive times the user has entered an incorrect PIN. The user will not be able to log on to the Unified Messaging system until their PIN is reset.	
1171	UMCallData	Information	LogAlways	Call data: "%1"	Subscriber Access

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.10 Unified Messaging System Errors and Events

Unified Messaging System Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-06-20*

Microsoft Exchange Server 2010 Unified Messaging generates system events in Event Viewer so that you can troubleshoot and verify the performance of Unified Messaging system components, features, and services. Event Viewer tracks the following kinds of events in the following order based on importance:

1. Error events
2. Warning events
3. Informational events

UM System Error and Events

The following table provides a list of Unified Messaging system events that you can use to troubleshoot and monitor Unified Messaging.

Unified Messaging system events

Event ID	Category	Event type	Logging	Value or description	Class
1000	UMWorkerProcess	Information	LogAlways	The Unified Messaging Worker Process was started successfully on port "%1".	System
1001	UMWorkerProcess	Error	LogAlways	The Microsoft Exchange Unified Messaging Worker Process (UMWorkerProcess.exe) was unable to start. More information: %1.	System
1002	UMWorkerProcess	Information	LogAlways	The Unified Messaging Worker Process has been stopped successfully.	System
1003	UMWorkerProcess	Error	LogAlways	An unhandled exception occurred while the UM Worker Process (UMWorkerProcess.exe) was stopping. Exception details follow: %1	System
1007	UMCore	Information	LogAlways	The Unified Messaging server has ended a call with ID "%1" because the user at the far end disconnected.	System
1008	UMCore	Error	LogAlways	The Microsoft Exchange Unified Messaging service failed to initialize because an	System

				exception occurred when it was loading the globcfg.xml configuration file or the finite state machine (FSM) files. To resolve this error, replace the globcfg.xml file or the FSM files with the default files located on the Exchange Server 2010 DVD. More information: "%1".	
1009	UMCore	Information	LogAlways	The telephone user interface is starting activity "%1" for the call with ID "%2".	System
1010	UMCore	Information	LogAlways	The telephone user interface definitions were successfully loaded from the configuration file: "%1"	System
1011	UMCore	Information	LogAlways	The telephone user interface activity "%1" will play the following prompts: "%2"	System
1014	UMCore	Error	LogAlways	The Unified Messaging Worker Process (UMWorkerProcess.exe) encountered an unhandled exception "%1" during an incoming call	System

				with ID "%2". The call was disconnected.	
1035	UMCore	Error	LogAlways	The Unified Messaging server encountered an error when trying to access the mailbox for user "%1". Error: %2 Object: %3	System
1037	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has started successfully.	System
1038	UMService	Error	LogAlways	The Microsoft Exchange Unified Messaging service was unable to start. More information: "%1"	System
1039	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has been stopped successfully.	System
1040	UMService	Error	LogAlways	The Microsoft Exchange Unified Messaging service could not be stopped. More information: "%1"	System
1041	UMService	Error	LogAlways	The operating system was unable to create job object "%1" during the initialization of the Microsoft	System

				Exchange Unified Messaging service. Job objects allow multiple processes to be managed as a unit. The Microsoft Exchange Unified Messaging service was stopped. To resolve this error, first try restarting the Unified Messaging server. The Win32 exception error that was returned was: "%2"	
1042	UMService	Error	LogAlways	The operating system was unable to set properties on job object "%1" during the initialization of the Microsoft Exchange Unified Messaging service. A job object allows a group of processes to be managed as a unit. The Microsoft Exchange Unified Messaging service was stopped. To resolve this error, first try restarting the Unified Messaging server. The Win32 exception error that was	System

				returned was: "%2"	
1043	UMService	Error	LogAlways	The Microsoft Exchange Unified Messaging service was not able to start because the executable file "%1" for the Unified Messaging Worker Process does not exist. To resolve this issue, copy the default file located on the Exchange Server 2010 DVD into the \bin folder in the installation directory.	System
1044	UMService	Error	LogAlways	The Microsoft Exchange Unified Messaging service failed to create an instance of the Unified Messaging Worker Process. %1	System
1045	UMService	Error	LogAlways	The Microsoft Exchange Unified Messaging service stopped because the Unified Messaging Worker Process exceeded the configured maximum number of consecutive crashes, %1.	System

				To resolve this error, restart the Microsoft Exchange Unified Messaging service.	
1046	UMService	Information	LogAlways	The Unified Messaging (UM) Worker Process has terminated. The state of the UM Worker Process is "%1".	System
1047	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has requested that a new Unified Messaging Worker Process be created.	System
1048	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has created a new Unified Messaging (UM) Worker Process because it was unable to get data from the old UM Worker Process.	System
1049	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has created a new Unified Messaging Worker Process because the	System

				number of incoming calls ("%1") has exceeded the configured maximum, "%2".	
1050	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has created a new Unified Messaging Worker Process because the number of threads ("%1") exceeded the configured maximum, "%2".	System
1051	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has created a new Unified Messaging Worker Process because the working set ("%1 MB") has exceeded the configured maximum: "%2 MB"	System
1052	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has created a new Unified Messaging Worker Process. The previous Worker Process had been running since "%1",	System

				and reached its configured maximum age at "%2".	
1053	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has created a new Unified Messaging Worker Process because the number of health monitoring "heartbeats" missed ("%1") exceeded the configured maximum, "%2".	System
1055	UMService	Information	LogAlways	The Unified Messaging Worker Process was terminated because the configured maximum lifetime was exceeded.	System
1056	UMService	Information	LogAlways	The state of the Unified Messaging Worker Process has changed. Previous state = "%1". Current state = "%2".	System
1057	UMWorkerProcess	Error	LogAlways	An unhandled exception occurred in a Unified Messaging Worker Process: "%1".	System
1058	UMService	Error	LogAlways	The Microsoft Exchange Unified	System

				Messaging service was not able to redirect the call with ID "%1" to an available Unified Messaging Worker Process.	
1059	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has terminated the Unified Messaging Worker Process because a control channel could not be established.	System
1074	UMService	Error	LogAlways	The Unified Messaging server failed to submit the message to the Hub Transport server using header file "%1". The header file was moved to "%2". Make sure that your antivirus software is not modifying the header files in the voice mail folder. Error "%3".	System
1077	UMCore	Information	LogAlways	The Unified Messaging server has received a request to disconnect the user "%1" on the call with	System

				ID "%2".	
1078	UMCore	Warning	LogAlways	The Unified Messaging Worker Process is attempting to recover from an exception "%1" that was encountered during a call with ID "%2".	System
1079	UMCore	Warning	LogAlways	The VoIP platform encountered an exception "%1" during the call with ID "%2". This exception occurred at the Microsoft Exchange Speech Engine VoIP platform during an event-based asynchronous operation submitted by the Unified Messaging server. The Unified Messaging server will attempt to recover from this exception. If this warning occurs frequently, contact Microsoft Product Support.	System
1083	UMClientAccess	Warning	LogAlways	The Unified Messaging Web service was unable to process a "%1" request for user "%2". The error was "%3".	System
1084	UMCore	Information	LogAlways	The call with	System

				ID "%1" ended because the Unified Messaging server disconnected.	
1090	UMService	Information	LogAlways	The IP gateway at %1 responded promptly to a PING request.	System
1091	UMService	Warning	LogAlways	The Unified Messaging server was unable to issue a Session Initiation Protocol (SIP) Option request to the IP gateway or IP PBX named "%1". The operational status of the IP gateway or IP PBX will not be sent to the server. The error received was "%2".	System
1092	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has created a new Unified Messaging Worker Process because the temporary directory size reached "%1" MB, which exceeded the maximum specified size, which is "%2" MB.	System
1103	UMService	Error	LogAlways	XML schema validation failed for file	System

				"%1" at line "%2". The error was "%3". A Unified Messaging configuration data file has been modified and the new changes do not match the expected schema. To resolve this issue, undo any recent changes you have made to the file or replace the file on the Unified Messaging server with the file of the same name located on the Exchange 2010 DVD.	
1104	UMService	Warning	LogAlways	The Microsoft Exchange Unified Messaging service was unable to read the Unified Messaging Worker Process retire time from the configuration data. The Unified Messaging Worker Process retire time is being set to the default value, which is "%1". Reason: "%2"	System
1105	UMWorkerProcess	Warning	LogAlways	The Unified Messaging server could not find a UM IP gateway that allows outgoing calls.	System

1112	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service will attempt to use a certificate with the following details: IssuerName = "%1", SerialNumber = "%2", Thumbprint = "%3", IsSelfSigned = "%4", NotValidAfter = "%5". The path to this certificate is "%6".	System
1113	UMService	Warning	LogPeriodic	The Unified Messaging server failed to exchange the required certificates with a UM IP gateway to enable Transport Layer Security (TLS) for an incoming call. More information: "%1".	System
1114	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service will attempt to start in secured mode.	System
1115	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service will attempt to start in unsecured mode.	System

1116	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service has received notification that a new Transport Layer Security (TLS) certificate must be used. The Microsoft Exchange Unified Messaging service will not process any new calls from an IP gateway until the new TLS certificate can be used.	System
1117	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service was configured to use a new certificate and used the new certificate successfully.	System
1118	UMService	Error	LogAlways	The Microsoft Exchange Unified Messaging service has encountered a problem trying to use the newly assigned certificate for Transport Layer Security (TLS). The Microsoft Exchange Unified Messaging service was stopped. To resolve this issue, replace	System

				the current certificate with another one. The exception error was "% 1".	
1119	UMService	Information	LogAlways	The Microsoft Exchange Unified Messaging service created a new Unified Messaging Worker Process so that a new certificate can be used.	System
1120	UMService	Warning	LogAlways	The certificate that is used to establish secure communication with an IP gateway using Transport Layer Security (TLS) is nearing its expiration date. By default, this event is first logged 30 days before the certificate expires, and then logged one time each day until the certificate is replaced. If the certificate that is stored on the Unified Messaging server is not replaced before it expires, the Microsoft Exchange Unified Messaging service will stop, and the	System

				Unified Messaging server will not be able to process any calls. To resolve this issue, install a new certificate on the Unified Messaging server and the IP gateways that are being used by the Unified Messaging server.	
1124	UMService	Warning	LogAlways	No IP gateways were found for the Microsoft Exchange Unified Messaging service.	System
1125	UMClientAccess	Information	LogAlways	The Microsoft Exchange Unified Messaging service will attempt to use a certificate with the following information: IssuerName = "%1", SerialNumber = "%2", Thumbprint = "%3", IsSelfSigned = "%4" , NotValidAfter = "%5"	System
1126	UMWorkerProcess	Warning	LogPeriodic	The Unified Messaging server failed to exchange the required certificates to enable Transport Layer Security (TLS) with an	System

				IP gateway. More information: "%1".	
1127	UMWorkerProcess	Warning	LogAlways	The Audio Compression Manager failed to convert from the audio format "%1" to audio format "%2": "%3". If this conversion continues to fail, you can either change the audio codec setting on the UM dial plan or change the audio codec setting on the user's UM-enabled mailbox.	System
1133	UMCore	Error	LogAlways	Unified Messaging detected a corrupted custom greeting "%1" for user "%2". The user's custom greeting will be deleted and the Unified Messaging server will use a default greeting until the user records another custom greeting.	System
1138	UMCore	Error	LogAlways	The Microsoft Exchange Unified Messaging service failed to start. The service was	System

				not able to create and register the Simple Mail Transfer Protocol (SMTP) service principal name (SPN) for the Unified Messaging server. The Win32 error code returned was "%1".	
1142	UMCore	Information	LogAlways	"%1" active calls that were associated with remote end point "% 2" were disconnected. An administrator with the appropriate permissions chose to disable all incoming calls immediately on Unified Messaging server "%3".	System
1143	UMCore	Information	LogAlways	"%1" active calls have been disabled on the Unified Messaging server. An administrator with the appropriate permissions chose to disable all incoming calls immediately.	System
1147	UMCore	Warning	LogAlways	The Unified Messaging server was unable to retrieve the IP address for IP gateway "% 1".	System

1148	UMService	Warning	LogAlways	The Unified Messaging server could not obtain a DNS record for the following hosts: "%1". Verify that your UM IP gateway and DNS server have been configured correctly.	System
1149	UMWorkerProcess	Warning	LogAlways	The Unified Messaging server could not locate a DNS record for the following hosts: "%1". To resolve this issue, verify that your UM IP gateways and your DNS server are configured correctly.	System
1151	UMService	Warning	LogPeriodic	The Session Initiation Protocol (SIP) stack that is installed on the Unified Messaging server has encountered an unhandled exception. More information: "%1".	System
1152	UMCore	Warning	LogAlways	The Unified Messaging server has received a SIP header that is not valid from an incoming call with ID "%1". Header details follow: "%2"	System
1159	UMCore	Warning	LogAlways	The call with ID "%1" was	System

				disconnected by the Unified Messaging server because of a system error.	
1165	UMWorkerProcess	Warning	LogAlways	No IP gateways were found for the Microsoft Exchange Unified Messaging service.	System
1166	UMWorkerProcess	Warning	LogAlways	The Unified Messaging server encountered an error while trying to access the Active Directory directory service to determine the UM IP gateways that are associated with this server. More information: "%1"	System
1167	UMService	Warning	LogAlways	The Unified Messaging server encountered an error while trying to access the Active Directory directory service to determine the UM IP gateways that are associated with this server. More information: "%1"	System
1168	UMCallData	Information	LogAlways	Call data: %1	System
1174	UMWorkerProcess	Warning	LogAlways	An error occurred while	System

				the Unified Messaging server was performing the following operation: "%1" for user "%2". "%3"	
1175	UMCore	Warning	LogAlways	The UM IP gateways "%1" and "%2" cannot be configured with the same IP address. Check your UM IP gateway and DNS server configuration.	System
1176	UMCore	Warning	LogAlways	UM dial plan "%2" does not include the following dial groups "%1".	System
1400	UMService	Warning	LogPeriodic	The IP gateway or IP PBX did not respond to a PING request from the Unified Messaging server. The error code that was returned is "%2" and the error text is "%3".	System

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.11 Unified Messaging Active Directory Errors and Events

Unified Messaging Active Directory Errors and Events

Exchange Server 2010 > Unified Messaging > Error and Event Reference for Unified Messaging Servers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates Active Directory errors and events in Event Viewer so that you can troubleshoot and verify the performance when an Exchange 2010 Unified Messaging server accesses the Active Directory directory service. Event Viewer tracks the following kinds of events in the following order based on importance:

1. Error events
2. Warning events
3. Informational events

Active Directory System Errors and Events

The following table provides a list of Active Directory events that you can use to troubleshoot and monitor Unified Messaging.

Active Directory system events

Event ID	Category	Event type	Logging	Value or description	Class
1020	UMCore	Information	LogAlways	Directory search key "%1" returned the following results: "%2".	Active Directory
1106	UMWorkerProcess	Warning	LogAlways	The Unified Messaging server encountered an error while trying to access Active Directory in the call with ID "%1". "%2"	Active Directory
1107	UMWorkerProcess	Warning	LogAlways	The Unified Messaging server encountered an error during the call with ID "%1" while trying to read from Active Directory. The operation cannot be retried. Additional information: "%2"	Active Directory
1108	UMWorkerProcess	Warning	LogAlways	The Unified Messaging	Active Directory

				server encountered a data error while trying to read information stored in Active Directory during the call with ID: "%1". This event may have been caused because the UM configuration data that is stored in Active Directory is internally inconsistent. Additional information follows: "%2"	
1110	UMCore	Warning	LogAlways	The Unified Messaging server failed to register for directory change notifications on the UM DialPlan container. The Unified Messaging server will retry this operation after "%1" minutes. Additional information: "%2"	Active Directory
1111	UMCore	Warning	LogAlways	The Unified Messaging server failed to register for directory change notifications on the UM IPGateway container. The Unified	Active Directory

				Messaging server will retry this operation after "%1" minutes. Additional information: "%2"	
1121	UMCore	Warning	LogAlways	The Unified Messaging server failed to register for directory change notifications on the Servers container. The Unified Messaging server will retry this operation after "%1" minutes. Additional information: "%2"	Active Directory
1122	UMCore	Warning	LogAlways	The Unified Messaging server failed to register for directory change notifications on the UM AutoAttendant container. The Unified Messaging server will retry this operation after "%1" minutes. Additional information: "%2"	Active Directory
1144	UMCore	Warning	LogAlways	An unhandled exception occurred while an Active Directory configuration change notification	Active Directory

				was being processed. This error may have been caused by network connectivity issues between Active Directory domain controllers and the Unified Messaging server. Additional information: "%1"	
1145	UMCore	Warning	LogAlways	The Unified Messaging server failed to register for directory change notifications on the UM HuntGroup container. The Unified Messaging server will retry this operation after "%1" minutes. Additional information: "%2"	Active Directory
1155	UMCore	Error	LogAlways	The Active Directory directory service failed to initialize. Additional information: "%1"	Active Directory

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.9.6.12 Unified Messaging Fax Answering Errors and Events

Unified Messaging Fax Answering Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-23*

Microsoft Exchange Server 2010 Unified Messaging (UM) generates fax answering events in Event Viewer so that you can troubleshoot and verify the performance of the Unified Messaging fax answering components, features, and services. Event Viewer tracks the following kinds of events in the following order based on importance:

1. Error events
2. Warning events
3. Informational events

Fax Answering Errors and Events

The following table provides a list of the fax answering events that you can use to troubleshoot and monitor Unified Messaging.

Fax answering events

Event ID	Category	Event type	Logging	Value or description	Class
1022	UMCore	Information	LogAlways	The Microsoft Exchange Unified Messaging service has received a fax call with ID "%1".	Fax
1023	UMCore	Information	LogAlways	The fax call with ID "%1" ended for the following reason: "%2"	Fax
1027	UMCore	Information	LogAlways	The Unified Messaging server has successfully received a fax from "%1" for "%2" at extension number "%3". The fax contains %4 pages. The fax call was %5 seconds long. The call was received from IP gateway	Fax

				"%6".	
1028	UMCore	Information	LogAlways	The fax call from "%1" for "%2" at number "%3" was received but no pages were received. The fax call was %4 seconds long. The fax call was received from UM IP gateway "%5".	Fax
1029	UMCore	Information	LogAlways	A fax call from "%1" for "%2" at number "%3" failed to complete. The fax contained %4 pages. The fax call was %5 seconds long. The call was received from UM IP gateway "%6".	Fax
1030	UMCore	Information	LogAlways	The Unified Messaging server has received both fax and audio media from "%1" for "%2" at number "%3". The fax contains %4 pages. The fax call was %5 seconds long. The call came through IP gateway "%6".	Fax
1031	UMCore	Warning	LogAlways	The fax call has exceeded the configured time for a call. The call was made from %1 for %2 at number %3.	Fax

				The fax contains %4 pages. The fax call was %5 seconds long. The call came through gateway %6.	
1032	UMCore	Warning	LogAlways	The UM dial plan that is associated with the Unified Messaging server is not configured to receive fax messages or the maximum number of concurrent fax calls on the Unified Messaging server is set to 0. The fax message that originated from telephone number "%1" and was destined for user "%2" at extension "%3" was terminated. To resolve this issue, use the Exchange Management Console or the Set-UMDialPlan cmdlet to enable the dial plan to receive incoming faxes or increase the maximum number of concurrent fax calls that can be accepted by the Unified Messaging server.	Fax

1033	UMCore	Warning	LogAlways	The Unified Messaging-enabled user "%1" is not configured to receive fax messages. The fax message that originated from phone number "%2", destined for extension "%3", was terminated. To resolve this issue, use the Exchange Management Console or the **Set-UMMailbox** cmdlet to enable the user to receive incoming fax messages.	Fax
1034	UMCore	Warning	LogAlways	The number of fax calls currently connected to the Unified Messaging server has exceeded the maximum number (%1) that is allowed. The fax call that originated from telephone number "%3" for user "%3" at extension "%4" was disconnected. To resolve this warning, increase the maximum number of concurrent fax connections that the	Fax

				Unified Messaging server will accept or install another Unified Messaging server to accept incoming fax calls.	
1150	UMCore	Warning	LogAlways	The Unified Messaging server was unable to create a message for the fax call with ID "%1". The following invalid media details were received in the session description: "%2".	Fax

For More Information

Performance Counter Reference for Unified Messaging Servers

Error and Event Reference for Unified Messaging Servers

1.10 High Availability and Site Resilience

High Availability and Site Resilience

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-08*

You can use high availability and site resilience to design, build, and operate a highly available messaging solution based on Microsoft Exchange Server 2010. You can design and deploy a configuration that enables site resilience, and use procedures related to the various backup, restore, and recovery operations supported by Exchange 2010.

Use the following links to access the information you need about high availability, disaster recovery, and site resilience.

Understanding High Availability and Site Resilience

Refer to this section for an overview of the architectural changes and new features in Exchange 2010 that enable high availability and site resilience. Learn about definitions for key terms, details of changes to high availability over previous versions of

Exchange, and key characteristics of the Exchange 2010 solution. Use links to learn about specific features, such as database availability groups (DAGs), mailbox database copies, Active Manager, shadow redundancy, online move mailbox, the third-party replication API, and more. This topic complements the guidance in Understanding Database Availability Groups, Understanding Mailbox Database Copies, and Understanding Active Manager.

Database Availability Group Design Examples

Review design examples for DAGs in a variety of environments:

- A two-member DAG, which is suited for small office and branch office deployments.
- A four-member DAG that provides high availability within a single datacenter by locating all members in the same datacenter.
- A four-member DAG that provides high availability within a single datacenter, and site resilience for that datacenter, by locating two of the members in the primary datacenter and two of the members in a second datacenter.

Planning for High Availability and Site Resilience

Get Microsoft guidance for planning high availability for Exchange 2010. Learn about the general hardware, software, and network requirements for Exchange 2010 high availability, and learn about best practices for planning DAGs and mailbox database copies. Get details about the requirements for site resilience and guidance for planning site resilience.

Deploying High Availability and Site Resilience

Get guidance and use links to detailed instructions for deploying Exchange 2010 high availability and site resilience using DAGs and mailbox database copies. Refer to this section for an overview of the deployment process, and use the links for performing each procedure. Get an example of deployment from start to finish of a four-member DAG extended across two datacenters.

Managing High Availability and Site Resilience

Use links to detailed procedures for managing Exchange 2010 high availability and site resilience. Get details about how to create a DAG, manage DAG membership, create and configure DAG networks, shut down DAG members, create and configure mailbox database copies, manage mailbox database copies, and perform database and server switchovers.

Managing Database Availability Groups

Refer to this section for an overview of the various management tasks associated with DAGs, and use links to detailed procedures for performing those tasks. These tasks include creating DAGs, managing DAG membership, configuring DAG properties, configuring DAG networks, and shutting down DAG members.

Managing Mailbox Database Copies

Refer to this section for an overview of the various management tasks associated with mailbox database copies, and use links to detailed procedures for performing those tasks. These tasks include suspending and resuming mailbox database copies, and performing database switchovers.

Switchovers and Failovers

Refer to this section for an overview of datacenter switchovers and server switchovers, and use the links to detailed procedures for performing those tasks.

Understanding Backup, Restore and Disaster Recovery

Refer to this section for an overview of backup, restore, and disaster recovery procedures, and use the links to detailed procedures for performing those tasks. Learn about supported backup technologies, server recovery, database portability, dial tone

portability, using the recovery database, and implementing flexible mailbox protection.

Using Windows Server Backup to Back Up and Restore Exchange Data

Refer to this section for an overview of the backup integration with Windows Server Backup, and use the links to detailed procedures for performing backups and restores using Windows Server Backup.

Recovery Databases

Refer to this section for an overview of the recovery database, as well as usage scenarios for a recovery database. Use the links to detailed procedures for creating a recovery database and restoring data using a recovery database.

Database Portability

Refer to this section for an overview of database portability, and use a link to a detailed procedure for using database portability.

Dial Tone Portability

Refer to this section for an overview of dial tone portability, and use the links to detailed procedures for using dial tone portability.

1.10.1 Understanding High Availability and Site Resilience

Understanding High Availability and Site Resilience

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-01-24*

Mailbox databases and the data they contain are one of the most critical components (perhaps the most critical component) of any Exchange organization. In Microsoft Exchange Server 2010, you can protect mailbox databases and the data they contain by configuring your mailbox databases for high availability and site resilience. Exchange 2010 reduces the cost and complexity of deploying a highly available and site resilient messaging solution while providing higher levels of end-to-end availability and supporting large mailboxes. Building on the native replication capabilities introduced in Exchange Server 2007, the new high availability architecture in Exchange 2010 provides a simplified, unified framework for high availability and site resilience. Exchange 2010 integrates high availability into the core architecture of Exchange, enabling customers of all sizes and in all segments to economically deploy a messaging continuity service in their organization.

Looking for management tasks related to high availability and site resilience? Check out Managing High Availability and Site Resilience.

Contents

Key Terminology

The following terms apply:

Address Book service
: A service on the Client Access server that provides a directory access endpoint for Microsoft Outlook clients.

Continuous replication - block mode
: A new form of continuous replication in SP1 whereby as each update is written to the active database copy's active log buffer, it's also shipped to a log buffer on each of the passive mailbox copies. When the log buffer is full, each database copy builds, inspects and creates the next log file in the generation sequence.

Continuous replication - file mode
: The name for the original form of continuous replication in the release to manufacturing (RTM) version of Exchange 2010, whereby closed transaction log files are pushed from the active database copy to one or more passive database copies.

Database availability group (DAG)
: A group of up to 16 Exchange 2010 Mailbox servers that hosts a set of replicated databases.

Database mobility
: The ability of a single Exchange 2010 mailbox database to be replicated to and mounted on other Exchange 2010 Mailbox servers.

Datacenter
: An Active Directory site.

Disaster recovery
: Any process used to manually recover from a failure. This can be a failure that affects a single item, or it can be a failure that affects an entire physical location.

Exchange third-party replication API
: An Exchange-provided API that enables use of third-party synchronous replication for a database availability group instead of continuous replication.

High availability
: A solution that provides service availability, data availability, and automatic recovery from failures that affect the service or data (such as a network, storage, or server failure).

Incremental deployment
: The ability to deploy high availability and site resilience after Exchange 2010 is installed.

Lagged mailbox database copy
: A passive mailbox database copy that has a log replay lag time greater than zero.

Mailbox database copy
: A mailbox database (.edb file and logs), which is either active or passive.

Mailbox resiliency

The name of a unified high availability and site resilience solution in Exchange 2010.

RPC Client Access service

A service on the Client Access server that provides a MAPI endpoint for Microsoft Outlook clients.

Site resilience

A manual disaster recovery process used to activate an alternate or standby datacenter when the primary datacenter is no longer able to provide a sufficient level of service to meet the needs of the organization. Also includes the process of re-activating a primary datacenter that has been recovered, restored or recreated. You can configure your messaging solution for high availability and enable site resilience using the built-in features and functionality in Exchange 2010.

Shadow redundancy

A transport server feature that provides redundancy for messages for the entire time they are in transit.

**over* (pronounced "star over")

Short for *switchovers* and *failovers*. A switchover is a manual activation of one or more database copies. A failover is an automatic activation of one or more database copies after a failure.

Return to top

Key Characteristics of the Exchange Server 2010 Solution

Exchange 2007 decreased the costs of high availability and made site resilience more economical by introducing technologies such as cluster continuous replication (CCR) and standby continuous replication (SCR). However, some challenges remained:

- Windows failover clustering could be confusing because of its complexity.
- Achieving a high level of uptime could require a high level of administrator intervention.
- Each type of continuous replication was managed differently and separately.
- Recovering from a failure of a single database on a large Mailbox server could result in a temporary disruption of service to all users on the Mailbox server.
- The transport dumpster feature of the Hub Transport server could only protect messages destined for mailboxes in a CCR environment. If a Hub Transport server fails while processing messages and can't be recovered, it could result in data loss.

Exchange 2010 includes significant core changes that integrate high availability in the architecture, making it less costly and easier to deploy and maintain than previous versions of Exchange. Exchange 2010 includes a new unified platform for both high availability and site resilience.

With the significant core improvements made to Exchange 2010, the recommended maximum mailbox database size when using continuous replication has increased from 200 gigabytes (GB) in Exchange 2007 to 2 terabytes in Exchange 2010. With more companies realizing the greater value in large mailboxes (from 2 GB through 10 GB), significantly larger database sizes can quickly become a reality. Supporting larger databases means moving away from legacy recovery mechanisms, such as backup and restore, and moving to newer, faster forms of protection, such as data replication and server redundancy. Ultimately, the size of your mailbox databases depends on many factors you derive during the Exchange 2010 planning process for. For detailed planning guidance for mailboxes and Mailbox servers, see Mailbox Server Storage Design.

Exchange 2010 combines the key availability and resilience features of CCR and SCR into a single solution that handles both on-site and off-site data replication. Mailbox servers

can be defined as part of a DAG to provide automatic recovery at the mailbox database level instead of at the server level. Other new high availability concepts are introduced in Exchange 2010, such as *database mobility* and *incremental deployment*.

Return to top

Database Mobility

Exchange 2007 introduced many architectural changes designed to make deploying high availability and site resiliency solutions for Exchange faster and simpler. These improvements included an integrated Setup experience, optimized configuration settings, and the ability to manage most aspects of the high availability solution using native Exchange management tools.

However, management of an Exchange 2007 high availability solution required complex clustering concepts, such as the concept of moving network identities and managing cluster resources. In addition, when troubleshooting issues related to a clustered mailbox server, Exchange tools and cluster tools were used to review and correlate logs and events from two different sources: one from Exchange and one from the cluster.

Two other limiting aspects of the Exchange 2007 architecture have been evaluated and revised based on customer feedback:

- Clustered Exchange 2007 servers require dedicated hardware. Only the Mailbox server role could be installed on a node in the cluster. This meant that a minimum of four Exchange servers were required to achieve full redundancy of the primary components of a deployment, for example, the core server roles (Mailbox, Hub Transport, and Client Access).
- In Exchange 2007, failover of a clustered mailbox server occurs at the server level. As a result, if a single database failure occurred, the administrator had to fail over the entire clustered mailbox server to another node in the cluster (which resulted in brief downtime for all users on the server, and not just those users with a mailbox on the affected database), or leave the users on the failed database offline (potentially for hours) while restoring the database from backup.

Exchange 2010 has been engineered with the concept of *database mobility*. Database mobility expands the system's use of continuous replication by replicating a database to multiple, different servers that are grouped together. This model provides better protection of the database and increased availability. In this model, automatic failover protection and manual switchover control is provided at the mailbox database level instead of at the server level.

In the case of failures, other servers that have copies of the database can mount the database. As a result of this and other architectural changes, failover actions now complete much faster than in previous versions of Exchange. For example, failover of a clustered mailbox server in a CCR environment running Exchange 2007 with Service Pack 1 completes in about 2 minutes (assuming an intra-site failure where the IP address of the clustered mailbox server doesn't change). By comparison, failover of a mailbox database in an Exchange 2010 environment completes within 30 seconds (measured from the time when the failure is detected to when a database copy is mounted, assuming the copy is healthy and up to date with log replay). The combination of database-level failovers and significantly faster failover times improves an organization's overall uptime.

Return to top

Incremental Deployment

Exchange 2010 introduces the concept of *incremental deployment*, which enables you to deploy service and data availability for all Mailbox servers and databases after Exchange is installed. Service and data redundancy is achieved by using new features in Exchange 2010 such as DAGs and database copies.

In previous versions of Exchange, service availability for the Mailbox server roles was achieved by deploying Exchange in a Windows failover cluster. To deploy Exchange in a cluster, you had to first build a failover cluster, and then install the Exchange program files. This process created a special Mailbox server called a clustered mailbox server (or Exchange Virtual Server in older versions of Exchange). If you had already installed the Exchange program files on a non-clustered server and you decided you wanted a clustered mailbox server, you had to build a cluster using new hardware, or remove Exchange from the existing server, install failover clustering, and reinstall Exchange.

Return to top

Database Availability Groups

A DAG is the base component of the high availability and site resilience framework built into Exchange 2010. A DAG is a group of up to 16 Mailbox servers that hosts a set of databases and provides automatic database-level recovery from failures that affect individual databases. Any server in a DAG can host a copy of a mailbox database from any other server in the DAG. When a server is added to a DAG, it works with the other servers in the DAG to provide automatic recovery from failures that affect mailbox databases, such as a disk failure or server failure.

Exchange 2007 introduced a built-in data replication technology called continuous replication. Continuous replication, which was available in three forms: local, cluster, and standby, significantly reduced the cost of deploying a highly available Exchange infrastructure, and provided a much improved deployment and management experience over previous versions of Exchange. Even with these cost savings and improvements, however, running a highly available Exchange 2007 infrastructure still required much time and expertise because the integration between Exchange and Windows failover clustering wasn't seamless. In addition, customers wanted an easier way to replicate their e-mail data to a remote location, to protect their Exchange environment against site-level disasters.

Exchange 2010 uses the same continuous replication technology found in Exchange 2007. Exchange 2010 combines on-site data replication (CCR) and off-site data replication (SCR) into a single framework called a *database availability group* (DAG). After servers are added to a DAG, you can add replicated database copies incrementally (up to 16 total), and Exchange 2010 switches between these copies automatically, to maintain availability.

Unlike Exchange 2007, where clustered mailbox servers required dedicated hardware, Mailbox servers in a DAG can host other Exchange roles (Client Access, Hub Transport, and Unified Messaging), providing full redundancy of Exchange services and data with just two servers.

This new high availability architecture also provides simplified recovery from a variety of failures (disk-level, server-level, and datacenter-level), and the architecture can be deployed on a variety of storage types.

For more information about DAGs, see Understanding Database Availability Groups.

Return to top

Mailbox Database Copies

The high availability and site resilience features first introduced in Exchange 2007 are used in Exchange 2010 to create and maintain database copies, so that you can achieve your availability goals in Exchange 2010. Exchange 2010 also introduces the concept of database mobility, which is Exchange-managed database-level failovers.

Database mobility disconnects databases from servers and adds support for up to 16 copies of a single database, and it provides a native experience for adding database copies to a database. In Exchange 2007, a feature called database portability also enabled you to move a mailbox database between servers. A significant distinction between database portability and database mobility, however, is that all copies of a database have the same GUID.

Setting a database copy as the active mailbox database is known as a *switchover*. When a failure affecting a database occurs and a new database becomes the active copy, this process is known as a *failover*. This process also refers to a server failure in which one or more servers bring online the databases previously online on the failed server. When either a switchover or failover occurs, other Exchange 2010 server roles become aware of the switchover almost immediately and redirect client and messaging traffic to the new active database.

For example, if an active database in a DAG fails because of an underlying storage failure, Active Manager will automatically recover by failing over to a database copy on another Mailbox server in the DAG. If the database is outside the automatic mount criteria and can't be automatically mounted, you can manually perform a database failover.

For more information about mailbox database copies, see Understanding Mailbox Database Copies.

Return to top

Active Manager

In Exchange 2007 and previous versions, Exchange used the cluster resource management model to install, implement, and manage the Mailbox server high availability solution. Historically, building a highly available Mailbox server involved first building a Windows failover cluster, and then running Exchange Setup in clustered mode. In this mode, the Exchange cluster resource DLL file, exres.dll, would be registered and allow the creation of a clustered mailbox server (called an Exchange Virtual Server in legacy versions). When deploying legacy shared storage clusters or single copy clusters, additional steps for configuring storage were needed before and after failover cluster formation, and after clustered mailbox server and storage group formation.

Exchange 2010 includes a new component called *Active Manager* that provides functionality that replaces the resource model and failover management features provided by integration with the Cluster service in previous versions of Exchange. For more information about Active Manager, see Understanding Active Manager.

Return to top

Changes to High Availability from Previous Versions of Exchange

There are several changes to the core architecture of Exchange 2010 that have a direct effect on how you configure Exchange for high availability, as well as a direct effect on how you perform site recovery. One significant change is the removal of clustered mailbox servers and the use of the Windows Failover Cluster resource model. Other significant changes include the globalization of databases and enhancements to the built-in

continuous replication technology first introduced in Exchange 2007.

Removal of Clustered Mailbox Servers

In Exchange 2010, Exchange is no longer a clustered application, and the cluster resource model is no longer used for Exchange high availability. Exres.dll and all Exchange cluster resources it provided also no longer exist, including clustered mailbox servers. Instead, Exchange 2010 uses its own internal high availability model. Some components of Windows failover clustering are still used, but they are now integrated into other functionality by Exchange 2010.

Globalization of Databases

In Exchange 2010, a database is associated with a single, dedicated log stream, represented by a series of sequentially-named, 1-megabyte (MB) log files. The concept of storage groups has also been removed from Exchange 2010. As a result of these changes, Exchange databases have a dedicated log stream, and no longer share log streams with other databases.

Unlike in previous versions of Exchange, databases are no longer closely tied to a specific Mailbox server. In addition, databases are no longer identified by the Mailbox servers on which they reside, and server names are no longer part of database identities. As a result of these changes, databases are now global objects in Active Directory and in each Exchange organization. When using the Exchange Management Console, databases are now managed from the Mailbox node under the Organization Configuration node.

Each Mailbox server can host a maximum of 100 databases (total combined number of active and passive databases). The total number of databases equals the combined number of active and passive databases on a server. The recovery database doesn't count against the 100 database limit.

Changes to Continuous Replication in Exchange 2010 RTM

The continuous replication technology introduced in Exchange 2007 is also available in Exchange 2010. However, the feature has evolved considerably to support new high availability features and greater scalability. Some of these architectural changes include:

- Because storage groups are removed in Exchange 2010, continuous replication now operates at the database level. Exchange 2010 still uses an Extensible Storage Engine (ESE) database that produces transaction logs replicated to one or more other locations and replayed into one or more mailbox database copies. Each mailbox database can have as many as 16 copies.
- Log shipping no longer uses Server Message Block (SMB) and Windows file system notifications. Log shipping no longer uses a pull model, where the passive copy pulls a closed log file from the active copy. Instead, the passive copy uses TCP-based notifications to notify the active copy about which log files are required by the passive copy. The active copy then pushes the log files to each configured passive copy through the TCP socket.
- Exchange 2010 continuous replication uses one administrator-defined TCP port for data transfer. In addition, Exchange 2010 includes built-in options for network encryption and compression for the data stream.
- Seeding is no longer restricted to using only the active copy of the database. Passive copies of mailbox databases can now be specified as sources for database copy seeding and reseeding.
- Database copies are for mailbox databases only. For redundancy and high availability of public folder databases, we recommend that you use public folder replication. Unlike CCR, where multiple copies of a public folder database couldn't exist in the same cluster, you can use public folder replication to replicate public folder databases between servers in a DAG.
- In Exchange 2007, the Microsoft Exchange Replication service was responsible for replaying logs into passive database copies. When the passive copy was activated, the database cache that had been built by the Microsoft Exchange Replication service as a result of replay activity would be lost when the

Microsoft Exchange Information Store service would mount the database. This put the database cache in a state known as a *cold state*. The database cache, which is used to cache read/write operations, is small in size (cold) during this period. Therefore, it has a significantly diminished ability to reduce read I/O operations. In Exchange 2010, the passive copy replay functionality previously performed by the Microsoft Exchange Replication service has been moved into the Microsoft Exchange Information Store service. As a result, a warm database cache is present and immediately available for use after a failover or switchover occurs.

Several concepts used in Exchange 2007 continuous replication also remain in Exchange 2010. These include the concepts of failover management, divergence, the use of the automatic database mount dial, and the use of replication and client access (MAPI) networks.

Changes to Continuous Replication in Exchange 2010 SP1

In the RTM version of Exchange 2010 and in all versions of Exchange Server 2007, continuous replication operates by shipping copies of the log files generated by the active database copy to the passive database copies. Beginning with Exchange 2010 SP1, this form of continuous replication is known as *continuous replication - file mode*. SP1 also introduces a new form of continuous replication known as *continuous replication - block mode*. In block mode, as each update is written to the active database copy's active log buffer, it's also shipped to a log buffer on each of the passive mailbox copies. When the log buffer is full, each database copy builds, inspects and creates the next log file in the generation sequence. In the event of a failure affecting the active copy, the passive copies will have been updated with most or all of the latest updates. The active copy doesn't wait for replication to complete in order to preclude replication issues from affecting the client experience.

Block mode dramatically reduces the latency between the time a change is made on the active copy and when the change is replicated to passive copies. In addition to replicating individual log file writes, block mode also changes the activation process for a passive copy. If a copy is in block mode when a failure occurs, the system uses whatever partial log content is available during the activation process. This eliminates the current log file on the active copy from being a single point of failure.

The initial mode of operation is always file mode. Block mode is only active when continuous replication is up-to-date in file mode. The transition into and out of block mode is performed automatically by the log copier. When the passive copy requests the current log file, it indicates that continuous replication is up-to-date (the copy queue length is 0), and the system should automatically switch from file mode to block mode.

You can determine if a passive database copy is in block mode by monitoring the **Continuous replication – block mode Active** performance counter under the **MSExchange Replication** performance object. Each database copy has its own instance of this counter. The value of the counter is set to 1 when the passive copy is in block mode and 0 when the passive copy is in file mode. You can also determine the value of this counter by using the Get-Counter or Get-WMIObject cmdlets, as shown in these examples:

```
Get-Counter -ComputerName <DAGMemberName> -Counter "\MSExchange Replication(*)\Co
Get-WMIObject -ComputerName <DAGMemberName> Win32_PerfRawData_MSExchangeReplicati
```

Changes to Transport Dumpster from Exchange 2007

The Exchange 2010 Hub Transport server role includes a feature called the transport dumpster, which was first introduced in Exchange 2007. The transport dumpster is designed to help protect against data loss by maintaining a queue of all recent e-mail messages sent to users whose mailboxes were protected by CCR or LCR. When a lossy failure occurred in either of these environments, the bulk of the data that would have ordinarily been lost as a result of the failure is automatically recovered by the transport dumpster.

The transport dumpster is used for replicated mailbox databases only. It doesn't protect messages sent to public folders, nor does it protect messages sent to recipients on mailbox databases that aren't replicated. The transport dumpster queue for a specific mailbox database is located on all Hub Transport servers in the Active Directory sites containing the DAG.

In Exchange 2007, messages were retained in the transport dumpster until the administrator-defined time limit or size limit is reached. In Exchange 2010, the transport dumpster now receives feedback from the replication pipeline to determine which messages have been delivered and replicated. As a message goes through Hub Transport servers on its way to a replicated mailbox database in a DAG, a copy is kept in the transport queue (mail.que) until the transaction logs representing the message have been successfully replicated to and inspected by all copies of the mailbox database. After the logs have been replicated to and inspected by all database copies, the messages in those logs are truncated from the transport dumpster. This keeps the transport dumpster queue smaller by maintaining only copies of messages whose transactions logs haven't yet been replicated.

Each DAG's Active Manager tracks the value for the last log inspected time on each passive database copy. The Active Manager client running on the Hub Transport server obtains this information from the DAG's Standby Active Manager (SAM) and converts that information into a time-based watermark. The Hub Transport server then compares the delivery time of messages in the transport dumpster with the watermark. If the delivery time of a message is older than the watermark, then the message is truncated from the transport dumpster.

The transport dumpster has also been enhanced to account for the changes to the Mailbox server role that enable a single mailbox database to move between Active Directory sites. DAGs can be extended to multiple Active Directory sites, and as a result, a single mailbox database in one Active Directory site can fail over to another Active Directory site. When this occurs, any transport dumpster redelivery requests will be sent to both Active Directory sites: the original site and the new site.

Changes to Routing Behavior When Hub Transport and Mailbox are Co-Located in a DAG

When the Hub Transport server is co-located with a Mailbox server that's a member of a DAG, there are changes in routing behavior to ensure that the resiliency features in both server roles will provide the necessary protection for messages sent to and received by users on that server. The Hub Transport server role was modified so that it now attempts to reroute a message for a local Mailbox server to another Hub Transport server in the same site if the Hub Transport server is also a DAG member and it has a copy of the mailbox database mounted locally. This extra hop was added to put the message in the transport dumpster on a different Hub Transport server.

For example, EX1 hosts the Hub Transport server role and Mailbox server role and is a member of a DAG. When a message arrives in transport for EX1 destined for a recipient whose mailbox is also on EX1, transport will reroute the message to another Hub Transport server in the site (for example, EX2), and that server will deliver the message to the mailbox on EX1.

There's a second, similar behavior change related to the Microsoft Exchange Mail Submission service. This service was modified so that it would not submit messages to a local Hub Transport server role when the Mailbox server or Hub Transport server is a member of a DAG. In this scenario, the behavior of transport is to load balance submission requests across other Hub Transport servers in the same Active Directory site, and fall back to a local Hub Transport server if there are no other available Hub Transport servers in the same site.

Return to top

High Availability for Non-Mailbox Server Roles

High availability for the Hub Transport, Edge Transport, Client Access, and Unified Messaging server roles is achieved through a combination of server redundancy, load balancing, and Domain Name System (DNS) round robin, as well as proactive server, service, and infrastructure management. In general, you can achieve high availability for the Client Access, Hub Transport, Edge Transport, and Unified Messaging server roles by using the following strategies and technologies:

- **Edge Transport** You can deploy multiple Edge Transport servers and use multiple DNS MX resource records to load balance activity across those servers. You can also use Network Load Balancing (NLB) to provide load balancing and high availability for Edge Transport servers.
- **Client Access** You can use NLB or a third-party hardware-based network load balancing device for Client Access server high availability.
- **Hub Transport** You can deploy multiple Hub Transport servers for internal transport high availability. Resiliency has been designed into the Hub Transport server role in the following ways:
  - **Hub Transport server to Hub Transport server (intra-organization)** Hub Transport server to Hub Transport server communication inside an organization automatically load balances between available Hub Transport servers in the target Active Directory site.
  - **Mailbox server to Hub Transport server (intra-Active Directory site)** The Microsoft Exchange Mail Submission service on Mailbox servers automatically load balances between all available Hub Transport servers in the same Active Directory site.
  - **Unified Messaging server to Hub Transport server** The Unified Messaging server automatically load balances connections between all available Hub Transport servers in the same Active Directory site.
  - **Edge Transport server to Hub Transport server** The Edge Transport server automatically load balances inbound SMTP traffic to all Hub Transport servers in the Active Directory site to which the Edge Transport server is subscribed.

  For additional redundancy (for example, applications that require an SMTP relay), you can create a DNS record (for example, relay.company.com), assign an IP address, and use a hardware load balancer to redirect that IP address to multiple Hub Transport servers. You can also use NLB for the client connectors on Hub Transport servers. When using a hardware load balancer, you need to confirm that no intra-organization traffic will be crossing the hardware load balancer because intra-organization traffic uses built-in load balancing algorithms (as previously described).
- **Unified Messaging** Unified Messaging deployments can be made more resilient by deploying multiple Unified Messaging servers where two or more are in a single dial plan. The Voice over IP (VoIP) gateways supported by Unified Messaging can be configured to route calls to Unified Messaging servers in a round-robin fashion. In addition, these gateways can retrieve the list of servers for a dial plan from DNS. In either case, the VoIP gateways will present a call to a Unified Messaging server and if the call isn't accepted, the call will be presented to another server, providing redundancy at the time the call is established.

Return to top

Site Resilience

Exchange 2010 includes a unified platform for both high availability and site resilience. By combining the native site resilience support in Exchange 2010 with proper planning, a second datacenter can be rapidly activated to serve a failed datacenter's clients. A datacenter or site failure is managed differently from the types of failures that can cause a server or database failover. In a high availability configuration, automatic recovery is initiated by the system, and the failure typically leaves the messaging system in a fully functional state. By contrast, a datacenter failure is considered to be a disaster recovery event. Recovery must be manually performed and completed for the client service to be restored and for the outage to end. The process you perform is referred to as a *datacenter switchover*. As with many disaster recovery scenarios, prior planning and preparation for a datacenter switchover can simplify the recovery process and reduce the duration of the outage.

For details about planning and deploying site resilience, see Planning for High Availability and Site Resilience, Deploying High Availability and Site Resilience and Datacenter Switchovers.

Return to top

End-to-End Availability

Exchange 2010 also includes many features designed to increase end-to-end availability of the system. These features include:

- Shadow redundancy
- Online move mailbox
- Flexible mailbox protection
- Incremental resync
- Third-party replication API

Shadow Redundancy

In addition to the transport dumpster and routing behavior enhancements described previously, a new Hub Transport server feature named *shadow redundancy* has been added. Shadow redundancy provides redundancy for messages for the entire time they are in transit. The solution involves a technique similar to the transport dumpster. With shadow redundancy, the deletion of a message from the transport database is delayed until the transport server verifies that all of the next hops for that message have completed delivery. If any of the next hops fail before reporting successful delivery, the message is resubmitted for delivery to that next hop. For more information about shadow redundancy, see Understanding Shadow Redundancy.

Online Move Mailbox

Exchange 2010 includes a new feature that enables you to move mailboxes asynchronously. In Exchange 2007, when you used the **Move-Mailbox** cmdlet to move a mailbox, the cmdlet logged on to both the source database and the target database and moved the content from one mailbox to the other mailbox. There were several disadvantages to having the cmdlets perform the move operation:

- Mailbox moves typically took hours to complete, and during the move, users weren't able to access their mailbox.
- If the Command Prompt window used to run the **Move-Mailbox** cmdlet was closed, the move was terminated and had to be restarted.
- The computer used to perform the move participated in the data transfer. If an administrator ran the cmdlets from his or her workstation, the mailbox data would flow from the source server to the administrator's workstation and then to the target server.

The **New-MoveRequest** cmdlet in Exchange 2010 can be used to perform asynchronous moves. Unlike in Exchange 2007, the cmdlets don't perform the actual move. The move is performed by the Microsoft Exchange Mailbox Replication service, a new service that runs on a Client Access server. The **New-MoveRequest** cmdlet sends requests to the Microsoft Exchange Mailbox Replication service. For more information about online mailbox moves, see Understanding Move Requests.

Flexible Mailbox Protection

There are several changes to the core architecture of Exchange 2010 that have a direct effect on how you will protect your mailbox databases and the mailboxes they contain.

One significant change is the removal of storage groups. In Exchange 2010, each database is associated with a single log stream, represented by a series of 1 megabyte (MB) log files. Each server can host a maximum of 100 databases.

Another significant change for Exchange 2010 is that databases are no longer closely tied to a specific Mailbox server. Database mobility expands the system's use of continuous replication by replicating a database to multiple, different servers. This provides better protection of the database and increased availability. In the case of failures, the other servers that have copies of the database can mount the database.

The ability to have multiple copies of a database hosted on multiple servers means that if you have a sufficient number of database copies, you can use these copies as your backups. For more information about this strategy, see Understanding Backup, Restore and Disaster Recovery.

Incremental Resync

Exchange 2007 introduced the concepts of lost log resilience and incremental reseed. Lost log resilience is an internal component of ESE that enables you to recover Exchange mailbox databases even if one or more of the most recently generated transaction log files have been lost or damaged. Lost log resilience enables a mailbox database to mount even when recently generated log files are unavailable. Lost log resilience works by delaying writes to the database until the specified number of log generations have been created. Lost log resilience delays recent updates to the database file for a short time. The length of time that writes are delayed depends on how quickly logs are being generated.

Exchange 2007 also introduced the concept of incremental reseed, which provided the ability to correct divergences in the transaction log stream between a source and target storage group, by relying on the delayed replay capabilities of lost log resilience. Incremental reseed didn't provide a means to correct divergences in the passive copy of a database, after divergent logs had been replayed, which forced the need for a complete reseed. Unlike Exchange 2007, there is no amount of log loss that requires a full reseed in Exchange 2010.

In Exchange 2010, *incremental resync* is the new name for the feature that automatically corrects divergences in database copies under the following conditions:

- After an automatic failover for all of the configured copies of a database
- When a new copy is enabled and some database and log files already exist at the copy location
- When replication is resumed following a suspension or restarting of the Microsoft Exchange Replication service

As a result of these changes, lost log resilience is now hard-coded to one log file for all Exchange 2010 mailbox databases.

When divergence between an active database and a copy of that database is detected, incremental resync performs the following tasks:

- Searches historically in the log file stream to locate the point of divergence.

- Locates the changed database pages on the diverged copy.
- Reads the changed pages from the active copy, and then copies the necessary log files from the active copy.
- Applies the database page changes to the diverged copy.
- Runs recovery on the diverged copy and replays the necessary log files into the database copy.

Third-Party Replication API

Exchange 2010 also includes a new third-party replication API that enables organizations to use third-party synchronous replication solutions instead of the built-in continuous replication feature. Microsoft supports third-party solutions that use this API, provided that the solution provides the necessary functionality to replace all native continuous replication functionality that is disabled as a result of using the API. Solutions are supported only when the API is used within a DAG to manage and activate mailbox database copies. Use of the API outside of these boundaries is not supported. In addition, the solution must meet the applicable Windows hardware support requirements (test validation is not required for support).

When deploying a solution that uses the built in third-party replication API, be aware that the solution vendor is responsible for primary support of the solution. Microsoft supports Exchange data for both replicated and non-replicated solutions. Solutions that use data replication must adhere to Microsoft's support policy for data replication, as described in Microsoft Knowledge Base article 895847, Multi-site data replication support for Exchange Server. In addition, solutions that utilize the Windows Failover Cluster resource model must meet Windows cluster supportability requirements as described in Microsoft Knowledge Base article 943984, The Microsoft Support Policy for Windows Server 2008 Failover Clusters.

Microsoft's backup and restore support policy for deployments that use third-party replication API-based solutions is the same as for native continuous replication deployments.

If you are a partner seeking information about the third-party API, contact your Microsoft representative. For information about partner products for Exchange 2010, see Microsoft Exchange Partners.

Return to top

1.10.1.1 Understanding Database Availability Groups

Understanding Database Availability Groups

Exchange Server 2010 > High Availability and Site Resilience > Understanding High Availability and Site Resilience >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-09*

A database availability group (DAG) is the base component of the high availability and site resilience framework built into Microsoft Exchange Server 2010. A DAG is a group of up to 16 Mailbox servers that hosts a set of databases and provides automatic database-level recovery from failures that affect individual servers or databases.

A DAG is a boundary for mailbox database replication, database and server switchovers, failovers, and an internal Exchange 2010 component called *Active Manager*. Active Manager, which runs on every server in a DAG, manages switchovers and failovers. For more information about Active Manager, see Understanding Active Manager.

Any server in a DAG can host a copy of a mailbox database from any other server in the DAG. When a server is added to a DAG, it works with the other servers in the DAG to provide automatic recovery from failures that affect mailbox databases, such as a disk failure or server failure.

Contents

Database Availability Group Lifecycle

DAGs leverage a feature of Exchange 2010 known as *incremental deployment*, which is the ability to deploy service and data availability for all Mailbox servers and databases after Exchange is installed. After you deploy Exchange 2010, you can create a DAG, add Mailbox servers to the DAG, and then replicate mailbox databases between the DAG members.

Note:
It is supported to create a DAG that contains a combination of physical Mailbox servers and virtualized Mailbox servers, provided that the servers and solution comply with the Exchange 2010 System Requirements. As with all Exchange high availability configurations, you must ensure that all Mailbox servers in the DAG are sized appropriately to handle the necessary workload during scheduled or unscheduled outages.

A DAG is created by using the New-DatabaseAvailabilityGroup cmdlet. A DAG is initially created as an empty object in Active Directory. This directory object is used to store relevant information about the DAG, such as server membership information. When you add the first server to a DAG, a failover cluster is automatically created for the DAG. This failover cluster is used exclusively by the DAG, and the cluster must be dedicated to the DAG. Use of the cluster for any other purpose isn't supported.

In addition to a failover cluster being created, the infrastructure that monitors the servers for network or server failures is initiated. The failover cluster heartbeat mechanism and cluster database are then used to track and manage information about the DAG that can change quickly, such as database mount status, replication status, and last mounted location.

During creation, the DAG is given a unique name, and either assigned one or more static IP addresses or configured to use Dynamic Host Configuration Protocol (DHCP). You can specify a single IP address or a comma-separated list of IP addresses by using the *DatabaseAvailabilityGroupIPAddresses* parameter.

This example shows a DAG that will have three servers. Two servers (EX1 and EX2) are on the same subnet (10.0.0.0), and the third server (EX3) is on a different subnet (192.168.0.0).

```
New-DatabaseAvailabilityGroup -Name DAG1 -DatabaseAvailabilityGroupIPAddresses 10
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer EX1
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer EX2
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer EX3
```

Note:
Configuring the *DatabaseAvailabilityGroupIPAddresses* parameter with a value of 0.0.0.0

configures the DAG (cluster) to use DHCP for its IP addresses or IP address resources.

The cluster for DAG1 is created when EX1 is added to the DAG. During cluster creation, the **Add-DatabaseAvailabilityGroupServer** cmdlet retrieves the IP addresses configured for the DAG and ignores the ones that don't match any of the subnets found on EX1. In this example, the cluster for DAG1 is created with an IP address of 10.0.0.5, and 192.168.0.5 is ignored.

Then, EX2 is added, and the **Add-DatabaseAvailabilityGroupServer** cmdlet again retrieves the IP addresses configured for the DAG. There are no changes to the cluster's IP addresses because EX2 is on the same subnet as EX1.

Then, EX3 is added, and the **Add-DatabaseAvailabilityGroupServer** cmdlet again retrieves the IP addresses configured for the DAG. Because a subnet matching 192.168.0.5 is present on EX3, the 192.168.0.5 address is added as an IP address resource in the cluster group. In addition, an **OR** dependency for the Network Name resource for each IP address resource is automatically configured. The 192.168.0.5 address will be used by the cluster when the cluster group moves to EX3.

Windows failover clustering registers the IP addresses for the cluster in the Domain Name System (DNS) when the Network Name resource is brought online. In addition, a cluster name object (CNO) is created in Active Directory. The name, IP addresses and CNO for the cluster are used only internally by the system to secure the DAG and for internal communication purposes. Administrators and end users don't need to interface with or connect to the DAG name or IP address for any reason.

In addition to a name and one or more IP addresses, the DAG is also configured to use a witness server and a witness directory. The witness server and witness directory are either automatically specified by the system, or they can be manually specified by the administrator.

By default, a DAG is designed to use the built-in continuous replication feature to replicate mailbox databases among servers in the DAG. If you're using third-party data replication that supports the Third Party Replication API in Exchange 2010, you must create the DAG in third-party replication mode by using the New-DatabaseAvailabilityGroup cmdlet with the *ThirdPartyReplication* parameter. After this mode is enabled, it can't be disabled.

After the DAG is created, Mailbox servers can be added to the DAG. When the first server is added to the DAG, a cluster is formed for use by the DAG. DAGs make limited use of Windows failover clustering technology, such as the cluster heartbeat, cluster networks, and the cluster database (for storing data that changes, such as database state changes from active to passive or vice versa, or from mounted to dismounted and vice versa). As each subsequent server is added to the DAG, it's joined to the underlying cluster, the cluster's quorum model is automatically adjusted by the system, and the server is added to the DAG object in Active Directory.

After Mailbox servers are added to a DAG, you can configure a variety of DAG properties, such as whether to use network encryption or network compression for database replication within the DAG. You can also configure DAG networks and create additional DAG networks.

After you add members to a DAG and configure the DAG, the active mailbox databases on each server can be replicated to the other DAG members. After you create mailbox database copies, you can monitor the health and status of the copies using a variety of built-in monitoring tools. In addition, you can perform database and server switchovers.

For more information about creating DAGs, managing DAG membership, configuring DAG properties, creating and monitoring mailbox database copies, and performing switchovers, see Managing High Availability and Site Resilience.

Database Availability Group Quorum Models

Underneath every DAG is a Windows failover cluster. Failover clusters use the concept of quorum, which uses a consensus of voters to ensure that only one subset of the cluster members (which could mean all members or a majority of members) is functioning at one time. Quorum isn't a new concept for Exchange 2010. Highly available Mailbox servers in previous versions of Exchange also use failover clustering and its concept of quorum. Quorum represents a shared view of members and resources, and the term quorum is also used to describe the physical data that represents the configuration within the cluster that is shared between all cluster members. As a result, all DAGs require their underlying failover cluster to have quorum. If the cluster loses quorum, all DAG operations terminate and all mounted databases hosted in the DAG will dismount. In this event, administrator intervention will be required to correct the quorum problem and restore DAG operations.

Quorum is important to ensure consistency, to act as a tie-breaker to avoid partitioning, and to ensure cluster responsiveness:

- **Ensuring consistency** A primary requirement for a Windows failover cluster is that each of the members always has a view of the cluster that's consistent with the other members. The cluster hive acts as the definitive repository for all configuration information relating to the cluster. If the cluster hive can't be loaded locally on a DAG member, the Cluster service doesn't start, because it isn't able to guarantee that the member meets the requirement of having a view of the cluster that's consistent with the other members.
- **Acting as a tie-breaker** A quorum witness resource is used in DAGs with an even number of members to avoid split brain syndrome scenarios and to make sure that only one collection of the members in the DAG is considered official. When the witness server is needed for quorum, any member of the DAG that can communicate with the witness server can place a Server Message Block (SMB) lock on the witness server's witness.log file. The DAG member that locks the witness server (referred to as the *locking node*) retains an additional vote for quorum purposes. The DAG members in contact with the locking node are in the majority and maintain quorum. Any DAG members that can't contact the locking node are in the minority and therefore lose quorum.
- **Ensuring responsiveness** To ensure responsiveness, the quorum model makes sure that, whenever the cluster is running, enough members of the distributed system are operational and communicative, and at least one replica of the cluster's current state can be guaranteed. No additional time is required to bring members into communication or to determine whether a specific replica is guaranteed.

DAGs with an even number of members use the failover cluster's Node and File Share Majority quorum mode, which employs an external witness server that acts as a tie-breaker. In this quorum mode, each DAG member gets a vote. In addition, the witness server is used to provide one DAG member with a weighted vote (e.g., it gets two votes instead of one). The cluster quorum data is stored by default on the system disk of each member of the DAG, and is kept consistent across those disks. However, a copy of the quorum data isn't stored on the witness server. A file on the witness server is used to keep track of which member has the most updated copy of the data, but the witness server doesn't have a copy of the cluster quorum data. In this mode, a majority of the voters (the DAG members plus the witness server) must be operational and able to communicate with each other to maintain quorum. If a majority of the voters can't communicate with each other, the DAG's underlying cluster loses quorum, and the DAG will require administrator intervention to become operational again.

DAGs with an odd number of members use the failover cluster's Node Majority quorum mode. In this mode, each member gets a vote, and each member's local system disk is used to store the cluster quorum data. If the configuration of the DAG changes, that change is reflected across the different disks. The change is only considered to have been committed and made persistent if that change is made to the disks on half the members (rounding down) plus one. For example, in a five-member DAG, the change must be made

on two plus one members, or three members total.

Quorum requires a majority of voters to be able to communicate with each other. Consider a DAG that has four members. Because this DAG has an even number of members, an external witness server is used to provide one of the cluster members with a fifth, tie-breaking vote. To maintain a majority of voters (and therefore quorum), at least three voters must be able to communicate with each other. At any time, a maximum of two voters can be offline without disrupting service and data access. If three or more voters are offline, the DAG loses quorum, and service and data access will be disrupted until you resolve the problem.

Return to top

Using a Database Availability Group for High Availability

To illustrate how a DAG can provide high availability for your mailbox databases, consider the following example, which uses a DAG with five members. This DAG is illustrated in the following figure.

In the preceding figure, the green databases are active mailbox database copies and the blue databases are passive mailbox database copies. In this example, the database copies aren't mirrored across each server, but rather spread across multiple servers. This ensures that no two servers in the DAG have the same set of database copies, providing the DAG with greater resilience to failures, including failures that occur while other components are unavailable as a result of regular maintenance.

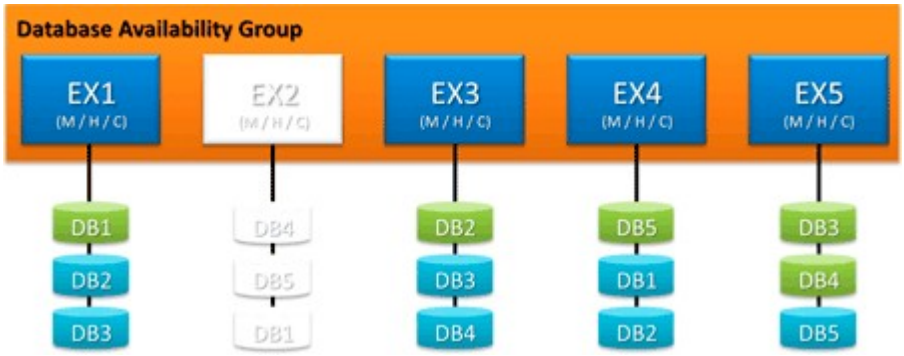
Consider the following scenario, using the preceding example DAG, which illustrates resilience to multiple database and server failures.

Initially, all databases and servers are healthy. You need to install some operating system updates on EX2. You perform a server switchover, which activates the copy of DB4 on another Mailbox server. A server switchover moves all active mailbox database copies from their current server to one or more other Mailbox servers in the DAG in preparation for a scheduled outage for the current server. You can perform a server switchover quickly by running the following command in the Exchange Management Shell.

```
Move-ActiveMailboxDatabase -Server EX2
```

In this example, there's only one active mailbox database on EX2 (DB4), so only one active mailbox database copy is moved. By omitting the *ActivateOnServer* parameter in the preceding command, you chose to have the system select the best possible new active copy, and the system chose the copy on EX5, as shown in the following figure.

DAG with a server offline for maintenance

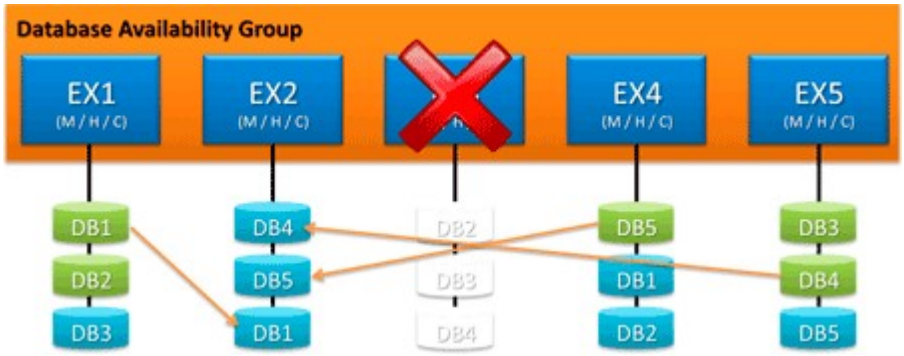


While you perform maintenance on EX2, EX3 experiences a catastrophic hardware failure and goes offline. Prior to going offline, EX3 hosted the active copy of DB2. To recover from the failure, the system automatically activates the copy of DB2 that's hosted on EX1 within 30 seconds. This is illustrated in the following figure.

DAG with a server offline for maintenance and a failed server

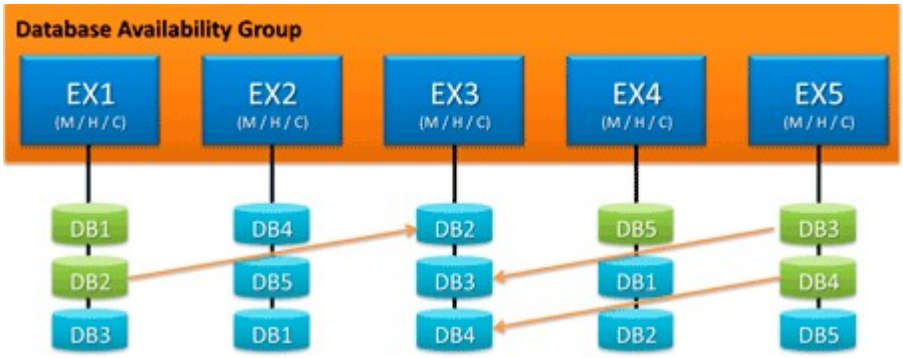
After the scheduled maintenance is completed for EX2, you bring the server online. As soon as EX2 is available, the other members of the DAG are notified, and the copies of DB1, DB4, and DB5 hosted on EX2 are automatically synchronized with the active copy of each database. This is illustrated in the following figure.

DAG with a restored server synchronizing its database copies



After the failed hardware component in EX3 is replaced with a new component, EX3 is brought online. After EX3 is available, the other members of the DAG are notified, and the copies of DB2, DB3, and DB4 hosted on EX3 are automatically synchronized with the active copy of each database. This is illustrated in the following figure.

DAG with a repaired server synchronizing its database copies

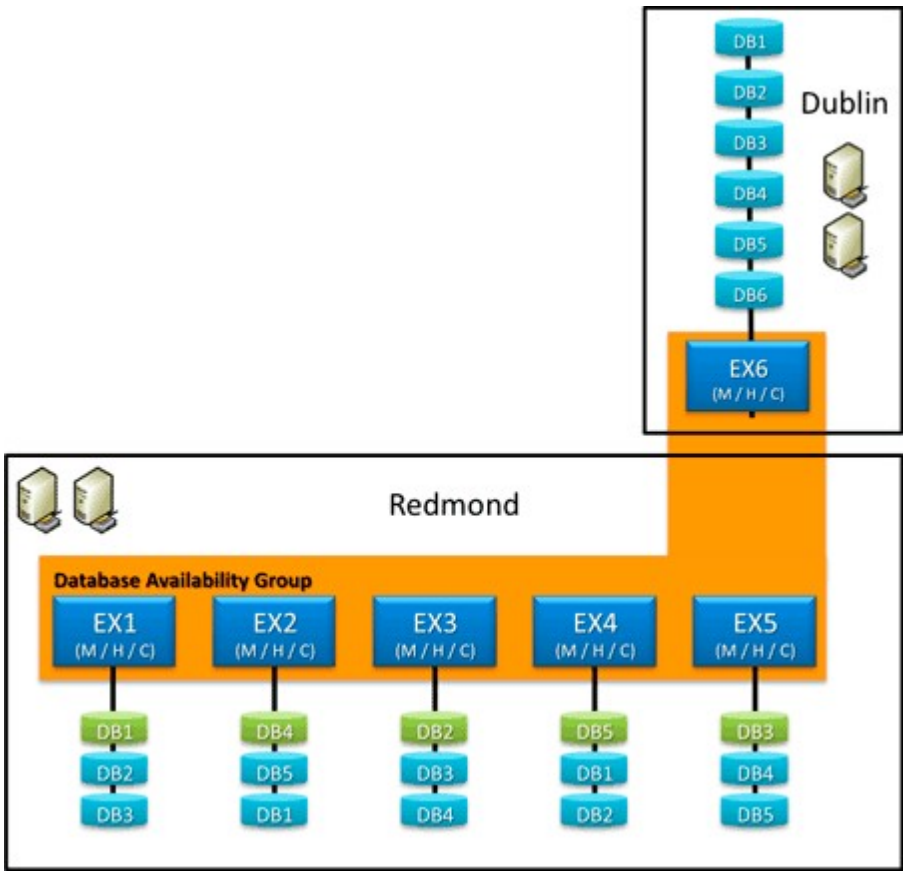


Return to top

Using a Database Availability Group for Site Resilience

In addition to providing high availability within a datacenter, a DAG can also be extended to one or more datacenters in a configuration that provides site resilience for one or multiple datacenters. In the preceding example figures, the DAG is located in a single datacenter and single Active Directory site. Incremental deployment can be used to extend this DAG to a second datacenter (and a second Active Directory site) by deploying a Mailbox server and the necessary supporting resources (one or more Active Directory servers, and one or more Hub Transport and Client Access servers). The Mailbox server is then added to the DAG, as illustrated in the following figure.

DAG extended across two Active Directory sites



In this example, a passive copy of each active database in the Redmond datacenter is configured on EX6 in the Dublin datacenter. However, there are many other examples of DAG configurations that provide site resilience. For example:

- Instead of hosting only passive database copies, EX6 could host all active copies, or it could host a mixture of active and passive copies.
- In addition to EX6, multiple DAG members could be deployed in the Dublin datacenter, providing protection against additional failures. This configuration also provides additional capacity, so that if the Redmond datacenter fails, the Dublin datacenter can support a much larger user population.

Using Multiple Database Availability Groups for Site Resilience

In the preceding example, a single DAG extends across multiple datacenters, providing site resilience for either or both datacenters. When using a single DAG to provide site resilience in an environment where each datacenter to which you extend the DAG has an active user population, there is a single point of failure in the wide area network (WAN) connection. This is because quorum requires a majority of the voters to be active and able to communicate with each other.

In the preceding example, the majority of voters are located in the Redmond datacenter. If the Dublin datacenter hosts active mailbox databases, and it has a local user population, a WAN outage would result in a messaging service outage for the Dublin users. When WAN connectivity breaks, only the DAG members in the Redmond datacenter retain quorum and continue providing messaging service.

To eliminate the WAN as a single point of failure when you need to provide site resilience for multiple datacenters that each have an active user population, you should deploy multiple DAGs, where each DAG has a majority of voters in a separate datacenter. When a WAN outage occurs, replication will be blocked until connectivity is restored. Users will

have messaging service, because each DAG continues to service its local user population.

Return to top

Client Experience When Using Database Availability Groups

DAGs can be used to provide both high availability and site resilience. The client experience when using a DAG depends on the type and version of the client and the protocol used by the client to access mailbox data. For example, if a cross-site database failover occurs, the behavior and reconnection logic used by a POP3 or IMAP4 client is different from the behavior and reconnection logic used by a Microsoft Outlook 2010 client.

The following sections describe the client behavior and logic in various scenarios. The behavior described assumes that:

- The environment contains a single Client Access server array in each Active Directory site, and each site contains at least two Client Access servers.
- An appropriate hardware-based or software-based load balancer is installed and configured in front of the Client Access server array.
- Proper namespace and certificate planning and configuration are complete, including the necessary DNS records.

Microsoft Outlook Behavior and Logic

Generally, all versions of Outlook behave the same for database failovers that occur within a single datacenter and single Active Directory site. Unlike previous versions of Exchange, in Exchange 2010, Outlook no longer connects directly to the Exchange store on the Mailbox server. Instead, Outlook (and any other MAPI client) connects to the RPC Client Access and Address Book services on the Client Access server role, and the user's Outlook is configured to connect to the Client Access server array, which then connects the client to an individual Client Access server. This abstraction of the Outlook connection away from the Mailbox server provides the following benefits:

- When a database failover occurs, Outlook remains connected to the same server in the Client Access server array. When this occurs, the Active Manager client running on the Client Access server learns which DAG member hosts the active database copy from the DAG's Active Manager. Then, the Client Access server connects to that Mailbox server, and Outlook indicates it's connected to the Exchange server.
- If one of the Client Access servers in the Client Access server array becomes unavailable because of a scheduled or unscheduled outage, the remaining Client Access servers in that array handle the client load. Because Outlook is configured to connect to the Client Access server array and not an individual Client Access server, Client Access server array members can individually experience failures or be manually taken offline without affecting the user's Outlook profile. This can happen automatically (for example, automatic array reconfiguration, based on monitoring performed by the load balancer solution in front of the array), or you can perform this manually.

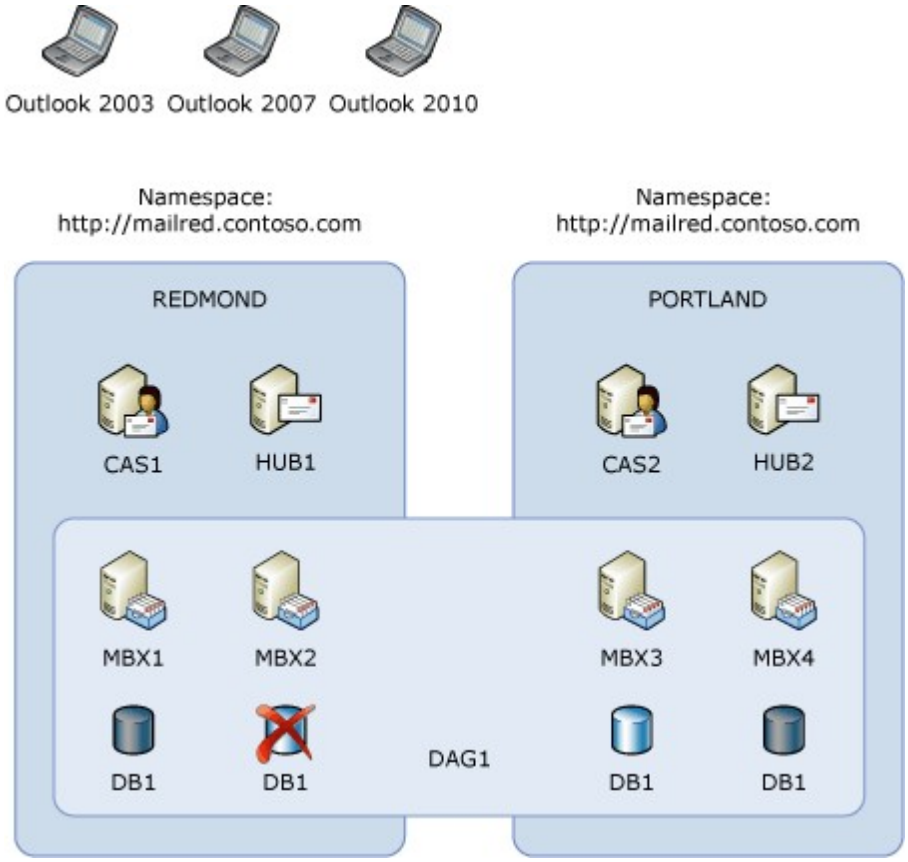
All versions of Outlook also behave the same for datacenter switchovers that occur between two datacenters and two Active Directory sites. Datacenter switchovers involve changing the IP addresses used by client access namespaces (for example, Microsoft Office Outlook Web App, SMTP, POP3, IMAP4, Autodiscover, Exchange Web Services, or RPC Client Access) from IP addresses in the primary datacenter to IP addresses in the secondary datacenter. As a result, the namespace used in the user's Outlook profile doesn't change, and Autodiscover continues to point clients to the same Client Access server array namespace.

The behavior of Outlook after a cross-site database failover is different from its behavior

after a database failover in a single Active Directory site or after a datacenter switchover.

Example Behavior for Outlook Versions

The following examples illustrate the behavior of Outlook 2010, Office Outlook 2007, and Office Outlook 2003 after a cross-site database failover occurs. The topology used in each example is a four-member DAG extended to two Active Directory sites: Redmond and Portland. The user's mailbox is hosted on DB1, which is replicated to each of the servers. In each example, the active copy of DB1 fails over from MBX2 to MBX3.



Each client is configured with CAS1 as its home server, making Redmond the *Outlook profile site*. Because the clients are located in Redmond, the **RPCClientAccessServer** property for DB1 is configured for CAS1, making Redmond the *preferred database site*. Because DB1 failed on MBX2 and has become active on MBX3, Portland is the *mounted database site*.

Example for Outlook 2010 and Outlook 2007

If a Client Access server is available in the Redmond site, Outlook 2010 and Outlook 2007 will continue to connect to the RPC Client Access array in the Redmond site. The Client Access server used by the client will communicate using MAPI RPC with the user's Mailbox server in the Portland site.

If there are no Client Access servers available in the Redmond site, then a datacenter switchover from Redmond to Portland must be performed in order to restore access to service and data. For detailed steps to perform a datacenter switchover, see Perform a Server Switchover.

Example for Outlook 2003

When Outlook 2003 attempts to connect to CAS1, it also receives an *ecWrongServer*

message in response. Unlike Outlook 2010 and Outlook 2007, Outlook 2003 doesn't include the Autodiscover feature, and it must use some other means to update the user's profile. MAPI profile redirection is the mechanism used by Outlook 2003. MAPI profile redirection requires that the original source server be online. If CAS1 is unavailable, and if all other Client Access servers in the array are also unavailable (or if the array contains only CAS1), Outlook 2003 can't perform MAPI redirection or connect to the user's mailbox database without manual intervention.

Outlook Behavior and Logic When Public Folders Are Used

Although public folder databases can be hosted on Mailbox servers that are members of a DAG, public folder databases don't use continuous replication, and they rely on public folder replication for high availability. The behavior for Outlook clients reconnecting to a public folder database after a mailbox database failover depends not only on the nature of the failure, but on your public folder replication configuration settings and the health and currency of your public folder databases. Because continuous replication can't be used for public folder databases, high availability for public folder databases is accomplished by deploying multiple public folder databases and configuring them to replicate with each other. We recommend that you configure more than one replica of each folder.

In any scenario where a user's default public folder database server is unavailable, you must manually reconfigure the default public folder database for the user's mailbox database so that Outlook can access public folder data. For detailed steps about how to change the default public folder database for a mailbox database, see Change the Default Public Folder Database for a Mailbox Database.

Non-Outlook Client Behavior and Logic

Generally, the behavior of clients and protocols other than Outlook and MAPI varies based on the application being used and the failure scenario. Generally, as with Outlook, the typical Exchange applications and clients (for example, Outlook Web App, Microsoft Exchange ActiveSync, POP3, IMAP4, and Exchange Web Services) behave the same for database failovers that occur within a single datacenter and single Active Directory site. Similarly, all these clients and protocols (including SMTP and Windows PowerShell) behave the same as Outlook after a datacenter switchover.

If a cross-site database failover occurs, the behavior varies among these clients and protocols. The following table lists the behavior for these clients.

Cross-site database failover behavior for typical Exchange clients

Client or protocol	Behavior
Outlook Web App	Manual redirection. In this scenario, the client namespace is changing from http://mailred.contoso.com to http://mailpdx.contoso.com. After the user enters logon credentials, the user is redirected to CAS2 in the Portland site through a manual redirection page explaining that the wrong URL was used and that the correct URL is https://mailpdx.contoso.com/owa.
Exchange ActiveSync	Proxy or redirection. In this scenario, the client behavior is determined by the implementation and version of the Exchange ActiveSync protocol on the client device.
POP3 and IMAP4	Proxy. This scenario always involves Client Access server to Client Access server proxying.
Exchange Web Services	Uses Autodiscover to determine new

	connection endpoint.

Return to top

1.10.1.1.1 Understanding Active Manager

Understanding Active Manager

High Availability and Site Resilience > Understanding High Availability and Site Resilience > Understanding Database Availability Groups >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-01-03*

Microsoft Exchange Server 2010 includes a new component called *Active Manager* that provides functionality that replaces the resource model and failover management features provided by integration with the Cluster service in previous versions of Exchange. Exchange no longer uses the cluster resource model for high availability. All Exchange cluster resources provided by exres.dll no longer exist, including the construct known as a clustered mailbox server. A Windows Failover Cluster is used by Exchange, but there are no cluster groups for Exchange, and there are no storage resources in the cluster. Thus, if you examine the cluster using cluster management tools, you'll see only the core cluster resources (IP Address and Network Name, and if needed, quorum resource). Cluster nodes and networks will also exist, but those are managed by Exchange and not cluster or cluster tools.

Active Manager runs as a role on all Mailbox servers. On Mailbox servers that are not configured for high availability, there is a single Active Manager role: *Standalone Active Manager*. On servers that are members of a database availability group (DAG), there are two Active Manager roles: *Primary Active Manager* (PAM) and *Standby Active Manager* (SAM). PAM is the Active Manager in a DAG that decides which copies will be active and passive. PAM is responsible for getting topology change notifications and reacting to server failures. The DAG member that holds the PAM role is always the member that currently owns the cluster quorum resource (default cluster group). If the server that owns the cluster quorum resource fails, the PAM role automatically moves to a surviving server that takes ownership of the cluster quorum resource. In addition, if you need to take the server that hosts the cluster quorum resource offline for maintenance or an upgrade, you must first move the PAM to another server in the DAG. The PAM controls all movement of the active designations between a database's copies (only one copy can be active at any specified time, and that copy may be mounted or dismounted). The PAM also performs the functions of the SAM role on the local system (detecting local database and local Information Store failures).

The SAM provides information on which server hosts the active copy of a mailbox database to other components of Exchange that are running an Active Manager client component (for example, RPC Client Access service or Hub Transport server). The SAM detects failures of local databases and the local Information Store. It reacts to failures by asking the PAM to initiate a failover (if the database is replicated). A SAM doesn't determine the target of failover, nor does it update a database's location state in the PAM. It will access the active database copy location state to answer queries for the active copy of the database that it receives.

Note:
Exchange 2010 is not a clustered application. Instead, it uses the cluster library functions implemented in clusapi.dll for cluster, group, cluster network (heartbeating), node management, cluster registry, and a few control code functions. In addition, Active

Manager stores current mailbox database information (for example, active and passive data, and mounted data) in the cluster database. Although the information is stored directly in the cluster database, it isn't accessed directly by any other components.

In Exchange 2010, the Microsoft Exchange Replication service periodically monitors the health of all mounted databases. In addition, it also monitors Extensible Storage Engine (ESE) for any I/O errors or failures. When the service detects a failure, it notifies Active Manager. Active Manager then determines which database copy should be mounted and what it requires to mount that database. In addition, it tracks the active copy of a mailbox database (based on the last mounted copy of the database) and provides the tracking results information to the RPC Client Access component on the Client Access server to which the client is connected.

Active Manager Best Copy Selection

When a failure occurs that affects a replicated mailbox database, Active Manager takes several steps to recover from the failure by selecting the best possible copy of the failed database to activate. The general process occurs in the following order:

1. Active Manager detects the failure.
2. The PAM runs an internal algorithm called best copy selection (BCS).
3. A process called *attempt copy last logs* (ACLL) occurs, which tries to copy any missing log files from the server that hosted the active database copy prior to the failover.
4. Once the ACLL process has completed, the PAM issues a mount request to the Microsoft Exchange Information Store via remote procedure call (RPC). At this point, either:
   4.a. The database mounts and is made available to clients; or
   4.b. The database does not mount, and PAM performs steps 3 and 4 on the next best copy (if one is available).

When searching for the best possible copy, the PAM uses up to ten separate sets of criteria to determine the best copy to activate. After locating the best possible copy, ACLL runs. After the ACLL process has completed, if all missing log files were copied from the previous active copy, the database mounts without any data loss. This is known as a lossless failover. If the ACLL process is unsuccessful, the configured value for *AutoDatabaseMountDial* is consulted. For more information about *AutoDatabaseMountDial*, see Set-MailboxServer. If the number of lost logs is within the configured value for *AutoDatabaseMountDial*, the database is mounted. If the number of lost logs is outside the configured value for *AutoDatabaseMountDial*, the database isn't mounted until either missing log files are recovered or until an administrator explicitly mounts the database and accepts the larger data loss. If the database doesn't mount automatically, the PAM will select the next best copy (if one is available). There are at least three reasons why the initially selected database copy does not mount automatically:

1. The number of lost log files is greater than the configured value for *AutoDatabaseMountDial*.
2. The server on which the mount attempt was made is configured with a soft maximum for the active number of databases, and the maximum number of active database copies has been reached on the server.
3. The database copy is suspended for activation.

Best Copy Selection Process

Active Manager begins the best copy selection process by creating a list of database copies that are potential candidates for activation. Any database copies that are unreachable or are administratively blocked from activation (by using the *DatabaseCopyAutoActivationPolicy* property of the **Set-MailboxServer** cmdlet) are ignored and not used during the selection process. The order of the list depends on the version of Exchange 2010:

- In the release to manufacturing (RTM) version of Exchange 2010, Active Manager sorts the resulting list using the copy queue length as the primary

key. The calculation is based on LastLogInspected (from the copy's point of view), so the list of potential copies is sorted by the highest value for LastLogInspected (which will be the copy with the lowest copy queue length). Then, Active Manager sorts the list a second time, using the value for ActivationPreference as a secondary key. The copy with the lowest ActivationPreference value has the higher priority on the list.

- In Exchange 2010 Service Pack 1 (SP1), the behavior is the same as in the RTM version, except for servers configured with an automatic database mount dial value of *Lossless*, and for target-less switchovers performed by an administrator or administrative script When a Lossless setting is used, Active Manager sorts the resulting list in ascending order by using the value for ActivationPreference as the primary key. In addition, when an administrator performs a lossless server or database switchover without specifying a target, Active Manager also sorts the resulting list in ascending order by using the value for ActivationPreference as the primary key.

Next, Active Manager attempts to locate a mailbox database copy on the list that has a status of Healthy, DisconnectedAndHealthy, DisconnectedAndResynchronizing, or SeedingSource, and then evaluates the activation potential of each of the copies on the list by using an order set of ten criteria. Active Manager determines if any of the candidates for activation meet the first set of criteria:

- It has a content index with a status of Healthy.
- It has a copy queue length less than 10 log files.
- It has a replay queue length of less than 50 log files.

If none of the database copies meet the first set of criteria, Active Manager tries to locate a database copy that meets the second set of criteria:

- It has a content index with a status of Crawling.
- It has a copy queue length less than 10 log files.
- It has a replay queue length of less than 50 log files.

If none of the database copies meet the second set of criteria, Active Manager tries to locate a database copy that meets the third set of criteria:

- It has a content index with a status of Healthy.
- It has a replay queue length of less than 50 log files.

If none of the database copies meet the third set of criteria, Active Manager tries to locate a database copy that meets the fourth set of criteria:

- It has a content index with a status of Crawling.
- It has a replay queue length of less than 50 log files.

If none of the database copies meet the fourth set of criteria, Active Manager tries to locate a database copy that meets the fifth set of criteria:

- It has a replay queue length of less than 50 log files.

If none of the database copies meet the fifth set of criteria, Active Manager tries to locate a database copy that meets the sixth set of criteria:

- It has a content index with a status of Healthy.
- It has a copy queue length less than 10 log files.

If none of the database copies meet the sixth criteria, Active Manager tries to locate a database copy that meets the seventh set of criteria:

- It has a content index with a status of Crawling.
- It has a copy queue length that is less than 10 log files.

If none of the database copies meet the seventh set of criteria, Active Manager tries to locate a database copy that meets the eighth set of criteria:

- It has a content index with a status of Healthy.

If none of the database copies meet all of the eighth set of criteria, Active Manager tries to locate a database copy that meets the ninth set of criteria:

- It has a content index with a status of Crawling.

If none of the database copies meet the ninth set of criteria, Active Manager tries to activate any database copy with a status of Healthy, DisconnectedAndHealthy, DisconnectedAndResynchronizing, or SeedingSource (the tenth set of criteria). If it can't find any database copies that meet the tenth set of criteria, it isn't able to automatically activate a database copy.

Once one or more copies are located that meet one or more sets of criteria, the ACLL process runs to copy any log files from the original source to the potential new active copy. Once the ACLL process has completed, the PAM issues a mount request and either the database mounts and is made available to clients or the database does not mount and the PAM searches for the next best copy (if one is available).

Best Copy Selection Examples

The following section illustrates some examples of Active Manager's best copy selection and activation process.

Example 1: Basic Scenario

In this example, there are four copies of mailbox database DB1. DB1 is currently active on Server1, which experiences a hardware failure. The following table shows the current status of the database copies of DB1 on Server2, Server3 and Server4.

Database Copy	Activation Preference	Copy Queue Length	Replay Queue Length	Content Index State	Database State	Activation Blocked
Server2\DB1	2	4	0	Healthy	Healthy	No
Server3\DB1	3	2	2	Healthy	DisconnectedAndHealthy	No
Server4\DB1	4	10	0	Crawling	Healthy	No

Sorting the available copies based on their copy queue lengths (using Activation Preference if necessary) results in the following ordered list:

- Server3\DB1
- Server2\DB1
- Server4\DB1

Out of this list, only two database copies meet the first set of criteria for activation:

- The copy on Server3, which has a database state of Disconnectedandhealthy, a copy queue length less than 10, a replay queue length less than 50, and a healthy content index.
- The copy on Server2, which has a database state of Healthy, a copy queue length less than 10, a replay queue length less than 50, and a healthy content index.

Of these two, the copy on Server3 has the lowest copy queue length; therefore, Server3 is selected as the copy to attempt to activate since it has the least amount of missing data.

After the copy on Server3 is activated, the Microsoft Exchange Replication service on the Server3 performs the ACLL process and attempts to copy any missing log files from the previous active server (in this case, Server1). When the ACLL process has completed, the PAM is notified of the results of the ACLL process. If all logs are successfully copied, then the database will be marked as the active copy and will be mounted with zero data loss.

If one or more logs are missing, the value for the AutoDatabaseMountDial parameter is consulted. If the data loss is within the configured value, then the database will be marked as the active copy and will be mounted with data loss. The majority of any missing data would then be recovered from the transport dumpster.

If Active Manager does send a mount request to the Information Store and the mount operation is unsuccessful, Active Manager will go back to the above sorted list and attempt to activate the next best copy (in this case, Server2).

Example 2: Two Copies with Same Copy Queue Length

In this example, there are four copies of mailbox database DB2. DB2 is currently active on Server1, which experiences a hardware failure. The following table shows the current status of the database copies of DB2 on Server2, Server3 and Server4.

Database Copy	Activation Preference	Copy Queue Length	Replay Queue Length	Content Index State	Database State	Activation Blocked
Server2\DB2	2	2	0	Healthy	Healthy	No
Server3\DB2	3	2	2	Healthy	DisconnectedAndHealthy	No
Server4\DB2	4	10	0	Crawling	Healthy	No

Sorting the available copies based on their copy queue lengths (using Activation Preference if necessary) results in the following ordered list:

- Server2\DB2
- Server3\DB2
- Server4\DB2

Out of this list, only two database copies meet the first set of criteria for activation:

- The copy on Server2, which has a database state of Healthy, a copy queue length less than 10, a replay queue length less than 50, and a healthy content index.
- The copy on Server3, which has a database state of DisconnectedandHealthy, a copy queue length less than 10, a replay queue length less than 50, and a healthy content index.

Of these two, the copy on Server2 has a copy queue length equal to the copy on Server3, but it also has a lower Activation Preference value; therefore, the copy on Server2 is on the top of the list and is selected as the copy to attempt to activate since it has the least amount of missing data and the lowest Activation Preference value.

Example 3: Copies with Identical Database State and Different Content Index State

In this example, there are four copies of mailbox database DB3. DB3 is currently active on Server1, which experiences a hardware failure. The following table shows the current status of the database copies of DB3 on Server2, Server3 and Server4.

Database Copy	Activation Preference	Copy Queue Length	Replay Queue Length	Content Index State	Database State	Activation Blocked
Server2\DB3	2	0	3	Crawling	Healthy	No
Server3\DB3	3	0	3	Healthy	DisconnectedAndHealthy	No

Server4\DB3	4	0	0	Healthy	Healthy	No

Sorting the available copies based on their copy queue lengths (using Activation Preference if necessary) results in the following ordered list:

- Server2\DB3
- Server3\DB3
- Server4\DB3

All three of the database copies hosted on the above servers meet the criteria for activation. Although Server2 has a lower Activation Preference value, its content index state is Crawling; as a result, when Active Manager checks the list against the first set of criteria (which includes a content index status of Healthy), the database copy on Server3 will be preferred, as it's content index state is Healthy.

Example 4: Effect of AutoDatabaseMountDial on Best Copy Selection

In this example, there are four copies of mailbox database DB4. DB4 is currently active on Server1, which experiences a failure that causes it to reboot. The following table shows the current status of the database copies of DB4 on Server2, Server3 and Server4. The *AutoDatabaseMountDial* parameter for all Mailbox servers in the DAG is configured for Lossless (copy queue length is 0).

Database Copy	Activation Preference	Copy Queue Length	Replay Queue Length	Content Index State	Database State	Activation Blocked
Server2\DB4	2	0	4523	Healthy	Healthy	No
Server3\DB4	3	100	25	Crawling	Healthy	No
Server4\DB4	4	6	62	Healthy	Healthy	No

Because the automatic database mount dial setting is set to Lossless, Active Manager uses Activation Preference instead of copy queue length as the primary sorting key. Sorting the available copies based on their Activation Preference results in the following ordered list:

- Server2\DB4
- Server3\DB4
- Server4\DB4

None of the databases meet the first, second or third set of criteria, but the database copy on Server3 does meet the fourth set of criteria (it has a content index state of Crawling and a replay queue length less than 50). The database copy on Server3 has a copy queue length of 100, but because Server1 has not finished rebooting, the ACLL process is unable to copy these missing logs files to Server3. The ACLL process tells the PAM that the amount of missing data is not within the configured value for the *AutoDatabaseMountDial* parameter, and this causes the PAM to select the next best available copy.

In the above scenario, the database copies on Server2 and Server4 match the sixth set of criteria (they have a healthy database and content index, and a copy queue length less than 10). As it is higher in the sorted listed of available copies, the database copy on Server2 is tried next. The ACLL process runs on Server2, but Server1 is still not communicating on the network, and ACLL is unable to copy any logs. But because the copy queue length is within the configured value for the *AutoDatabaseMountDial* parameter, ACLL sends a success message to the PAM and the PAM issues a database mount request via RPC.

Understanding Datacenter Activation Coordination Mode

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-01*

Datacenter Activation Coordination (DAC) mode is a property setting for a database availability group (DAG). DAC mode is disabled by default and should be enabled for all DAGs with two or more members that use continuous replication. DAC mode shouldn't be enabled for DAGs in third-party replication mode unless specified by the third-party vendor.

If a catastrophic failure occurs that affects the DAG (for example, a complete failure of one of the datacenters), DAC mode is used to control the startup database mount behavior of a DAG. When DAC mode isn't enabled, and a failure occurs that affects multiple servers in the DAG, when a majority of the DAG members are restored after the failure, the DAG will restart and attempt to mount databases. In a multi-datacenter configuration, this behavior could cause *split brain syndrome*, a condition that occurs when all networks fail, and DAG members can't receive heartbeat signals from each other. Split brain syndrome can also occur when network connectivity is severed between the datacenters. Split brain syndrome is prevented by always requiring a majority of the DAG members (and in the case of DAGs with an even number of members, the DAG's witness server) to be available and interacting for the DAG to be operational. When a majority of the members are communicating, the DAG is said to have quorum.

For example, consider a scenario where the first datacenter contains two DAG members and the witness server, and the second datacenter contains two other DAG members. If the first datacenter loses power and you activate the DAG in the second datacenter (for example, by activating the alternate witness server in the second datacenter), if the first datacenter is restored without network connectivity to the second datacenter, the active databases within the DAG may enter a split brain condition.

How DAC Mode Works

DAC mode is designed to prevent split brain from occurring by including a protocol called Datacenter Activation Coordination Protocol (DACP). After a catastrophic failure, when the DAG recovers, it won't automatically mount databases even though the DAG has a quorum. Instead DACP is used to determine the current state of the DAG and whether Active Manager should attempt to mount the databases.

You might think of DAC mode as an application level of quorum for mounting databases. To understand the purpose of DACP and how it works, it's important to understand the primary scenario it's intended to deal with. Consider the two-datacenter scenario. Suppose there is a complete power failure in the primary datacenter. In this event, all of the servers and the WAN are down, so the organization makes the decision to activate the standby datacenter. In almost all such recovery scenarios, when power is restored to the primary datacenter, WAN connectivity is typically not immediately restored. This means that the DAG members in the primary datacenter will power up, but they won’t be able to communicate with the DAG members in the activated standby datacenter. The primary datacenter should always contain the majority of the DAG quorum voters, which means that when power is restored, even in the absence of WAN connectivity to the DAG members in the standby datacenter, the DAG members in the primary datacenter have a majority and therefore have quorum. This is a problem because with quorum, these servers may be able to mount their databases, which in turn would cause divergence from the actual active databases that are now mounted in the activated standby datacenter.

DACP was created to address this issue. Active Manager stores a bit in memory (either a 0 or a 1) that tells the DAG whether it's allowed to mount local databases that are assigned as active on the server. When a DAG is running in DAC mode (which would be any DAG with three or more members), each time Active Manager starts up the bit is set to 0, meaning it isn't allowed to mount databases. Because it's in DAC mode, the server must try to communicate with all other members of the DAG that it knows to get another DAG member to give it an answer as to whether it can mount local databases that are assigned as active to it. The answer comes in the form of the bit setting for other Active Managers in the DAG. If another server responds that its bit is set to 1, it means servers are allowed to mount databases, so the server starting up sets its bit to 1 and mounts its databases.

But when you recover from a primary datacenter power outage where the servers are recovered but WAN connectivity has not been restored, all of the DAG members in the primary datacenter will have a DACP bit value of 0; and therefore none of the servers starting back up in the recovered primary datacenter will mount databases, because none of them can communicate with a DAG member that has a DACP bit value of 1.

DAC Mode for DAGs with Two Members

DAGs with two members have inherent limitations that prevent the DACP bit alone from fully protecting against application-level split brain syndrome. For DAGs with only two members, DAC mode also uses the boot time of the DAG's alternate witness server to determine whether it can mount databases on startup. The boot time of the alternate witness server is compared to the time when the DACP bit was set to 1.

- If the time the DACP bit was set is earlier than the boot time of the alternate witness server, the system assumes that the DAG member and witness server were rebooted at the same time (perhaps because of power loss in the primary datacenter), and the DAG member isn't permitted to mount databases.
- If the time that the DACP bit was set is more recent than the boot time of the alternate witness server, the system assumes that the DAG member was rebooted for some other reason (perhaps a scheduled outage in which maintenance was performed or perhaps a system crash or power loss isolated to the DAG member), and the DAG member is permitted to mount databases.

Important:

Because the alternate witness server's boot time is used to determine whether a DAG member can mount its active databases on startup, you should never restart the alternate witness server and the sole DAG member at the same time. Doing so may leave the DAG member in a state where it cannot mount databases on startup. If this happens, you must run the Restore-DatabaseAvailabilityGroup cmdlet on the DAG. This resets the DACP bit and permits the DAG member to mount databases.

Other Benefits of DAC Mode

In addition to preventing split brain syndrome at the application level, DAC mode also enables the use of the built-in site resilience cmdlets used to perform datacenter switchovers. These include the following:

- Stop-DatabaseAvailabilityGroup
- Restore-DatabaseAvailabilityGroup
- Start-DatabaseAvailabilityGroup

Performing a datacenter switchover for DAGs that are not in DAC mode involves using a combination of Exchange tools and cluster management tools.

For more information about datacenter switchovers, see Datacenter Switchovers.

Enabling DAC Mode

DAC mode can be enabled only by using the Exchange Management Shell. Specifically, you can use the Set-DatabaseAvailabilityGroup cmdlet to enable and disable DAC mode, as illustrated in the following example.

```
Set-DatabaseAvailabilityGroup -Identity DAG2 -DatacenterActivationMode DagOnly
```

In the preceding example, a DAG named DAG2 is enabled for DAC mode.

For more information about enabling DAC mode, see Configure Database Availability Group Properties and Set-DatabaseAvailabilityGroup.

1.10.1.1.3 Database Availability Group Design Examples

Database Availability Group Design Examples

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-10-01*

The ability of a database availability group (DAG) to contain as many as 16 Mailbox servers, combined with the ability to extend a DAG across multiple physical locations and Active Directory sites, provides a large number of architectural design possibilities for DAGs.

You can use design examples for DAGs in a variety of environments:

- Two-member DAG, which is suited for small office and branch office deployments
- Four-member DAG that provides high availability within a single datacenter by locating all members in the same datacenter
- Four-member DAG that provides high availability within a single datacenter, and site resilience for that datacenter, by locating two of the members in the primary datacenter and two of the members in a second datacenter

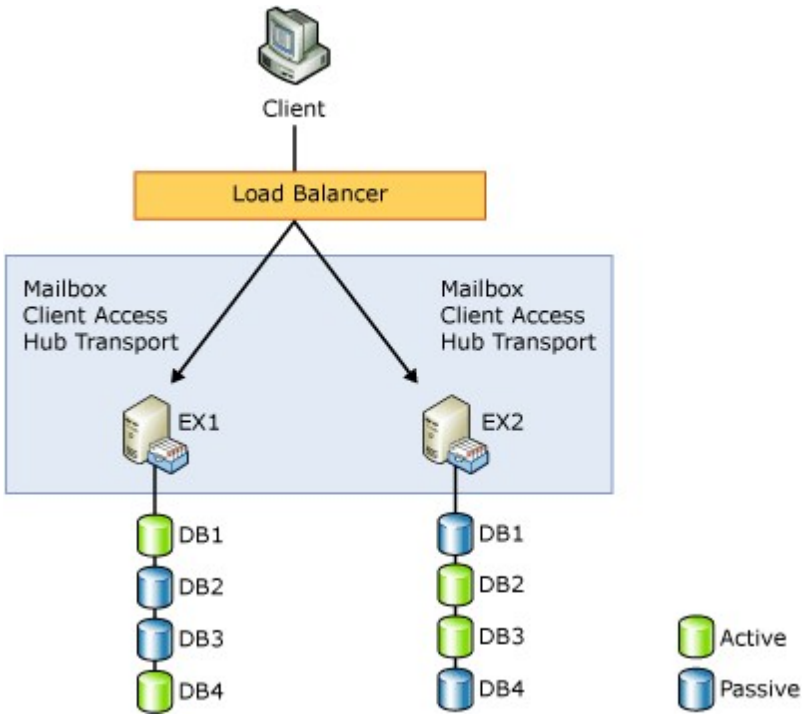
The design you use for your DAGs and the distribution of mailbox database copies will be based on your organization's service level agreements (SLAs) and the recovery time objective and recovery point objective for the mailbox service and data as stated in those SLAs.

Contents

Looking for management tasks related to high availability and site resilience? See Managing High Availability and Site Resilience.

Two-Member DAG in Single Datacenter/ Active Directory Site

A two-member DAG is the smallest possible DAG that can provide high availability. Two-member DAGs are best suited for organizations that require some form of high availability for mailbox services and data, but that don't require site resilience. This configuration works especially well in small office and branch office deployments because it enables redundancy for the Client Access, Mailbox, and Hub Transport server roles using only two Exchange servers. The following figure illustrates this configuration.



There are several aspects worth noting about this configuration:

- In this design, only the Client Access, Mailbox, and Hub Transport server roles are co-located. Although it's supported to co-locate the Unified Messaging server role, we don't recommend that configuration for performance reasons.
- To achieve high availability for Client Access and Hub Transport server roles, some form of load balancing should be used between the clients and those server roles. Because these server roles are co-located with a Mailbox server that's a member of a DAG, Windows Network Load Balancing can't be used (because Network Load Balancing and Windows failover clustering can't be installed on the same server). Instead, a non-Windows Network Load Balancing solution must be used (for example, a hardware load balancer or a third-party software-based load balancer).
- As with all DAGs that contain an even number of members, a two-member DAG requires a witness server to maintain quorum. The witness server (not pictured) is a Windows server that isn't and will never be a member of the DAG. For example, smaller organizations that use this configuration may use a file server or a directory server as the witness server. Quorum is maintained as long as more than half of the quorum voters are available and in communication. A two-member DAG with a witness server provides three quorum voters. (Each DAG member and the witness server can vote whenever

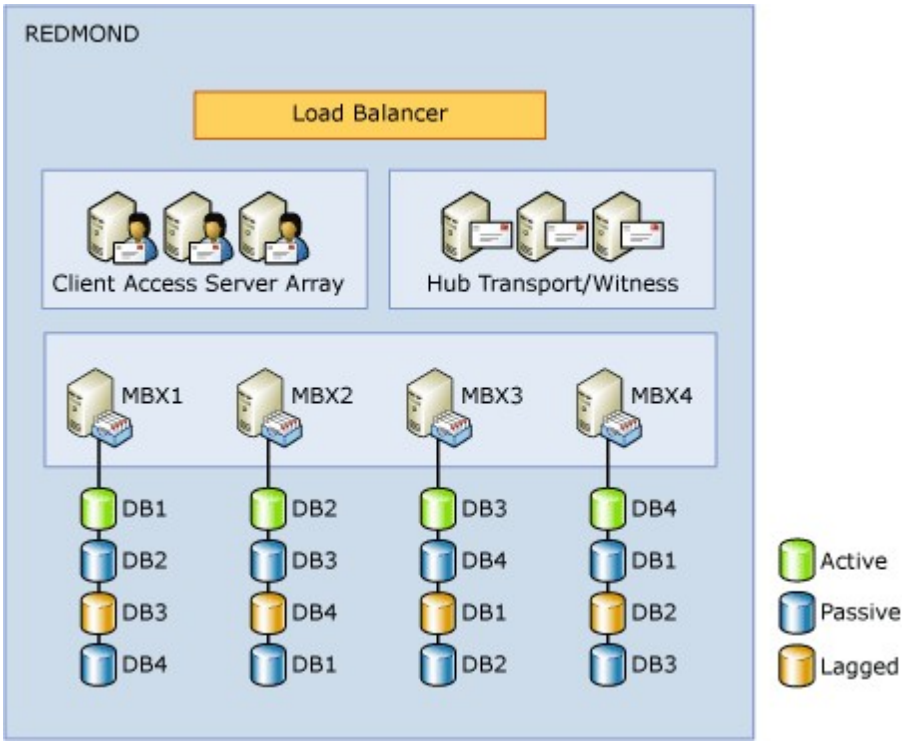
they are available and in communication.) Therefore, a two-member DAG can survive the failure or outage of a single voter (for example, either of the DAG members, or just the witness server) without an interruption in service. However, the loss of two of the voters (for example, a DAG member and the witness server) will result in a loss of quorum, which will result in an interruption in service.

Return to top

Four-Member DAG in Single Datacenter/ Active Directory Site

A four-member DAG in a single datacenter deployment provides greater resilience to failures than a two-member or three-member DAG. Larger DAGs inherently provide greater resilience because they can sustain more failures without an interruption in service. Whereas a two-member or three-member DAG can sustain the loss of only a single voter without losing quorum and compromising service, a four-member DAG, which by definition has five quorum voters, can sustain the loss of two voters without losing quorum and compromising service.

The following figure illustrates a four-member DAG with all members located in a single datacenter.



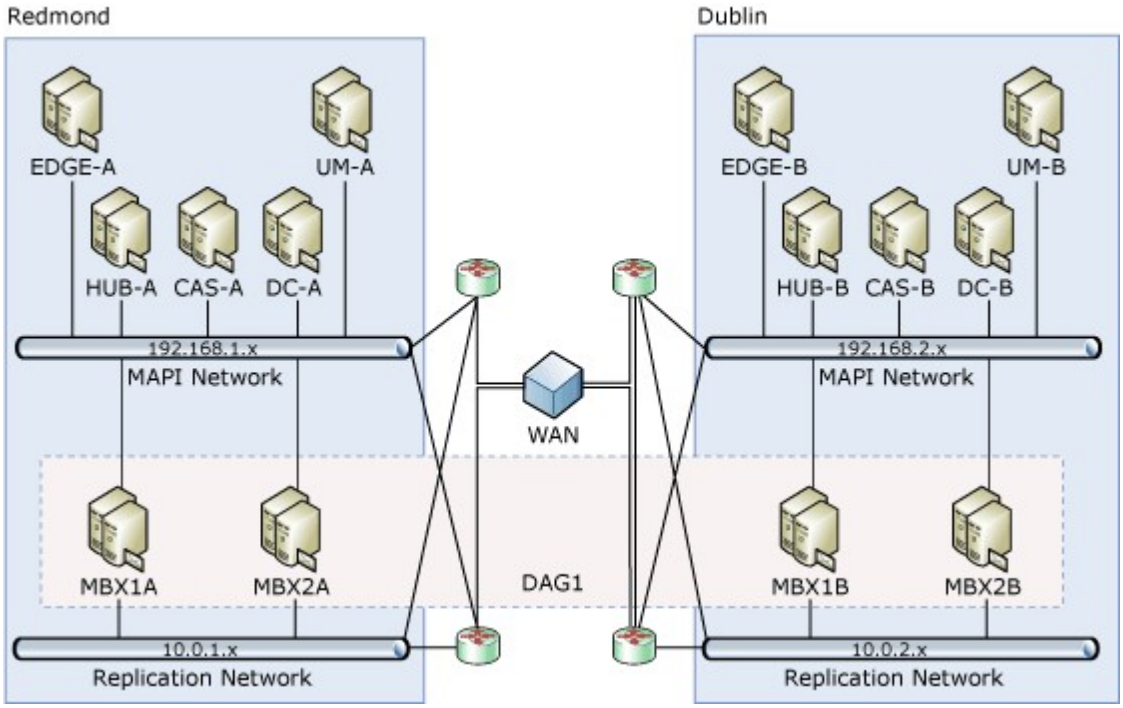
Using a four-member DAG, you can create a maximum of four copies of each database. This is a sufficient number of database copies to enable the use of alternate data protection scenarios, such as flexible mailbox protection. Flexible mailbox protection enables you to combine the Microsoft Exchange Server 2010 high availability and Extensible Storage Engine (ESE) resilience features with other built-in protection features, such as lagged mailbox database copies, retention policies, the Recoverable Items folder, and the hold policy, to create a solution that can reduce the need for other forms of protection, such as using Redundant Array of Independent Disks (RAID) or making data

backups. For more information about flexible mailbox protection, see Understanding Backup, Restore and Disaster Recovery. For more information about using replication for your backups and using just a bunch of disks (JBOD), see Mailbox Server Storage Design.

Return to top

Four-Member DAG in Two Datacenter/ Active Directory Sites

A four-member DAG extended across two datacenters provides both datacenters high availability and site resilience for the mailbox services and data. This configuration is illustrated in the following figure.



There are several aspects worth noting about this configuration:

- The witness server for the DAG should be located in the primary datacenter. Generally, the primary datacenter is the datacenter containing the majority of the user population. Using a witness server in the primary datacenter enables continued functionality for the majority of the user population in the event of a wide area network (WAN) outage. You can use multiple DAGs to eliminate the WAN as a single point of failure and to allow service and data access to remain functional for multiple datacenters in the event of a WAN outage. For more information, see the next example.
- There's no direct routing that allows traffic from the replication network on one DAG member server to the MAPI network on another DAG member server, or the reverse, or between multiple replication networks in the DAG. For example, you would want to block traffic between the MAPI network on each DAG member and the replication networks on each other DAG network. (In the previous figure, the MAPI network on MBX1A shouldn't have any network connectivity with the replication networks on MBX1B or MBX2B.) You can use router access control lists (ACLs) to block this traffic. In addition, if you're using Dynamic Host Configuration Protocol (DHCP) for the replication network, you

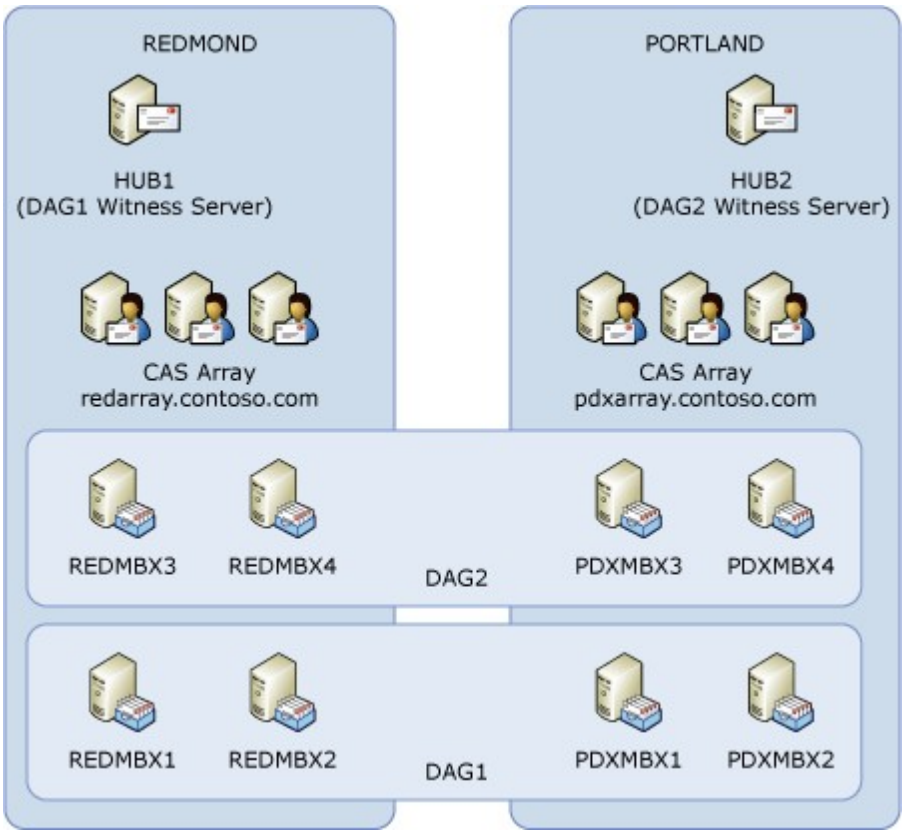
can use DHCP to configure static routes for the DAG members.
- Because this DAG configuration is intended to provide site resilience, the Time to Live (TTL) value for the Exchange client access namespaces (Microsoft Office Outlook Web App, Autodiscover, Microsoft Exchange ActiveSync, Outlook Anywhere, POP3, IMAP4, SMTP, and the RPC Client Access array) should be set to 5 minutes in both the internal and external DNS zones.
- In this example, the Exchange server roles are deployed on dedicated hardware. Because the Client Access and Hub Transport server roles aren't co-located with the Mailbox server in the DAG, Windows Network Load Balancing is used to load balance the Client Access and Hub Transport server roles.

Return to top

Two Four-Member DAGs in Two Datacenter/Active Directory Sites

As illustrated in the previous example, using a single four-member DAG extended across two datacenters can provide high availability and site resilience for the mailbox services and data. However, if a WAN outage occurs, only the primary datacenter retains service because it contains the majority of the voters. The datacenter with the minority of voters loses majority, and the DAG members in that datacenter lose quorum and go offline.

To deploy highly available Mailbox servers in a multiple datacenter environment, where each datacenter is actively serving a local user population, we recommend that you deploy multiple DAGs, where each DAG has a majority of voters in a different datacenter, as illustrated in the following figure.



Because DAG1 and DAG2 contain an even number of members, they use a witness server.

Although multiple DAGs can use the same witness server, multiple witness servers in separate datacenters are used to maintain service to each datacenter's local user population in the event of a WAN outage.

Users located in Portland would have their active mailbox database located on PDXMBX3 and/or PDXMBX4, with passive database copies on REDMBX3 and/or REDMBX4. Similarly, users located in Redmond would have their active mailbox database located on REDMBX1 and/or REDMBX2, with passive database copies on PDXMBX1 and/or PDXMBX2. If all network connectivity is lost between Redmond and Portland, the following occurs:

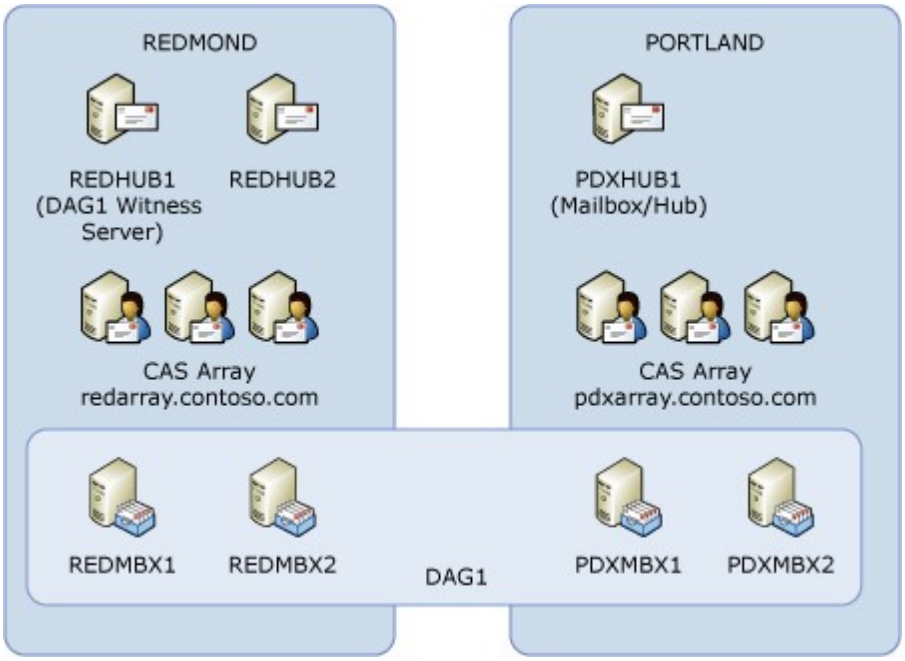
- For DAG1, members REDMBX1 and REDMBX2 would be in the majority and would continue to service users in the Redmond datacenter because they can communicate with the DAG1's witness server, HUB1.
- For DAG2, members PDXMBX3 and PDXMBX4 would be in the majority and would continue to service users in the Portland datacenter because they can communicate with DAG2's witness server, HUB2.

Return to top

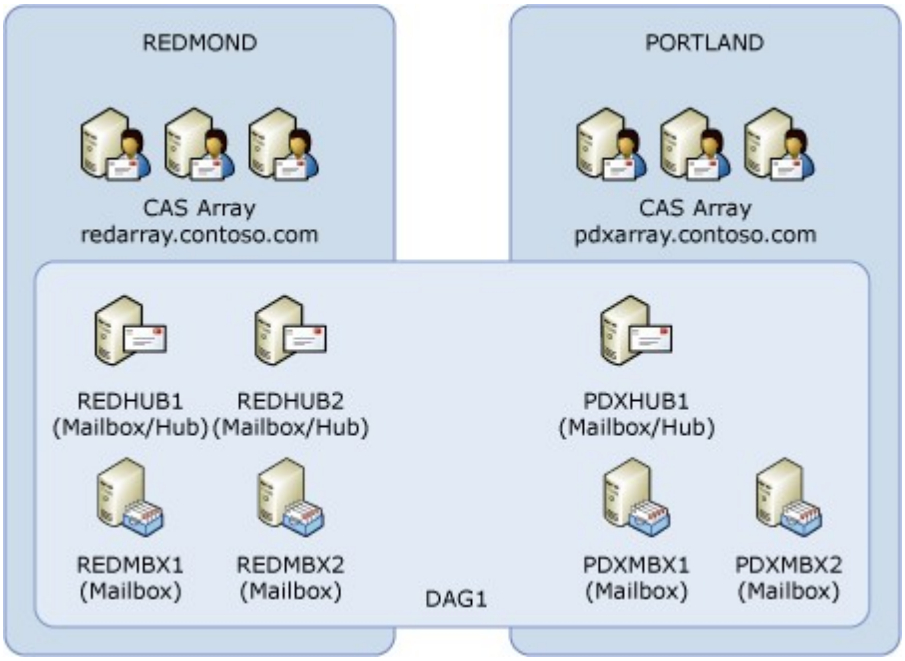
Using Mailbox Servers That Don't Contain Databases in a DAG for Additional Votes

As previously mentioned, larger DAGs inherently provide greater resilience because they can sustain more failures without an interruption in service. One design strategy that can help increase resilience when dealing with DAG member failures is to leverage the existing Hub Transport servers in the DAG's primary datacenter. This strategy involves adding the Mailbox server role (without any databases or database copies) to the Hub Transport server, and then adding that server to the DAG. In this scenario, the Mailbox server role is being used only for voting and quorum purposes. The more voters in a DAG, the more voter failures the DAG can sustain and still maintain quorum.

For example, consider a four-member DAG extended across two datacenters. The primary datacenter contains two DAG members and the witness server, and a second datacenter contains two DAG members. As illustrated in the following figure, there are five quorum voters. Therefore, this DAG can lose two voters and still maintain quorum. If the DAG loses a third voter, it loses quorum and requires manual administrative intervention to restore service.



Using the same servers in this example, you can add the Mailbox server role to the Hub Transport servers REDHUB1, REDHUB2, and PDXHUB1, and then add these servers to DAG1 (assuming these servers are capable of running Windows failover clustering).



At this point, you don't create any production mailbox databases on these servers. You also don't replicate any database copies to these servers. In this configuration, you can delete the default mailbox database and stop the Microsoft Exchange Information Store service (which can also be optionally disabled).

Note:

Although the Microsoft Exchange Information Store service isn't needed for a Mailbox server that doesn't contain a database to participate in quorum voting, the Microsoft

Exchange Replication service must be running for the Mailbox server to participate in quorum and DAG functions.

After the Mailbox servers that don't contain databases are added as members of the DAG, they become participants in quorum for the DAG. In this configuration, DAG1 now has seven quorum voters. As a result, it can lose three servers and still maintain quorum.

Return to top

1.10.1.1.4 Database Copy Layout Design

Database Copy Layout Design

High Availability and Site Resilience > Understanding High Availability and Site Resilience > Understanding Database Availability Groups >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-11*

When designing a highly available solution for Mailbox servers, you need to ensure high availability for a variety of infrastructure components, including:

- Infrastructure services, such as Active Directory and Domain Name System (DNS)
- Database availability group (DAG) member servers
- Individual storage components, such as disks, storage controllers, and storage shelves
- Individual network components, such as routers, switches, and aggregators
- Server and storage racks
- Power buses
- Datacenters

Each of these component areas represents potential points of failure, which are sometimes referred to as *failure domains*. As a result, the availability level of your DAG ultimately depends on how you design the solution to isolate and minimize the negative effects that a failure in one of these domains can have on your DAG environment. To achieve independence between failure domains, each failure domain must have one copy of the database. In addition, because a failure would result in multiple copies being unavailable, no more than one copy is required per failure domain.

For example, consider a scenario in which you have two copies of a database. Each copy is stored on a separate set of disks but both are located within the same storage array. If the storage array fails or becomes unavailable for any reason, both copies would be unavailable. In this example, the failure domain is the storage array. Only a single copy of each mailbox database should reside on the array. Otherwise, if the array fails, multiple (perhaps all) copies of the database will be unavailable.

When planning your mailbox architecture, consider the following additional design points:

- Will you deploy multiple database copies?
- How many database copies will you deploy?
- Will you have a site-resilient architecture?
- What kind of Mailbox server resiliency model will you deploy?
- How many Mailbox servers will you deploy?
- What backup model will you utilize?
- What storage architecture will you utilize?

For detailed information about how to plan for these questions, see Understanding High

Availability Factors.

Contents

Looking for management tasks related to high availability and site resilience? See Managing High Availability and Site Resilience.

Unbalanced Database Copy Layouts

To understand how the database copies should be distributed within a DAG, consider a DAG design that Contoso, Ltd is planning for their highly available Mailbox server solution. Contoso is building a DAG comprised of:

- 4 Mailbox servers
- 20 mailbox databases
- 2 copies of each mailbox database

All servers are deployed in a single datacenter, each server has its own dedicated storage, and each server is deployed in its own server rack.

Contoso requires that two highly available database copies (for example, non-lagged) be available at all times, and that the solution survive two simultaneous DAG member outages without negatively affecting the availability of the databases.

Based on these requirements, the database copy layout used is shown in the following figure.

	Server1	Server2	Server3	Server4
DB1	Active			Passive
DB2	Active			Passive
DB3	Active			Passive
DB4	Active			Passive
DB5	Active			Passive
DB6		Active	Passive	
DB7		Active	Passive	
DB8		Active	Passive	
DB9		Active	Passive	
DB10		Active	Passive	
DB11		Passive	Active	
DB12		Passive	Active	
DB13		Passive	Active	
DB14		Passive	Active	
DB15		Passive	Active	
DB16	Passive			Active
DB17	Passive			Active
DB18	Passive			Active
DB19	Passive			Active
DB20	Passive			Active

Initially, the design looks sound because it spreads the active copies of each database across the four DAG members. However, there are concerns with this design. The layout isn't optimal from a server resource perspective. For example, when a single server fails, it results in an uneven distribution of databases, as shown in the following figure.

	Server1	Server2	Server3	Server4
DB1	Active			
DB2	Active			
DB3	Active			
DB4	Active			
DB5	Active			
DB6		Active	Passive	
DB7		Active	Passive	
DB8		Active	Passive	
DB9		Active	Passive	
DB10		Active	Passive	
DB11		Passive	Active	
DB12		Passive	Active	
DB13		Passive	Active	
DB14		Passive	Active	
DB15		Passive	Active	
DB16	Active			
DB17	Active			
DB18	Active			
DB19	Active			
DB20	Active			

The failure of Server4 results in databases DB16 through DB20 being activated on Server1, instead of being distributed across the remaining three servers. The result is an uneven distribution of activated mailbox databases and an uneven utilization of server resources. Compared to the other two remaining servers (Server2 and Server3), the utilization of Server1 doubled.

Another concern is the DAG doesn't contain enough copies to survive two simultaneous server outages in all cases. Another server failure could result in 50 percent of the databases being unavailable. If Server1 and Server4 fail or become unavailable within

moments of each other, 10 databases would be unavailable, as shown in the following figure.

	Server1	Server2	Server3	Server4
DB1				
DB2				
DB3				
DB4				
DB5				
DB6		Active	Passive	
DB7		Active	Passive	
DB8		Active	Passive	
DB9		Active	Passive	
DB10		Active	Passive	
DB11		Passive	Active	
DB12		Passive	Active	
DB13		Passive	Active	
DB14		Passive	Active	
DB15		Passive	Active	
DB16				
DB17				
DB18				
DB19				
DB20				

This design doesn't meet the core requirement of being able to survive a double server failure. To survive a double server failure and maintain all active databases, a third copy must be deployed, and a new layout must be devised.

Return to top

Designing a Balanced Database Copy Layout

Designing a balanced database copy layout may require you to revisit several design decisions to derive the optimal design. Use the following design principles when planning the database copy layout:

- Make sure that you minimize multiple database copy failures of a mailbox database by isolating each copy from one another and placing them in different failure domains. For example, don't place more than a single database copy of a specific mailbox database within the same server rack or in the same storage array.
- Lay out the database copies in a consistent, distributed fashion to make sure that the active mailbox databases are evenly distributed after a failure. The sum of the activation preferences of each database copy on any specific server must be equal or close to equal. This results in an approximately equal distribution after failure, assuming replication is healthy and up to date.

Building Blocks

To adhere to the previous design principles, we recommend placing the database copies in a particular arrangement that ensures all active copies are symmetrically distributed across as many servers as possible. The arrangement of database copies is based on a *building block* concept.

The first building block (known as the level 1 building block) is based on the number of Mailbox servers that will host active database copies. Assume this number is *N*. *N* defines not only the number of Mailbox servers, but also the number of databases within the building block. One active database copy is distributed on each server, forming a diagonal pattern. As in the previous example, there are 4 Mailbox servers and 20 mailbox databases. The size of the first level 1 building block is 4, as shown in the following figure.

		Server1	Server2	Server3	Server4
Level 1 Building Block Set 1	DB1	Active			
	DB2		Active		
	DB3			Active	
	DB4				Active

The same pattern is repeated for each remaining level 1 building block set. Because there are 20 databases, there are five level 1 building block sets, as shown in the following figure.

	Server1	Server2	Server3	Server4
DB1	Active			
DB2		Active		
DB3			Active	
DB4				Active
DB5	Active			
DB6		Active		
DB7			Active	
DB8				Active
DB9	Active			
DB10		Active		
DB11			Active	
DB12				Active
DB13	Active			
DB14		Active		
DB15			Active	
DB16				Active
DB17	Active			
DB18		Active		
DB19			Active	
DB20				Active

When you add a second database copy, you place it differently for each building block set. Because one server already hosts the active copy, there are $N - 1$ servers available to host the second database copy. As you use each of these $N - 1$ servers once, you have a complete symmetric distribution that forms the new larger building block. Therefore, the new building block (known as the level 2 building block) size becomes $N \times (N - 1)$ databases. This means that the second database copy for the first database is placed on the second server, and each second copy thereafter is deployed in a diagonal pattern within the building block. After the pattern is completed within the first level 1 building block set, the starting position of the second copy for the next block is offset by one so

the second copy starts on the third server.

In the example, the building block size now becomes 4 × (4 – 1) = 4 × 3 = 12, which means that 12 databases make up each level 2 building block set. For the level 1 building block set 1 (DB1 through DB4), the second copy for DB1 is placed on Server2, while for the level 1 building block set 2 (DB5 through DB8), the second copy for DB5 is placed on Server3. The placement of the starting server for each level 1 building block set is offset from the previous level 1 building block set by one server. This layout is continued by placing the second copy of DB9 on Server4. This ensures that a Server1 failure activates second copies across all three remaining servers rather than activating multiple databases on the same server.

			Server1	Server2	Server3	Server4
Level 2 Building Block (4 x 3 = 12) Set 1	Level 1 Building Block Set 1	DB1	Active	Passive		
		DB2		Active		
		DB3			Active	
		DB4				Active
	Level 1 Building Block Set 2	DB5	Active		Passive	
		DB6		Active		
		DB7			Active	
		DB8				Active
	Level 1 Building Block Set 3	DB9	Active			Passive
		DB10		Active		
		DB11			Active	
		DB12				Active

This pattern is repeated for each remaining second building block set. Because there are 20 databases, there are two level 2 building block sets in this example. Note that the second copy for DB13 is placed on Server2.

			Server1	Server2	Server3	Server4
Level 2 Building Block (4 x 3 = 12) Set 2	Level 1 Building Block Set 4	DB13	Active	Passive		
		DB14		Active		
		DB15			Active	
		DB16				Active
	Level 1 Building Block Set 5	DB17	Active		Passive	
		DB18		Active		
		DB19			Active	
		DB20				Active

To understand this logic better, compare database copy placement for DB1, DB5, and DB9. These databases each have an active copy hosted on Server1. If Server1 fails, you want to have second database copies activated on different remaining servers to achieve equal load distribution. You can achieve this by placing a second database copy of DB1 on Server2, a second database copy of DB5 on Server3, and a second database copy of DB9

on Server4. Starting with DB13, you simply repeat the pattern. The remaining database copies are added in a diagonal pattern, as shown in the following figure.

	Server1	Server2	Server3	Server4
DB1	Active	Passive		
DB2		Active	Passive	
DB3			Active	Passive
DB4	Passive			Active
DB5	Active		Passive	
DB6		Active		Passive
DB7	Passive		Active	
DB8		Passive		Active
DB9	Active			Passive
DB10	Passive	Active		
DB11		Passive	Active	
DB12			Passive	Active
DB13	Active	Passive		
DB14		Active	Passive	
DB15			Active	Passive
DB16	Passive			Active
DB17	Active		Passive	
DB18		Active		Passive
DB19	Passive		Active	
DB20		Passive		Active

Note that the second building block (DB13 through DB20) contains only 8 databases, not 12. As a result, this design won't be entirely symmetrical if a single failure occurs. To provide a fully symmetric distribution, plan your architecture so the number of databases is a multiple of the largest building block size. (In this example, optimal numbers are 24, 36, 48, or 60 databases, and so on.)

As you add a third database copy, again you must place it differently for each group of

now $N \times (N - 1)$ databases. Because you now have only $N - 2$ servers available from which to select for the third database copy placement, this generates $N - 2$ variations. The new building block (known as the level 3 building block) becomes $N \times (N - 1) \times (N - 2)$ databases. Therefore, the third database copy for the first database is placed on the third server, and each third copy thereafter is deployed in a diagonal pattern according to the starting position within this new building block. After the pattern is completed within the first level 1 building block set, the starting position is offset by one so that the third copy is placed in the fourth position.

In this example, the building block now becomes $4 \times (4 - 1) \times (4 - 2) = 4 \times 3 \times 2 = 24$, which means that 24 databases make up each level 3 building block set. To produce the symmetric database placement pattern, place the third database copy of DB1 on Server3 (which is the first available server because Server1 hosts the first copy and Server2 hosts the second copy), and offset each additional copy by one until you reach the end of the level 1 building block set 1. For the next building block set, again place the third database copy on the next available server (Server4) and continue in the same manner until you reach DB12, which marks the end of the level 2 building block set 1. For DB13 through DB20, follow the same pattern but offset the third database copy placement by one so it doesn't end up on the same servers as DB1 through DB12.

				Server1	Server2	Server3	Server4
Level 3 Building Block (4x3x2 = 24)	Level 2 Building Block (4x3 = 12) Set 1	Level 1 Building Block Set 1	DB1	Active	Passive1	Passive2	
			DB2		Active	Passive1	Passive2
			DB3	Passive2		Active	Passive1
			DB4	Passive1	Passive2		Active
		Level 1 Building Block Set 2	DB5	Active		Passive1	Passive2
			DB6	Passive2	Active		Passive1
			DB7	Passive1	Passive2	Active	
			DB8		Passive1	Passive2	Active
		Level 1 Building Block Set 3	DB9	Active	Passive2		Passive1
			DB10	Passive1	Active	Passive2	
			DB11		Passive1	Active	Passive2
			DB12	Passive2		Passive1	Active
	Level 2 Building Block (4x3 = 12) Set 2	Level 1 Building Block Set 4	DB13	Active	Passive1		Passive2
			DB14	Passive2	Active	Passive1	
			DB15		Passive2	Active	Passive1
			DB16	Passive1		Passive2	Active
		Level 1 Building Block Set 5	DB17	Active	Passive2	Passive1	
			DB18		Active	Passive2	Passive1
			DB19	Passive1		Active	Passive2
			DB20	Passive2	Passive1		Active

Again, to understand this logic better, compare database copy placement for databases

DB1 through DB13. These databases have the active database copy hosted on Server1, and the second database copy hosted on Server2. If these servers fail, you want to have the third database copies activated on different remaining servers to achieve equal load distribution. You can achieve this by placing the third database copy of DB1 on Server3 and the third database copy of DB13 on Server4. Similar pairs are formed by DB2 and DB14, DB3 and DB15, and so on. Starting with DB25, you simply repeat the pattern (this example doesn't address that many databases).

Note that the third building block (DB1 through DB20) contains only 20 databases, not 24 databases. As a result, this design won't be entirely symmetrical if double failures occur. Again, to provide a fully symmetric distribution, plan your architecture so the number of databases is a multiple of the largest building block size. (In this example, the optimal numbers are 24, 48, or 72 databases, and so on.)

As you add a fourth database copy, again you must place it differently for each group of now $N \times (N - 1) \times (N - 2)$ databases. The new building block becomes $N \times (N - 1) \times (N - 2) \times (N - 3)$ databases. This follows the same logical approach and ensures that the database distribution is even within the new building block in case three servers fail.

The example of four servers leaves only one variation for placing the fourth database copy (only one remaining server is available). Therefore, the building block size actually remains at 24. This is also apparent when using the formula for building block size: $4 \times 3 \times 2 \times (4 - 3) = 4 \times 3 \times 2 \times 1 = 24$.

As you continue to add more database copies, the building block keeps growing such that the general formula for the building block size is $Perm(N,M) = N \times (N - 1) \ldots (N - M + 1) = N!/(N - M)! = C(N,M)$, where N = number of servers and M = number of database copies. This becomes obvious as you realize that complete symmetric distribution of the database copies is achieved by selecting all possible permutations of M database copies across N available servers.

There are several caveats to using this methodology:

- Deploying a number of databases that isn't a multiple of the largest building block size results in a nonsymmetrical distribution of active databases during failure events.
- Deploying architectures to mitigate multiple domain failures may result in a nonsymmetrical distribution of active databases during failure events. This is because failure domain definitions impose restraints on database copy placement, which breaks the symmetry of the pattern.
- Deploying site-resilient solutions that result in out-of-site database *over events may result in a nonsymmetrical distribution of databases activated in the secondary datacenter during primary datacenter server failure events.

Return to top

Active Database Distribution in Example Scenario During Server Failures

Using the previous example, in the event of a single server failure (for example, a failure of Server4), the active mailbox databases are distributed as shown in the following figure. The second copy is activated for DB4, DB8, DB12, DB16, and DB20, denoted as Active in orange.

	Server1	Server2	Server3	Server4
DB1	Active	Passive1	Passive2	
DB2		Active	Passive1	
DB3	Passive2		Active	
DB4	Active	Passive2		
DB5	Active		Passive1	
DB6	Passive2	Active		
DB7	Passive1	Passive2	Active	
DB8		Active	Passive2	
DB9	Active	Passive2		
DB10	Passive2	Active	Passive2	
DB11		Passive2	Active	
DB12	Passive2		Active	
DB13	Active	Passive2		
DB14	Passive2	Active	Passive2	
DB15		Passive2	Active	
DB16	Active		Passive2	
DB17	Active	Passive2	Passive1	
DB18		Active	Passive2	
DB19	Passive2		Active	
DB20	Passive2	Active		
Active Database Count	7	7	6	

If double server failure occurs (the third copy is activated for several databases and denoted as Active in green), the remaining two servers, Server1 and Server3, will have an equal number of activated mailbox databases.

	Server1	Server2	Server3	Server4
DB1	Active		Passive2	
DB2			Active	
DB3	Passive2		Active	
DB4	Active			
DB5	Active		Passive1	
DB6	Active			
DB7	Passive1		Active	
DB8			Active	
DB9	Active			
DB10	Active		Passive2	
DB11			Active	
DB12	Passive2		Active	
DB13	Active			
DB14	Passive2		Active	
DB15			Active	
DB16	Active		Passive2	
DB17	Active		Passive1	
DB18			Active	
DB19	Passive2		Active	
DB20	Active			
Active Database Count	10		10	

However, because the number of databases in this example isn't a multiple of the largest building block size (24 databases), not all double server failure events will result in a symmetrical distribution.

	Server1	Server2	Server3	Server4
DB1		Active	Passive2	
DB2		Active	Passive1	
DB3			Active	
DB4		Active		
DB5			Active	
DB6		Active		
DB7		Passive2	Active	
DB8		Active	Passive2	
DB9		Active		
DB10		Active	Passive2	
DB11		Passive1	Active	
DB12			Active	
DB13		Active		
DB14		Active	Passive1	
DB15		Passive2	Active	
DB16			Active	
DB17		Passive2	Active	
DB18		Active	Passive2	
DB19			Active	
DB20		Active		
Active Database Count		11	9	

Return to top

Design Scenarios

To understand the design principle of the database copy layout, including the associated mathematical formula, consider two other architectural layouts.

Design Scenario: Active/Passive User Distribution Site-Resilient Solution

In this scenario, Contoso decides to deploy the following architecture:

- The DAG is extended across two datacenters, operating in an active/passive user distribution model.
- Each server is deployed in a separate server rack.
- Each server's storage is isolated from the other servers' storage within the datacenter.
- There are four Mailbox servers per datacenter.
- There are a total of 24 mailbox databases.
- The desire is to have four highly available database copies and to survive a double server failure or a single datacenter failure.

In this example, the level 1 building block is 4, the databases are grouped into units of four, and the active copies are distributed across the four servers within the building block.

	Server1	Server2	Server3	Server4	Server5	Server6	Server7	Server8
DB1	COPY							
DB2		COPY						
DB3			COPY					
DB4				COPY				
DB5	COPY							
DB6		COPY						
DB7			COPY					
DB8				COPY				
DB9	COPY							
DB10		COPY						
DB11			COPY					
DB12				COPY				
DB13	COPY							
DB14		COPY						
DB15			COPY					
DB16				COPY				
DB17	COPY							
DB18		COPY						
DB19			COPY					
DB20				COPY				
DB21	COPY							
DB22		COPY						
DB23			COPY					
DB24				COPY				

For each server hosting active copies, the second database copy is distributed as evenly as possible across all remaining member servers, continuing with a diagonal pattern because each copy is isolated from one another. In this example, the level 2 building block becomes 12, which becomes the repeating set every 12 databases.

	Server1	Server2	Server3	Server4		Server5	Server6	Server7	Server8
DB1	COPY	COPY							
DB2		COPY	COPY						
DB3			COPY	COPY					
DB4	COPY			COPY					
DB5	COPY		COPY						
DB6		COPY		COPY					
DB7	COPY		COPY						
DB8		COPY		COPY					
DB9	COPY			COPY					
DB10	COPY	COPY							
DB11		COPY	COPY						
DB12			COPY	COPY					
DB13	COPY	COPY							
DB14		COPY	COPY						
DB15			COPY	COPY					
DB16	COPY			COPY					
DB17	COPY		COPY						
DB18		COPY		COPY					
DB19	COPY		COPY						
DB20		COPY		COPY					
DB21	COPY			COPY					
DB22	COPY	COPY							
DB23		COPY	COPY						
DB24			COPY	COPY					

Because this site resilient solution is for an active/passive user distribution model with an equal number of servers and database copies in both datacenters, the third database copy is placed in a diagonal pattern across Server5 and Server6, using the level 1 building block value of 4. This ensures that Server5 and Server6 mirror the first database copy placement on Server1 through Server4.

	Server1	Server2	Server3	Server4	Server5	Server6	Server7	Server8
DB1	COPY	COPY			COPY			
DB2		COPY	COPY			COPY		
DB3			COPY	COPY			COPY	
DB4	COPY			COPY				COPY
DB5	COPY		COPY		COPY			
DB6		COPY		COPY		COPY		
DB7	COPY		COPY				COPY	
DB8		COPY		COPY				COPY
DB9	COPY			COPY	COPY			
DB10	COPY	COPY				COPY		
DB11		COPY	COPY				COPY	
DB12			COPY	COPY				COPY
DB13	COPY	COPY			COPY			
DB14		COPY	COPY			COPY		
DB15			COPY	COPY			COPY	
DB16	COPY			COPY				COPY
DB17	COPY		COPY		COPY			
DB18		COPY		COPY		COPY		
DB19	COPY		COPY				COPY	
DB20		COPY		COPY				COPY
DB21	COPY			COPY	COPY			
DB22	COPY	COPY				COPY		
DB23		COPY	COPY				COPY	
DB24			COPY	COPY				COPY

Because this site resilient solution is for an active/passive user distribution model with an equal number of servers and database copies in both datacenters, the fourth database copy is placed in a diagonal pattern across Server5 and Server6, using the level 2 building block value of 12. This ensures that Server5 and Server6 mirror the second database copy placement on Server1 through Server4.

	Server1	Server2	Server3	Server4	Server5	Server6	Server7	Server8
DB1	COPY	COPY			COPY	COPY		
DB2		COPY	COPY			COPY	COPY	
DB3			COPY	COPY			COPY	COPY
DB4	COPY			COPY	COPY			COPY
DB5	COPY		COPY		COPY		COPY	
DB6		COPY		COPY		COPY		COPY
DB7	COPY		COPY		COPY		COPY	
DB8		COPY		COPY		COPY		COPY
DB9	COPY			COPY	COPY			COPY
DB10	COPY	COPY			COPY	COPY		
DB11		COPY	COPY			COPY	COPY	
DB12			COPY	COPY			COPY	COPY
DB13	COPY	COPY			COPY	COPY		
DB14		COPY	COPY			COPY	COPY	
DB15			COPY	COPY			COPY	COPY
DB16	COPY			COPY	COPY			COPY
DB17	COPY		COPY		COPY		COPY	
DB18		COPY		COPY		COPY		COPY
DB19	COPY		COPY		COPY		COPY	
DB20		COPY		COPY		COPY		COPY
DB21	COPY			COPY	COPY			COPY
DB22	COPY	COPY			COPY	COPY		
DB23		COPY	COPY			COPY	COPY	
DB24			COPY	COPY			COPY	COPY

If a single server failure occurs, the remaining three servers in the primary datacenter will have an equal number of activated mailbox databases (8 per server).

	Server1	Server2	Server3	Server4		Server5	Server6	Server7	Server8
DB1		COPY				COPY	COPY		
DB2		COPY	COPY				COPY	COPY	
DB3			COPY	COPY				COPY	COPY
DB4				COPY		COPY			COPY
DB5			COPY			COPY		COPY	
DB6		COPY		COPY			COPY		COPY
DB7			COPY			COPY		COPY	
DB8		COPY		COPY			COPY		COPY
DB9				COPY		COPY			COPY
DB10		COPY				COPY	COPY		
DB11		COPY	COPY				COPY	COPY	
DB12			COPY	COPY				COPY	COPY
DB13		COPY				COPY	COPY		
DB14		COPY	COPY				COPY	COPY	
DB15			COPY	COPY				COPY	COPY
DB16				COPY		COPY			COPY
DB17			COPY			COPY		COPY	
DB18		COPY		COPY			COPY		COPY
DB19			COPY			COPY		COPY	
DB20		COPY		COPY			COPY		COPY
DB21				COPY		COPY			COPY
DB22		COPY				COPY	COPY		
DB23		COPY	COPY				COPY	COPY	
DB24			COPY	COPY				COPY	COPY
Active Database Count		8	8	8					

If two simultaneous server failures occur, the remaining two servers in the primary datacenter will have an equal number of activated mailbox databases (10 per server), while 4 databases will be activated in the secondary datacenter.

	Server1	Server2	Server3	Server4		Server5	Server6	Server7	Server8
DB1		COPY				COPY	COPY		
DB2		COPY					COPY	COPY	
DB3				COPY				COPY	COPY
DB4				COPY		COPY			COPY
DB5						COPY		COPY	
DB6		COPY		COPY			COPY		COPY
DB7						COPY		COPY	
DB8		COPY		COPY			COPY		COPY
DB9				COPY		COPY			COPY
DB10		COPY				COPY	COPY		
DB11		COPY					COPY	COPY	
DB12				COPY				COPY	COPY
DB13		COPY				COPY	COPY		
DB14		COPY					COPY	COPY	
DB15				COPY				COPY	COPY
DB16				COPY		COPY			COPY
DB17						COPY		COPY	
DB18		COPY		COPY			COPY		COPY
DB19						COPY		COPY	
DB20		COPY		COPY			COPY		COPY
DB21				COPY		COPY			COPY
DB22		COPY				COPY	COPY		
DB23		COPY					COPY	COPY	
DB24				COPY				COPY	COPY
Active Database Count		10		10		2		2	

Design Scenario: Multiple Failure Domains

In this example, Wingtip Toys decides to deploy the following architecture:

- All servers are deployed in a single datacenter.
- Servers are grouped in units of two.
- Each of the two servers is placed in the same rack with its storage.
- There are a total of 3 racks and 6 servers.
- There are a total of 18 mailbox databases.
- The desire is to have three highly available database copies and to survive two member server failures or one rack failure.

In this example, the level 1 building block is 6, so the databases are grouped into units of 6, and the active copies are distributed across the six servers within the building block.

	Server1	Server2	Server3	Server4	Server5	Server6
DB1	COPY1					
DB2		COPY1				
DB3			COPY1			
DB4				COPY1		
DB5					COPY1	
DB6						COPY1
DB7	COPY1					
DB8		COPY1				
DB9			COPY1			
DB10				COPY1		
DB11					COPY1	
DB12						COPY1
DB13	COPY1					
DB14		COPY1				
DB15			COPY1			
DB16				COPY1		
DB17					COPY1	
DB18						COPY1
DB19	COPY1					
DB20		COPY1				
DB21			COPY1			
DB22				COPY1		
DB23					COPY1	
DB24						COPY1
DB25	COPY1					
DB26		COPY1				
DB27			COPY1			
DB28				COPY1		
DB29					COPY1	
DB30						COPY1
DB31	COPY1					
DB32		COPY1				
DB33			COPY1			
DB34				COPY1		
DB35					COPY1	

For each server hosting active copies, the second database copy is spread as evenly as possible across all remaining member servers, while also ensuring that two copies of the same database aren't placed in the same server rack. In this example, instead of the level 2 building block formula of $N \times (N - 1)$, the formula of $N \times (N - 2)$ is used to ensure two copies of the same database aren't placed in the same rack. This means that the level 2 building block is $6 \times 4 = 24$.

	Server1	Server2	Server3	Server4	Server5	Server6
DB1	COPY1		COPY2			
DB2		COPY1		COPY2		
DB3			COPY1		COPY2	
DB4				COPY1		COPY2
DB5	COPY2				COPY1	
DB6		COPY2				COPY1
DB7	COPY1			COPY2		
DB8		COPY1			COPY2	
DB9			COPY1			COPY2
DB10	COPY2			COPY1		
DB11		COPY2			COPY1	
DB12			COPY2			COPY1
DB13	COPY1				COPY2	
DB14		COPY1				COPY2
DB15	COPY2		COPY1			
DB16		COPY2		COPY1		
DB17			COPY2		COPY1	
DB18				COPY2		COPY1
DB19	COPY1					COPY2
DB20		COPY1	COPY2			
DB21		COPY2	COPY1			
DB22				COPY1	COPY2	
DB23				COPY2	COPY1	
DB24	COPY2					COPY1
DB25	COPY1		COPY2			
DB26		COPY1		COPY2		
DB27			COPY1		COPY2	
DB28				COPY1		COPY2
DB29	COPY2				COPY1	
DB30		COPY2				COPY1
DB31	COPY1			COPY2		
DB32		COPY1			COPY2	
DB33			COPY1			COPY2
DB34	COPY2			COPY1		
DB35		COPY2			COPY1	
DB36			COPY2			COPY1
DB37	COPY1				COPY2	

The third database copy is placed in a diagonal pattern across the servers, again ensuring that multiple copies of the same database aren't placed in the same server rack. In this example, instead of the level 3 building block formula $N \times (N - 2)$, the formula of $N \times (N - 2) \times (N - 4)$ is used to ensure two copies of the same database aren't placed in the same rack. This means that the level 3 building block is $6 \times 4 \times 2 = 48$.

	Server1	Server2	Server3	Server4	Server5	Server6
DB1	COPY1		COPY2		COPY3	
DB2		COPY1		COPY2		COPY3
DB3	COPY3		COPY1		COPY2	
DB4		COPY3		COPY1		COPY2
DB5	COPY2		COPY3		COPY1	
DB6		COPY2		COPY3		COPY1
DB7	COPY1			COPY2		COPY3
DB8		COPY1	COPY3		COPY2	
DB9		COPY3	COPY1			COPY2
DB10	COPY2			COPY1	COPY3	
DB11		COPY2		COPY3	COPY1	
DB12	COPY3		COPY2			COPY1
DB13	COPY1		COPY3		COPY2	
DB14		COPY1		COPY3		COPY2
DB15	COPY2		COPY1		COPY3	
DB16		COPY2		COPY1		COPY3
DB17	COPY3		COPY2		COPY1	
DB18		COPY3		COPY2		COPY1
DB19	COPY1			COPY3		COPY2
DB20		COPY1	COPY2		COPY3	
DB21		COPY2	COPY1			COPY3
DB22	COPY3			COPY1	COPY2	
DB23		COPY3		COPY2	COPY1	
DB24	COPY2		COPY3			COPY1
DB25	COPY1		COPY2			COPY3
DB26		COPY1		COPY2	COPY3	
DB27		COPY3	COPY1		COPY2	
DB28	COPY3			COPY1		COPY2
DB29	COPY2			COPY3	COPY1	
DB30		COPY2	COPY3			COPY1
DB31	COPY1			COPY2	COPY3	
DB32		COPY1		COPY3	COPY2	
DB33		COPY3	COPY1			COPY2
DB34	COPY2			COPY1		COPY3
DB35		COPY2	COPY3		COPY1	

If a single server failure occurs, the remaining five servers in the primary datacenter will have a near equal number of activated mailbox databases. Four servers will have 10 activated databases per server, while one server (the rack partner) will have 8 activated databases.

	Server1	Server2	Server3	Server4	Server5	Server6
DB1	COPY1		COPY2		COPY3	
DB2		COPY1				COPY3
DB3	COPY3		COPY1		COPY2	
DB4		COPY3				COPY2
DB5	COPY2		COPY3		COPY1	
DB6		COPY2				COPY1
DB7	COPY1					COPY3
DB8		COPY1	COPY3		COPY2	
DB9		COPY3	COPY1			COPY2
DB10	COPY2				COPY3	
DB11		COPY2			COPY1	
DB12	COPY3		COPY2			COPY1
DB13	COPY1		COPY3		COPY2	
DB14		COPY1				COPY2
DB15	COPY2		COPY1		COPY3	
DB16		COPY2				COPY3
DB17	COPY3		COPY2		COPY1	
DB18		COPY3				COPY1
DB19	COPY1					COPY2
DB20		COPY1	COPY2		COPY3	
DB21		COPY2	COPY1			COPY3
DB22	COPY3				COPY2	
DB23		COPY3			COPY1	
DB24	COPY2		COPY3			COPY1
DB25	COPY1		COPY2			COPY3
DB26		COPY1			COPY3	
DB27		COPY3	COPY1		COPY2	
DB28	COPY3					COPY2
DB29	COPY2				COPY1	
DB30		COPY2	COPY3			COPY1
DB31	COPY1				COPY3	
DB32		COPY1			COPY2	
DB33		COPY3	COPY1			COPY2
DB34	COPY2					COPY3
DB35		COPY2	COPY3		COPY1	
DB36	COPY3		COPY2			COPY1
DB37	COPY1		COPY3		COPY2	
DB38		COPY1				COPY2

If two simultaneous server failures occur (different racks), the remaining four servers will have a near equal number of activated mailbox databases.

	Server1	Server2	Server3	Server4	Server5	Server6
DB1			COPY2		COPY3	
DB2		COPY1				COPY3
DB3			COPY1		COPY2	
DB4		COPY3				COPY2
DB5			COPY3		COPY1	
DB6		COPY2				COPY1
DB7						COPY3
DB8		COPY1	COPY3		COPY2	
DB9		COPY3	COPY1			COPY2
DB10					COPY3	
DB11		COPY2			COPY1	
DB12			COPY2			COPY1
DB13			COPY3		COPY2	
DB14		COPY1				COPY2
DB15			COPY1		COPY3	
DB16		COPY2				COPY3
DB17			COPY2		COPY1	
DB18		COPY3				COPY1
DB19						COPY2
DB20		COPY1	COPY2		COPY3	
DB21		COPY2	COPY1			COPY3
DB22					COPY2	
DB23		COPY3			COPY1	
DB24			COPY3			COPY1
DB25			COPY2			COPY3
DB26		COPY1			COPY3	
DB27		COPY3	COPY1		COPY2	
DB28						COPY2
DB29					COPY1	
DB30		COPY2	COPY3			COPY1
DB31					COPY3	
DB32		COPY1			COPY2	
DB33		COPY3	COPY1			COPY2
DB34						COPY3
DB35		COPY2	COPY3		COPY1	
DB36			COPY2			COPY1
DB37			COPY3		COPY2	
DB38		COPY1				COPY2

If two simultaneous server failures occur (same rack), the remaining four servers will have an equal number of activated mailbox databases.

	Server1	Server2	Server3	Server4	Server5	Server6
DB1	COPY1				COPY3	
DB2		COPY1				COPY3
DB3	COPY3				COPY2	
DB4		COPY3				COPY2
DB5	COPY2				COPY1	
DB6		COPY2				COPY1
DB7	COPY1					COPY3
DB8		COPY1			COPY2	
DB9		COPY3				COPY2
DB10	COPY2				COPY3	
DB11		COPY2			COPY1	
DB12	COPY3					COPY1
DB13	COPY1				COPY2	
DB14		COPY1				COPY2
DB15	COPY2				COPY3	
DB16		COPY2				COPY3
DB17	COPY3				COPY1	
DB18		COPY3				COPY1
DB19	COPY1					COPY2
DB20		COPY1			COPY3	
DB21		COPY2				COPY3
DB22	COPY3				COPY2	
DB23		COPY3			COPY1	
DB24	COPY2					COPY1
DB25	COPY1					COPY3
DB26		COPY1			COPY3	
DB27		COPY3			COPY2	
DB28	COPY3					COPY2
DB29	COPY2				COPY1	
DB30		COPY2				COPY1
DB31	COPY1				COPY3	
DB32		COPY1			COPY2	
DB33		COPY3				COPY2
DB34	COPY2					COPY3
DB35		COPY2			COPY1	
DB36	COPY3					COPY1
DB37	COPY1				COPY2	
DB38		COPY1				COPY2

Return to top

1.10.1.2 Understanding Mailbox Database Copies

Understanding Mailbox Database Copies

Exchange Server 2010 > High Availability and Site Resilience > Understanding High Availability and Site Resilience >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-24*

Microsoft Exchange Server 2010 introduces the concept of database mobility, which is Exchange-managed database-level failovers. An enhanced version of the continuous replication feature first introduced in Exchange Server 2007 is used in Exchange 2010 to create and maintain database copies.

Database mobility disconnects databases from servers, adds support for up to 16 copies of a single database, and provides a native experience for adding database copies to a database. In Exchange 2007, a feature called database portability also enabled you to move a mailbox database between servers. A significant distinction between database portability and database mobility, however, is that with database mobility, all copies of a database have the same GUID.

Because clustered mailbox servers and storage groups have been removed from Exchange 2010, continuous replication now operates at the database level. In Exchange 2010, transaction logs are replicated to one or more Mailbox servers and replayed into a copy of a mailbox database that's stored on those servers. A failover or switchover can occur at either the database level or at the server level.

Key Characteristics

The key characteristics of mailbox database copies are:

- Database copies are for mailbox databases only. For redundancy and high availability for public folder databases, we recommend that you use public folder replication.
- Up to 16 copies of an Exchange 2010 mailbox database can be created on multiple Mailbox servers, provided the servers are grouped into a database availability group (DAG), which is a boundary for continuous replication. Exchange 2010 mailbox databases can be replicated only to other Exchange 2010 Mailbox servers within a DAG. You can't replicate a database outside of a DAG, nor can you replicate an Exchange 2010 mailbox database to a server running Exchange 2007. For detailed information about DAGs, see Understanding Database Availability Groups.
- All Mailbox servers in a DAG must be in the same Active Directory domain.
- Like standby continuous replication (SCR), all mailbox database copies support the concepts of replay lag time and truncation lag time. Note however, careful planning must be performed before enabling these features.
- All database copies can be backed up using an Exchange-aware, Volume Shadow Copy Service (VSS)-based backup application. However, the built-in support for Windows Server Backup is for active copies only. You can't use Windows Server Backup to back up passive copies.
- Database copies can be created only on Mailbox servers that don't host the active (mounted and in-use) copy of a database. You can't create two copies of the same database on the same server.

- All copies of a database use the same path on each server containing a copy. The database and log file paths for a database copy on each Mailbox server must not conflict with any other database paths.
- Database copies can be created in the same or different Active Directory sites, and on the same or different network subnets.
- Database copies aren't supported between Mailbox servers with round trip network latency greater than 500 milliseconds (ms).

Mailbox Database Copies

You can create a mailbox database copy at any time. Mailbox database copies can be distributed across Mailbox servers in a flexible and granular way. You can replicate one, some, or all mailbox databases on a server in a variety of ways.

You can create a mailbox database copy using the Add Mailbox Database Copy wizard in the Exchange Management Console or by using the **Add-MailboxDatabaseCopy** cmdlet in the Exchange Management Shell.

When creating a mailbox database copy, specify the following parameters:

- *Identity* This parameter specifies the name of the database being copied. Database names must be unique within the Exchange organization.
- *MaliboxServer* This parameter specifies the name of the Mailbox server that will host the database copy. This server must be a member of the same DAG and must not already host a copy of the database.

Optionally, you can also specify:

- *ActivationPreference* This parameter specifies the activation preference number, which is used as part of Active Manager's best copy selection process. It's also used to redistribute active mailbox databases throughout the DAG when using the RedistributeActiveDatabases.ps1 script. The value for the activation preference is a number equal to or greater than one, where one is at the top of the preference order. The position number cannot be larger than the number of mailbox database copies.
- *ReplayLagTime* This parameter specifies the amount of time that the Microsoft Exchange Replication service should wait before replaying log files that are copied to the database copy. The format for this parameter is (Days.Hours:Minutes:Seconds). The default setting for this value is 0 seconds. The maximum allowable setting for this value is 14 days. The minimum allowable setting is 0 seconds. Setting the value for replay lag time to 0 turns off log replay delay.
- *TruncationLagTime* This parameter specifies the amount of time that the Microsoft Exchange Replication service should wait before truncating log files that have replayed into a copy of the database. The time period begins after the log has been successfully replayed into the copy of the database. The format for this parameter is (Days.Hours:Minutes:Seconds). The default setting for this value is 0 seconds. The maximum allowable setting for this value is 14 days. The minimum allowable setting is 0 seconds. Setting the value for truncation lag time to 0 turns off log truncation delay.
- *SeedingPostponed* This parameter specifies that the task shouldn't automatically seed the database copy on the specified Mailbox server. This option is typically used when you intend to seed a new mailbox database copy by using an existing passive copy of the database (for example, adding a second copy of a specific database to a remote location). When you use this parameter, you must manually seed the database copy using the Update-MailboxDatabaseCopy cmdlet.

For more information about creating, using, and managing mailbox database copies, see Managing Mailbox Database Copies.

1.10.2 Planning for High Availability and Site Resilience

Planning for High Availability and Site Resilience

Exchange Server 2010 > High Availability and Site Resilience >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-09*

Microsoft Exchange Server 2010 includes a new unified framework for mailbox resiliency that includes new features such as the database availability group (DAG) and mailbox database copies. Although deploying these new features is a quick and simple process, careful planning must be performed beforehand to ensure that any high availability and site resilient solution using these features meets your expectations and your business requirements.

During the planning phase, the system architects, administrators, and other key stakeholders should identify the requirements for the deployment; in particular the requirements for high availability and site resilience. There are general requirements that must be met for deploying these features, as well as hardware, software, and networking requirements that must also be met. For guidance on the storage requirements for DAGs, see Mailbox Server Storage Design.

Contents

General Requirements

Before deploying a DAG and creating mailbox database copies, make sure that the following system-wide recommendations are met:

- Domain Name System (DNS) must be running. Ideally, the DNS server should accept dynamic updates. If the DNS server doesn't accept dynamic updates, you must create a DNS host (A) record for each Exchange server. Otherwise, Exchange won't function properly.
- Each Mailbox server in a DAG must be a member server in the same domain.
- It isn't supported to add an Exchange 2010 Mailbox server that's also a directory server to a DAG.
- The name that you assign to the DAG must be a valid, available, and unique computer name of 15 characters or less.

Hardware Requirements

Generally, there are no special hardware requirements that are specific to DAGs or mailbox database copies. The servers used must meet all of the requirements set forth in the topics for Exchange 2010 Prerequisites and Exchange 2010 System Requirements. For hardware planning information, see the following topics:

- Understanding Processor Configurations and Exchange Performance
- Understanding Memory Configurations and Exchange Performance
- Mailbox Server Storage Design
- Understanding Server Role Ratios and Exchange Performance

Storage Requirements

Generally, there are no special storage requirements that are specific to DAGs or mailbox database copies. DAGs don't require or use cluster-managed shared storage. Cluster-managed shared storage is supported for use in a DAG only when the DAG is configured to use a solution that leverages the Third Party Replication API built into Exchange 2010. For storage planning information, see Mailbox Server Storage Design.

Software Requirements

DAGs are available in both Exchange 2010 Standard Edition and Exchange 2010 Enterprise Edition. In addition, a DAG can contain a mix of servers running Exchange 2010 Standard Edition and Exchange 2010 Enterprise Edition.

Each member of the DAG must also be running the same operating system. Exchange 2010 is supported on both the Windows Server 2008 and Windows Server 2008 R2 operating systems. All members of a DAG must run either Windows Server 2008 or Windows Server 2008 R2. They can't contain a combination of both Windows Server 2008 and Windows Server 2008 R2.

In addition to meeting the prerequisites for installing Exchange 2010, there are operating system requirements that must be met. DAGs use Windows Failover Clustering technology, and as a result, they require the Enterprise version of Windows.

Network Requirements

There are specific networking requirements that must be met for each DAG and for each DAG member. DAG networks are similar to the public, mixed, and private networks used in previous versions of Exchange. However, unlike previous versions, using a single network in each DAG member is a supported configuration. In addition, the terminology has changed somewhat. Instead of public, private or mixed networks, each DAG has a single *MAPI network*, which is used by other servers (e.g., other Exchange 2010 servers, directory servers, etc.) to communicate with the DAG member, and zero or more *Replication networks*, which are networks that are dedicated to log shipping and seeding.

Although a single network is supported, we recommend that each DAG have at least two networks: a single MAPI network and a single Replication network. This provides redundancy for the network and the network path, and enables the system to distinguish between a server failure and a network failure. Using a single network adapter prevents the system from distinguishing between these two types of failures.

Note:

The product documentation in this content area is written with the assumption that each DAG member contains at least two network adapters, that each DAG is configured with a MAPI network and at least one Replication network, and that the system is able to distinguish between a network failure and a server failure.

Consider the following when designing the network infrastructure for your DAG:

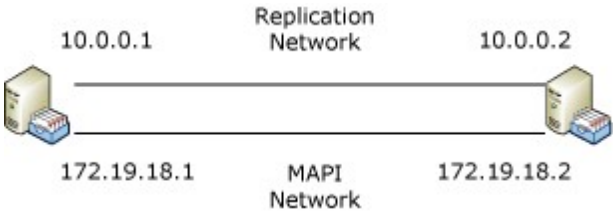
- Each member of the DAG must have at least one network adapter that is able to communicate with all other DAG members. If you are using a single network path, we recommend that you use gigabit Ethernet. When using a single network adapter in each DAG member, the DAG network does need to be enabled for replication and should be configured as a MAPI network. Because there are no other networks, the system will use the MAPI network as a Replication network, as well. In addition, when using a single network adapter in each DAG member, we recommend that you design the overall solution with the single network adapter and path in mind.
- Using two network adapters in each DAG member provides you with one MAPI network and one Replication network, and the following recovery behaviors:
  - In the event of a failure affecting the MAPI network, a server failover will occur (assuming there are healthy mailbox database copies that can be activated).
  - In the event of a failure affecting the Replication network, if the MAPI network is unaffected by the failure, log shipping and seeding operations will revert to use the MAPI network, even if the MAPI network has it's *ReplicationEnabled* property set to False. When the failed Replication network is restored to health and ready to resume log shipping and seeding operations, you must manually switch over to the Replication network. To change replication from the MAPI network to a restored Replication network, you can either suspend and resume continuous replication by using the Suspend-MailboxDatabaseCopy and Resume-MailboxDatabaseCopy cmdlets, or restart the Microsoft Exchange Replication service. We recommend using the suspend and resume operations to avoid the brief outage caused by restarting the Microsoft Exchange Replication service.
- Each DAG member must have the same number of networks. For example, if you plan on using a single network adapter in one DAG member, then all members of the DAG must also use a single network adapter.
- Each DAG must have no more than one MAPI network. The MAPI network must provide connectivity to other Exchange servers and other services, such as Active Directory and DNS.
- Additional Replication networks can be added, as needed. You can also prevent an individual network adapter from being a single point of failure by using network adapter teaming or similar technology. However, even when using teaming, this does not prevent the network itself from being a single point of failure.
- Each network in each DAG member server must be on its own network subnet. Each server in the DAG can be on a different subnet, but the MAPI and Replication networks must be routable and provide connectivity, such that:
  - Each network in each DAG member server is on its own network subnet that's separate from the subnet used by each other network in the server.
  - Each DAG member server's MAPI network can communicate with each other DAG member's MAPI network.
  - Each DAG member server's Replication network can communicate with each other DAG member's Replication network.
  - There is no direct routing that allows heartbeat traffic from the Replication network on one DAG member server to the MAPI network on another DAG member server, or vice versa, or between multiple Replication networks in the DAG.
- Regardless of their geographic location relative to other DAG members, each member of the DAG must have round trip network latency no greater than 500 milliseconds (ms) between each other member. As the round trip latency between two mailbox servers hosting copies of a database increases, the potential for replication being not up-to-date also increases. Regardless of the latency of the solution, customers should validate that the network(s) between all DAG members is capable of satisfying the data protection and availability goals of the deployment. Configurations with higher latency values may require special tuning of DAG, replication and network parameters, such as increasing the number of databases or decreasing the number of mailboxes

per database, to achieve the desired goals.
- Round trip latency requirements may not be the most stringent network bandwidth and latency requirement for a multi-datacenter configuration. You must evaluate the total network load, which includes client access, Active Directory, transport, continuous replication, and other application traffic, to determine the necessary network requirements for your environment.
- DAG networks support Internet Protocol Version 4 (IPv4) and IPv6. IPv6 is supported only when IPv4 is also used; a pure IPv6 environment isn't supported. Using IPv6 addresses and IP address ranges is supported only when both IPv6 and IPv4 are enabled on that computer, and the network supports both IP address versions. If Exchange 2010 is deployed in this configuration, all server roles can send data to and receive data from devices, servers, and clients that use IPv6 addresses.
- Automatic Private IP Addressing (APIPA) is a feature of Microsoft Windows that automatically assigns IP addresses when no Dynamic Host Configuration Protocol (DHCP) server is available on the network. APIPA addresses (including manually assigned addresses from the APIPA address range) aren't supported for use by DAGs or by Exchange 2010.

DAG Name and IP Address Requirements

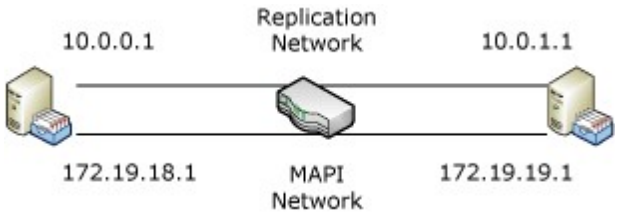
During creation, each DAG is given a unique name, and either assigned one or more static IP addresses, or configured to use DHCP. Regardless of whether you use static or dynamically-assigned addresses, any IP address assigned to the DAG must be on the MAPI network.

Each DAG requires a minimum of one IP address on the MAPI network. A DAG requires additional IP addresses when the MAPI network is extended across multiple subnets. The following figure illustrates a DAG where all nodes in the DAG have the MAPI network on the same subnet.



In this example, the MAPI network in each DAG member is on the 172.19.18.*x* subnet. As a result, the DAG requires a single IP address on that subnet.

The next figure illustrates a DAG that has a MAPI network which extends across two subnets: 172.19.18.*x* and 172.19.19.*x*.



In this example, the MAPI network in each DAG member is on a separate subnet. As a result, the DAG requires two IP addresses, one for each subnet on the MAPI network.

Each time the DAG's MAPI network is extended across an additional subnet, an additional IP address for that subnet must be configured for the DAG. Each IP address that's configured for the DAG is assigned to and used by the DAG's underlying failover cluster. The name of the DAG is also used as the name for the underlying failover cluster.

At any specific time, the cluster for the DAG will use only one of the assigned IP addresses. Windows Failover Clustering registers this IP address in DNS when the cluster IP address and Network Name resources are brought online. In addition to using an IP address and network name, a cluster name object (CNO) is created in Active Directory. The name, IP address and CNO for the cluster are used internally by the system to secure the DAG and for internal communication purposes. Administrators and end-users don't need to interface with or connect to the DAG name or IP address.

Note:

Although the cluster's IP address and network name are used internally by the system, there is no hard dependency in Exchange 2010 that these resources be available. Even if the underlying cluster's IP Address and Network Name resources are offline, internal communication still occurs within the DAG by using the DAG member's server names. However, we recommend that you periodically monitor the availability of these resources to ensure that they aren't offline for more than 30 days. If the underlying cluster is offline for more than 30 days, the cluster CNO account may be invalidated by the garbage collection mechanism in Active Directory.

Network Adapter Configuration for DAGs

Each network adapter must be configured properly based on its intended use. A network adapter that's used for a MAPI network is configured differently from a network adapter that's used for a Replication network. In addition to configuring each network adapter correctly, you must also configure the network connection order in Windows so that the MAPI network is at the top of the connection order. For detailed steps about how to modify the network connection order, see Modify the Protocol Bindings Order.

MAPI Network Adapter Configuration

A network adapter intended for use by a MAPI network should be configured as described in the following table.

Networking Features	Setting
Client for Microsoft Networks	Enabled
QoS Packet Scheduler	Optionally enable
File and Printer Sharing for Microsoft Networks	Enable
Internet Protocol Version 6 (TCP/IP v6)	Optionally enable
Internet Protocol Version 4 (TCP/IP v4)	Enabled
Link-Layer Topology Discovery Mapper I/O Driver	Enabled
Link-Layer Topology Discovery Responder	Enabled

The TCP/IP v4 properties for a MAPI network adapter are configured as follows:

- The IP address for a DAG member's MAPI network can be manually assigned or configured to use DHCP. If DHCP is used, we recommend using persistent reservations for server's IP address.
- The MAPI network typically uses a default gateway, although one isn't required.
- At least one DNS server address must be configured. Using multiple DNS servers is recommended for redundancy.
- The **Register this connection's addresses in DNS** checkbox should be checked.

Replication Network Adapter Configuration

A network adapter intended for use by a Replication network should be configured as

described in the following table.

Networking Features	Setting
Client for Microsoft Networks	Disabled
QoS Packet Scheduler	Optionally enable
File and Printer Sharing for Microsoft Networks	Disabled
Internet Protocol Version 6 (TCP/IP v6)	Optionally enable
Internet Protocol Version 4 (TCP/IP v4)	Enabled
Link-Layer Topology Discovery Mapper I/O Driver	Enabled
Link-Layer Topology Discovery Responder	Enabled

The TCP/IP v4 properties for a Replication network adapter are configured as follows:

- The IP address for a DAG member's Replication network can be manually assigned or configured to use DHCP. If DHCP is used, we recommend using persistent reservations for server's IP address.
- Replication networks typically do not have default gateways, and if the MAPI network has a default gateway, then no other networks should have default gateways. Routing of network traffic on a Replication network can be configured by using persistent, static routes to the corresponding network on other DAG members using gateway addresses that have the ability to route between the Replication networks. All other traffic not matching this route will be handled by the default gateway that's configured on the adapter for the MAPI network.
- DNS server addresses should not be configured.
- The **Register this connection's addresses in DNS** checkbox should not be checked.

Return to top

Witness Server Requirements

A *witness server* is a server outside of a DAG that's used to achieve and maintain quorum when the DAG has an even number of members. DAGs with an odd number of members do not use a witness server. All DAGs with an even number of members will use a witness server. The witness server can be any computer running Windows Server. There is no requirement that the version of the Windows Server operating system of the witness server match the operating system used by the DAG members.

Quorum is maintained at the cluster level, underneath the DAG. A DAG has quorum when the majority of its members are online and can communicate with the other online members of the DAG. This notion of quorum is one aspect of the concept of quorum in Windows failover clustering. A related and necessary aspect to quorum in failover clusters is the *quorum resource*. The quorum resource is a resource inside a failover cluster that provides a means for arbitration leading to cluster state and membership decisions. The quorum resource also provides persistent storage for storing configuration information. A companion to the quorum resource is the *quorum log*, which is a configuration database for the cluster. The quorum log contains information such as which servers are members of the cluster, what resources are installed in the cluster, and the state of those resources (for example, online or offline).

It is critical that each DAG member have a consistent view of how the DAG's underlying

cluster is configured. The quorum acts as the definitive repository for all configuration information relating to the cluster. The quorum is also used as a tie-breaker to avoid "split-brain" syndrome. Split brain syndrome is a condition that occurs when DAG members cannot communicate with each other but are up and running. Split brain syndrome is prevented by always requiring a majority of the DAG members (and in the case of DAGs with an even number of member, the DAG witness server) to be available and interacting for the DAG to be operational.

Planning for Site Resilience

Every day, more and more businesses recognize that access to a reliable and available messaging system is fundamental to their success. For many organizations, the messaging system is part of the business continuity plans, and their messaging service deployment is designed with site resilience in mind. Fundamentally, many site resilient solutions involve the deployment of hardware in a second datacenter.

Ultimately, the overall design of a DAG, including the number of DAG members and the number of mailbox database copies, will depend on each organization's recovery service level agreements (SLAs) that cover various failure scenarios. During the planning stage, the solution's architects and administrators identify the requirements for the deployment, including in particular the requirements for site resilience. They identify the location(s) to be used and the required recovery SLA targets. The SLA will identify two specific elements that should be the basis for the design of a solution that provides high availability and site resilience: the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). Both of these values are measured in minutes. The RTO is how long it takes to restore service. The RPO refers to how current the data is after the recovery operation has completed. An SLA may also be defined for restoring the primary datacenter to full service after its problems are corrected.

The solution's architects and administrators will also identify which set of users require site resilience protection, and determine if the multi-site solution will be active/passive or active/active configuration. In an active/passive configuration, no users are normally hosted in the standby datacenter. In an active/active configuration, users are hosted in both locations, and some percentage of the total number of databases within the solution has a preferred active location in a second datacenter. When service for the users of one datacenter fails, those users are activated in the other datacenter.

Constructing the appropriate SLAs often requires answering the following basic questions:

- What level of service is required after the primary datacenter fails?
- Do users need their data or just messaging services?
- How rapidly is data required?
- How many users must be supported?
- How will users access their data?
- What is the standby datacenter activation service level agreement (SLA)?
- How is service moved back to the primary datacenter?
- Are the resources dedicated to the site resilience solution?

By answering these questions, you begin to shape a site resilient design for your messaging solution. A core requirement of recovery from site failure is to create a solution that gets the necessary data to the backup datacenter that hosts the backup messaging service.

Namespace Planning

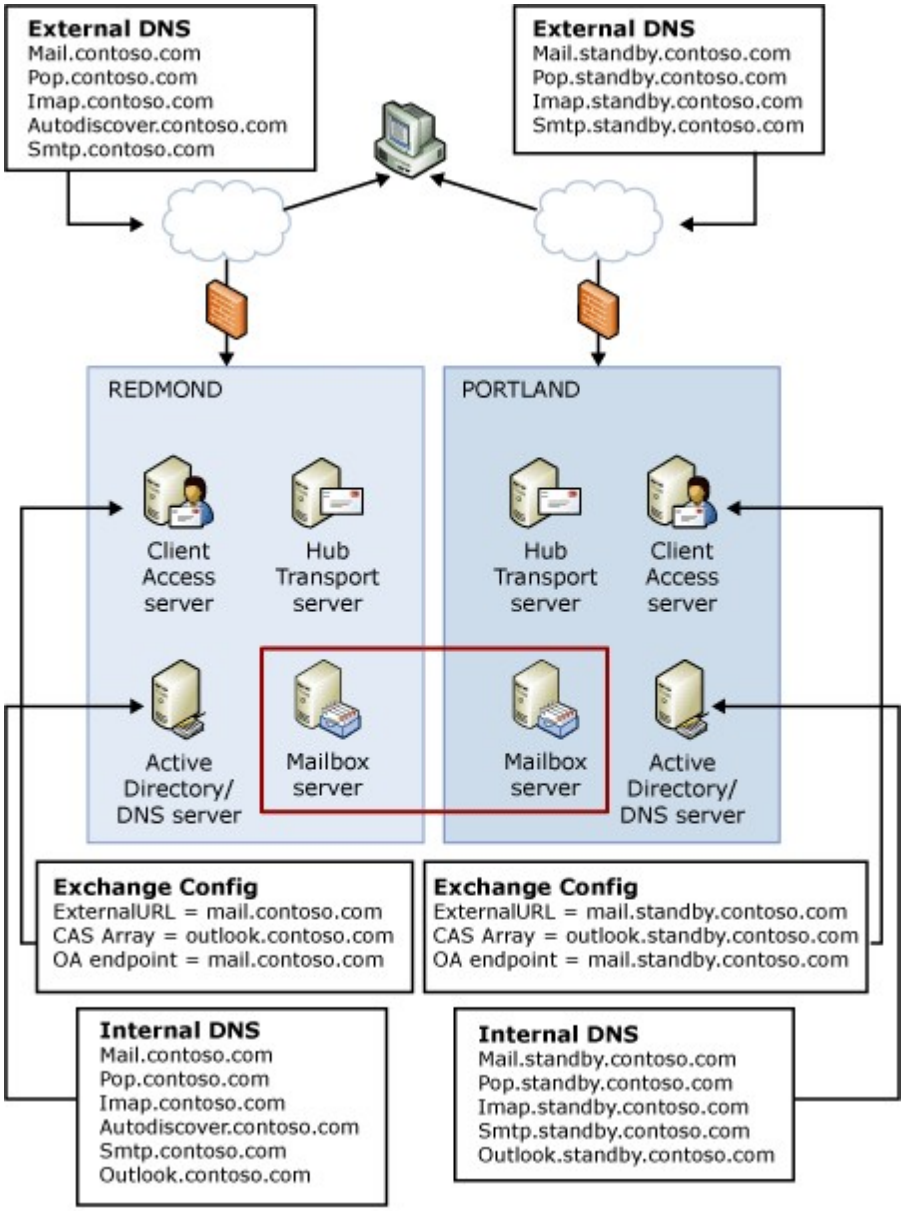
Exchange 2010 changes the way in which you plan your namespace design when deploying a site resilient configuration. Proper namespace planning is essential in order for datacenter switchovers to be successful. From a namespace perspective, each datacenter used in a site resilience configuration is considered to be active. As a result,

each datacenter will require its own unique namespace for the various Exchange 2010 services in that site, including namespaces for Outlook Web App, Outlook Anywhere, Exchange ActiveSync, Exchange Web Services, RPC Client Access, Post Office Protocol version 3 (POP3), Internet Message Access Protocol version 4 (IMAP4), and Simple Mail Transfer Protocol (SMTP). In addition, one of the datacenters also hosts the namespace for Autodiscover. This design also enables you to perform a single database switchover from the primary datacenter to a second datacenter to validate the configuration of the second data as part of validation of and practice for a datacenter switchover.

As a best practice, we recommend that you use *split DNS* for the Exchange hostnames that are used by clients. Split DNS refers to a DNS server configuration in which internal DNS servers return an internal IP address for a hostname and external (Internet-facing) DNS servers return a public IP address for the same hostname. Because using split DNS uses the same hostnames internally and externally, this strategy enables you to minimize the number of hostnames you'll need.

The following figure illustrates namespace planning for a site resilient configuration.

Namespaces for site resilient DAG deployment



As shown above, each datacenter uses a separate and unique namespace and each contains DNS servers in a split DNS configuration for those namespaces. The Redmond datacenter, which is considered the primary datacenter, is configured with a namespace of *protocol*.contoso.com. The Portland datacenter is configured with a namespace of *protocol*.standby.contoso.com. Namespaces can include designations of standby, as in the example figure, they can be based on region (e.g., *protocol*.portland.contoso.com), or they can be based on other naming conventions that suit your organization's needs. The key requirement is that, regardless of the naming convention you use, each datacenter should have its own unique namespace.

FailbackURL Configuration

Some Web browsers, including Microsoft Internet Explorer, maintain a DNS name cache during each browser session that is separate from the DNS cache provided by the operating system. During failback to the primary datacenter after a datacenter switchover has occurred, the Web browser's use of this separate cache can result in logon loops for Outlook Web App users wherein users are redirected to the same URL in a repeating

loop.

During the failback process, the IP address for the Outlook Web App namespace is changed in DNS from an endpoint in the standby datacenter back to its original endpoint in the primary datacenter. After the TTL for the DNS record has expired and even after the operating system's DNS cache is cleared, Web browsers that maintain their own separate name cache may continue to connect to the endpoint in the standby datacenter, even though the namespace is hosted in the primary datacenter.

Typically, closing the Web browser is sufficient to clear its separate name cache and prevent the logon loops. However, to mitigate this issue for all Web browsers and Outlook Web App users, you can configure the *FailbackURL* property of your Outlook Web App virtual directory. The *FailbackUrl* parameter specifies the host name that Outlook Web App uses to connect to the Client Access server after failback to a primary site. This namespace requires a separate DNS entry pointing to the original Client Access server's IP address. The value of the *FailbackUrl* parameter must be different from the value of the *ExternalUrl* parameter for the Outlook Web App virtual directory. When an Outlook Web App user provides their credentials, the Client Access server will detect if the redirection URL is the same URL the user is visiting. If the URLs are the same, the Client Access server will check to see if the *FailbackUrl* parameter is configured:

- If the *FailbackUrl* parameter is configured, it will redirect the user to that URL where they should be able to access Outlook Web App.
- If the *FailbackUrl* parameter is not configured, the user will receive an error message that indicates that a server configuration change is temporarily preventing access to their mailbox. The message instructs the user to close all browser windows (thereby clearing the browser's name cache) and try again in a few minutes.

Certificate Planning

There are no unique or special design considerations for certificates when deploying a DAG in a single datacenter. However, when extending a DAG across multiple datacenters in a site resilient configuration, there are some specific considerations with respect to certificates. Generally, your certificate design will depend on the clients in use, as well as the certificate requirements by other applications that use certificates. But there are some specific recommendations and best practices you should follow with respect to the type and number of certificates.

As a best practice, you should minimize the number of certificates you use for your Client Access servers, reverse proxy servers, and transport servers (Edge and Hub). We recommend using a single certificate for all of these service endpoints in each datacenter. This approach minimizes the number of certificates that are needed, which reduces both cost and complexity for the solution.

For Outlook Anywhere clients, we recommend that you use a single Subject Alternative Name (SAN) certificate for each datacenter, and include multiple host names in the certificate. To ensure Outlook Anywhere connectivity after a database, server or datacenter switchover, you must use the same Certificate Principal Name on each certificate, and configure the Outlook Provider Configuration object Active Directory with the same Principal Name in Microsoft-Standard Form (msstd). For example, if you use a Certificate Principal Name of mail.contoso.com, you would configure the attribute as follows:

```
Set-OutlookProvider EXPR -CertPrincipalName "msstd:mail.contoso.com"
```

Some applications that integrate with Exchange have specific certificates requirements that may require using additional certificates. Exchange 2010 can co-exist with Office Communications Server (OCS). OCS requires certificates with 1024-bit or greater certificates that use the OCS server name for the Certificate Principal Name. Because using an OCS server name for the Certificate Principal Name would prevent Outlook Anywhere from working properly, you would need to use an additional and separate

certificate for the OCS environment.

For more information about using SAN certificates for Exchange 2010 client access, see Configure SSL Certificates to Use Multiple Client Access Server Host Names.

Network Planning

In addition to the specific networking requirements that must be met for each DAG, as well as for each server that's a member of a DAG, there are some requirements and recommendations that are specific to site resilience configurations. As with all DAGs, whether the DAG members are deployed in a single site or in multiple sites, the round-trip return network latency between DAG members DAG must be no greater than 500 milliseconds (ms). In addition, there are specific configuration settings that are recommended for DAGs that are extended across multiple sites:

- **MAPI networks should be isolated from Replication networks** Windows network policies, Windows firewall policies or router access control lists (ACLs) should be used to block traffic between the MAPI network and the Replication network(s). This configuration is necessary to prevent network heartbeat cross-talk.
- **Client-facing DNS records should have a Time to Live (TTL) of 5 minutes** The amount of downtime that clients experience is dependent not just on how quickly a switchover can occur, but also on how quickly DNS replication occurs and how quickly the clients query for updated DNS information. DNS records for all Exchange client services, including Outlook Web App, Exchange ActiveSync, Exchange Web services, Outlook Anywhere, SMTP, POP3, IMAP4, and RPC Client Access in both the internal and external DNS servers should be set with a TTL of 5 minutes.
- **Use static routes to configure connectivity across Replication networks** To provide network connectivity between each of the Replication network adapters, use persistent static routes. This is a quick and one-time configuration that is performed on each DAG member when using static IP addresses. If you are using DHCP to obtain IP addresses for your Replication networks, you can also use it to assign static routes for the Replication, thereby simplifying the configuration process.

General Site Resilience Planning

In addition to the requirements listed above for high availability, there are other recommendations for deploying Exchange 2010 in a site resilient configuration (e.g., extending a DAG across multiple datacenters). What you do during the planning phase will directly affect the success of your site resilience solution. For example, poor namespace design can cause difficulties with certificates, and an incorrect certificate configuration can prevent users from accessing services.

In order to minimize the time it takes to activate a second datacenter, and allow the second datacenter to host the service endpoints of a failed datacenter, the appropriate planning must be completed. For example:

- The Service Level Agreement (SLA) goals for the site resilience solution must be well understood and documented.
- The servers in the second datacenter must have sufficient capacity to host the combined user population of both datacenters.
- The second datacenter must have all services enabled that are provided in primary datacenter (unless the service isn't included as part of the site resilience SLA). This includes Active Directory, networking infrastructure (DNS, TCP/IP, etc.), telephony services (if Unified Messaging is in use), and site infrastructure (power, cooling, etc.).
- In order for some services to be able to service users from the failed datacenter, they must have the proper server certificates configured. Some services do not allow instancing (for example, POP3 and IMAP4) and only allow the use of a single certificate. In these cases, either the certificate must be a subject alternative name (SAN) certificate that includes multiple names, or the

multiple names must be similar enough so that a wildcard certificate can be used (assuming the security policies of the organization allows the use of wildcard certificates).

- The necessary services must be defined in the second datacenter. For example, if first datacenter has three different SMTP URLs on different transport servers, then the appropriate configuration must be defined in the second datacenter to enable at least one (if not all three) transport server(s) to host the workload.
- The necessary network configuration must be in place to support the datacenter switchover. This might mean making sure that load balancing configurations are in place, that global DNS is configured, and that the Internet connection is enabled with the appropriate routing configured.
- The strategy for the enabling the DNS changes necessary for a datacenter switchover must be understood. The specific DNS changes, including their Time to Live (TTL) settings, must be defined and documented to support the SLA(s) in effect.
- A strategy for testing the solution must also be established and factored into the SLA. Periodic validation of the deployment is the only way to guarantee that the quality and viability of the deployment does not degrade over time. After the deployment is validated, we recommend that the part of the configuration that directly affects the success of the solution be explicitly documented. In addition, we recommend that you enhance your change management processes around those segments of the deployment.

Return to top

Planning for Datacenter Switchovers

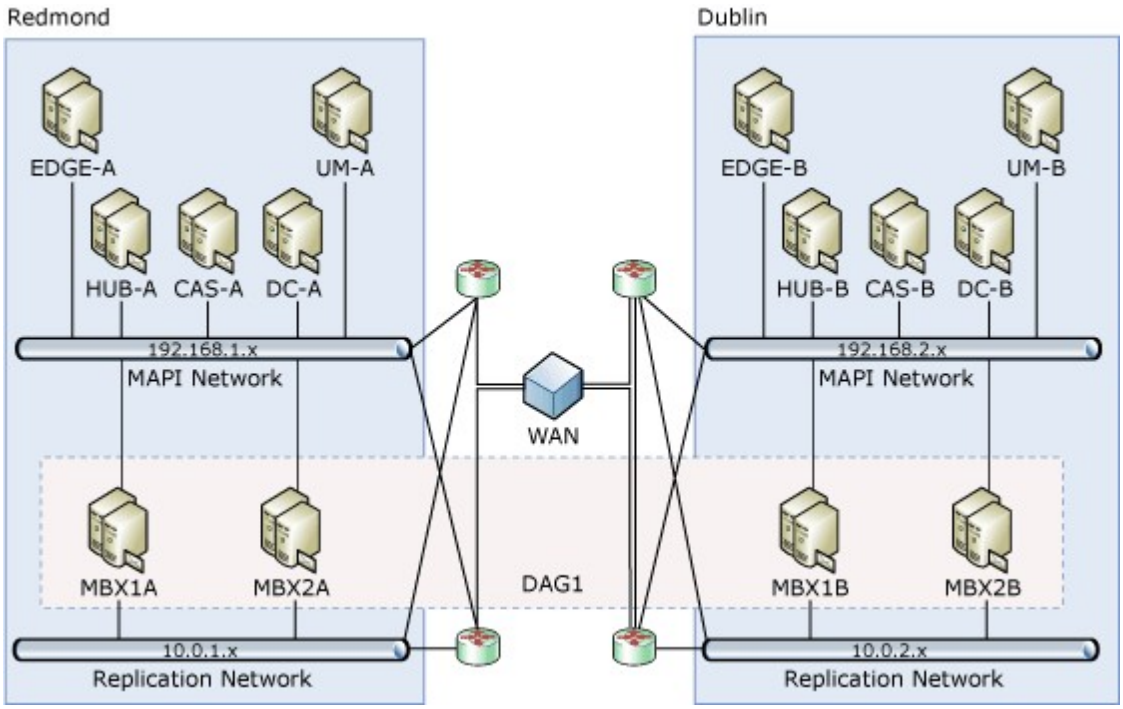
The proper planning and preparation involves not only the deployment of the second datacenter resources, such as live Client Access and Hub Transport servers, but also pre-configuration of those resources to minimize the changes required as part of a datacenter switchover operation.

Note:

Client Access and Hub Transport services are required in the second datacenter even when automatic activation of the mailbox databases in the second datacenter is blocked. These services are necessary in order to perform database switchovers, as well as to perform testing and validation of the services and data in the second datacenter.

To better understand the how a datacenter switchover process works, it's helpful to understand the basic operation of an Exchange 2010 datacenter switchover.

As illustrated in the following figure, a site resilient deployment consists of a DAG that has members in both datacenters.



When a DAG is extended across multiple datacenters, it should be designed so that either the majority of the DAG members are located in the primary datacenter or, when each datacenter has the same number of members, the primary datacenter hosts the witness server. This design guarantees that service will provided in the primary datacenter even if network connectivity between the two datacenters fails. It also means that when the primary datacenter fails, however, quorum will be lost for the members in the second datacenter.

Partial datacenter failures are also possible and will happen. The presumption is that if enough functionality is lost in the primary datacenter to preclude effective service and management then a datacenter switchover should be performed to activate the second datacenter. The activation process involves the administrator configuring the surviving servers of partially operational state to cease service. Activation can then proceed in the second datacenter. This is done to preclude both sets of services to try and operate at the same time.

As a result of the loss of the quorum, the DAG members in the second datacenter cannot automatically come online. Thus, activating the mailbox servers in the second datacenter also requires a step where the DAG member servers are forced to create quorum, at which point the servers in the failed datacenter are internally (but only temporarily) removed from the DAG. This provides a partial-service solution that's stable and able to experience some level of additional failures and still continue to function.

Note:

One prerequisite of being able to experience additional failures is that the DAG has at least four members and the four members are spread between two Active Directory sites (e.g., at least two members in each datacenter).

This is the basic process used to re-establish Mailbox role functionality in the second datacenter. The activation of the other roles in the second datacenter does not involve explicit actions on the impacted servers in the second datacenter. Instead, servers in the second datacenter become the service endpoints for those services normally hosted by the primary datacenter. For example, a user normally hosted in the primary datacenter might use https://mail.contoso.com/owa to connect to Outlook Web App. After the

datacenter failure, these service endpoints are moved to endpoints in the second datacenter as part of the switchover operation. During the switchover operation, the service endpoints for the primary datacenter are re-targeted at alternate IP addresses for the same services in the second datacenter. This minimizes the amount of changes that must be made to configuration information stored in Active Directory during the switchover process. Generally, there are two ways to complete this step:

- Update DNS records; or
- Reconfigure DNS and load balancer(s) to enable and disable alternate IP addresses, thus moving services between datacenters.

A strategy for testing the solution must be established. It must be factored into the SLA. Periodic validation of the deployment is the only way to guarantee the deployment does not degrade over time.

Careful completion of these planning steps will directly impact the success of a datacenter switchover. For example, poor namespace design can cause difficulties with certificates, and an incorrect certificate configuration can preclude users from being able to access services.

After the deployment is validated, we recommend that all parts of the configuration that directly affect the success of a datacenter switchover be explicitly documented. In addition, it might be prudent to enhance the change management processes around those segments of the deployment.

For more information about datacenter switchovers, including activating a secondary datacenter, and re-activating a failed (primary) datacenter, see Datacenter Switchovers.

Return to top

1.10.3 Deploying High Availability and Site Resilience

Deploying High Availability and Site Resilience

Exchange Server 2010 > High Availability and Site Resilience >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-09*

To create a highly available Mailbox server in previous versions of Exchange, you would install Exchange on a server that was configured as a member of a Microsoft Windows failover cluster. If you wanted a highly available Mailbox server, you had to build and configure the cluster prior to running Exchange Setup. The Exchange Setup program (and other Exchange components, such as the Exchange store and the Microsoft Exchange System Attendant service) was cluster-aware, and therefore behaved differently from when it was run on a stand-alone server. If Exchange was already installed on a stand-alone Windows server, you couldn't configure that server for high availability without first removing Exchange, building a cluster, and then reinstalling Exchange using the cluster-aware version of Setup.

Microsoft Exchange Server 2010 uses the concept known as *incremental deployment* for both high availability and site resilience. Unlike previous versions, Exchange 2010 no longer uses the cluster resource model for high availability. As a result of this architectural change, there is no longer a cluster-aware version of Setup, and you no longer configure high availability during Setup. Instead, you simply install all Exchange 2010 servers as standalone servers, and then incrementally configure mailbox servers and mailbox databases for high availability and site resilience as needed.

Overview of the Deployment Process

While the actual steps used by each organization may vary slightly, the overall process for deploying Exchange 2010 in a highly available or site resilient configuration is generally the same. After performing the necessary planning and design tasks for building and deploying a database availability group (DAG) and creating mailbox database copies, you would:

1. Create a DAG. For detailed steps, see Create a Database Availability Group.
2. If necessary, pre-stage the cluster name object (CNO). Pre-staging the CNO is required when deploying a DAG with Mailbox servers running Windows Server 2012. Pre-staging is also required in environments where computer account creation is restricted or where computer accounts are created in a container other than the default computers container. For detailed steps, see Pre-stage the Cluster Name Object for a Database Availability Group.
3. Add two or more Mailbox servers to the DAG. For detailed steps, see Manage Database Availability Group Membership.
4. Configure the DAG properties as needed:
   4.a. Optionally configure DAG encryption and compression, replication port, DAG IP addresses, and other DAG properties. For detailed steps, see Configure Database Availability Group Properties.
   4.b. If the DAG contains three or more Mailbox servers that are deployed in multiple Active Directory sites, Datacenter Activation Coordination (DAC) mode should be enabled. For more information, see Understanding Datacenter Activation Coordination Mode.
   4.c. For detailed steps about how to create a DAG network, see Create a Database Availability Group Network. To manage a DAG network, see Configure Database Availability Group Network Properties.
5. Add mailbox database copies across Mailbox servers in the DAG. For detailed steps, see Add a Mailbox Database Copy.

Example Deployment: Four Member DAG in Two Datacenters

This example details how an organization, Contoso, Ltd., is configuring and deploying a four-member DAG that will be extended across two physical locations: a primary datacenter referred to as Active Directory SITEA and a second datacenter referred to as Active Directory SITEB. SITEA is located in Redmond, Washington, and SITEB is located in Dublin, Ireland.

Base Infrastructure

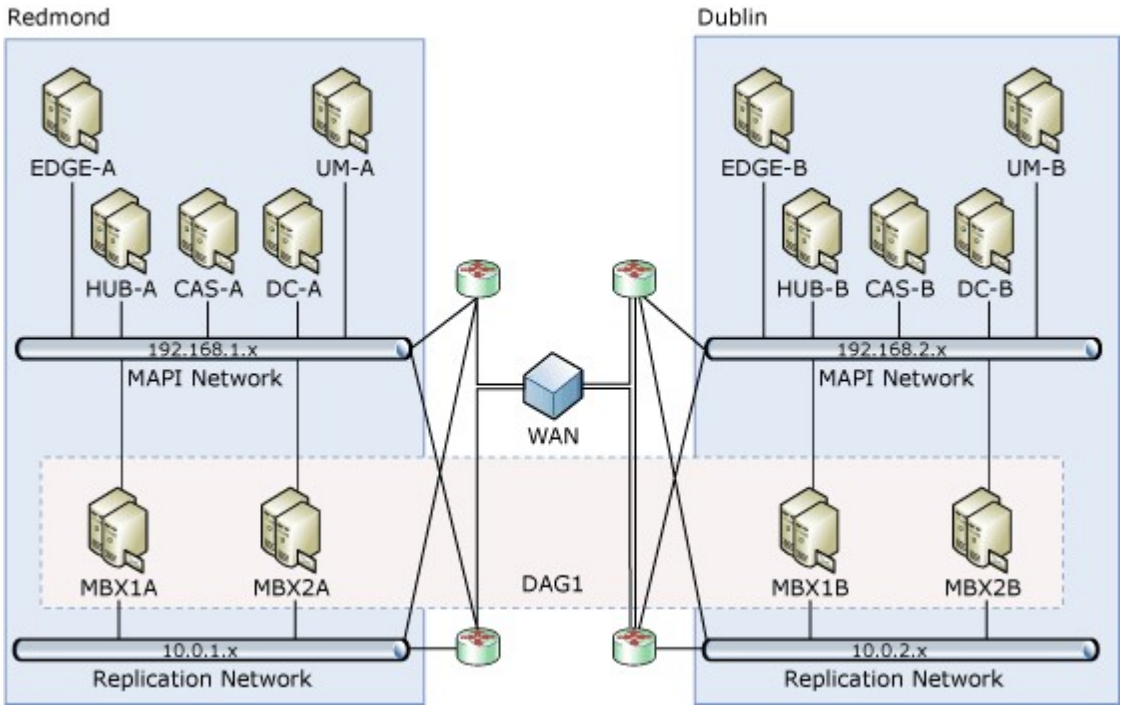
Each location contains the infrastructure elements that are necessary to operate a messaging infrastructure based on Exchange 2010, namely:

- Directory services (either Active Directory or Active Directory Domain Services (AD DS))
- Domain Name System (DNS) name resolution
- One or more Exchange 2010 Client Access servers
- One or more Exchange 2010 Hub Transport servers
- One or more Exchange 2010 Mailbox servers

Note:

The Client Access, Hub Transport, and Mailbox server roles can be co-located on a single computer. In this example deployment, the server roles are installed on separate computers.

The following figure illustrates the Contoso configuration.



Except for the Mailbox servers, all of the servers in the Contoso environment are running the Windows Server 2008 R2 Standard operating system. The Mailbox servers, which were planned with DAGs in mind, are running Windows Server 2008 R2 Enterprise.

In addition to the preceding infrastructure components, each location contains other messaging elements, such as Edge Transport servers and Unified Messaging servers.

Network Configuration

As illustrated in the previous figure, the solution involves the use of multiple subnets and multiple networks. Each Mailbox server in the DAG has two network adapters on separate subnets. In each Mailbox server, one network adapter will be used for the MAPI network (192.168.*x*.*x*) and one network adapter will be used for the Replication network (10.0.*x*.*x*). Only the MAPI network provides connectivity to Active Directory, DNS services, other Exchange servers and clients. The adapter used for the Replication network in each member provides connectivity only to the Replication network adapters in the other members of the DAG.

The settings for each network adapter in each node are detailed in the following table.

Name	IPv4 address	Subnet mask	Default gateway
MBX1A (MAPI)	192.168.1.4	255.255.255.0	192.168.1.1
MBX2A (MAPI)	192.168.1.5	255.255.255.0	192.168.1.1
MBX1B (MAPI)	192.168.2.4	255.255.255.0	192.168.2.1
MBX2B (MAPI)	192.168.2.5	255.255.255.0	192.168.2.1
MBX1A (Replication)	10.0.1.4	255.255.0.0	None
MBX2A (Replication)	10.0.1.5	255.255.0.0	None
MBX1B (Replication)	10.0.2.4	255.255.0.0	None
MBX2B (Replication)	10.0.2.5	255.255.0.0	None

As shown in the preceding table, adapters used for Replication networks don't use default gateways. To provide network connectivity between each of the Replication network adapters, Contoso uses persistent static routes, which they configure by using Netsh.exe tool. Netsh.exe is a tool you can use to configure and monitor Windows-based computers at a command prompt. With the Netsh.exe tool, you can direct the context commands you enter to the appropriate helper, and the helper then carries out the command. A helper is a dynamic-link library file (.dll) that extends the functionality of the Netsh.exe tool by providing configuration, monitoring, and support for one or more services, utilities, or protocols.

To configure routing for the Replication network adapters on MBX1A and MBX2A, the following command was run on each server.

```
netsh interface ipv4 add route 10.0.2.0/24 <NetworkName> 10.0.1.254
```

To configure routing for the Replication network adapters on MBX1B and MBX2B, the following command was run on each server.

```
netsh interface ipv4 add route 10.0.1.0/24 <NetworkName> 10.0.2.254
```

The following additional network settings have also been configured:

- The **Register this connection's addresses in DNS** check box is selected for each DAG member's MAPI network adapter, and cleared for each Replication network adapter.
- At least one DNS server address is configured for each DAG member's MAPI network adapter, and none are configured for the Replication network adapters. For redundancy, Contoso is using multiple DNS server addresses for their MAPI network adapters.
- Contoso doesn't use IPv6, and they disabled the protocol on their servers.
- Contoso doesn't use the Windows Firewall and have turned it off on their servers.

After the network adapters have been configured, Contoso is ready to create a DAG and add the Mailbox servers to the DAG.

Database Availability Group Creation and Configuration

The administrator has decided to create a Windows PowerShell command-line interface script that performs several tasks:

- It uses the New-DatabaseAvailabilityGroup cmdlet to create the DAG. Because SITEA is considered to be the primary datacenter, Contoso has chosen to use a witness server in the same datacenter, namely, HUB-A.
- It uses the Set-DatabaseAvailabilityGroup cmdlet to preconfigure an alternate witness server and alternate witness directory in case a site switchover is ever necessary.
- It uses the Add-DatabaseAvailabilityGroupServer cmdlet to add each of the four Mailbox servers to the DAG.
- It uses the Set-DatabaseAvailabilityGroup cmdlet to configure the DAG for DAC mode. For more information about DAC mode, see Understanding Datacenter Activation Coordination Mode.

The following are the commands used in the script:

```
New-DatabaseAvailabilityGroup -Name DAG1 -WitnessServer HUB-A -WitnessDirectory C
```

The preceding command creates a DAG named DAG1, configures Hub-A to act as the witness server, configures a specific witness directory (C:\DAGWitness \DAG1.contoso.com), and configures two IP addresses for the DAG (one for each subnet on the MAPI network).

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -AlternateWitnessDirectory C:\DAGWit
```

The preceding command configures DAG1 to use an alternate witness server of Hub-B and an alternate witness directory on Hub-B that uses the same path that was configured on Hub-A.

Note:

Using the same path isn't required; Contoso has chosen to do this to standardize their configuration.

```
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1A
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1B
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX2A
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX2B
```

The preceding commands add each of the Mailbox servers, one at a time, to the DAG. The commands also install the Windows Failover Clustering component on each Mailbox server (if it isn't already installed), create a failover cluster, and join each Mailbox server to the newly created cluster.

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -DatacenterActivationMode DagOnly
```

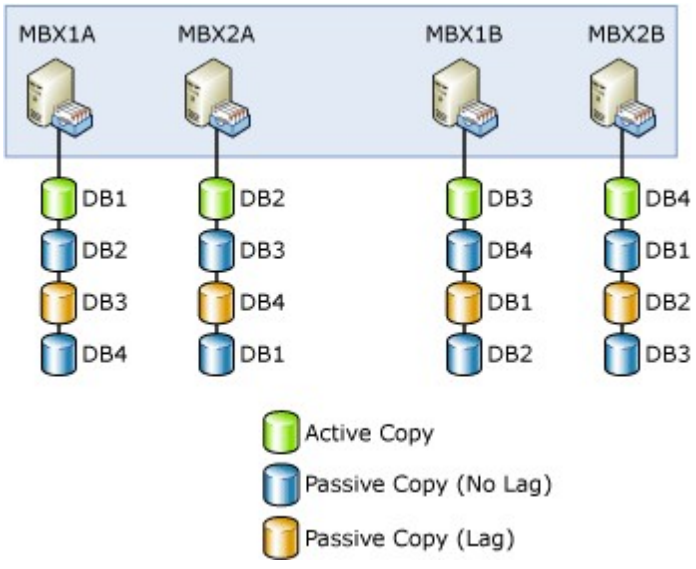
The preceding command enables DAC mode for the DAG.

Mailbox Databases and Mailbox Database Copies

After creating the DAG and adding the Mailbox servers to the DAG, Contoso prepares to create mailbox databases and mailbox database copies. To meet their criteria for failure resistance, Contoso is planning to configure each mailbox database with three non-lagged database copies, and one lagged database copy. The lagged copy will have a configured log replay delay of three days.

This configuration provides a total of four copies for each database (one active, two non-lagged passives, and a lagged passive). Contoso plans on having four active databases per server. With four active databases per server, and three passive copies of each database, the Contoso solution contains 16 total database copies.

As shown in the following figure, Contoso is taking a balanced approach to their database layout.



Each Mailbox server hosts an active mailbox database copy, two non-lagged passive database copies, and one lagged passive database copy. The lagged copy of each active mailbox database is hosted on a Mailbox server in the other site.

To create this configuration, the administrator runs several commands.

On MBX1A, run the following commands.

```
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX2A
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX2B
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX1B -ReplayLagTime 3.00:00
Suspend-MailboxDatabaseCopy -Identity DB1\MBX1B -SuspendComment "Seed from MBX2B"
Update-MailboxDatabaseCopy -Identity DB1\MBX1B -SourceServer MBX2B
Suspend-MailboxDatabaseCopy -Identity DB1\MBX1B -ActivationOnly
```

On MBX2A, run the following commands.

```
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX1A
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX1B
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX2B -ReplayLagTime 3.00:00
Suspend-MailboxDatabaseCopy -Identity DB2\MBX2B -SuspendComment "Seed from MBX1B"
Update-MailboxDatabaseCopy -Identity DB2\MBX2B -SourceServer MBX1B
Suspend-MailboxDatabaseCopy -Identity DB2\MBX2B -ActivationOnly
```

On MBX1B, run the following commands.

```
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX2B
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX2A
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX1A -ReplayLagTime 3.00:00
Suspend-MailboxDatabaseCopy -Identity DB3\MBX1A -SuspendComment "Seed from MBX2A"
Update-MailboxDatabaseCopy -Identity DB3\MBX1A -SourceServer MBX2A
Suspend-MailboxDatabaseCopy -Identity DB3\MBX1A -ActivationOnly
```

On MBX2B, run the following commands.

```
Add-MailboxDatabaseCopy -Identity DB4 -MailboxServer MBX1B
Add-MailboxDatabaseCopy -Identity DB4 -MailboxServer MBX1A
Add-MailboxDatabaseCopy -Identity DB4 -MailboxServer MBX2A -ReplayLagTime 3.00:00
Suspend-MailboxDatabaseCopy -Identity DB4\MBX2A -SuspendComment "Seed from MBX1A"
Update-MailboxDatabaseCopy -Identity DB4\MBX2A -SourceServer MBX1A
Suspend-MailboxDatabaseCopy -Identity DB4\MBX2A -ActivationOnly
```

In the preceding examples for the **Add-MailboxDatabaseCopy** cmdlet, the *ActivationPreference* parameter wasn't specified. The task automatically increments the activation preference number with each copy that's added. The original database always has a preference number of 1. The first copy added with the **Add-MailboxDatabaseCopy** cmdlet is automatically assigned a preference number of 2. Assuming no copies are removed, the next copy added is automatically assigned a preference number of 3, and so forth. Thus, in the preceding examples, the passive copy in the same datacenter as the active copy has an activation preference number of 2; the non-lagged passive copy in the remote datacenter has an activation preference number of 3, and the lagged passive copy in the remote datacenter has an activation preference number of 4.

Although there are two copies of each active database across the WAN in the other location, seeding over the WAN was only performed once. This is because Contoso is leveraging the Exchange 2010 ability to use a passive copy of a database as the source for seeding. Using the Add-MailboxDatabaseCopy cmdlet with the *SeedingPostponed* parameter prevents the task from automatically seeding the new database copy being created. Then, the administrator can suspend the un-seeded copy, and by using the Update-MailboxDatabaseCopy cmdlet with the *SourceServer* parameter, the administrator can specify the local copy of the database as the source of the seeding operation. As a result, seeding of the second database copy added to each location happens locally and not over the WAN.

Note:

In the preceding example, the non-lagged database copy is seeded over the WAN, and that copy is then used to seed the lagged copy of the database that's in the same datacenter as the non-lagged copy.

Contoso has configured one of the passive copies of each mailbox database as a lagged database copy to provide protection against the extremely rare but catastrophic case of database logical corruption. As a result, the administrator is configuring the lagged copies as blocked for activation by using the Suspend-MailboxDatabaseCopy cmdlet with the *ActivationOnly* parameter. This ensures that the lagged database copies won't be activated if a database or server failover occurs.

Validating the Solution

After the solution has been deployed and configured, the administrator performs several tasks that validate the solution's readiness prior to moving production mailboxes to the databases in the DAG. The solution should be tested and inspected using several methods, including failure simulations. To validate the solution, the administrator performs several tasks.

To verify the overall health of the DAG, the administrator runs the Test-ReplicationHealth cmdlet. This cmdlet checks several aspects of the replication and replay status to provide information about each Mailbox server and database copy in the DAG.

To verify replication and replay activity, the administrator runs the Get-MailboxDatabaseCopyStatus cmdlet. This cmdlet can provide real-time status information about a specific mailbox database copy or for all mailbox database copies on a specific server. For more information about monitoring the health and status of replicated databases in a DAG, see Monitoring High Availability and Site Resilience.

To verify switchovers work as expected, the administrator uses the Move-ActiveMailboxDatabase cmdlet to perform a series of database switchovers and server switchovers. When these tasks have completed successfully, the administrator uses the same cmdlet to move the active database copies back to their original locations.

To verify the expected behaviors in various failure scenarios, the administrator performs several tasks that either simulate failures or actually cause failures to occur. For example, the administrator might:

- Unplug the power cord on MBX1A, thereby triggering a server failover. The administrator then verifies that DB1 becomes active on another server (preferably MBX2A, based on the activation preference values).
- Unplug the network cable for the MAPI network adapter on MBX2A, thereby triggering a server failover. The administrator then verifies that DB2 becomes active on another server (preferably MBX1A, based on the activation preference values).
- Take the disk used by the active copy of DB3 offline, thereby triggering a database failover. The administrator then verifies that DB3 becomes active on another server (preferably MBX2B, based on activation preference values).

There may be other failure scenarios that are tested by an organization, based on the business needs. After simulating a single failure (such as pulling the power plug), and verifying the solution's recovery behavior, the administrator may revert the solution back to its original configuration. In some cases, the solution may be tested for multiple concurrent failures. Ultimately, your solution test plan will dictate whether the solution is reverted back to its original configuration after each failure simulation has been completed.

In addition, an administrator may decide to disconnect the network connection between the two datacenters, thereby simulating a site failure. Performing a datacenter switchover is a much more involved and coordinated process; however, it's a recommended process if the solution being deployed is intended to provide site resilience for the messaging services and data. For details on datacenter switchovers, see Datacenter Switchovers.

Transitioning to Operations

After the solution has been deployed, it can be extended further using incremental

deployment. At this point, management of the solution would also transition to operation processes, in which the following tasks would be performed:

- Monitor the health and status of DAGs and mailbox database copies. For more information, see Monitoring High Availability and Site Resilience.
- Perform database and server switchovers as needed. For detailed steps to perform a database switchover, see Move the Active Mailbox Database. For detailed steps to perform a server switchover, see Perform a Server Switchover. If necessary, initiate a datacenter switchover. For more information about datacenter switchovers, see Datacenter Switchovers.

For more information about managing the solution, see Managing High Availability and Site Resilience.

1.10.4 Managing High Availability and Site Resilience

Managing High Availability and Site Resilience

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-05-06*

After you build, validate, and deploy a Microsoft Exchange Server 2010 high availability or site resilience solution, the solution transitions from the deployment phase to the operational phase of the overall solution lifecycle. The operational phase consists of several tasks, and all tasks are related to one of the following areas: database availability groups (DAGs), mailbox database copies, performing proactive monitoring, and managing switchovers and failovers.

Management of an Exchange 2010 high availability or site resilience solution is performed differently from previous versions of Exchange. Several architectural and design changes have been made in Exchange 2010 that eliminate the need to perform tasks required in previous versions of Exchange, and that provide you with greater granularity and control over the solution. For example:

- Exchange 2010 doesn't use the concept of a clustered mailbox server (referred to as an Exchange Virtual Server in Exchange Server 2003 and earlier). As a result, Exchange is no longer a clustered application, and Exchange server identities no longer move between clustered servers.
- Exchange 2010 doesn't use the concept of storage groups. As a result, databases are uncoupled from servers and are now managed globally, databases no longer share log streams, and continuous replication (including switchovers and failovers) operates at the database level.
- Exchange 2010 doesn't use the concepts of public and private networks. These concepts are replaced with the concepts of MAPI networks and replication networks. Each DAG should contain one MAPI network and one or more replication networks.

Contents

Database Availability Group Management

The operational management tasks associated with DAGs include:

- **Creating one or more DAGs** Creating a DAG is typically a one-time procedure performed during the deployment phase of the solution lifecycle. However, there may be reasons for creating DAGs that occur during the operational phase. For example:
  - The DAG is configured for third-party replication mode, and you want to revert to using continuous replication. You can't convert a DAG back to continuous replication; you need to create a DAG.
  - You have servers in multiple domains. All members of the same DAG must also be members of the same domain.
- **Managing DAG membership** Managing DAG members is an infrequent task typically performed during the deployment phase of the solution lifecycle. However, because of the flexibility provided by incremental deployment, managing DAG membership may also be performed throughout the solution lifecycle.
- **Configuring DAG properties** Each DAG has various properties that can be configured as needed. These properties include:
  - **Witness server and witness directory** The witness server is a server outside the DAG that acts as a quorum voter when the DAG contains an even number of members. The witness directory is a directory created and shared on the witness server for use by the system in maintaining a quorum.
  - **IP addresses** Each DAG will have one or more IPv4 addresses, and optionally, one or more IPv6 addresses. The IP addresses assigned to the DAG are used by the DAG's underlying cluster. The number of IPv4 addresses assigned to the DAG equals the number of subnets that comprise the MAPI network used by the DAG. You can configure the DAG to use static IP addresses or to obtain addresses automatically by using Dynamic Host Configuration Protocol (DHCP).
  - **Database activation coordination mode** Database activation coordination mode is a property setting on a DAG that's designed for DAGs with three or more members that have been deployed to multiple sites. Database activation coordination mode is used to handle conditions that would otherwise lead to a split-brain syndrome within the DAG, such as a site failure. For more information about database activation coordination mode, see Understanding Datacenter Activation Coordination Mode.
  - **Alternate witness server and alternate witness directory** The alternate witness server and alternate witness directory are values that you can preconfigure as part of the planning process for DAGs configured for site resilience.
  - **Replication port** By default, all DAGs use TCP port 64327 for continuous replication. You can modify the DAG to use a different TCP port for replication by using the *ReplicationPort* parameter of the Set-DatabaseAvailabilityGroup cmdlet.
  - **Network discovery** You can force the DAG to rediscover networks and network interfaces. This operation is used when you add or remove networks or change DAG network subnets. Rediscovery of all DAG networks can be forced by using the *DiscoverNetworks* parameter of the Set-DatabaseAvailabilityGroup cmdlet.
  - **Network compression** By default, DAGs use compression only between DAG networks on different subnets. You can enable compression for all DAG networks or for seeding operations only, or you can disable compression for all DAG networks.
  - **Network encryption** By default, DAGs use encryption only between DAG networks on different subnets. You can enable encryption for all DAG

networks or for seeding operations only, or you can disable encryption for all DAG networks.

- **Managing DAG networks** Although using a single network interface card (NIC) is supported, we recommend that each DAG member have at least two NICs. One NIC is used for the MAPI network, and one NIC is used for the replication network. Additional NICs can be added to create additional replication networks, for use as dedicated backup networks, or for use by the system as Internet SCSI (iSCSI) storage. DAG network management involves designating a network as a MAPI network or as a replication network, and configuring network subnets.
- **Shutting down DAG members** The Exchange 2010 high availability solution is integrated with the Windows shutdown process. If an administrator or application initiates a shutdown of a Windows server in a DAG that has a mounted database that's replicated to one or more DAG members, the system will try to activate another copy of the mounted databases prior to allowing the shutdown process to complete. However, this new behavior doesn't guarantee that all of the databases on the server being shut down will experience a loss-less activation. As a result, it's a best practice to perform a server switchover prior to shutting down a server that's a member of a DAG.

For detailed steps to create a DAG, see Create a Database Availability Group. For detailed steps to configure DAGs and DAG properties, see Configure Database Availability Group Properties. For more information about each of the preceding management tasks, and about managing DAGs in general, see Managing Database Availability Groups.

Return to top

Mailbox Database Copy Management

The operational management tasks associated with mailbox database copies include:

- **Adding mailbox database copies** When you add a copy of a mailbox database, continuous replication is automatically enabled between the existing database and the database copy.
- **Configuring mailbox database copy properties** You can configure a variety of properties, such as the database activation policy, the amount of time, if any, for replay lag and truncation lag, and the activation preference for the database copy.
- **Suspending or resuming a mailbox database copy** You can suspend a mailbox database copy in preparation for seeding, or for other forms of maintenance. You can also suspend a mailbox database copy for activation only. This configuration prevents the system from automatically activating the copy as a result of a failure, but it still allows the system to keep the database copy up to date with log shipping and replay.
- **Updating a mailbox database copy** Updating, also known as *seeding*, is the process in which a copy of a mailbox database is added to another Mailbox server. This becomes the baseline database for the copy. After the initial first seed of the baseline database copy, only in rare circumstances will the database need to be seeded again.
- **Activating a mailbox database copy** Activating is the process of designating a specific passive copy as the new active copy of a mailbox database. This process is referred to as a *switchover*. For more information, see "Switchovers and Failovers" later in this topic.
- **Removing a mailbox database copy** You can remove a mailbox database copy at any time. Occasionally, it may be necessary to remove a mailbox database copy. For example, you can't remove a Mailbox server from a DAG until all mailbox database copies are removed from the server. In addition, you must remove all copies of a mailbox database before you can change the path for a mailbox database.

For detailed steps to add a mailbox database copy, see Add a Mailbox Database Copy. For detailed steps to configure mailbox database copies, see Configure Mailbox Database Copy Properties. For more information about each of the preceding management tasks, and about managing mailbox database copies in general, see Managing Mailbox Database Copies. For detailed steps to remove a mailbox database copy, see Remove a Mailbox Database Copy.

Return to top

Proactive Monitoring

Making sure that your servers are operating reliably and that your database copies are healthy are key objectives for daily messaging operations. Exchange 2010 includes a number of features that can be used to perform a variety of health monitoring tasks for DAGs and mailbox database copies, including:

- Get-MailboxDatabaseCopyStatus
- Test-ReplicationHealth
- Crimson channel event logging

In addition to monitoring the health and status, it is also critical to monitor for situations that can compromise availability. For example, we recommend that you monitor the redundancy of your replicated databases. It is critical to avoid situations where you are down to a single copy of a database. This scenario should be treated with the highest priority and resolved as soon as possible.

For more detailed information about monitoring the health and status of DAGs and mailbox database copies, see Monitoring High Availability and Site Resilience.

Return to top

Switchovers and Failovers

A *switchover* is a manual process in which an administrator manually activates one or more mailbox database copies. Switchovers, which can occur at the database or server level, are typically performed as part of preparation for maintenance activities. Switchover management involves performing database or server switchovers as needed. For example, if you need to perform maintenance on a Mailbox server in a DAG, you would first perform a server switchover so that the server didn't host any active mailbox database copies. For detailed steps to perform a database switchover, see Move the Active Mailbox Database. For detailed steps to perform a server switchover, see Perform a Server Switchover. Switchovers can also be performed at the datacenter level. For more information about datacenter switchovers, see Datacenter Switchovers.

A *failover* is the automatic activation by the system of one or more database copies in reaction to a failure. For example, the loss of a disk drive will trigger a database failover. The loss of the MAPI network or a power failure will trigger a server failover.

For more information about switchovers and failovers, see Switchovers and Failovers.

Return to top

1.10.4.1 Managing Database Availability Groups

Managing Database Availability Groups

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-09*

A database availability group (DAG) is a set of up to 16 Microsoft Exchange Server 2010 Mailbox servers that provides automatic, database-level recovery from a database, server, or network failure. DAGs use continuous replication and a subset of Windows failover clustering technologies to provide high availability and site resilience. Mailbox servers in a DAG monitor each other for failures. When a Mailbox server is added to a DAG, it works with the other servers in the DAG to provide automatic, database-level recovery from database failures.

When you create a DAG, it's initially empty, and a directory object is created in Active Directory that represents the DAG. The directory object is used to store relevant information about the DAG, such as server membership information. When you add the first server to a DAG, a failover cluster is automatically created for the DAG. In addition, the infrastructure that monitors the servers for network or server failures is initiated. The failover cluster heartbeat mechanism and cluster database are then used to track and manage information about the DAG that can change quickly, such as database mount status, replication status, and last mounted location.

Contents

Creating DAGs

A DAG can be created using the New Database Availability Group wizard in the Exchange Management Console (EMC), or by running the **New-DatabaseAvailabilityGroup** cmdlet in the Exchange Management Shell. When creating a DAG, you provide a name for the DAG, and optional witness server and witness directory settings. In addition, one or more IP addresses are assigned to the DAG, either by using static IP addresses or by allowing the DAG to be automatically assigned the necessary IP addresses using Dynamic Host Configuration Protocol (DHCP). You can manually assign IP addresses to the DAG by using the *DatabaseAvailabilityGroupIpAddresses* parameter. If you omit this parameter, the DAG attempts to obtain an IP address by using a DHCP server on your network.

For detailed steps about how to create a DAG, see Create a Database Availability Group.

When you create a DAG, an empty object representing the DAG with the name you specified and an object class of **msExchMDBAvailabilityGroup** is created in Active Directory.

DAGs use a subset of Windows failover clustering technologies, such as the cluster heartbeat, cluster networks, and cluster database (for storing data that changes or can change quickly, such as database state changes from active to passive or the reverse, or from mounted to dismounted or the reverse). Because DAGs rely on Windows failover clustering, they can only be created on Exchange 2010 Mailbox servers running the Windows Server 2008 Enterprise operating system or Windows Server 2008 R2 Enterprise operating system.

Note:

The failover cluster created and used by the DAG must be dedicated to the DAG. The cluster can't be used for any other high availability solution or for any other purpose. For example, the failover cluster can't be used to cluster other applications or services. Using a DAG's underlying failover cluster for purposes other than the DAG isn't supported.

DAG Witness Server and Witness Directory

When creating a DAG, you need to specify a name for the DAG no longer than 15 characters that's unique within the Active Directory forest. In addition, each DAG is configured with a witness server and witness directory. The witness server and its directory are used only for quorum purposes where there's an even number of members in the DAG. You don't need to create the witness directory in advance. Exchange automatically creates and secures the directory for you on the witness server. The directory shouldn't be used for any purpose other than for the DAG witness server.

The requirements for the witness server are as follows:

- The witness server can't be a member of the DAG.
- The witness server must be in the same Active Directory forest as the DAG.
- The witness server must be running Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 R2, or Windows Server 2003.
- A single server can serve as a witness for multiple DAGs. However, each DAG requires its own witness directory.

We recommend that you use an Exchange 2010 Hub Transport server in the Active Directory site containing the DAG. This allows the witness server and directory to remain under the control of an Exchange administrator. Regardless of what server is used as the witness server, if the Windows Firewall is enabled on the intended witness server, you must enable the Windows Firewall exception for File and Printer Sharing.

Important:

If the witness server you specify isn't an Exchange 2010 server, you must add the Exchange Trusted Subsystem universal security group (USG) to the local Administrators group on the witness server prior to creating the DAG. These security permissions are necessary to ensure that Exchange can create a directory and share on the witness server as needed.

Neither the witness server nor the witness directory needs to be fault tolerant or use any form of redundancy or high availability. There's no need to use a clustered file server for the witness server or employ any other form of resiliency for the witness server. There are several reasons for this. With larger DAGs (for example, six members or more), several failures are required before the witness server is needed. Because a six-member DAG can tolerate as many as two voter failures without losing quorum, it would take as many as three voters failing before the witness server would be needed to maintain a quorum. Also, if there's a failure that affects your current witness server (for example, you lose the witness server because of a hardware failure), you can use the Set-DatabaseAvailabilityGroup cmdlet to configure a new witness server and witness directory

(provided you have a quorum).

Note:

You can also use the **Set-DatabaseAvailabilityGroup** cmdlet to configure the witness server and witness directory in the original location if the witness server lost its storage or if someone changed the witness directory or share permissions.

As a best practice, in an environment where a DAG is extended across multiple datacenters (and Active Directory sites) and configured for site resilience, we recommend that you use a witness server in your primary data center (the data center containing the majority of your user population). If each data center has a similar number of users, the data center you choose to host the witness server is considered to be the primary datacenter from the solution's perspective. If the witness server is in the datacenter with the majority of the client population, the majority of clients retain access after a failure.

If the datacenter is remote to large user populations, this may affect your decision. You would then need to determine if there's a requirement for the primary datacenter to remain healthy and active if there's a loss of wide are network (WAN) connectivity to the other two datacenters. In that event, the witness server should also be in the primary datacenter.

Although it's supported to use a witness server in a third datacenter, we don't recommend this scenario. From an Exchange perspective, this configuration doesn't provide you with greater availability. It's important that you examine the critical path factors if you use a witness server in a third datacenter. For example, if the WAN connection between the primary datacenter and the second and third datacenter fails, the solution in the primary datacenter becomes unavailable.

Specifying a Witness Server and Witness Directory During DAG Creation

When creating a DAG, you must provide a name for the DAG. You can optionally also specify a witness server and witness directory. If you specify a witness server, we recommend that you use a Hub Transport server, because this allows an Exchange administrator to be aware of the availability of the witness server.

When creating a DAG, the following combinations of options and behaviors are available:

- You can specify only a name for the DAG, and leave the **Witness server** and **Witness directory** fields blank. In this scenario, the wizard searches for a Hub Transport server that doesn't have the Mailbox server role installed, and it automatically creates the default directory (%SystemDrive% :\DAGFileShareWitnesses\<*DAGFQDN*>) and default share (<*DAGFQDN*>) on that server and uses that Hub Transport server as the witness server. For example, consider a witness server named EXMBX3 on which the operating system has been installed onto drive C. A DAG named DAG1 in a domain named contoso.com would use a default witness directory of C:\DAGFileShareWitnesses\DAG1.contoso.com, which would be shared as \ \EXMBX3\DAG1.contoso.com.
- You can specify a name for the DAG, the witness server that you want to use, and the directory you want created and shared on the witness server.
- You can specify a name for the DAG and the witness server that you want to use, and leave the **Witness directory** field blank. In this scenario, the wizard creates the default directory on the specified witness server.
- You can specify a name for the DAG, leave the **Witness server** field blank, and specify the directory you want created and shared on the witness server. In this scenario, the wizard searches for a Hub Transport server that doesn't have the Mailbox server role installed, and it automatically creates the specified DAG on that server, shares the directory, and uses that Hub Transport server as the witness server.

When a DAG is formed, it initially uses the Node Majority quorum model. When the second

Mailbox server is added to the DAG, the quorum is automatically changed to a Node and File Share Majority quorum model. When this change occurs, the DAG begins using the witness server for maintaining a quorum. If the witness directory doesn't exist, Exchange automatically creates it, shares it, and provisions the share with full control permissions for the cluster name object (CNO) computer account for the DAG.

Note:

Using a file share that is part of a Distributed File System (DFS) namespace is not supported.

If Windows Firewall is enabled on the witness server before the DAG is created, it may block the creation of the DAG. Exchange uses Windows Management Instrumentation (WMI) to create the directory and file share on the witness server. If Windows Firewall is enabled on the witness server and there are no firewall exceptions configured for WMI, the **New-DatabaseAvailabilityGroup** cmdlet fails with an error. If you specify a witness server, but not a witness directory, you receive the following error message.

```
The task was unable to create the default witness directory on server <Server Name>.
Please manually specify a witness directory.
```

If you specify a witness server and witness directory, you receive the following warning message.

```
Unable to access file shares on witness server 'ServerName'. Until this problem is
corrected, the database availability group may be more vulnerable to failures. You can
use the Set-DatabaseAvailabilityGroup cmdlet to try the operation again. Error: The
network path was not found.
```

If Windows Firewall is enabled on the witness server after the DAG is created but before servers are added, it may block the addition or removal of DAG members. If Windows Firewall is enabled on the witness server and there are no firewall exceptions configured for WMI, the **Add-DatabaseAvailabilityGroupServer** cmdlet displays the following warning message.

```
Failed to create file share witness directory 'C:\DAGFileShareWitnesses\DAG_FQDN' on
witness server 'ServerName'. Until this problem is corrected, the database availability
group may be more vulnerable to failures. You can use the Set-DatabaseAvailabilityGroup
cmdlet to try the operation again. Error: WMI exception occurred on server 'ServerName':
The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)
```

To resolve the preceding error and warnings, do one of the following:

- Manually create the witness directory and share on the witness server, and assign the CNO for the DAG full control for the directory and share.
- Enable the WMI exception in Windows Firewall.
- Disable Windows Firewall.

Return to top

DAG Membership

After a DAG has been created, you can add servers to or remove servers from the DAG using the Manage Database Availability Group wizard in the EMC, or using the **Add-DatabaseAvailabilityGroupServer** or **Remove-DatabaseAvailabilityGroupServer** cmdlets in the Shell. For detailed steps about how to manage DAG membership, see Manage Database Availability Group Membership.

Note:

Each Mailbox server that's a member of a DAG is also a node in the underlying cluster used by the DAG. As a result, at any one time, a Mailbox server can be a member of only one DAG.

If the Mailbox server being added to a DAG doesn't have the failover clustering component installed, the method used to add the server (for example, the **Add-DatabaseAvailabilityGroupServer** cmdlet or the Manage Database Availability Group wizard) installs the failover clustering feature.

When the first Mailbox server is added to a DAG, the following occurs:

- The Windows failover clustering component is installed, if it isn't already installed.
- A failover cluster is created using the name of the DAG. This failover cluster is used exclusively by the DAG, and the cluster must be dedicated to the DAG. Use of the cluster for any other purpose isn't supported.
- A CNO is created in the default computers container.
- The name and IP address of the DAG is registered as a Host (A) record in Domain Name System (DNS).
- The server is added to the DAG object in Active Directory.
- The cluster database is updated with information on the databases mounted on the added server.

In a large or multiple site environment, especially those in which the DAG is extended to multiple Active Directory sites, you must wait for Active Directory replication of the DAG object containing the first DAG member to complete. If this Active Directory object isn't replicated throughout your environment, adding the second server may cause a new cluster (and new CNO) to be created for the DAG. This is because the DAG object appears empty from the perspective of the second member being added, thereby causing the **Add-DatabaseAvailabilityGroupServer** cmdlet to create a cluster and CNO for the DAG, even though these objects already exist. To verify that the DAG object containing the first DAG server has been replicated, use the **Get-DatabaseAvailabilityGroup** cmdlet on the second server being added to verify that the first server you added is listed as a member of the DAG.

When the second and subsequent servers are added to the DAG, the following occurs:

- The server is joined to the Windows failover cluster for the DAG.
- The quorum model is automatically adjusted:
  - A Node Majority quorum model is used for DAGs with an odd number of members.
  - A Node and File Share Majority quorum model is used for DAGs with an even number of members.
- The witness directory and share are automatically created by Exchange when needed.
- The server is added to the DAG object in Active Directory.
- The cluster database is updated with information about mounted databases.

Note:

The quorum model change should happen automatically. However, if the quorum model doesn't automatically change to the proper model, you can run the **Set-DatabaseAvailabilityGroup** cmdlet with only the *Identity* parameter to correct the quorum settings for the DAG.

Pre-Staging the Cluster Name Object for a DAG

The CNO is a computer account created in Active Directory and associated with the cluster's Name resource. The cluster's Name resource is tied to the CNO, which is a Kerberos-enabled object that acts as the cluster's identity and provides the cluster's security context. In Exchange 2007, this Kerberos-enabled machine account was created in the domain using the security context of the user performing the tasks. This required the user's account to have permissions to create and enable machine accounts in the

domain or that the computer account was properly pre-staged and provisioned.

The formation of the DAG's underlying cluster and the CNO for that cluster is performed when the first member is added to the DAG. When the first server is added to the DAG, Powershell contacts the Microsoft Exchange Replication service on the Mailbox server being added. The Microsoft Exchange Replication service installs the failover clustering feature (if it isn't already installed) and begins the cluster creation process. The Microsoft Exchange Replication service runs under the LOCAL SYSTEM security context, and it's under this context in which cluster creation is performed.

Warning:
If your DAG members are running Windows Server 2012, you must pre-stage the CNO prior to adding the first server to the DAG.

In environments where computer account creation is restricted, or where computer accounts are created in a container other than the default computers container, you can pre-stage and provision the CNO. You create and disable a computer account for the CNO, and then either:

- Assign full control of the computer account to the computer account of the first Mailbox server you're adding to the DAG.
- Assign full control of the computer account to the Exchange Trusted Subsystem USG.

Assigning full control of the computer account to the computer account of the first Mailbox server you're adding to the DAG ensures that the LOCAL SYSTEM security context will be able to manage the pre-staged computer account. Assigning full control of the computer account to the Exchange Trusted Subsystem USG can be used instead because the Exchange Trusted Subsystem USG contains the machine accounts of all Exchange servers in the domain.

For detailed steps about how to pre-stage and provision the CNO for a DAG, see Pre-stage the Cluster Name Object for a Database Availability Group.

Removing Servers from a DAG

Mailbox servers can be removed from a DAG by using the Manage Database Availability Group wizard in the EMC or the **Remove-DatabaseAvailabilityGroupServer** cmdlet in the Shell. Before a Mailbox server can be removed from a DAG, all replicated mailbox databases must first be removed from the server. If you attempt to remove a Mailbox server with replicated mailbox databases from a DAG, the task fails.

There are scenarios in which you must remove a Mailbox server from a DAG before performing certain operations. These scenarios include:

- **Performing a server recovery operation** If a Mailbox server that's a member of a DAG is lost, or otherwise fails and is unrecoverable and needs replacement, you can perform a server recovery operation using the **Setup /m:RecoverServer** switch. However, before you can perform the recovery operation, you must first remove the server from the DAG using the Remove-DatabaseAvailabilityGroupServer cmdlet with the *ConfigurationOnly* parameter.
- **Removing the database availability** There may be situations in which you need to remove a DAG (for example, when disabling third-party replication mode). If you need to remove a DAG, you must first remove all servers from the DAG. If you attempt to remove a DAG that contains one or more members, the task fails.

Return to top

Configuring DAG Properties

After servers have been added to the DAG, you can use the EMC or the Shell to configure

the properties of a DAG, including the witness server and witness directory used by the DAG, and the IP addresses assigned to the DAG.

Configurable properties include:

- **Witness server** The name of the server that you want to host the file share for the file share witness. We recommend that you specify a Hub Transport server outside the DAG as the witness server. This enables the system to automatically configure, secure, and use the share, as needed.
- **Witness directory** The name of a directory that will be used to store file share witness data. This directory will automatically be created by the system on the specified witness server.
- **Database availability group IP addresses** One or more IP addresses assigned to the DAG. These addresses can be configured using manually assigned static IP addresses, or they can be automatically assigned to the DAG using a DHCP server in your organization.

The Shell enables you to configure DAG properties that aren't available in the EMC, such as DAG IP addresses, network encryption and compression settings, network discovery, the TCP port used for replication, and alternate witness server and witness directory settings, and to enable Datacenter Activation Coordination mode.

For detailed steps about how to configure DAG properties, see Configure Database Availability Group Properties.

DAG Network Encryption

DAGs support the use of encryption by leveraging the encryption capabilities of the Windows Server operating system. DAGs use Kerberos authentication between Exchange servers. Microsoft Kerberos security support provider (SSP) EncryptMessage and DecryptMessage APIs handle encryption of DAG network traffic. Microsoft Kerberos SSP supports multiple encryption algorithms. (For the complete list, see section 3.1.5.2, "Encryption Types" of Kerberos Protocol Extensions). The Kerberos authentication handshake selects the strongest encryption protocol supported in the list: typically Advanced Encryption Standard (AES) 256-bit, potentially with a SHA Hash-based Message Authentication Code (HMAC) to maintain integrity of the data. For details, see HMAC.

Network encryption is a property of the DAG and not a DAG network. You can configure DAG network encryption using the **Set-DatabaseAvailabilityGroup** cmdlet in the Shell. The possible encryption settings for DAG network communications are shown in the following table.

DAG network communication encryption settings

Setting	Description
Disabled	Network encryption isn't used.
Enabled	Network encryption is used on all DAG networks for replication and seeding.
InterSubnetOnly	Network encryption is used on DAG networks when replicating across different subnets. This is the default setting.
SeedOnly	Network encryption is used on all DAG networks for seeding only.

DAG Network Compression

DAGs support built-in compression. When compression is enabled, DAG network communication uses XPRESS, which is the Microsoft implementation of the LZ77 algorithm. For details, see An Explanation of the Deflate Algorithm and section 3.1.7.2 "Compression Algorithm" of Wire Format Protocol Specification. This is the same type of compression

used in many Microsoft protocols, in particular, MAPI RPC compression between Microsoft Outlook and Exchange.

As with network encryption, network compression is also a property of the DAG and not a DAG network. You configure DAG network compression by using the Set-DatabaseAvailabilityGroup cmdlet in the Shell. The possible compression settings for DAG network communications are shown in the following table.

DAG network communication compression settings

Setting	Description
Disabled	Network compression isn't used.
Enabled	Network compression is used on all DAG networks for replication and seeding.
InterSubnetOnly	Network compression is used on DAG networks when replicating across different subnets. This is the default setting.
SeedOnly	Network compression is used on all DAG networks for seeding only.

Return to top

DAG Networks

A DAG network is a collection of one or more subnets used for either replication traffic or MAPI traffic. Each DAG contains a maximum of one MAPI network and zero or more replication networks. In a single network adapter configuration, the network is used for both MAPI and replication traffic. Although a single network adapter and path is supported, we recommend that each DAG have a minimum of two DAG networks. In a two-network configuration, one network is typically dedicated for replication traffic, and the other network is used primarily for MAPI traffic. You can also add network adapters to each DAG member and configure additional DAG networks as replication networks.

Note:
When using multiple replication networks, there's no way to specify an order of precedence for network use. Exchange randomly selects a replication network from the group of replication networks to use for log shipping.

You can use the New Database Availability Group Network wizard in the EMC or the **New-DatabaseAvailabilityGroupNetwork** cmdlet in the Shell to create a DAG network. For detailed steps about how to create a DAG network, see Create a Database Availability Group Network.

You can use the DAG network's **Properties** dialog box in the EMC or the **Set-DatabaseAvailabilityGroupNetwork** cmdlet in the Shell to configure DAG network properties. For detailed steps about how to configure DAG network properties, see Configure Database Availability Group Network Properties. Each DAG network has required and optional parameters to configure:

- **Network name** A unique name for the DAG network of up to 128 characters.
- **Network description** An optional description for the DAG network of up to 256 characters.
- **Network subnets** One or more subnets entered using a format of *IPAddress/Bitmask* (for example, 192.168.1.0/24 for Internet Protocol version 4 (IPv4) subnets; 2001:DB8:0:C000::/64 for Internet Protocol version 6 (IPv6) subnets).
- **Enable replication** In the EMC, select the check box to dedicate the DAG

network to replication traffic, and block MAPI traffic. Clear the check box to prevent replication from using the DAG network, and to enable MAPI traffic. In the Shell, use the *ReplicationEnabled* parameter in the Set-DatabaseAvailabilityGroupNetwork cmdlet to enable and disable replication.

Note:

Disabling replication for the MAPI network doesn't guarantee that the system won't use the MAPI network for replication. When all configured replication networks are offline, failed, or otherwise unavailable, and only the MAPI network remains (which is configured as disabled for replication), the system uses the MAPI network for replication.

The initial DAG networks (for example, DAGNetwork01 and DAGNetwork02) created by the system are based on the subnets enumerated by the Cluster service. Each DAG member must have the same number of network adapters, and each network adapter must have an IPv4 address (and optionally, an IPv6 address as well) on a unique subnet. Multiple DAG members can have IPv4 addresses on the same subnet, but each network adapter and IP address pair in a specific DAG member must be on a unique subnet. In addition, only the adapter used for the MAPI network should be configured with a default gateway. Replication networks shouldn't be configured with a default gateway.

For example, consider DAG1, a two-member DAG where each member has two network adapters (one dedicated for the MAPI network and the other for a replication network). Example IP address configuration settings are shown in the following table.

Example network adapter settings

Server-network adapter	IP address/subnet mask	Default gateway
EX1-MAPI	192.168.1.15/24	192.168.1.1
EX1-Replication	10.0.0.15/24	Not applicable
EX2-MAPI	192.168.1.16	192.168.1.1
EX2-Replication	10.0.0.16	Not applicable

In the following configuration, there are two subnets configured in the DAG: 192.168.1.0 and 10.0.0.0. When EX1 and EX2 are added to the DAG, two subnets will be enumerated and two DAG networks will be created: DAGNetwork01 (192.168.1.0) and DAGNetwork02 (10.0.0.0). These networks will be configured as shown in the following table.

Enumerated DAG network settings for a single-subnet DAG

Name	Subnets	Interfaces	MAPI access enabled	Replication enabled
DAGNetwork01	192.168.1.0/24	EX1 (192.168.1.15) EX2 (192.168.1.16)	True	True
DAGNetwork02	10.0.0.0/24	EX1 (10.0.0.15) EX2 (10.0.0.16)	False	True

To complete the configuration of DAGNetwork02 as the dedicated replication network, disable replication for DAGNetwork01 by running the following command.

```
Set-DatabaseAvailabilityGroupNetwork -Identity DAG1\DAGNetwork01 -ReplicationEnab
```

After replication is disabled for DAGNetwork01, the Microsoft Exchange Replication service

uses DAGNetwork02 for continuous replication. If DAGNetwork02 experiences a failure, the Microsoft Exchange Replication service reverts to using DAGNetwork01 for continuous replication. This is done intentionally by the system to maintain high availability.

DAG Networks and Multiple Subnet Deployments

In the preceding example, even though there are two different subnets in use by the DAG (192.168.1.0 and 10.0.0.0), the DAG is considered a single-subnet DAG because each member uses the same subnet to form the MAPI network. When DAG members use different subnets for the MAPI network, the DAG is referred to as a *multi-subnet DAG*. In a multi-subnet DAG, additional configuration of the DAG networks must be performed to associate the proper subnets with each DAG network.

For example, consider DAG2, a two-member DAG where each member has two network adapters (one dedicated for the MAPI network and the other for a replication network), and each DAG member is located in a separate Active Directory site, with its MAPI network on a different subnet. Example IP address configuration settings are shown in the following table.

Example network adapter settings for a multi-subnet DAG

Server-network adapter	IP address/subnet mask	Default gateway
EX1-MAPI	192.168.0.15/24	192.168.0.1
EX1-Replication	10.0.0.15/24	Not applicable
EX2-MAPI	192.168.1.15	192.168.1.1
EX2-Replication	10.0.1.15	Not applicable

In the following configuration, there are four subnets configured in the DAG: 192.168.0.0, 192.168.1.0, 10.0.0.0, and 10.0.1.0. When EX1 and EX2 are added to the DAG, four subnets will be enumerated and two DAG networks will be created: DAGNetwork01 (192.168.0.0), DAGNetwork02 (10.0.0.0), DAGNetwork03 (192.168.1.0), and DAGNetwork04 (10.0.1.0). These networks will be configured as shown in the following table.

Enumerated DAG network settings for a multi-subnet DAG

Name	Subnets	Interfaces	MAPI access enabled	Replication enabled
DAGNetwork01	192.168.0.0/24	EX1 (192.168.0.15)	True	True
DAGNetwork02	10.0.0.0/24	EX1 (10.0.0.15)	False	True
DAGNetwork03	192.168.1.0/24	EX2 (192.168.1.15)	True	True
DAGNetwork04	10.0.1.0/24	EX2 (10.0.1.15)	False	True

To complete the necessary configuration, DAGNetwork03 and DAGNetwork04 should be collapsed into DAGNetwork01 and DAGNetwork02, respectively. This involves adding the subnet currently associated with DAGNetwork03 to DAGNetwork01, and adding the subnet currently associated with DAGNetwork04 to DAGNetwork02. This will remove the subnet associations from DAGNetwork03 and DAGNetwork04, leaving them as empty DAG networks that can then be removed. To collapse the subnets into two DAG networks and disable replication on the MAPI network, run the following commands.

```
Set-DatabaseAvailabilityGroupNetwork -Identity DAG2\DAGNetwork01 -Subnets 192.168
Set-DatabaseAvailabilityGroupNetwork -Identity DAG2\DAGNetwork02 -Subnets 10.0.0.
```

```
Remove-DatabaseAvailabilityGroupNetwork -Identity DAG2\DAGNetwork03
Remove-DatabaseAvailabilityGroupNetwork -Identity DAG2\DAGNetwork04
```

DAG Networks and iSCSI Networks

By default, DAGs perform discovery of all networks detected and configured for use by the underlying cluster. This includes any Internet SCSI (iSCSI) networks in use as a result of using iSCSI storage for one or more DAG members. As a best practice, iSCSI storage should use dedicated networks and network adapters. These networks shouldn't be managed by the DAG or its cluster, or used as DAG networks (MAPI or replication). Instead, these networks should be manually disabled from use by the DAG, so they can be dedicated to iSCSI storage traffic. To disable iSCSI networks from being detected and used as DAG networks, configure the DAG to ignore any currently detected iSCSI networks using the Set-DatabaseAvailabilityGroupNetwork cmdlet, as shown in this example:

```
Set-DatabaseAvailabilityGroupNetwork -Identity DAG2\DAGNetwork02 -ReplicationEnab
```

This command will also disable the network for use by the cluster. Although the iSCSI networks will continue to appear as DAG networks, they will not be used for MAPI or replication traffic after running the above command.

Return to top

Configuring DAG Members

Mailbox servers that are members of a DAG have some properties specific to high availability that should be configured as described in the following sections:

- Automatic Database Mount Dial
- Database Copy Automatic Activation Policy
- Maximum Active Databases

Automatic Database Mount Dial

The *AutoDatabaseMountDial* parameter specifies the automatic database mount behavior after a database failover. You can use the Set-MailboxServer cmdlet to configure the *AutoDatabaseMountDial* parameter with any of the following values:

- `BestAvailability` If you specify this value, the database automatically mounts immediately after a failover if the copy queue length is less than or equal to 12. The copy queue length is the number of logs recognized by the passive copy that needs to be replicated. If the copy queue length is more than 12, the database doesn't automatically mount. When the copy queue length is less than or equal to 12, Exchange attempts to replicate the remaining logs to the passive copy and mounts the database.
- `GoodAvailability` If you specify this value, the database automatically mounts immediately after a failover if the copy queue length is less than or equal to six. The copy queue length is the number of logs recognized by the passive copy that needs to be replicated. If the copy queue length is more than six, the database doesn't automatically mount. When the copy queue length is less than or equal to six, Exchange attempts to replicate the remaining logs to the passive copy and mounts the database.
- `Lossless` If you specify this value, the database doesn't automatically mount until all logs generated on the active copy have been copied to the passive copy. This setting also causes the Active Manager best copy selection algorithm to sort potential candidates for activation based on the database copy's activation preference value and not its copy queue length.

The default value is `GoodAvailability`. If you specify either `BestAvailability` or `GoodAvailability`, and all the logs from the active copy can't be copied to the passive copy being activated, you may lose some mailbox data. However, the transport dumpster feature (which is enabled by default) helps protect against most data loss by resubmitting messages that are in the transport dumpster queue.

In addition to the preceding values, you can also configure the *AutoDatabaseMountDial* parameter with a custom value by using ADSI Edit or Ldp.exe to modify the attribute directly in Active Directory. The *AutoDatabaseMountDial* parameter is represented by the **msExchDataLossForAutoDatabaseMount** attribute of the Mailbox server object. The whole number numeric value for this attribute represents the maximum number of transaction log files you are willing to lose to mount a database without human intervention. If you configure the *AutoDatabaseMountDial* parameter with a custom value greater than 12, we recommend that you also increase the size of the transport dumpster to enable increased protection against a greater number of lost logs.

Example: Configuring Automatic Database Mount Dial

The following example configures a Mailbox server with an *AutoDatabaseMountDial* setting of `GoodAvailability`.

```
Set-MailboxServer -Identity EX1 -AutoDatabaseMountDial GoodAvailability
```

Database Copy Automatic Activation Policy

The *DatabaseCopyAutoActivationPolicy* parameter specifies the type of automatic activation available for mailbox database copies on the selected Mailbox servers. You can use the Set-MailboxServer cmdlet to configure the *DatabaseCopyAutoActivationPolicy* parameter with any of the following values:

- `Blocked` If you specify this value, databases can't be automatically activated on the selected Mailbox servers.
- `IntrasiteOnly` If you specify this value, the database copy is allowed to be activated on servers in the same Active Directory site. This prevents cross-site failover or activation. This property is for incoming mailbox database copies (for example, a passive copy being made an active copy). Databases can't be activated on this Mailbox server for database copies that are active in another Active Directory site.
- `Unrestricted` If you specify this value, there are no special restrictions on activating mailbox database copies on the selected Mailbox servers.

Example: Configuring Database Copy Automatic Activation Policy

The following example configures a Mailbox server with a *DatabaseCopyAutoActivationPolicy* setting of `Blocked`.

```
Set-MailboxServer -Identity EX1 -DatabaseCopyAutoActivationPolicy Blocked
```

Maximum Active Databases

The *MaximumActiveDatabases* parameter (also used with the Set-MailboxServer cmdlet) specifies the number of databases that can be mounted on a Mailbox server. You can configure Mailbox servers to meet your deployment requirements by ensuring that an individual Mailbox server doesn't become overloaded.

The *MaximumActiveDatabases* parameter is configured with a whole number numeric value. When the maximum number is reached, the database copies on the server won't be activated if a failover or switchover occurs. If the copies are already active on a server, the server won't allow databases to be mounted.

Example: Configuring Maximum Active Databases

The following example configures a Mailbox server to support a maximum of 20 active databases.

```
Set-MailboxServer -Identity EX1 -MaximumActiveDatabases 20
```

Return to top

Performing Maintenance on DAG Members

Before performing any type of software or hardware maintenance on a DAG member, you

should first remove the DAG member from service by using the StartDagServerMaintenance.ps1 script. This script moves all the active databases off the server and blocks active databases from moving to that server. The script also ensures that all critical DAG support functionality that may be on the server (for example, the Primary Active Manager (PAM) role) is moved to another server and blocked from moving back to the server. Specifically, the StartDagServerMaintenance.ps1 script performs the following tasks:

- Runs Suspend-MailboxDatabaseCopy with the *ActivationOnly* parameter to suspend each database copy hosted on the DAG member for activation.
- Pauses the node in the cluster, which prevents the node from being and becoming the PAM.
- Sets the value of the *DatabaseCopyAutoActivationPolicy* parameter on the DAG member to `Blocked`.
- Moves all active databases currently hosted on the DAG member to other DAG members.
- If the DAG member currently owns the default cluster group, the script moves the default cluster group (and therefore the PAM role) to another DAG member.

If any of the preceding tasks fails, all operations, except for successful database moves, are undone.

After the maintenance is complete and the DAG member is ready to return to service, you can use the StopDagServerMaintenance.ps1 script to take the DAG member out of maintenance mode and put it back into production. Specifically, the StopDagServerMaintenance.ps1 script performs the following tasks:

- Runs the Resume-MailboxDatabaseCopy cmdlet for each database copy hosted on the DAG member.
- Resumes the node in the cluster, which enables full cluster functionality for the DAG member.
- Sets the value of the *DatabaseCopyAutoActivationPolicy* parameter on the DAG member to `Unrestricted`.

Both scripts accept the *-ServerName* parameter (which can be either the host name or the fully qualified domain name (FQDN) of the DAG member) and the *-WhatIf* parameter. Both scripts can be run locally or remotely. The server on which the scripts are executed must have the Windows Failover Cluster Management tools installed (RSAT-Clustering).

Return to top

Shutting Down DAG Members

The Exchange 2010 high availability solution is integrated with the Windows shutdown process. If an administrator or application initiates a shutdown of a Windows server in a DAG that has a mounted database that's replicated to one or more DAG members, the system attempts to activate another copy of the mounted database prior to allowing the shutdown process to complete.

However, this new behavior doesn't guarantee that all of the databases on the server being shut down will experience a `lossless` activation. As a result, it's a best practice to perform a server switchover prior to shutting down a server that's a member of a DAG. For detailed steps about how to perform a server switchover, see Perform a Server Switchover.

Return to top

Installing Update Rollups on DAG Members

Installing Microsoft Exchange Server 2010 update rollups on a server that is a member of a database availability group (DAG) is a relatively straightforward process. When you install an update rollup on a server that's a member of a DAG, several services are stopped during the installation, including all Exchange services and the Cluster service. The general process for applying update rollups to a DAG member is as follows:

1. Use the StartDagServerMaintenance.ps1 script to put the DAG member in maintenance mode.
2. Install the update rollup.
3. Use the StopDagServerMaintenance.ps1 script to take the DAG member out of maintenance mode and put it back into production.
4. Use the RedistributeActiveDatabases.ps1 script to rebalance the active database copies across the DAG.

You can download the latest update rollup for Exchange 2010 from the Microsoft Download Center. For detailed steps about how to install an update rollup on a DAG member, see Installing Update Rollups on Database Availability Group Members.

Return to top

1.10.4.1.1 Pre-stage the Cluster Name Object for a Database Availability Group

Pre-stage the Cluster Name Object for a Database Availability Group

High Availability and Site Resilience > Managing High Availability and Site Resilience > Managing Database Availability Groups >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-09*

In environments where computer account creation is restricted or where computer accounts are created in a container other than the default computers container, you can pre-stage the cluster name object (CNO) and then provision the CNO by assigning permissions to it. In addition, when deploying a database availability group (DAG) using Mailbox servers that are running Windows Server 2012, you must pre-stage and provision the CNO. Pre-staging the CNO is required for Windows Server 2012 DAG members due to permissions changes in Windows Server 2012 for computer objects. You create and disable a computer account for the CNO and then either:

- Assign full control of the computer account to the computer account of the first mailbox server you're adding to the DAG.
- Assign full control of the computer account to the Exchange Trusted Subsystem universal security group (USG).

After completing the following steps, allow time for Active Directory replication to occur. After the object is replicated, you can add the first member to the DAG.

Pre-stage the CNO

1. Open Active Directory Users and Computers.
2. Expand the forest node.
3. Right-click the organizational unit (OU) in which you want to create the new

account, select **New** and then select **Computer**.
4. In **New Object - Computer**, type the computer account name for the CNO in the **Computer name** box. This is the name that you'll use for the DAG itself. Click **OK** to create the account.
5. Right-click the new computer account, and then click **Disable Account**. Click **Yes** to confirm the disable action, and then click **OK**.

Assign permissions to the CNO

1. Open Active Directory Users and Computers.
2. If Advanced Features aren't enabled, turn them on by clicking **View**, and then clicking **Advanced Features**.
3. Right-click the new computer account, and then click **Properties**.
4. In **<Computer Name> Properties**, on the **Security** tab, click **Add** to add either the computer account for the first node to be added to the DAG or to add the Exchange Trusted Subsystem USG:
   - To add the Exchange Trusted Subsystem, type **Exchange Trusted Subsystem** in the **Enter the object names to select** field. Click **OK** to add the USG. Then select the Exchange Trusted Subsystem USG and in **Permissions for Exchange Trusted Subsystem field**, select **Full Control** in the **Allow** column. Click **OK** to save the permission settings.
   - To add the computer account for the first node to be added to the DAG, click **Object Types**. In the **Object Types** dialog box, clear the **Built-in security principals**, **Groups**, and **Users** check boxes. Select the **Computers** check box. Click **OK**. In the **Enter the object names to select** field, type the name of the first Mailbox server to be added to the DAG, and then click **OK**. Then, select the first node's computer account, and in the **Permissions for <NodeName>** field, select **Full Control** in the **Allow** column. Click **OK** to save the permission settings.

1.10.4.1.2 Create a Database Availability Group

Create a Database Availability Group

High Availability and Site Resilience > Managing High Availability and Site Resilience > Managing Database Availability Groups >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-09*

A database availability group (DAG) is a set of up to 16 Microsoft Exchange Server 2010 Mailbox servers that provide automatic database-level recovery from a database, server, or network failure. Mailbox servers in a DAG monitor each other for failures. When a Mailbox server is added to a DAG, it works with the other servers in the DAG to provide automatic, database-level recovery from database, server, and network failures.

When creating a DAG, you provide a unique name for the DAG of up to 15 characters. In addition to providing a name for the DAG, you must also assign one or more IP addresses (either IPv4 or both IPv4 and IPv6) to the DAG. The IP addresses you assign must be on the subnet intended for the MAPI network and must be available for use. You can assign static IP addresses to the DAG by using the *DatabaseAvailabilityGroupIpAddresses* parameter. If you use the Exchange Management Console (EMC) to create the DAG, or if you use the **New-DatabaseAvailabilityGroup** cmdlet without the *DatabaseAvailabilityGroupIpAddresses* parameter, the task will configure the DAG to use Dynamic Host Configuration Protocol (DHCP) to obtain the necessary IPv4 addresses. If

you don't want the DAG to use DHCP, you can use the **Set-DatabaseAvailabilityGroup** cmdlet to configure one or more IP addresses for the DAG after it has been created. If your system is configured to use IPv6, the task will also attempt to automatically assign the DAG one or more IPv6 addresses.

Optionally, you can also specify a witness server and witness directory. If you do specify a witness server, we recommend that you use a Hub Transport server. This allows an Exchange administrator to be aware of the availability of the witness.

The following combinations of options and behaviors are available:

- You can specify only a name for the DAG and leave the **Witness Server** and **Witness Directory** check boxes cleared. In this scenario, the wizard will search for a Hub Transport server that doesn't have the Mailbox server role installed. It will automatically create the default directory and share on that Hub Transport server and use that server as the witness server.
- You can specify a name for the DAG, the witness server that you want to use, and the directory you want created and shared on the witness server.
- You can specify a name for the DAG and the witness server that you want to use, and leave the **Witness Directory** check box cleared. In this scenario, the wizard will create the default directory on the specified witness server.
- You can specify a name for the DAG, leave the **Witness Server** check box cleared, and specify the directory you want created and shared on the witness server. In this scenario, the wizard will search for a Hub Transport server that doesn't have the Mailbox server role installed, and it will automatically create the specified directory on that server, share the directory, and use that Hub Transport server as the witness server.

Important:

If the witness server you specify isn't an Exchange 2010 server, you must add the Exchange Trusted Subsystem universal security group to the local Administrators group on the witness server. These security permissions are necessary to ensure that Exchange can create a directory and share on the witness server as needed. If the proper permissions aren't configured, the following error is returned:
Error: An error occurred during discovery of the database availability group topology. Error: An error occurred while attempting a cluster operation. Error: Cluster API "AddClusterNode() (MaxPercentage=12) failed with 0x80070005. Error: Access is denied."

When creating a DAG with Mailbox servers running Windows Server 2012, you must pre-stage the cluster name object (CNO) before adding members to the DAG. For detailed steps, see Pre-stage the Cluster Name Object for a Database Availability Group.

Looking for other management tasks related to DAGs? Check out Managing Database Availability Groups.

What Do You Want to Do?

- Use the EMC to create a database availability group
- Use the Shell to create a database availability group

Use the EMC to create a database availability group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database availability groups" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Database Availability Group**.

3. On the **New Database Availability Group** page, provide the following information for the new DAG:
   - **Database availability group name** Use this box to type a valid and unique name for the DAG of up to 15 characters. The name is equivalent to a computer name, and a corresponding Cluster Name Object (CNO) will be created in Active Directory with the name of the DAG. The name of the DAG isn't used by end users or administrators. It is used only by the system for internal communication and to secure the DAG.
   - **Witness Server** Select this check box and use the corresponding text box to specify a witness server for the DAG. If you don't select this check box, the system will attempt to automatically select a Hub Transport server that doesn't have the Mailbox server role installed to be used as the witness server.

     Note:
     If you specify a witness server, you must use either a host name or a fully-qualified domain name (FQDN). Using an IP address or a wildcard name isn't supported. In addition, the witness server cannot be a member of the DAG.
   - **Witness Directory** Select this check box and use the corresponding text box to type the path to a directory that will be used to store witness data. If the directory doesn't exist, the system will create it for you on the witness server. If you don't select this check box, the default directory will be created on the witness server.
4. Click **New** to create the database availability group.
5. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to close the wizard.

After you create a DAG, it will be configured to use DHCP. If you don't want the DAG to use DHCP, you can use the **Set-DatabaseAvailabilityGroup** cmdlet to configure one or more IP addresses for the DAG.

Use the Shell to create a database availability group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database availability groups" entry in the High Availability Permissions topic.

This example creates a DAG named DAG1 that is configured to use the witness server EXHUB1 and the local directory C:\DAG1. DAG1 is also configured to use DHCP for the DAG's IP addresses.

```
New-DatabaseAvailabilityGroup -Name DAG1 -WitnessServer EXHUB1 -WitnessDirectory
```

This example creates a DAG named DAG2. The system will automatically select a Hub Transport server that doesn't have the Mailbox server role installed in the same site as the DAG to use as the witness server. DAG2 is assigned a single static IP address because all members are on the same subnet.

```
New-DatabaseAvailabilityGroup -Name DAG2 -DatabaseAvailabilityGroupIPAddresses 10
```

This example creates a DAG named DAG3. DAG3 is configured to use the witness server EXHUB2 and the local directory C:\DAG3. DAG3 is assigned multiple static IP addresses because its members are or will be on different subnets.

```
New-DatabaseAvailabilityGroup -Name DAG3 -WitnessServer EXHUB2 -WitnessDirectory
```

This example creates a w DAG named DAG4 that is configured to use DHCP. In addition, the witness server will be automatically selected by the system and the default witness directory will be created.

```
New-DatabaseAvailabilityGroup -Name DAG4
```

For More Information

Understanding Database Availability Groups

Configure Database Availability Group Properties

Set-DatabaseAvailabilityGroup

New-DatabaseAvailabilityGroup

New-DatabaseAvailabilityGroupNetwork

Add-DatabaseAvailabilityGroupServer

1.10.4.1.3 Configure Database Availability Group Properties

Configure Database Availability Group Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-01-23*

You can use the Exchange Management Console (EMC) or the Exchange Management Shell to configure the properties of a database availability group (DAG), including the *witness* server and directory used by the DAG. The Shell enables you to configure DAG properties that are not available in EMC, network discovery and settings, the TCP port used for replication, and datacenter activation coordination (DAC) mode.

DAG property values are stored in both Active Directory and the cluster database. However, some properties are stored on in the cluster database. As a result, the underlying cluster for the DAG must be up and running and have quorum in order to set the properties for:

- ReplicationPort
- NetworkCompression
- NetworkEncryption
- DiscoverNetworks

What Do You Want to Do?

- Use the EMC to configure database availability group properties

Use the EMC to configure database availability group properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the" Database availability group" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Availability Group** tab, right-click the DAG you want to configure, and then click **Properties**.
3. Use the **General** tab to view DAG membership, configure the DAG's witness server, and to configure network encryption and compression for the DAG networks.
   - **Modified** This read-only field displays the date and time at which the DAG's properties were last changed.
   - **Member servers** This read-only field displays the Mailbox servers that are members of the DAG.
   - **Witness Server** This box displays the host name or fully-qualified domain name (FQDN) of a server that's external to the DAG that is used when the DAG contains an even number of members.
   - **Witness Directory** This box displays the full name and path of the directory used to store the witness.log file on the witness server.
   - **Alternate Witness Server** This box displays the host name or FQDN of a server that's external to the DAG and is used as a replacement for the witness server during a datacenter switchover process.
   - **Alternate Witness Directory** This box displays the name of the directory used to store the witness.log file on the alternate witness server.
4. Use the **IP Addresses** tab to view and modify the IP addresses assigned to the DAG.
   - **Add** Click this button to add a static IPv4 address to the DAG.
   - **Edit** Select an existing IPv4 address and then click this button to modify it.
   -  Select one or more existing IPv4 addresses and then click this button to remove them from them DAG.
5. Use the **Operational Servers** tab to view the list of DAG members that are currently operational.

Use the Shell to configure database availability group properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database availability group" entry in the High Availability Permissions topic.

This example sets the witness directory to C:\DAG1DIR for a DAG named DAG1.

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -WitnessDirectory C:\DAG1DIR
```

This example pre-configures an alternate witness server of EXHUB3 and an alternate witness directory of C:\DAGFileShareWitnesses\DAG1.contoso.com for a DAG named DAG1.

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -AlternateWitnessDirectory C:\DAGFil
```

This example configures a DAG named DAG1 to use DHCP to obtain an IP address.

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -DatabaseAvailabilityGroupIPAddresse
```

This example configures a DAG named DAG1 to use a static IP address of 10.0.0.8.

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -DatabaseAvailabilityGroupIPAddresse
```

This example configures a multi-subnet DAG named DAG1 with multiple static IP addresses.

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -DatabaseAvailabilityGroupIPAddresse
```

This example configures a DAG named DAG1 for datacenter activation mode.

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -DatacenterActivationMode DagOnly
```

This example configures the replication port for a DAG named DAG1 to be 63132.

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -ReplicationPort 63132
```

Note:
After changing the default replication port for a DAG, you must manually modify the Windows Firewall exceptions on each member of the DAG to allow communication to occur over the specified port.

For More Information

Create a Database Availability Group

Remove a Database Availability Group

Create a Database Availability Group Network

Manage Database Availability Group Membership

Get-DatabaseAvailabilityGroup

Set-DatabaseAvailabilityGroup

1.10.4.1.4 Manage Database Availability Group Membership

Manage Database Availability Group Membership

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-09*

When you add a server to a database availability group (DAG), it works with the other servers in the DAG to provide automatic, database-level recovery from database, server, or network failures. When you remove a server from a DAG, it is no longer automatically protected from failures.

DAGs use Windows Failover Clustering (WFC) technologies. Each Mailbox server that is a member of a DAG is also a node in the underlying cluster that is used by the DAG. As a

result, at any given time, a Mailbox server can be a member of only one DAG.

Looking for other management tasks related to DAGs? Check out Managing Database Availability Groups.

Prerequisites

- A DAG has been created. For detailed steps, see Create a Database Availability Group.
- Because DAGs use WFC technology, all servers added to a DAG must be running either Windows Server 2008 Service Pack 2 (SP2) Enterprise Edition or Windows Server 2008 R2 Enterprise Edition.
- All servers in a DAG must be running the same operating system. You can't have DAG members that are running Windows Server 2008 SP2 and others that are running Windows Server 2008 R2.
- If you're adding Mailbox servers running Windows Server 2012, you must pre-stage the cluster name object (CNO) for the DAG. For detailed steps, see Pre-stage the Cluster Name Object for a Database Availability Group.
- You must remove all replicated database copies from the server before you can remove it from a DAG.

What Do You Want to Do?

- Use the EMC to manage database availability group membership
- Use the Shell to manage database availability group membership

Use the EMC to manage database availability group membership

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database availability groups" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Availability Group** tab, right-click the DAG you want to manage, and then click **Manage Database Availability Group Membership**.
3. On the **Manage Database Availability Group Membership** page, you can perform the following tasks.
   - To add a local server to the DAG, click **Add** and then use the **Select Mailbox Server** dialog box to select the server you want.
   - To remove a local server from the DAG, select a server from the list of members, and the click  .
4. Click **Manage** to perform the configured management action (adding or removing a server).
5. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to manage database

availability group membership

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database availability groups" entry in the High Availability Permissions topic.

This example adds a Mailbox server named MBX1 to a DAG named DAG1.

```
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1
```

This example removes a Mailbox server named MBX1 from a DAG named DAG1. Before running this command, make sure that no replicated databases exist on the Mailbox server.

```
Remove-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1
```

This example removes the configuration settings for Mailbox server named MBX4 from a DAG named DAG2. MBX4 is expected to be offline for an extended period, so its configuration is being removed from the DAG while it is offline in order to establish quorum with the remaining online DAG members.

```
Remove-DatabaseAvailabilityGroupServer -Identity DAG2 -MailboxServer MBX4 -Config
```

For More Information

Add-DatabaseAvailabilityGroupServer

Remove-DatabaseAvailabilityGroupServer

1.10.4.1.5 Recover a Database Availability Group Member Server

Recover a Database Availability Group Member Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-06-08*

If a Mailbox server that's a member of a database availability group (DAG) is lost or otherwise fails and is unrecoverable and needs replacement, you can perform a server recovery operation. Microsoft Exchange Server 2010 Setup includes the switch **/m:RecoverServer** that can be used to perform the server recovery operation. Running Setup with the **/m:RecoverServer** switch causes Setup to read the server's configuration information from Active Directory for a server with the same name as the server from which you're running Setup. After the server's configuration information is gathered from Active Directory, the original Exchange files and services are then installed on the server, and the roles and settings that were stored in Active Directory are then applied to the server.

Looking for other management tasks related to DAGs? Check out Managing Database Availability Groups.

Note:

If Exchange is installed in a location other than the default location, you must use the **/TargetDir** Setup switch to specify the location of the Exchange program files. If you don't

use the **/TargetDir** switch, the Exchange program files will be installed in the default location (%programfiles%\Microsoft\Exchange Server\V14).
To determine the install location, follow these steps:

1. Open ADSIEDIT.MSC or LDP.EXE.
2. Navigate to the following location:
   CN=ExServerName,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=ExOrg Name,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=DomainName,CN=Com
3. Right-click the Exchange server object, and then click **Properties**.
4. Locate the **msExchInstallPath** attribute. This attribute stores the current installation path.

Use Setup /m:RecoverServer to recover a server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Mailbox database copies" entry in the High Availability Permissions topic.

1. Retrieve any replay lag or truncation lag settings for any mailbox database copies that exist on the server being recovered by using the Get-MailboxDatabase cmdlet.

```
Get-MailboxDatabase DB1 | Format-List *lag*
```

2. Remove any mailbox database copies that exist on the server being recovered by using the Remove-MailboxDatabaseCopy cmdlet.

```
Remove-MailboxDatabaseCopy DB1\MBX1
```

3. Remove the failed server's configuration from the DAG by using the Remove-DatabaseAvailabilityGroupServer cmdlet.

```
Remove-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer M
```

Note:
If the DAG member being removed is offline and cannot be brought online, you must add the *ConfigurationOnly* parameter to the above command.

1. Reset the server's computer account in Active Directory. For detailed steps, see Reset a Computer Account.
2. Open a Command Prompt window. Using the original Setup media, run the following command.

```
Setup /m:RecoverServer
```

3. When the Setup recovery process is complete, add the recovered server to the DAG by using the Add-DatabaseAvailabilityGroupServer cmdlet.

```
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1
```

4. After the server has been added back to the DAG, you can reconfigure mailbox database copies by using the Add-MailboxDatabaseCopy cmdlet. If any of the database copies being added previously had replay lag or truncation lag times greater than 0, you can use the *ReplayLagTime* and *TruncationLagTime* parameters of the Add-MailboxDatabaseCopy cmdlet to reconfigure those settings.

```
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX1
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX1 -ReplayLagTi
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX1 -ReplayLagTi
```

Create a Database Availability Group Network

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can create multiple networks in a database availability group (DAG) and dedicate them for client access or for replication purposes.

Looking for other management tasks related to DAGs? Check out Managing Database Availability Groups.

What Do You Want to Do?

- Use the EMC to create a database availability group network
- Use the Shell to create a database availability group network

Use the EMC to create a database availability group network

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database availability group" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Availability Group** tab.
3. Right-click the DAG for which you want to create the new network, and then click **New Database Availability Group Network**. You can also select the DAG and then click **New Database Availability Group Network** in the action pane.
4. On the **New Database Availability Group Network** page, provide the following configuration information for the new DAG network.
   - **Network name** Provide a unique name for the DAG network (a name that doesn't conflict with the name of any other DAG network). The limit is 128 characters.
   - **Network description** Provide an optional description for the DAG network. The limit is 256 characters.
   - **Database Availability Group network subnets** Click **Add** to add each network subnet to the DAG network. Subnets should be entered using a format of IP address/bitmask (for example, 192.168.1.0/24 for IPv4 subnets; 2001:DB8:0:C000::/54 for IPv6 subnets). If you add a subnet that's currently associated with another DAG network, the subnet will be removed from the other DAG network and associated with the network being created.
   - **Enable replication** Select this check box to enable the DAG network for use by replication. When a DAG network is enabled for replication, MAPI traffic is restricted on that network. Clear this check box to prevent replication from using the DAG network and to enable MAPI traffic on that network.
5. Click **New** to create the DAG network.
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task

successfully.
- A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

7. Click **Finish** to close the wizard.

Use the Shell to create a database availability group network

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database availability group" entry in the High Availability Permissions topic.

In this example, the network DagNet1 is being created with a subnet of 10.0.0.0 and a bitmask of 8 in a DAG named DAG1. Replication is enabled for the network, and an optional description of the network is also being added.

```
New-DatabaseAvailabilityGroupNetwork -DatabaseAvailabilityGroup DAG1 -Name DagNet
```

For More Information

Set-DatabaseAvailabilityGroupNetwork

Get-DatabaseAvailabilityGroupNetwork

New-DatabaseAvailabilityGroupNetwork

Remove-DatabaseAvailabilityGroupNetwork

1.10.4.1.7 Configure Database Availability Group Network Properties

Configure Database Availability Group Network Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Each database availability group (DAG) network has several properties that you can configure, including the name of the DAG network, a description field for the DAG network, a list of subnets that are used by the DAG network, and whether or not the DAG network is enabled for replication.

Looking for other management tasks related to DAGs? Check out Managing Database Availability Groups.

What Do You Want to Do?

- Use the EMC to configure database availability group network properties
- Use the Shell to configure database availability group network properties

Use the EMC to configure database

availability group network properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the" database availability group" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Availability Group** tab, select the DAG you want.
3. In the work pane, on the **Networks** tab, right-click the DAG network you want, and then click **Properties**.
4. Use the **General** tab to configure DAG network properties.
   - The top field contains the name of the DAG network. Each DAG network name must be unique and can't contain more than 128 characters.
   - **Description of this network** Use this box to provide an optional description of up to 256 characters for the DAG network.
   - **Edit subnets for this network** Each DAG network must contain at least one subnet. Subnets using should be added using a format of IPAddress/Bitmask (for example, 192.168.1.0/24 for IPv4 subnets; 2001:DB8:0:C000::/54 for IPv6 subnets).
   - **Enable replication** Leave this check box checked to enable replication traffic on the DAG network. When a DAG network is enabled for replication, MAPI traffic is restricted on that network. Clear this check box to prevent the DAG network from being used for replication (provided one or more replication networks are available) and to enable MAPI traffic on that network.

Use the Shell to configure database availability group network properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the" database availability group" entry in the High Availability Permissions topic.

In this example, a DAG network in a DAG named DAG1 is being renamed from its default network of DAGNetwork01 to a new name of CRNET1.

```
Set-DatabaseAvailabilityGroupNetwork -Name DAGNET1 -Identity DAG1\DAGNetwork01
```

In this example, a subnet of 10.0.0.0 and subnet mask of 255.0.0.0 is being added to a DAG network named DAGNET1 in a DAG named DAG1.

```
Set-DatabaseAvailabilityGroupNetwork -Subnets 10.0.0.0/8 -Identity DAG1\DAGNET1
```

For More Information

Set-DatabaseAvailabilityGroupNetwork

Get-DatabaseAvailabilityGroupNetwork

New-DatabaseAvailabilityGroupNetwork

Remove-DatabaseAvailabilityGroupNetwork

1.10.4.1.8 Remove a Database Availability Group

Remove a Database Availability Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Before you can remove a database availability group (DAG), the DAG must be empty. If the DAG you want to remove contains any Mailbox servers, you must first remove the servers from the DAG. For detailed steps about how to remove a Mailbox server from a DAG, see Manage Database Availability Group Membership.

Looking for other management tasks related to DAGs? Check out Managing Database Availability Groups.

Use the EMC to remove a database availability group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Database availability groups" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Availability Group** tab, right-click the DAG you want to remove, and then click **Remove**.
3. Click **Yes** to confirm the action and remove the DAG.

Use the Shell to remove a database availability group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Database availability groups" entry in the High Availability Permissions topic.

This example removes a DAG named DAG1.

```
Remove-DatabaseAvailabilityGroup -Identity DAG1 -Confirm:$False
```


1.10.4.2 Managing Mailbox Database Copies

Managing Mailbox Database Copies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-03*

Database mobility is a new architecture in Microsoft Exchange Server 2010 that removes the concept of storage groups and uncouples the Exchange 2010 mailbox database from Mailbox servers. Because storage groups have been removed from Exchange 2010, continuous replication now operates at the database level. In Exchange 2010, transaction

logs are replicated to one or more Mailbox servers in a database availability group (DAG), and replayed into one or more copies of a mailbox database stored on those servers. Several concepts used in Exchange Server 2007 continuous replication remain in Exchange 2010. These include the concepts of divergence, the use of the automatic database mount dial, and the use of public and private networks.

Managing Database Copies

After multiple copies of a database are created, you can use the Exchange Management Console (EMC) and the Exchange Management Shell to monitor the health and status of each copy and to perform other management tasks associated with database copies. Some of the management tasks you may need to perform include suspending or resuming a database copy, seeding a database copy, monitoring database copies, configuring database copy settings, and removing a database copy.

Suspending and Resuming Database Copies

For a variety of reasons, such as performing planned maintenance, it may be necessary to suspend and resume continuous replication activity for a database copy. In addition, some administrative tasks, such as seeding, require you to first suspend a database copy. We also recommend that all replication activity be suspended when the path for the database or its log files is being changed. You can suspend and resume database copy activity by using the EMC, or by running the **Suspend-MailboxDatabaseCopy** and **Resume-MailboxDatabaseCopy** cmdlets in the Shell. For detailed steps to suspend or resume continuous replication activity for a database copy, see Suspend or Resume a Mailbox Database Copy.

Log truncation doesn't occur on the active mailbox database copy when one or more passive copies are suspended. If your planned maintenance activities are going to take an extended period of time (for example, several days), you may have considerable log file buildup. To prevent the log drive from filling up with transaction logs, you can remove the affected passive database copy instead of suspending it. When the planned maintenance is completed, you can re-add the passive database copy.

Seeding a Database Copy

Seeding, also known as *updating*, is the process in which a database, either a blank database or a copy of the production database, is added to the target copy location on another Mailbox server in the same DAG as the active database. This becomes the baseline database for the copy maintained by that server.

Depending on the situation, seeding can be an automatic process or a manual process that you initiate. When a database copy is added, the copy will be automatically seeded, provided that the target server and its storage are properly configured. If you want to manually seed a database copy and don't want automatic seeding to occur when creating the copy, you can use the *SeedingPostponed* parameter when running the Add-MailboxDatabaseCopy cmdlet.

Database copies rarely need to be reseeded after the initial seeding has occurred. But if reseeding is necessary, or if you want to manually seed a database copy instead of having the system automatically seed the copy, these tasks can be performed by using the Update Database Copy wizard in the EMC or by using the Update-MailboxDatabaseCopy cmdlet in the Shell. Before seeding a database copy, you must first suspend the mailbox database copy. For detailed steps to seed a database copy, see Update a Mailbox Database Copy.

After a manual seed operation has completed, replication for the seeded mailbox database copy is automatically resumed. If you don't want replication to automatically resume, you can use the *ManualResume* parameter when running the Update-MailboxDatabaseCopy cmdlet.

Choosing What to Seed

When performing a seed operation, you can choose to seed the mailbox database copy, the content index catalog for the mailbox database copy, or both the database copy and the content index catalog copy. The default behavior of the Update Database Copy wizard and the Update-MailboxDatabaseCopy cmdlet is to seed both the mailbox database copy and the content index catalog copy. To seed just the mailbox database copy without seeding the content index catalog, use the *DatabaseOnly* parameter when running the Update-MailboxDatabaseCopy cmdlet. To seed just the content index catalog copy, use the *CatalogOnly* parameter when running the Update-MailboxDatabaseCopy cmdlet.

Selecting the Seeding Source

In Exchange 2007, continuous replication could only seed a database copy by copying the active copy of the database. In Exchange 2010, any healthy database copy can be used as the seeding source for an additional copy of that database. This is particularly useful when you have a DAG that has been extended across multiple physical locations. For example, consider a four-member DAG deployment, where two members (MBX1 and MBX2) are located in Portland, Oregon and two members (MBX3 and MBX4) are located in New York, New York. A mailbox database named DB1 is active on MBX1 and there are passive copies of DB1 on MBX2 and MBX3. When adding a copy of DB1 to MBX4, you have the option of using the copy on MBX3 as the source for seeding, and in doing so, you avoid seeding over the wide area network (WAN) link between Portland and New York.

To use a specific copy as a source for seeding when adding a new database copy, you would do the following:

- Use the *SeedingPostponed* parameter when running the Add-MailboxDatabaseCopy cmdlet to add the database copy. If the *SeedingPostponed* parameter isn't used, the database copy will be explicitly seeded using the active copy of the database as the source.
- Use the *SourceServer* parameter when running the Update-MailboxDatabaseCopy cmdlet and specify the desired source server for seeding. In the preceding example, you would specify MBX3 as the source server. If the *SourceServer* parameter isn't used, the database copy will be explicitly seeded using the active copy of the database as the source.

Seeding and Networks

In addition to selecting a specific source server for seeding a mailbox database copy, you can also specify which DAG networks to use, and optionally override the DAG network's compression and encryption settings during the seed operation.

To specify the networks you want to use for seeding, use the *Network* parameter when running the Update-MailboxDatabaseCopy cmdlet and specify the DAG networks that you want to use. If you don't use the *Network* parameter, the system uses the following default behavior for selecting a network to use for the seeding operation:

- If the source server and target server are on the same subnet and a replication network has been configured that includes the subnet, the replication network will be used.
- If the source server and target server are on different subnets, even if a replication network that contains those subnets has been configured, the client (MAPI) network will be used for seeding.
- If the source server and target server are in different datacenters, the client (MAPI) network will be used for seeding.

At the DAG level, DAG networks are configured for encryption and compression. The default settings are to use encryption and compression only for communications on different subnets. If the source and target are on different subnets and the DAG is configured with the default values for *NetworkCompression* and *NetworkEncryption*, you can override these values by using the *NetworkCompressionOverride* and *NetworkEncryptionOverride* parameters, respectively, when running the Update-

MailboxDatabaseCopy cmdlet.

Seeding Process

When you initiate a seeding process by using the Add-MailboxDatabaseCopy or Update-MailboxDatabaseCopy cmdlets, the following tasks are performed:

1. Database properties from Active Directory are read to validate the specified database and servers, and to verify that the source and target servers are running Exchange 2010, they are both members of the same DAG, and that the specified database isn't a recovery database. The database file paths are also read.
2. Preparations occur for reseed checks from the Microsoft Exchange Replication service on the target server.
3. The Microsoft Exchange Replication service on the target server checks for the presence of database and transaction log files in the file directories read by the Active Directory checks in step 1.
4. The Microsoft Exchange Replication service returns the status information from the target server to the administrative interface from where the cmdlet was run.
5. If all preliminary checks have passed, you are prompted to confirm the operation before continuing. If you confirm the operation, the process continues. If an error is encountered during the preliminary checks, the error is reported and the operation fails.
6. The seed operation is started from the Microsoft Exchange Replication service on the target server.
7. The Microsoft Exchange Replication service suspends database replication for the active database copy.
8. The state information for the database is updated by the Microsoft Exchange Replication service to reflect a status of Seeding.
9. If the target server doesn't already have the directories for the target database and log files, they are created.
10. A request to seed the database is passed from the Microsoft Exchange Replication service on the target server to the Microsoft Exchange Replication service on the source server using TCP. This request and the subsequent communications for seeding the database occur on a DAG network that has been configured as a replication network.
11. The Microsoft Exchange Replication service on the source server initiates an Extensible Storage Engine (ESE) streaming backup via the Microsoft Exchange Information Store service interface.
12. The Microsoft Exchange Information Store service streams the database data to the Microsoft Exchange Replication service.
13. The database data is moved from the source server's Microsoft Exchange Replication service to the target server's Microsoft Exchange Replication service.
14. The Microsoft Exchange Replication service on the target server writes the database copy to a temporary directory located in the main database directory called **temp-seeding**.
15. The streaming backup operation on the source server ends when the end of the database is reached.
16. The write operation on the target server completes and the database is moved from the temp-seeding directory to the final location. The temp-seeding directory is deleted.
17. On the target server, the Microsoft Exchange Replication service proxies a request to the Microsoft Exchange Search service to mount the content index catalog for the database copy, if it exists. If there are existing out-of-date catalog files from a previous instance of the database copy, the mount operation fails, which triggers the need to replicate the catalog from the source server. Likewise, if the catalog doesn't exist, and it doesn't on a new instance of the database copy on the target server, a copy of the catalog is required. The Microsoft Exchange Replication service directs the Microsoft Exchange Search service to suspend indexing for the database copy while a

new catalog is copied from the source.
18. The Microsoft Exchange Replication service on the target server sends a seed catalog request to the Microsoft Exchange Replication service on the source server.
19. On the source server, the Microsoft Exchange Replication service requests the directory information from the Microsoft Exchange Search service and requests that indexing be suspended.
20. The Microsoft Exchange Search service on the source server returns the search catalog directory information to the Microsoft Exchange Replication service.
21. The Microsoft Exchange Replication service on the source server reads the catalog files from the directory.
22. The Microsoft Exchange Replication service on the source server moves the catalog data to the Microsoft Exchange Replication service on the target server using a connection across the replication network. After the read is complete, the Microsoft Exchange Replication service sends a request to the Microsoft Exchange Search service to resume indexing of the source database.
23. If there are any existing catalog files on the target server in the directory, the Microsoft Exchange Replication service on the target server deletes them.
24. The Microsoft Exchange Replication service on the target server writes the catalog data to a temporary directory called **CiSeed.Temp** until the data is completely transferred.
25. The Microsoft Exchange Replication service moves the complete catalog data to the final location.
26. The Microsoft Exchange Replication service on the target server resumes search indexing on the target database.
27. The Microsoft Exchange Replication service on the target server returns a completion status.
28. The final result of the operation is passed to the administrative interface from which the cmdlet was called.

Configuring Database Copies

After a database copy is created, you can view and modify its configuration settings when needed. You can view some configuration information by examining the **Properties** page for a database copy in the EMC. You can also use the Get-MailboxDatabase and Set-MailboxDatabaseCopy cmdlets in the Shell to view and configure database copy settings, such as replay lag time, truncation lag time, and activation preference order. For detailed steps to view and configure database copy settings, see Configure Mailbox Database Copy Properties.

Using Replay Lag and Truncation Lag Options

Mailbox database copies support the use of a *replay lag time* and a *truncation lag time*, both of which are configured in minutes. Setting a replay lag time enables you to take a database copy back to a specific point in time. Setting a truncation lag time enables you to use the logs on a passive database copy to recover from the loss of log files on the active database copy. Because both of these features result in the temporary build-up of log files, using either of them will affect your storage design.

Replay Lag Time

Replay lag time is a property of a mailbox database copy that specifies the amount of time, in minutes, to delay log replay for the database copy. The replay lag timer starts when a log file has been replicated to the passive copy and has successfully passed inspection. By delaying the replay of logs to the database copy, you have the capability to recover the database to a specific point in time in the past. A mailbox database copy configured with a replay lag time greater than 0 is referred to as a *lagged mailbox database copy*, or simply, a *lagged copy*.

A strategy that uses database copies and the litigation hold features in Exchange 2010 can provide protection against a range of failures that would ordinarily cause data loss.

However, these features can't provide protection against data loss in the event of logical corruption, which although rare, can cause data loss. Lagged copies are designed to prevent loss of data in the case of logical corruption. Generally, there are two types of logical corruption:

- **Database logical corruption** The database pages checksum matches, but the data on the pages is wrong logically. This can occur when ESE attempts to write a database page and even though the operating system returns a success message, the data is either never written to the disk or it's written to the wrong place. This is referred to as a *lost flush*. To prevent lost flushes from losing data, ESE includes a lost flush detection mechanism in the database along with a page patching feature (single page restore).
- **Store logical corruption** Data is added, deleted, or manipulated in a way that the user doesn't expect. These cases are generally caused by third-party applications. It is generally only corruption in the sense that the user views it as corruption. The Exchange store considers the transaction that produced the logical corruption to be a series of valid MAPI operations. The litigation hold feature in Exchange 2010 provides protection from store logical corruption (because it prevents content from being permanently deleted by a user or application). However, there may be scenarios where a user mailbox becomes so corrupted that it would be easier to restore the database to a point in time prior to the corruption, and then export the user mailbox to retrieve uncorrupted data.

The combination of database copies, hold policy, and ESE single page restore leaves only the rare but catastrophic store logical corruption case. Your decision on whether to use a database copy with a replay lag (a lagged copy) will depend on which third-party applications you use and your organization's history with store logical corruption.

If you choose to use lagged copies, be aware of the following implications for their use:

- Unlike standby continuous replication (SCR) in Exchange 2007, which had a hard-coded replay lag of 50 log files, there's no hard-coded number of lagged log files. Instead, the replay lag time is an administrator-configured value, and by default, it's disabled.
- The replay lag time setting has a default setting of 0 days, and a maximum setting of 14 days.
- Lagged copies aren't considered highly available copies. Instead, they are designed for disaster recovery purposes, to protect against store logical corruption.
- The greater the replay lag time, the longer the database recovery process. Depending on the number of log files that need to replayed during recovery, and the speed at which your hardware can replay them, it may take several hours or more to recover a database.
- We recommend that you determine whether lagged copies are critical for your overall disaster recovery strategy. If using them is critical to your strategy, we recommend using multiple lagged copies, or using a redundant array of independent disks (RAID) to protect a single lagged copy, if you don't have multiple lagged copies. If you lose a disk or if corruption occurs, you don't lose your lagged point in time.
- Lagged copies aren't patchable with the ESE single page restore feature. If a lagged copy encounters database page corruption (for example, a -1018 error), it will have to be reseeded (which will lose the lagged aspect of the copy).

Activating and recovering a lagged mailbox database copy is an easy process if you want the database to replay all log files and make the database copy current. If you want to replay log files up to a specific point in time, it's a more difficult operation because you manually manipulate log files and run the Eseutil tool.

For detailed steps to activate a lagged mailbox database copy, see Activate a Lagged Mailbox Database Copy.

Truncation Lag Time

Truncation lag time is a property of a mailbox database copy that specifies the amount of time, in minutes, to delay log deletion for the database copy after the log file has been replayed into the database copy. The truncation lag timer starts when a log file has been replicated to the passive copy, and successfully passed inspection, and has been successfully replayed into the copy of the database. By delaying the truncation of log files from the database copy, you have the capability to recover from failures that affect the log files for the active copy of the database.

Database Copies and Log Truncation

Log truncation works the same in Exchange 2010 as it did in Exchange 2007. Truncation behavior is determined by the replay lag time and truncation lag time settings for the copy.

The following criteria must be met for a database copy's log file to be truncated when lag settings are left at their default values of 0 (disabled):

- The log file must have been successfully backed up, or circular logging must be enabled.
- The log file must be below the checkpoint (the minimum log file required for recovery) for the database.
- All other lagged copies must have inspected the log file.
- All other copies (not lagged copies) must have replayed the log file.

The following criteria must be met for truncation to occur for a lagged database copy:

- The log file must be below the checkpoint for the database.
- The log file must be older than ReplayLagTime + TruncationLagTime.
- The log file must have been truncated on the active copy.

Database Activation Policy

There are scenarios in which you may want to create a mailbox database copy and prevent the system from automatically activating that copy in the event of a failure. For example:

- If you deploy one or more mailbox database copies to a second or standby data center.
- If you configure a database copy as a lagged copy for recovery purposes.
- If you are performing maintenance or an upgrade of a server.

In each of the preceding scenarios, you have database copies that you don't want the system to activate automatically. To prevent the system from automatically activating a mailbox database copy, you can configure the copy to be blocked (suspended) for activation. This allows the system to maintain the currency of the database through log shipping and replay, but prevents the system from automatically activating and using the copy. Copies blocked for activation must be manually activated by an administrator. You can configure the database activation policy by using the Set-MailboxServer cmdlet to set the *DatabaseCopyAutoActivationPolicy* parameter to Blocked.

For more information about configuring database activation policy, see Configure Activation Policy for a Mailbox Database Copy.

Effect of Mailbox Moves on Continuous Replication

On a very busy mailbox database with a high log generation rate, there is a greater chance for data loss if replication to the passive database copies can’t keep up with log generation. One scenario that can introduce a high log generation rate is mailbox moves. Exchange 2010 includes a Data Guarantee API that is used by services such as the Mailbox Replication Service (MRS) to check the health of the database copy architecture based on the value of the *DataMoveReplicationConstraint* parameter that was set by the

system or an administrator. Specifically, the Data Guarantee API can be used to:

- **Check replication health** Confirms that the prerequisite number of database copies is available.
- **Check replication flush** Confirms that the required log files have been replayed against the prerequisite number of database copies.

When executed, the API returns the following status information to the calling application:

- **Retry** Signifies that there are transient errors that prevent a condition from being checked against the database.
- **Satisfied** Signifies that the database meets the required conditions or the database isn't replicated.
- **NotSatisfied** Signifies that the database doesn't meet the required conditions. In addition, information is provided to the calling application as to why the **NotSatisfied** response was returned.

The value of the *DataMoveReplicationConstraint* parameter for the mailbox database determines how many database copies should be evaluated as part of the request. The *DataMoveReplicationConstraint* parameter has the following possible values:

- `None` When you create a mailbox database, this value is set by default. When this value is set, the Data Guarantee API conditions are ignored. This setting should be used only for mailbox databases that aren't replicated.
- `SecondCopy` This is the default value when you add the second copy of a mailbox database. When this value is set, at least one passive database copy must meet the Data Guarantee API conditions.
- `SecondDatacenter` When this value is set, at least one passive database copy in another Active Directory site must meet the Data Guarantee API conditions.
- `AllDatacenters` When this value is set, at least one passive database copy in each Active Directory site must meet the Data Guarantee API conditions.
  `AllCopies` When this value is set, all copies of the mailbox database must meet the Data Guarantee API conditions.

Check Replication Health

When the Data Guarantee API is executed to evaluate the health of the database copy infrastructure, several items are evaluated.

If the *DataMoveReplicationConstraint* parameter is set to...	**Then, for a given database...**	**Conditions**
`SecondCopy`	At least one passive database copy for a replicated database must meet the conditions in the next column.	The passive database copy must: • Be healthy. • Have a replay queue within 10 minutes of the replay lag time. • Have a copy queue length less than 10 logs. • Have an average copy queue length less than 10 logs. The average copy queue length is computed based on the number of times the application has queried the database status.
`SecondDatacenter`	At least one passive database copy in another Active Directory	

	site must meet the conditions in the next column.	
AllDatacenters	The active copy must be mounted, and a passive copy in each Active Directory site must meet the conditions in the next column.	
AllCopies	The active copy must be mounted, and all passive database copies must meet the conditions in the next column.	

Check Replication Flush

The Data Guarantee API can also be used to validate that a prerequisite number of database copies have replayed the required transaction logs. This is verified by comparing the last log replayed timestamp with that of the calling service's commit timestamp (in most cases, this is the timestamp of the last log file that contains required data) plus an additional five seconds (to deal with system time clock skews or drift). If the replay timestamp is greater than the commit timestamp, then the *DataMoveReplicationConstraint* parameter is satisfied. If the replay timestamp is less than the commit timestamp, then the *DataMoveReplicationConstraint* isn't satisfied.

Before moving large numbers of mailboxes to or from replication databases within a DAG, we recommend that you configure the *DataMoveReplicationConstraint* parameter on each mailbox database according to the following:

If you are deploying...	Set DataMoveReplicationConstraint to...
Mailbox databases that do not have any database copies	None
A DAG within a single Active Directory site	SecondCopy
A DAG in multiple datacenters using a stretched Active Directory site	SecondCopy
A DAG that spans two Active Directory sites, and you will have highly available database copies in each site	SecondDatacenter
A DAG that spans two Active Directory sites, and you will have only lagged database copies in the second site SecondCopy	SecondCopy This is because the Data Guarantee API will not guarantee data being committed until the log file is replayed into the database copy and due to the nature of the database copy being lagged this constraint will fail the move request, unless the lagged database copy ReplayLagTime value is less than 30 minutes.
A DAG that spans three or more Active Directory sites, and each site will contain highly available database copies	AllDatacenters

Balancing Database Copies

Due to the inherent nature of DAGs, as the result of database switchovers and failovers, active mailbox database copies will change hosts several times throughout a DAG's lifetime. As a result, DAGs can become unbalanced in terms of active mailbox database copy distribution. The following table shows an example of a DAG that has four databases with four copies of each database (for a total of 16 databases on each server) with an uneven distribution of active database copies.

DAG with unbalanced active copy distribution

Server	Number of active database	Number of passive databases	Number of mounted databases	Number of dismounted databases	Preference count list
EX1	5	11	5	0	4, 4, 3, 5
EX2	1	15	1	0	1, 8, 6, 1
EX3	12	4	12	0	13, 2, 1, 0
EX4	1	15	1	0	1, 1, 5, 9

In the preceding example, there are four copies of each database, and therefore, only four possible values for activation preference (1, 2, 3, or 4). The **Preference count list** column shows the count of the number of databases with each of these values. For example, on EX3, there are 13 database copies with an activation preference of 1, two copies with an activation preference of 2, one copy with an activation preference of 3, and no copies with an activation preference of 4.

As you can see, this DAG is not balanced in terms of the number of active databases hosted by each DAG member, the number of passive databases hosted by each DAG member, or the activation preference count of the hosted databases.

You can use the RedistributeActiveDatabases.ps1 script to balance the active mailbox databases copies across a DAG. This script moves databases between their copies in an attempt to have an equal number of mounted databases on each server in DAG. If required, the script also attempts to balance active databases across sites.

The script provides two options for balancing active database copies within a DAG:

- **BalanceDbsByActivationPreference** When this option is specified, the script attempts to move databases to their most preferred copy (based on Activation Preference) without regard to Active Directory site.
- **BalanceDbsBySiteAndActivationPreference** When this option is specified, the script attempts to move active databases to their most preferred copy, while also trying to balance active databases within each Active Directory site.

After running the script with the first option, the preceding unbalanced DAG becomes balanced, as shown in the following table.

DAG with balanced active copy distribution

Server	Number of active database	Number of passive databases	Number of mounted databases	Number of dismounted databases	Preference count list
EX1	4	12	4	0	4, 4, 4, 4
EX2	4	12	4	0	4, 4, 4, 4
EX3	4	12	4	0	4, 4, 4, 4
EX4	4	12	4	0	4, 4, 4, 4

As shown in the preceding table, this DAG is now balanced in terms of number of active and passive databases on each server and activation preference across the servers.

The following table lists the available parameters for the RedistributeActiveDatabases.ps1 script.

RedistributeActiveDatabases.ps1 script parameters

Parameter	Description
DagName	Specifies the name of the DAG you want to rebalance. If this parameter is omitted, the DAG of which the local server is a member is used.
BalanceDbsByActivationPreference	Specifies that the script should move databases to their most preferred copy without regard to Active Directory site.
BalanceDbsBySiteAndActivationPreference	Specifies that the script should attempt to move active databases to their most preferred copy, while also trying to balance active databases within each Active Directory site.
ShowFinalDatabaseDistribution	Specifies that a report of current database distribution be displayed after redistribution is complete.
AllowedDeviationFromMeanPercentage	Specifies the allowed variation of active databases across sites, expressed as a percentage. The default is 20%. For example, if there were 99 databases distributed between three sites, the ideal distribution would be 33 databases in each site. If the allowed deviation is 20%, the script attempts to balance the databases so that each site has no more than 10% more or less than this number. 10% of 33 is 3.3, which is rounded up to 4. Therefore, the script attempts to have between 29 and 37 databases in each site.
ShowDatabaseCurrentActives	Specifies that the script produce a report for each database detailing how the database was moved and whether it is now active on its most-preferred copy.
ShowDatabaseDistributionByServer	Specifies that the script produce a report for each server showing its database distribution.
RunOnlyOnPAM	Specifies that the script run only on the DAG member that currently has the PAM role. The script verifies it is being run from the PAM. If it is not being run from the PAM, the script exits.
LogEvents	Specifies that the script logs an event (MsExchangeRepl event 4115) containing a summary of the actions.

IncludeNonReplicatedDatabases	Specifies that the script should include non-replicated databases (databases without copies) when determining how to redistribute the active databases. Although non-replicated databases can't be moved, they may affect the distribution of the replicated databases.
Confirm	The Confirm switch can be used to suppress the confirmation prompt that appears by default when this script is run. To suppress the confirmation prompt, use the syntax -Confirm:$False. You must include a colon (:) in the syntax.

RedistributeActiveDatabases.ps1 Examples

This example shows the current database distribution for a DAG, including preference count list.

```
RedistributeActiveDatabases.ps1 -DagName DAG1 -ShowDatabaseDistributionByServer |
```

This example redistributes and balances the active mailbox database copies in a DAG using activation preference without prompting for input.

```
RedistributeActiveDatabases.ps1 -DagName DAG1 -BalanceDbsByActivationPreference -
```

This example redistributes and balances the active mailbox database copies in a DAG using activation preference, and produces a summary of the distribution.

```
RedistributeActiveDatabases.ps1 -DagName DAG1 -BalanceDbsByActivationPreference -
```

Monitoring Database Copies

A database copy is your first defense if a failure occurs that affects the active copy of a database. It is therefore critical to monitor the health and status of database copies to ensure that they will be available when needed. You can view some health and status information by examining the **Properties** page for a database copy in the EMC. You can also use the **Get-MailboxDatabaseCopyStatus** cmdlet in the Shell to view a variety of status information for a database copy.

For more information about monitoring database copies, see Monitoring High Availability and Site Resilience.

Removing a Database Copy

A database copy can be removed at any time by using the EMC or by using the **Remove-MailboxDatabaseCopy** cmdlet in the Shell. After removing a database copy, you must manually delete any database and transaction log files from the server from which the database copy is being removed. For detailed steps to remove a database copy, see Remove a Mailbox Database Copy.

Database Switchovers

The Mailbox server that hosts the active copy of a database is referred to as the *mailbox database master*. The process of activating a passive database copy changes the mailbox database master for the database and turns the passive copy into the new active copy. This process is called a database *switchover*. In a database switchover, the active copy of a database is dismounted on one Mailbox server and a passive copy of that database is mounted as the new active mailbox database on another Mailbox server. When performing a switchover, you can optionally override the database mount dial setting on the new mailbox database master.

You can quickly identify which Mailbox server is the current mailbox database master by reviewing the **Copy Status** column under the **Database Copies** tab in the EMC. Only the active copy will have a status of **Mounted**. All other database copies will display the current status of replication for the database copy. You can perform a switchover by using the Move Mailbox Database Master wizard in the EMC, or by using the **Move-ActiveMailboxDatabase** cmdlet in the Shell.

There are several internal checks that will be performed before activating a passive copy:

- The status of the database copy is checked. If the database copy is in a failed state, the switchover is blocked. You can override this behavior and bypass the health check by using the *SkipHealthChecks* parameter of the **Move-ActiveMailboxDatabase** cmdlet. This parameter allows you to move the active copy to a database copy in a failed state.
- The active database copy is checked to see if it is currently a seeding source for any passive copies of the database. If the active copy is currently being used as a source for seeding, the switchover is blocked. You can override this behavior and bypass the seeding source check by using the *SkipActiveCopyChecks* parameter of the **Move-ActiveMailboxDatabase** cmdlet. This parameter allows you to move an active copy that is being used as a seeding source. Using this parameter will cause the seeding operation to be cancelled and considered failed.
- The copy queue and replay queue lengths for the database copy are checked to ensure their values are within the configured criteria. Also, the database copy is verified to ensure that it isn't currently in use as a source for seeding. If the values for the queue lengths are outside the configured criteria, or if the database is currently used as a source for seeding, the switchover is blocked. You can override this behavior and bypass these checks by using the *SkipLagChecks* parameter of the **Move-ActiveMailboxDatabase** cmdlet. This parameter allows a copy to be activated that has replay and copy queues outside of the configured criteria.
- The state of the search catalog (content index) for the database copy is checked. If the search catalog isn't up to date, is in an unhealthy state, or is corrupt, the switchover is blocked. You can override this behavior and bypass the search catalog check by using the *SkipClientExperienceChecks* parameter of the **Move-ActiveMailboxDatabase** cmdlet. This parameter causes this search to skip the catalog health check. If the search catalog for the database copy you are activating is in an unhealthy or unusable state and you use this parameter to skip the catalog health check and activate the database copy, you will need to either crawl or seed the search catalog again.

When performing a database switchover, you also have the option of overriding the mount dial settings configured for the server that hosts the passive database copy being activated. Using the *MountDialOverride* parameter of the **Move-ActiveMailboxDatabase** cmdlet instructs the target server to override its own mount dial settings and use those specified by the *MountDialOverride* parameter.

For detailed steps to perform a switchover of a database copy, see Move the Active Mailbox Database. For more information about database switchovers, see Switchovers and Failovers.

1.10.4.2.1 Add a Mailbox Database Copy

Add a Mailbox Database Copy

High Availability and Site Resilience > Managing High Availability and Site Resilience > Managing Mailbox Database Copies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-10*

When you add a copy of a mailbox database, continuous replication is automatically enabled between the existing database and the database copy. Database copies are automatically assigned an identity in the format of *<DatabaseName>* *<HostMailboxServerName>*. For example, a copy of a database named DB1 that's hosted on a server named MBX3 would be named DB1\MBX3.

Looking for other management tasks related to mailbox database copies? Check out Managing Mailbox Database Copies.

Prerequisites

- The active copy of the mailbox database must be mounted.
- The specified database must be a mailbox database. You can't use continuous replication for public folder databases. For public folder database availability, we recommend deploying multiple public folder databases and using public folder replication. For more information, see Understanding Public Folder Replication.
- The specified Mailbox server must not already host a copy of the specified mailbox database.
- The path for the specified mailbox database and its log files must be available on the specified Mailbox server.
- The server hosting the specified database and the server that will host the database copy must both be in the same database availability group (DAG). The DAG must also have quorum and be healthy.
- If you're adding the second copy of a database (for example, creating the first passive copy of the database), circular logging must not be enabled for the specified mailbox database. If circular logging is enabled, you must first disable it. After the mailbox database copy has been added, circular logging can be enabled. After circular logging is enabled for a replicated mailbox database, continuous replication circular logging (CRCL) is used instead of JET circular logging. If you're adding the third or subsequent copy of a database, CRCL can remain enabled. For information about how to enable and disable circular logging, see Configure Mailbox Database Properties.

What Do You Want to Do?

- Use the EMC to add a mailbox database copy
- Use the Shell to add a mailbox database copy

Use the EMC to add a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copy" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Management** tab, right-click the mailbox database that you want to copy, and then click **Add Mailbox Database Copy**.
3. On the **Add Mailbox Database Copy** page, complete the following fields.
   - **Mailbox database name** This read-only box displays the name of the database for which you are going to make a copy.

- **Server name** Click **Browse** to open the **Select Mailbox Server** dialog box. Use this dialog box to select the Mailbox server that will host the copy of the mailbox database, and then click **OK**.

  Note:
  The **Select Mailbox Server** dialog displays all Mailbox servers. You must select a Mailbox server that it is in the same DAG as the Mailbox server hosting the active copy.

- **Activation preference number** Use this box to specify the activation preference number for the database copy. The activation preference number is used as part of Active Manager's best copy selection process and to redistribute active mailbox databases throughout the DAG when using the RedistributeActiveDatabases.ps1 script. The value for the activation preference is a number equal to or greater than 1, where 1 is at the top of the preference order. The position number cannot be larger than the number of copies of the mailbox database.

4. Click **Add** to add the copy of the mailbox database.

5. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
6. Click **Finish** to close the wizard.

Use the Shell to add a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copy" entry in the High Availability Permissions topic.

In this example, a copy of mailbox database DB1 is being added to a Mailbox server named MBX3. Replay lag time and truncation lag time are left at the default values of zero, and the activation preference is configured with a value of 2.

```
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX3 -ActivationPreference 2
```

In this example, a copy of mailbox database DB2 is being added to a Mailbox server named MBX4. Replay lag time and truncation lag time are left at the default values of zero, and the activation preference is configured with a value of 5. In addition, seeding is being postponed for this copy so that it can be seeded using a local source server instead of the current active database copy, which is geographically distant from MBX4.

```
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX4 -ActivationPreference 5
```

In this example, a copy of mailbox database DB3 is being added to a Mailbox server named MBX5. Replay lag time is set to 3 days, and truncation lag time is left at the default value of zero, and the activation preference is configured with a value of 4.

```
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX5 -ReplayLagTime 3.00:00:
```

For More Information

Understanding Mailbox Database Copies

Managing Mailbox Database Copies

1.10.4.2.2 Configure Mailbox Database Copy Properties

Configure Mailbox Database Copy Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Each mailbox database copy has its own properties that you can configure. These include the amount of time, if any, for replay lag and truncation lag, and the activation preference number. For more information about replay lag, truncation lag and the activation preference number, see Managing Mailbox Database Copies.

What Do You Want to Do?

Use the EMC to configure mailbox database copy properties

Use the Shell to configure mailbox database copy properties

Use the EMC to configure mailbox database copy properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copies" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Management** tab, select the database with the copy whose status you want to check.
3. In the work pane, on the **Database Copies** tab, right-click the database copy whose status you want to view, and then click **Properties**.
4. Use the **General** tab to view status about the mailbox database copy, and to configure for replay lag and truncation lag, and the activation preference number.
   - **Database** This is a read-only field that displays the name of the selected database.
   - **Mailbox server** This is a read-only field that displays the name of the mailbox server that currently hosts the active copy of the mailbox database.
   - **Status** This is a read-only field that displays the current status of the selected database or database copy.
   - **Copy queue length (logs)** Indicates the number of log files waiting to be copied and inspected.
   - **Replay queue length (logs)** Indicates the number of log files waiting to be replayed into this copy of the database.
   - **Activation preference number** The activation preference number is used as part of Active Manager's best copy selection process and to redistribute active mailbox databases throughout the DAG when using the RedistributeActiveDatabases.ps1 script. The value for activation preference

is a number equal to or greater than 1, where 1 is at the top of the preference order. The number cannot be larger than the number of database copies of the mailbox database.

5. Use the **Status** tab to view additional details about the health and status of replication for the database copy.
   - **Seeding** Indicates whether a seeding operation is currently in progress.
   - **Messages** If any failures have occurred, the **View** button is made available. Click this button to view messages about conditions that triggered the failure.
   - **Latest available log time** The time associated with the latest available log generated by the active database copy. This log is available to be copied.
   - **Last inspected log time** The modification time of the last log that was successfully validated by the Mailbox server hosting the database copy.
   - **Last copied log time** The modification time of the last log that was successfully copied.
   - **Last replayed log time** The modification time of the last log that was successfully replayed by the Mailbox server hosting the database copy.

Use the Shell to configure mailbox database copy properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copies" entry in the High Availability Permissions topic.

This example configures a mailbox database copy with an activation preference number of 3.

```
Set-MailboxDatabaseCopy -Identity DB3\EX3 -ActivationPreference 3
```

This example configures a copy of a database named DB1 that is hosted on Server1 with a replay lag time and truncation lag time of 1 day, and an activation preference number of 2.

```
Set-MailboxDatabaseCopy -Identity DB1\Server1 -ReplayLagTime 1.0:0:0 -TruncationL
```

This example returns information about the health and status of replication for a database named DB3 on a server named EX3. This provides the same information as the **General** tab on the **Mailbox Database Properties** page, except it does not display the activation preference number.

```
Get-MailboxDatabaseCopyStatus DB3\EX3
```

This example returns information about the health and status of replication for a database named DB7 on a server named EX5.

```
Get-MailboxDatabaseCopyStatus DB7\EX5 | Format-List
```

This example returns status and Hub Transport shadow redundancy information for a database named DB2. The status results are displayed in a list format.

```
Get-MailboxDatabaseCopyStatus -Identity DB2 -DumpsterStatistics | Format-List
```

This example returns the status and Hub Transport shadow redundancy information for all database copies on a Mailbox server named MBX2. The status results are also displayed in a list format.

```
Get-MailboxDatabaseCopyStatus -Server MBX2 -DumpsterStatistics | Format-List
```

For More Information

Set-MailboxDatabaseCopy

Get-MailboxDatabaseCopyStatus

Get-MailboxDatabase

1.10.4.2.3 Move the Mailbox Database Path for a Mailbox Database Copy

Move the Mailbox Database Path for a Mailbox Database Copy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After a mailbox database is created, you can move it to another volume, folder, location, or path by using either the EMC or the Shell. For step-by-step instructions about how to move a mailbox database path, see Move the Database Path. That topic provides information about how to move a non-replicated mailbox database to another path.

If the mailbox database being moved is replicated to one or more mailbox database copies, you must follow the procedure in this topic to move the mailbox database path. All copies of a mailbox database must be located in the same path on each server that hosts a copy. For example, if database DB1 is located at C:\mountpoints\DB1 on server EX1, copies of DB1 on servers EX2, EX3, and so on, must also be located at C:\mountpoints\DB1.

Looking for other management tasks related to mailbox database copies? Check out Managing Mailbox Database Copies.

Prerequisites

- To perform the move operation, the database must be temporarily dismounted, making it inaccessible to all users. If the database is currently dismounted, it isn't remounted upon completion.
- To perform the move operation, replication for the database must be disabled for all copies. It's not enough to suspend replication; you must disable it by using the Remove-MailboxDatabaseCopy cmdlet to remove the database copies.

Use the Shell to move a replicated mailbox database to a new path

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copies" entry in the High Availability Permissions topic.

Note:

You can't use the EMC to move a replicated mailbox database to a new path.

1. Note any replay lag or truncation lag settings for all copies of the mailbox database being moved. You can obtain this information by using the Get-

MailboxDatabase cmdlet, as shown in this example.

```
Get-MailboxDatabase DB1 | fl *lag*
```

2. If circular logging is enabled for the database, it must be disabled before proceeding. You can disable circular logging for a mailbox database by using the Set-MailboxDatabase cmdlet, as shown in this example.

```
Set-MailboxDatabase DB1 -CircularLoggingEnabled $false
```

3. Remove all mailbox database copies for the database being moved. For detailed steps, see Remove a Mailbox Database Copy. After all copies are removed, preserve the database and transaction log files from each server from which the database copy is being removed by moving them to another location. These files are being be preserved so the database copies to not require re-seeding after they have been re-added.
4. Move the mailbox database path to the new location. For detailed steps, see Move the Database Path.

Important:

During the move operation, the database being moved must be dismounted. Until the move is complete, this process will cause an interruption in service and an outage for all users with mailboxes on the database being moved. After the move operation completes, the database is automatically mounted.

5. Create the necessary folder structure on each Mailbox server that previously contained a passive copy of the moved mailbox database. For example, if you moved the database to C:\mountpoints\DB1, you must create this same path on each Mailbox server that will host a mailbox database copy.
6. After creating the folder structure, move the passive copy of the mailbox database and its log stream to the new location. These are the files that were left from and preserved after Step 3. Repeat this process for each database copy that was removed in Step 3.
7. Add all of the database copies that were removed in Step 3. For detailed steps, see Add a Mailbox Database Copy.
8. On each server that contains a copy of the mailbox database being moved, run the following commands to stop and restart the content index services.

```
Net stop msftesql-Exchange
Net start MSExchangeSearch
```

9. Optionally, enable circular logging by using the Set-MailboxDatabase cmdlet, as shown in this example.

```
Set-MailboxDatabase DB1 -CircularLoggingEnabled $true
```

10. Reconfigure any previously set values for replay lag time and truncation lag time by using the Set-MailboxDatabaseCopy cmdlet, as shown in this example.

```
Set-MailboxDatabaseCopy DB1\MBX2 -ReplayLagTime 00:15:00
```

11. As each copy is added, we recommend that you verify the health and status of the copy prior to adding the next copy. You can verify the health and status by:
    - 11.a. Examining the event log for any error or warning events related to the database or the database copy.
    - 11.b. Using the Get-MailboxDatabaseCopyStatus cmdlet to check the health and status of continuous replication for the database copy.
    - 11.c. Using the Test-ReplicationHealth cmdlet to verify the health and status of the database availability group and continuous replication.

For detailed syntax and parameter information, see the following topics:

- Get-MailboxDatabase
- Set-MailboxDatabase
- Set-MailboxDatabaseCopy
- Get-MailboxDatabaseCopyStatus
- Test-ReplicationHealth

1.10.4.2.4 Configure Activation Policy for a Mailbox Database Copy

Configure Activation Policy for a Mailbox Database Copy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Activation is the process of changing a mailbox database copy from a *passive copy* to an *active copy*. Activation occurs automatically as part of a database or server failover operation, and it can be performed manually as part of a database or server switchover operation. Blocking a database for activation prevents it from becoming the active copy during a database or server failover.

Looking for other management tasks related to mailbox database copies? Check out Managing Mailbox Database Copies.

Use the Shell to suspend or resume a database for activation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copies" entry in the High Availability Permissions topic.

Note:

You can't use the EMC to suspend or resume a database for activation.

This example blocks the copy of the database DB1 on the server MBX2 for activation.

```
Suspend-MailboxDatabaseCopy -Identity DB1\MBX2 -ActivationOnly
```

This example resumes the copy of the database DB1 on the server MBX2 for activation.

```
Resume-MailboxDatabaseCopy -Identity DB1\MBX2
```

For detailed syntax and parameter information, see Suspend-MailboxDatabaseCopy or Resume-MailboxDatabaseCopy.

1.10.4.2.5 Suspend or Resume a Mailbox Database Copy

Suspend or Resume a Mailbox Database Copy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

These procedures show you how to suspend and resume continuous replication activity for a *mailbox database copy*. You may need to suspend continuous replication for a database copy for a variety of reasons, such as maintenance on the disk that contains a database copy.

Note:
After a database copy has been resumed, the Summary Copy Status for the database copy will display a status of Initializing until a log file has been generated by the active copy of the database.

Looking for other management tasks related to mailbox database copies? Check out Managing Mailbox Database Copies.

Use the EMC to suspend a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "mailbox database copies" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Management** tab, select the database whose copy you want to suspend.
3. In the work pane, on the **Database Copies** tab, right-click the database for which you want to suspend continuous replication, and then click **Suspend Database Copy**.
4. Add an optional comment of up to 430 characters in the **Comment** field.
5. Click **Yes** to suspend continuous replication.

Use the EMC to resume a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "mailbox database copies" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Management** tab, select the database whose copy you want to resume.
3. In the work pane, on the **Database Copies** tab, right-click the database for which you want to resume continuous replication, and then click **Resume Database Copy**.
4. Optionally review any comments in the read-only **Comment** field.
5. Click **Yes** to resume continuous replication.

Use the Shell to suspend a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "mailbox database copies" entry in the High Availability Permissions topic.

This example suspends continuous replication for a copy of a database named DB1 that is hosted on a server named MBX3. An optional comment has also been specified.

```
Suspend-MailboxDatabaseCopy -Identity DB1\MBX3 -SuspendComment "Maintenance on EX
```

Use the Shell to resume a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "mailbox database copies" entry in the High Availability Permissions topic.

This example resumes a copy of a database named DB1 on a server named MBX3.

```
Resume-MailboxDatabaseCopy -Identity DB1\MBX3
```

This example resumes a copy of a database named DB1 on a server named EX1 for replication only.

```
Resume-MailboxDatabaseCopy -Identity DB1\EX1 -ReplicationOnly
```


1.10.4.2.6 Update a Mailbox Database Copy

Update a Mailbox Database Copy

High Availability and Site Resilience > Managing High Availability and Site Resilience > Managing Mailbox Database Copies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Updating, also known as *seeding*, is the process in which a copy of a mailbox database is added to another Mailbox server. This becomes the baseline database for the copy. Seeding is required under the following conditions:

- When a new passive copy of a database is created. Seeding can be postponed for a new mailbox database copy, but eventually, each passive database copy must be seeded in order to function as a redundant database copy.
- After a failover occurs in which data is lost as a result of the passive database copy having become diverged and unrecoverable.
- When the system has detected a corrupted log file that cannot be replayed into the passive copy of the database.
- After an offline defragmentation of any copy of the database occurs.
- After the log generation sequence for the database has been reset back to 1.

You can perform seeding by using the following methods:

- **Automatic seeding** An automatic seed produces a copy of the active database on the target mailbox server. Automatic seeding only occurs during the creation of a new database.
- **Seeding using the Update-MailboxDatabaseCopy cmdlet** You can use the Update-MailboxDatabaseCopy cmdlet in the Exchange Management Shell to seed a database copy at any time.
- **Seeding using the Update Database Copy wizard** You can use the **Update Database Copy** wizard in the Exchange Management Console (EMC) to seed a database copy at any time.
- **Manually copying the offline database** You can dismount the active copy of the database and copy the database file to the same location on another mailbox server in the same database availability group. If you use this method, there will be an interruption in service because the procedure requires you to dismount the database.

Updating a database copy can take a very long time, especially if the database being copied is very large, or if there is high network latency or low network bandwidth. Once the seeding process has started, don't close the EMC or the Shell until the process has completed. If you do, the seeding operation will be terminated.

A database copy can be seeded using either the active copy or an up-to-date passive copy as the source for the seed. When seeding from a passive copy, be aware that the seed operation will terminate with a network communication error under the following circumstances:

- If the status of the seeding source copy changes to Failed or FailedAndSuspended.
- If the database fails over to another copy.

Multiple database copies can be seeded simultaneously. However, when seeding multiple copies simultaneously, you must seed only the database file, and omit the content index catalog. You can do this by using the *DatabaseOnly* parameter with the Update-MailboxDatabaseCopy cmdlet.

Note:

If you do not use the *DatabaseOnly* parameter when seeding multiple targets from the same source, the task will fail with SeedInProgressException error FE1C6491.

Looking for other management tasks related to mailbox database copies? Check out Managing Mailbox Database Copies.

Prerequisites

- The mailbox database copy must be suspended. For detailed steps, see Suspend or Resume a Mailbox Database Copy.
- The Remote Registry service must be running on the server hosting the passive database copy you're updating.

What Do You Want to Do?

- Use the EMC to update a mailbox database copy
- Use the Shell to update a mailbox database copy
- Manually copy an offline database

Use the EMC to update a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Mailbox database copies" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab.
3. In the work pane, on the **Database Copies** tab, right-click the database copy you want to update, and then select **Update Database Copy**.
4. On the **Update Database Copy** page, configure the available options for updating a database copy:
   - By default, the active copy of the database is used as the source database for seeding. If you prefer to use a passive copy of the database for seeding, check the Select a source server for seeding checkbox, and then click **Browse** to select the server containing the passive copy you want to use for the source.

- Configure the task's behavior if files exist in the path of the database copy being seeded. If any existing files are in the database path, you can either select **Delete them and continue to update process** to remove all existing files and proceed with the seeding operation, or you can select **Cancel the update process** to terminate the task.
- By default, once seeding has completed, continuous replication will automatically resume for the database. If you don't want replication to automatically resume, select **Leave the database copy suspended. I will manually resume replication later**.
- Optionally specify a DAG network to be used for seeding. Click **Browse** to select the DAG network you want to use.

5. Once you have configured the available options, click **Update** to update the database copy.

6. On the **Completion** page, the **Summary** states whether the operation was successful. The summary also displays the Shell command that was used to perform this procedure.
7. Click **Finish** to exit the wizard.

Use the Shell to update a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Mailbox database copies" entry in the High Availability Permissions topic.

This example shows how to seed a copy of a database named DB1 on MBX1.

```
Update-MailboxDatabaseCopy -Identity DB1\MBX1
```

This example shows how to seed a copy of a database named DB1 on MBX1 using MBX2 as the source Mailbox server for the seed.

```
Update-MailboxDatabaseCopy -Identity DB1\MBX1 -SourceServer MBX2
```

This example shows how to seed a copy of a database named DB1 on MBX1 without seeding the content index catalog.

```
Update-MailboxDatabaseCopy -Identity DB1\MBX1 -DatabaseOnly
```

This example shows how to seed the content index catalog for the copy of a database named DB1 on MBX1 without seeding the database file.

```
Update-MailboxDatabaseCopy -Identity DB1\MBX1 -CatalogOnly
```

Manually copy an offline database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Mailbox database copies" entry in the High Availability Permissions topic.

1. If circular logging is enabled for the database, it must be disabled before proceeding. You can disable circular logging for a mailbox database by using the Set-MailboxDatabase cmdlet, as shown in this example.

   ```
   Set-MailboxDatabase DB1 -CircularLoggingEnabled $false
   ```

2. Dismount the database. You can use the Dismount-Database cmdlet, as shown in this example.

   ```
   Dismount-Database DB1 -Confirm $false
   ```

3. Manually copy the database files (the database file and all log files) to a

second location, such as an external disk drive or a network share.

4. Mount the database. You can use the Mount-Database cmdlet, as shown in this example.

```
Mount-Database DB1
```

5. On the server that will host the copy, copy the database files from the external drive or network share to the same path as the active database copy. For example, if the active copy database path is D:\DB1\DB1.edb and log file path is D:\DB1, then you would copy the database files to D:\DB1 on the server that will host the copy.
6. Add the mailbox database copy by using the Add-MailboxDatabaseCopy cmdlet with the *SeedingPostponed* parameter, as shown in this example.

```
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX3 -SeedingPost
```

7. If circular logging is enabled for the database, enable it again by using the Set-MailboxDatabase cmdlet, as shown in this example.

```
Set-MailboxDatabase DB1 -CircularLoggingEnabled $true
```


1.10.4.2.7 Remove a Mailbox Database Copy

Remove a Mailbox Database Copy

High Availability and Site Resilience > Managing High Availability and Site Resilience > Managing Mailbox Database Copies >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

These procedures show you how to remove a copy of a mailbox database. You cannot use these procedures to remove the last copy of a mailbox database. For detailed steps about how to remove the last copy of a mailbox database, see Remove a Mailbox Database or Remove-MailboxDatabase. Mailbox database copies can only be removed from a healthy database availability group (DAG). If the DAG isn't healthy (for example, the DAG's underlying cluster is down because quorum was lost), you won't be able to remove any mailbox database copies.

In addition, if you're removing the last passive copy of the database, continuous replication circular logging (CRCL) must not be enabled for the specified mailbox database. If CRCL is enabled, you must first disable it. After the mailbox database copy has been removed, circular logging can be enabled. Once enabled for a non-replicated mailbox database, JET circular logging is used instead of CRCL. If you aren't removing the last passive copy of a database, CRCL can remain enabled.

After removing a database copy, you must manually delete any database and transaction log files from the server from which the database copy is being removed.

Looking for other management tasks related to mailbox database copies? Check out Managing Mailbox Database Copies.

Use the EMC to remove a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "mailbox database copies" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Database Management** tab, select the mailbox database whose copy you want to remove.
3. In the work pane, on the **Database Copies** tab, right-click the database copy that you want to remove, and then click **Remove**.
4. Click **Yes** to remove the database copy.

Use the Shell to remove a mailbox database copy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "mailbox database copies" entry in the High Availability Permissions topic.

This example removes a copy of a mailbox database named DB1 from a Mailbox server named MBX3.

```
Remove-MailboxDatabaseCopy -Identity DB1\MBX3 -Confirm:$False
```


1.10.4.2.8 Move the Active Mailbox Database

Move the Active Mailbox Database

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Moving the active mailbox database is the process of designating a specific passive copy as the new active copy of a mailbox database. This process is referred to as a *database switchover*. A database switchover involves dismounting the current active database and mounting the database copy on the specified server as the new active mailbox database copy. The database copy that will become the active mailbox database must be healthy and current.

Looking for other management tasks related to mailbox database copies? Check out Managing Mailbox Database Copies.

What Do You Want to Do?

- Use the EMC to move the active mailbox database
- Use the Shell to move the active mailbox database

Use the EMC to move the active mailbox database

There are two ways you can use the EMC to move the active mailbox database. You can use the Move Active Mailbox Database wizard or you can use the Activate Database Copy option in the work pane.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copies" entry in the High Availability

Permissions topic.

Use the Move Active Mailbox Database wizard

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab, and then right-click the mailbox database whose copy you want to activate.
3. In the action pane, click **Move Active Mailbox Database**.
4. On the **Move Active Mailbox Database** page, click **Browse** to select the server you want to host the active copy of the database.
5. Select the desired setting for the automatic database mount dial setting on the server that you specified in the previous step.
6. In the **Override automatic database mount dial setting on the target mailbox server** list, optionally override the database mount dial settings on target master by selecting a value other than **None**. Possible values are:
   - **Lossless** If you specify this value, the database doesn't automatically mount until all logs that were generated on the active copy have been copied to the passive copy.
   - **Good Availability** If you specify this value, the database automatically mounts immediately after a failover if the copy queue length is less than or equal to 6. If the copy queue length is greater than 6, the database doesn't automatically mount. When the copy queue length is less than or equal to 6, Exchange attempts to replicate the remaining logs to the passive copy and then mounts the database.
   - **Best Effort** If you specify this value, the database automatically mounts regardless of the size of the copy queue length. We recommend using caution when using this setting. Because the database will mount with any amount of log loss, using this value could result in a large amount of data loss.
   - **Best Availability** If you specify this value, the database automatically mounts immediately after a failover if the copy queue length is less than or equal to 12. The copy queue length is the number of logs recognized by the passive copy that needs to be replicated. If the copy queue length is more than 12, the database doesn't automatically mount. When the copy queue length is less than or equal to 12, Exchange attempts to replicate the remaining logs to the passive copy and then mounts the database.
7. Click **Move** to move the active copy of the selected database to the specified server.
8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the work pane

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab, and then click the mailbox database whose copy you want to activate
3. In the **Database Copies** work pane, right-click the passive mailbox database copy that you want to activate, and then click **Activate Database Copy**.
4. In **Activate Database Copy**, you can use the **Override mount dial** list to optionally override the database mount dial settings on target master by selecting a value other than **None**. Possible values are:
   - **Lossless** If you specify this value, the database doesn't automatically mount until all logs that were generated on the active copy have been copied to the passive copy.

- **Good Availability** If you specify this value, the database automatically mounts immediately after a failover if the copy queue length is less than or equal to 6. If the copy queue length is greater than 6, the database doesn't automatically mount. When the copy queue length is less than or equal to 6, Exchange attempts to replicate the remaining logs to the passive copy and then mounts the database.
- **Best Effort** If you specify this value, the database automatically mounts regardless of the size of the copy queue length. Because the database will mount with any amount of log loss, using this value could result in a large amount of data loss.
- **Best Availability** If you specify this value, the database automatically mounts immediately after a failover if the copy queue length is less than or equal to 12. The copy queue length is the number of logs recognized by the passive copy that needs to be replicated. If the copy queue length is more than 12, the database doesn't automatically mount. When the copy queue length is less than or equal to 12, Exchange attempts to replicate the remaining logs to the passive copy and then mounts the database.

5. Click **OK** to activate the passive copy. This action dismounts the current active mailbox database and makes the selected passive copy the new active mailbox database.

Use the Shell to Move the Active Mailbox Database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copies" entry in the High Availability Permissions topic.

In this example, a copy of the database DB4 hosted on MBX3 is activated and mounted as the new active mailbox database. This command makes DB4 the new active mailbox database and it doesn't override the database mount dial settings on MBX3.

```
Move-ActiveMailboxDatabase DB4 -ActivateOnServer MBX3 -MountDialOverride:None
```

This example performs a switchover of the database DB2 to the Mailbox server MBX1. When the command completes, MBX1 hosts the active copy of DB2. Because the *MountDialOverride* parameter is set to None, MBX1 mounts the database using its own defined database auto mount dial settings.

```
Move-ActiveMailboxDatabase DB2 -ActivateOnServer MBX1 -MountDialOverride:None
```

This example performs a switchover of the database DB1 to the Mailbox server MBX3. When the command completes, MBX3 hosts the active copy of DB1. Because the *MountDialOverride* parameter is specified with a value of Good Availability, MBX3 mounts the database using a database auto mount dial setting of *GoodAvailability*.

```
Move-ActiveMailboxDatabase DB1 -ActivateOnServer MBX3 -MountDialOverride:GoodAvai
```

This example performs a switchover of the database DB3 to the Mailbox server MBX4. When the command completes, MBX4 hosts the active copy of DB3. Because the *MountDialOverride* parameter isn't specified, MBX4 mounts the database using a database auto mount dial setting of *Lossless*.

```
Move-ActiveMailboxDatabase DB3 -ActivateOnServer MBX4
```

This example performs a server switchover for the Mailbox server MBX1. All active mailbox database copies on MBX1 will be activated on one or more other Mailbox servers with healthy copies of the active databases on MBX1.

```
Move-ActiveMailboxDatabase -Server MBX1
```

This example performs a switchover of the database DB4 to the Mailbox server MBX5. In this example, the database copy on MBX5 has a replay queue greater than 6. As a result, the *SkipLagChecks* parameter must be specified to activate the database copy on MBX5.

```
Move-ActiveMailboxDatabase DB4 MBX5 -SkipLagChecks
```

This example performs a switchover of the database DB5 to the Mailbox server MBX6. In this example, the database copy on MBX6 has a *ContentIndexState* of Failed. As a result, the *SkipClientExperienceChecks* parameter must be specified to activate the database copy on MBX6.

```
Move-ActiveMailboxDatabase DB5 MBX6 -SkipClientExperienceChecks
```

For More Information

Understanding Mailbox Database Copies

Configure Mailbox Database Copy Properties

1.10.4.2.9 Activate a Lagged Mailbox Database Copy

Activate a Lagged Mailbox Database Copy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

A lagged mailbox database copy is a mailbox database copy configured with a replay lag time value greater than 0. Activating and recovering a lagged mailbox database copy is a simple process if you want the database to replay all log files and make the database copy current. If you want to replay log files up to a specific point in time, it's a more difficult operation because you have to manually manipulate log files and run Eseutil.

Looking for other management tasks related to mailbox database copies? Check out Managing Mailbox Database Copies.

Note:

The amount of time it takes to activate a lagged mailbox database copy directly depends on how many log files need to be replayed and how fast the hardware can replay them. At a minimum, you should see a log replay rate of two logs per second per database.

Prerequisites

- The mailbox database copy being activated must be configured with a replay lag time greater than 0.
- The mailbox database copy being activated must have all log files to the point in time to which you want to recover it. Keep in mind that database transactions can span multiple log files when determining the point in time to which you want to recover.

Use the Shell to activate a lagged mailbox

database copy to a specific point in time

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copies" entry in the High Availability Permissions topic.

Note:
You can't use the Exchange Management Console (EMC) to activate a lagged mailbox database copy to a specific point in time.

1. Suspend replication for the lagged copy being activated by using the Suspend-MailboxDatabaseCopy cmdlet, as shown in this example.

```
Suspend-MailboxDatabaseCopy DB1\EX3 -SuspendComment "Activate lagged c
```

2. Optionally (to preserve a lagged copy), take a file system-based (non-Exchange aware) Volume Shadow Copy Service (VSS) snapshot of the volumes containing the database copy and its log files. You can use the vssadmin.exe tool that's included in Windows to take a VSS snapshot, as shown in this example.

```
vssadmin create shadow /For=C:\mountpoints\db01
vssadmin create shadow /For=C:\mountpoints\db01_logs
```

Note:
At this point, you have shadow copies outstanding for the database and log volumes. Continuing to perform this procedure on the existing volume would incur a copy on write performance penalty. If this isn't desirable, you can copy the database and log files to another volume to perform the recovery.

3. Determine which log files are required to replay into the database to meet your point-in-time requirement for this recovery (based on log file date and time, as shown in Windows Explorer). All logs created after this point should be moved to a different directory, until the recovery process is completed, and the logs are no longer needed.
4. Delete the checkpoint (.chk) file for the database.
5. Use Eseutil to perform the recovery operation, as shown in this example.

```
Eseutil.exe /r eXX /a
```

Note:
In the preceding example, *eXX* is the log generation prefix for the database (for example, E00, E01, E02, and so on).

Important:
This step may take a considerable amount of time, depending on several factors, such as the length of the replay lag time, the number of log files generated during that period, and the speed at which your hardware can replay those logs into the database being recovered.

6. After log replay is finished, the database is in a clean shutdown state and can be copied and used for recovery purposes.
7. After the recovery process is complete, resume replication for the database that was used as part of the recovery process, as shown in this example.

```
Resume-MailboxDatabaseCopy DB1\EX3
```

For detailed syntax and parameter information, see Suspend-MailboxDatabaseCopy or Resume-MailboxDatabaseCopy.

Use the Shell to activate a lagged mailbox

database copy by replaying all uncommitted log files

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox database copies" entry in the High Availability Permissions topic.

1. Optionally (to preserve a lagged copy), take a file system-based (non-Exchange aware) Volume Shadow Copy Service (VSS) snapshot of the volumes containing the database copy and its log files.
   1.a. Suspend replication for the lagged copy being activated by using the Suspend-MailboxDatabaseCopy cmdlet, as shown in this example.

```
Suspend-MailboxDatabaseCopy DB1\EX3 -SuspendComment "Activa
```

   1.b. You can use the vssadmin.exe tool that's included in Windows to take a VSS snapshot, as shown in this example.

```
vssadmin create shadow /For=C:\mountpoints\db01
vssadmin create shadow /For=C:\mountpoints\db01_logs
```

   Note:
   At this point, you have shadow copies outstanding for the database and log volumes. Continuing to perform this procedure on the existing volume would incur a copy on write performance penalty. If this isn't desirable, you can copy the database and log files to another volume to perform the recovery.

2. Activate the lagged mailbox database copy using the Move-ActiveMailboxDatabase cmdlet with the *SkipLagChecks* parameter, as shown in this example:

```
Move-ActiveMailboxDatabase DB1 -ActivateOnServer EX3 -SkipLagChecks
```


1.10.4.3 Monitoring High Availability and Site Resilience

Monitoring High Availability and Site Resilience

Exchange Server 2010 > High Availability and Site Resilience > Managing High Availability and Site Resilience >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-20*

Making sure that your servers are operating reliably and that your database copies are healthy are key objectives for daily messaging operations. To help ensure the availability and reliability of your Microsoft Exchange Server 2010 organization, you must actively monitor the hardware, the Windows operating system, and Exchange 2010 services. Proactive monitoring combined with preventive maintenance can help you identify potential errors before a serious problem interferes with the operation of your Exchange organization.

Monitoring your Exchange organization involves regular checking for problems with services or data. Monitoring typically also includes a notification system that sends alerts

when problems occur. Windows Server 2008 and Exchange 2010 include several tools and services to help make sure that your Exchange organization is running smoothly. The key advantages to daily monitoring are as follows:

- Meeting the requirements of your service level agreements (SLAs)
- Ensuring the successful completion of specific administrative tasks, such as daily backup operations
- Detecting and addressing issues, such as issues that may affect messaging service or data availability

Within an Exchange 2010 organization, the procedures, roles, and responsibilities involved in operations should be formalized. It's important to understand the connection between sound operational practices and procedures and a healthy infrastructure. Well-documented, thorough operational processes and procedures help make sure that all components in an organization's environment on which Exchange relies are managed efficiently and effectively.

Exchange 2010 includes several built-in tools, scripts and features that can be used as part of regular proactive monitoring when Exchange is configured for high availability or site resilience. The primary monitoring cmdlets for high availability and site resilience are Get-MailboxDatabaseCopyStatus and Test-ReplicationHealth. In addition to providing cmdlets that can perform monitoring functions and report status, Exchange 2010 also features a new event log stream that leverages the crimson channel capabilities in Windows Server, as well as built-in scripts that can collect and analyze data from these event channels.

You can use the details in this topic for monitoring the health and status of mailbox database copies for database availability groups (DAGs).

Contents

Get-MailboxDatabaseCopyStatus Cmdlet

You can use the Get-MailboxDatabaseCopyStatus cmdlet to view status information about mailbox database copies. This cmdlet enables you to view information about all copies of a particular database, information about a specific copy of a database on a specific server, or information about all database copies on a server. The following table describes possible values for the copy status of a mailbox database copy.

Database copy status

Database copy status	Description
Failed	The mailbox database copy is in a Failed state because it isn't suspended, and it isn't able to copy or replay log files. While in a Failed state and not suspended, the system will periodically check whether the problem

	that caused the copy status to change to Failed has been resolved. After the system has detected that the problem is resolved, and barring no other issues, the copy status will automatically change to Healthy.
Seeding	The mailbox database copy is being seeded, the content index for the mailbox database copy is being seeded, or both are being seeded. Upon successful completion of seeding, the copy status should change to Initializing.
SeedingSource	The mailbox database copy is being used as a source for a database copy seeding operation.
Suspended	The mailbox database copy is in a Suspended state as a result of an administrator manually suspending the database copy by running the **Suspend-MailboxDatabaseCopy** cmdlet.
Healthy	The mailbox database copy is successfully copying and replaying log files, or it has successfully copied and replayed all available log files.
ServiceDown	The Microsoft Exchange Replication service isn't available or running on the server that hosts the mailbox database copy.
Initializing	The mailbox database copy will be in an Initializing state when a database copy has been created, when the Microsoft Exchange Replication service is starting or has just been started, and during transitions from Suspended, ServiceDown, Failed, Seeding, SinglePageRestore, LostWrite, or Disconnected to another state. While in this state, the system is verifying that the database and log stream are in a consistent state. In most cases, the copy status will remain in the Initializing state for about 15 seconds, but in all cases, it should generally not be in this state for longer than 30 seconds.
Resynchronizing	The mailbox database copy and its log files are being compared with the active copy of the database to check for any divergence between the two copies. The copy status will remain in this state until any divergence is detected and resolved.
Mounted	The active copy is online and accepting client connections. Only the active copy of the mailbox database copy can have a copy status of Mounted.
Dismounted	The active copy is offline and not accepting

	client connections. Only the active copy of the mailbox database copy can have a copy status of Dismounted.
Mounting	The active copy is coming online and not yet accepting client connections. Only the active copy of the mailbox database copy can have a copy status of Mounting.
Dismounting	The active copy is going offline and terminating client connections. Only the active copy of the mailbox database copy can have a copy status of Dismounting.
DisconnectedAndHealthy	The mailbox database copy is no longer connected to the active database copy, and it was in the Healthy state when the loss of connection occurred. This state represents the database copy with respect to connectivity to its source database copy. It may be reported during DAG network failures between the source copy and the target database copy.
DisconnectedAndResynchronizing	The mailbox database copy is no longer connected to the active database copy, and it was in the Resynchronizing state when the loss of connection occurred. This state represents the database copy with respect to connectivity to its source database copy. It may be reported during DAG network failures between the source copy and the target database copy.
FailedAndSuspended	The Failed and Suspended states have been set simultaneously by the system because a failure was detected, and because resolution of the failure explicitly requires administrator intervention. An example is if the system detects unrecoverable divergence between the active mailbox database and a database copy. Unlike the Failed state, the system won't periodically check whether the problem has been resolved, and automatically recover. Instead, an administrator must intervene to resolve the underlying cause of the failure before the database copy can be transitioned to a healthy state.
SinglePageRestore	This state indicates that a single page restore operation is occurring on the mailbox database copy.

The **Get-MailboxDatabaseCopyStatus** cmdlet also includes a parameter called *ConnectionStatus*, which returns details about the in-use replication networks. If you use this parameter, two additional output fields, *IncomingLogCopyingNetwork* and *SeedingNetwork*, will be populated in the task's output.

Get-MailboxDatabaseCopyStatus Examples

The following examples use the **Get-MailboxDatabaseCopyStatus** cmdlet. Each example pipes the results to the **Format-List** cmdlet to display the output in list format.

This example returns status information for all copies of the database DB2.

```
Get-MailboxDatabaseCopyStatus -Identity DB2 | Format-List
```

This example returns the status for all database copies on the Mailbox server MBX2.

```
Get-MailboxDatabaseCopyStatus -Server MBX2 | Format-List
```

This example returns the status for all database copies on the local Mailbox server.

```
Get-MailboxDatabaseCopyStatus -Local | Format-List
```

This example returns status, log shipping, and seeding network information for the database DB3 on the Mailbox server MBX1.

```
Get-MailboxDatabaseCopyStatus -Identity DB3\MBX1 -ConnectionStatus | Format-List
```

For more information about using the **Get-MailboxDatabaseCopyStatus** cmdlet, see Get-MailboxDatabaseCopyStatus.

Return to top

Test-ReplicationHealth Cmdlet

You can use the Test-ReplicationHealth cmdlet to view continuous replication status information about mailbox database copies. This cmdlet can be used to check all aspects of the replication and replay status to provide a complete overview of a specific Mailbox server in a DAG.

The **Test-ReplicationHealth** cmdlet is designed for the proactive monitoring of continuous replication and the continuous replication pipeline, the availability of Active Manager, and the health and status of the underlying cluster service, quorum, and network components. It can be run locally on or remotely against any Mailbox server in a DAG. The **Test-ReplicationHealth** cmdlet performs the tests listed in the following table.

Test-ReplicationHealth cmdlet tests

Test name	Description
ClusterService	Verifies that the Cluster service is running and reachable on the specified DAG member, or if no DAG member is specified, on the local server.
ReplayService	Verifies that the Microsoft Exchange Replication service is running and reachable on the specified DAG member, or if no DAG member is specified, on the local server.
ActiveManager	Verifies that the instance of Active Manager running on the specified DAG member (or if no DAG member is specified, the local server) is in a valid role (primary, secondary,

	or stand-alone).
TasksRpcListener	Verifies that the tasks remote procedure call (RPC) server is running and reachable on the specified DAG member, or if no DAG member is specified, on the local server.
TcpListener	Verifies that the TCP log copy listener is running and reachable on the specified DAG member, or if no DAG member is specified, on the local server.
DagMembersUp	Verifies that all DAG members are available, running, and reachable.
ClusterNetwork	Verifies that all cluster-managed networks on the specified DAG member (or if no DAG member is specified, the local server) are available.
QuorumGroup	Verifies that the default cluster group (quorum group) is in a healthy and online state.
FileShareQuorum	Verifies that the witness server and witness directory and share configured for the DAG are reachable.
DBCopySuspended	Checks whether any mailbox database copies are in a state of Suspended on the specified DAG member, or if no DAG member is specified, on the local server.
DBCopyFailed	Checks whether any mailbox database copies are in a state of Failed on the specified DAG member, or if no DAG member is specified, on the local server.
DBInitializing	Checks whether any mailbox database copies are in a state of Initializing on the specified DAG member, or if no DAG member is specified, on the local server.
DBDisconnected	Checks whether any mailbox database copies are in a state of Disconnected on the specified DAG member, or if no DAG member is specified, on the local server.
DBLogCopyKeepingUp	Verifies that log copying and inspection by the passive copies of databases on the specified DAG member (or if no DAG member is specified, on the local server) are able to keep up with log generation activity on the active copy.
DBLogReplayKeepingUp	Verifies that replay activity for the passive copies of databases on the specified DAG member (or if no DAG member is specified, on the local server) is able to keep up with log copying and inspection activity.

Test-ReplicationHealth Example

This example uses the **Test-ReplicationHealth** cmdlet to test the health of replication for the Mailbox server MBX1.

```
Test-ReplicationHealth -Identity MBX1
```

Return to top

Crimson Channel Event Logging

Windows Server 2008 includes two categories of event logs: Windows logs, and Applications and Services logs. The Windows logs category includes the event logs available in previous versions of Windows: Application, Security, and System event logs. It also includes two new logs: the Setup log and the ForwardedEvents log. Windows logs are intended to store events from legacy applications and events that apply to the entire system.

Applications and Services logs are a new category of event logs. These logs store events from a single application or component rather than events that might have system-wide impact. This new category of event logs is referred to as an application's crimson channel.

The Applications and Services logs category includes four subtypes: Admin, Operational, Analytic, and Debug logs. Events in Admin logs are of particular interest if you use event log records to troubleshoot problems. Events in the Admin log should provide you with guidance about how to respond to the events. Events in the Operational log are also useful, but may require more interpretation. Admin and Debug logs aren't as user friendly. Analytic logs (which by default are hidden and disabled) store events that trace an issue, and often a high volume of events are logged. Debug logs are used by developers when debugging applications.

Exchange 2010 logs events to crimson channels in the Applications and Services logs area. You can view these channels by performing these steps:

1. Open Event Viewer.
2. In the console tree, navigate to **Applications and Services Logs** > **Microsoft** > **Exchange**.
3. Under **Exchange**, select a crimson channel: **HighAvailability** or **MailboxDatabaseFailureItems**.

The HighAvailability channel contains events related to startup and shutdown of the Microsoft Exchange Replication service, and the various components that run within the Microsoft Exchange Replication service, such as Active Manager, the third-party synchronous replication API, the tasks RPC server, TCP listener, and Volume Shadow Copy Service (VSS) writer. The HighAvailability channel is also used by Active Manager to log events related to Active Manager role monitoring and database action events, such as a database mount operation and log truncation, and to record events related to the DAG's underlying cluster.

The MailboxDatabaseFailureItems channel is used to log events associated with any failures that affect a replicated mailbox database.

Return to top

CollectOverMetrics.ps1 Script

Exchange 2010 includes a script called CollectOverMetrics.ps1, which can be found in the Scripts folder. CollectOverMetrics.ps1 reads DAG member event logs to gather information about database operations (such as database mounts, moves, and failovers) over a specific time period. For each operation, the script records the following information:

- Identity of the database

- Time at which the operation began and ended
- Servers on which the database was mounted at the start and finish of the operation
- Reason for the operation
- If the operation was successful, including the error details if the operation failed

The script writes this information to .csv files with one operation per row. It writes a separate .csv file for each DAG.

The script supports parameters that allow you to customize the script's behavior and output. For example, the results can be restricted to a specified subset by using the *Database* or *ReportFilter* parameters. Only the operations that match these filters will be included in the summary HTML report. The available parameters are listed in the following table.

CollectOverMetrics.ps1 script parameters

Parameter	Description
DatabaseAvailabilityGroup	Specifies the name of the DAG from which you want to collect metrics. If this parameter is omitted, the DAG of which the local server is a member will be used. Wildcard characters can be used to collect information from and report on multiple DAGs.
Database	Provides a list of databases for which the report needs to be generated. Wildcard characters are supported, for example, –Database:"DB1","DB2" or –Database:"DB*".
StartTime	Specifies the duration of the time period to report on. The script gathers only the events logged during this period. As a result, the script may capture partial operation records (for example, only the end of an operation at the start of the period or vice-versa). If neither *StartTime* nor *EndTime* is specified, the script defaults to the past 24 hours. If only one parameter is specified, the period will be 24 hours, either beginning or ending at the specified time.
EndTime	Specifies the duration of the time period to report on. The script gathers only the events logged during this period. As a result, the script may capture partial operation records (for example, only the end of an operation at the start of the period or vice-versa). If neither *StartTime* nor *EndTime* is specified, the script defaults to the past 24 hours If only one parameter is specified, the period will be 24 hours, either beginning or ending at the specified time.
ReportPath	Specifies the folder used to store the results of event processing. If this parameter is omitted, the Scripts folder will be used. When specified, the script takes a list of .csv

	files generated by the script and uses them as the source data to generate a summary HTML report. The report is the same one that is generated with the -GenerateHtmlReport option. The files can be generated across multiple database availability groups at many different times, or even with overlapping times, and the script will merge all of their data together.
GenerateHtmlReport	Specifies that the script gather all the information it has recorded, group the data by the operation type, and then generate an HTML file that includes statistics for each of these groups. The report includes the total number of operations in each group, the number of operations that failed, and statistics for the time taken within each group. The report also contains a breakdown of the types of errors that resulted in failed operations.
ShowHtmlReport	Specifies that the HTML-generated report should be displayed in a Web browser after its generated.
SummariseCSVFiles	Specifies that the script read the data from existing .csv files that were previously generated by the script. This data is then used to generate a summary report similar to the report generated by the *GenerateHtmlReport* parameter.
ActionType	Specifies the type of operational actions the script should collect. The values for this parameter are `Move`, `Mount`, `Dismount`, and `Remount`. The `Move` value refers to any time that the database changes its active server, whether by controlled moves or by failovers. The `Mount`, `Dismount`, and `Remount` values refer to times that the database changes its mounted status without moving to another computer.
ActionTrigger	Specifies which administrative operations should be collected by the script. The values for this parameter are `Admin` or `Automatic`. Automatic actions are those performed automatically by the system (for example, a failover when a server goes offline). Admin actions are any actions that were performed by an administrator using either the Exchange Management Shell or the Exchange Management Console.
RawOutput	Specifies that the script writes the results that would have been written to .csv files directly to the output stream, as would happen with write-output. This information can then be piped to other commands.

IncludedExtendedEvents	Specifies that the script collects the events that provide diagnostic details of times spent mounting databases. This can be a very time-consuming stage if the Application event log on the servers is very large.
MergeCSVFiles	Specifies that the script takes all the .csv files containing data about each operation and merges them into a single .csv file.
ReportFilter	Specifies that a filter should be applied to the operations using the fields as they appear in the .csv files. This parameter uses the same format as a `Where` operation, with each element set to `$_` and returning a Boolean value. For example: `{$_DatabaseName -notlike "Mailbox Database*"}` can be used to exclude the default databases from the report.

CollectOverMetrics.ps1 Examples

The following example collects metrics for all databases that match DB* (which includes a wildcard character) in a DAG named DAG1. After the metrics are collected, an HTML report is generated and displayed.

```
CollectOverMetrics.ps1 -DatabaseAvailabilityGroup DAG1 -Database:"DB*" -GenerateH
```

The following examples demonstrate ways that the summary HTML report may be filtered. The first uses the *Database* parameter, which takes a list of database names. The summary report then contains data only about those databases. The next two examples use the *ReportFilter* option. The last example filters out all the default databases.

```
CollectOverMetrics -SummariseCsvFiles (dir *.csv) -Database MailboxDatabase123,Ma
CollectOverMetrics -SummariseCsvFiles (dir *.csv) -ReportFilter { $_.DatabaseName
CollectOverMetrics -SummariseCsvFiles (dir *.csv) -ReportFilter { ($_.ActiveOnSta
```

Return to top

CollectReplicationMetrics.ps1 Script

CollectReplicationMetrics.ps1 is another health metric script included in Exchange 2010. This script provides an active form of monitoring because it collects metrics in real time, while the script is running. CollectReplicationMetrics.ps1 collects data from performance counters related to database replication. The script gathers counter data from multiple Mailbox servers, writes each server's data to a .csv file, and can then report various statistics across all of this data (for example, the amount of time each copy was failed or suspended, the average copy or replay queue length, or the amount of time that copies were outside of their failover criteria).

You can either specify the servers individually, or you can specify entire DAGs. You can either run the script can to first collect the data and then generate the report, or you can run it just gather the data or to only report on data that's already been collected. You can specify the frequency at which data should be sampled and the total duration to gather data.

The data collected from each server is written to a file named **CounterData.<ServerName>.<TimeStamp>.csv**. The summary report will be written to a file named **HaReplPerfReport.<DAGName>.<TimeStamp>.csv**, or **HaReplPerfReport.<TimeStamp>.csv** if you didn't run the script was with the *DagName* parameter.

The script starts PowerShell jobs to collect the data from each server. These jobs run for the full period in which data is being collected. If you specify a large number of servers, this process can use a considerable amount of memory. The final stage of the process, when data is processed into a summary report, can also be quite time consuming for large amounts of data. It's possible to run the collection stage on one computer, and then copy the data elsewhere for processing.

The CollectReplicationMetrics.ps1 script supports parameters that allow you to customize the script's behavior and output. The available parameters are listed in the following table.

CollectReplicationMetrics.ps1 script parameters

Parameter	Description
DagName	Specifies the name of the DAG from which you want to collect metrics. If this parameter is omitted, the DAG of which the local server is a member will be used.
DatabaseNames	Provides a list of databases for which the report needs to be generated. Wildcards characters are supported for use, for example, –`DatabaseNames:"DB1","DB2"` or –`DatabaseNames:"DB*"`.
ReportPath	Specifies the folder used to store the results of event processing. If this parameter is omitted, the Scripts folder will be used.
Duration	Specifies the amount of time the collection process should run. Typical values would be one to three hours. Longer durations should be used only with long intervals between each sample or as a series of shorter jobs run by scheduled tasks.
Frequency	Specifies the frequency at which data metrics are collected. Typical values would be 30 seconds, one minute, or five minutes. Under normal circumstances, intervals that are shorter than these won't show significant changes between each sample.
Servers	Specifies the identity of the servers from which to collect statistics. You can specify any value, including wildcard characters or GUIDs.
SummariseFiles	Specifies a list of .csv files to generate a summary report. These files are the files named **CounterData.<CounterData>*** and are generated by the CollectReplicationMetrics.ps1 script.
Mode	Specifies the processing stages that the script executes. You can use the following values: • `CollectAndReport` This is the default value. This value signifies that the script should both collect the data from the servers and then process them to produce the summary report. • `CollectOnly` This value signifies that the script should just collect the data and not produce the report.

	• `ProcessOnly` This value signifies that the script should import data from a set of .csv files and process them to produce the summary report. The *SummariseFiles* parameter is used to provide the script with the list of files to process.
MoveFilestoArchive	Specifies that the script should move the files to a compressed folder after processing.
LoadExchangeSnapin	Specifies that the script should load the Exchange Shell commands. This parameter is useful when the script needs to run from outside the Exchange Management Shell, such as in a scheduled task.

CollectReplicationMetrics.ps1 Example

The following example gathers one hour's worth of data from all the servers in the DAG "DAG1", sampled at one minute intervals, and then generates a summary report. In addition, the *ReportPath* parameter is used, which causes the script to place all the files in the current directory.

```
CollectReplicationMetrics.ps1 -DagName DAG1 -Duration "01:00:00" -Frequency "00:0
```

The following example reads the data from all the files matching "CounterData*" and then generates a summary report.

```
CollectReplicationMetrics.ps1 -SummariseFiles (dir CounterData*) -Mode ProcessOnl
```

Return to top

CheckDatabaseRedundancy.ps1 Script

As its name implies, the purpose of the CheckDatabaseRedundancy.ps1 script is to monitor the redundancy of replicated mailbox databases by validating that there is at least two configured and healthy and current copies, and to alert you when only a single healthy copy of a replicated database exists. In this case, both active and passive copies are counted when determining redundancy.

When the Mailbox server role is installed, the CheckDatabaseRedundancy.ps1 script is automatically configured by Exchange to run as a scheduled task named **Database One Copy Alert**. By default, the Database One Copy Alert scheduled task is configured to run every 60 minutes. You can modify this behavior and the scheduled task settings using the Windows Task Scheduler. The script is designed to first check for DAG membership, so if the Mailbox server is not a member of a DAG, the script exits out right away.

The script can also be run interactively from the scripts folder. When running the script interactively, you must specify either a database name or a DAG member name. To specify a database, you use the *MailboxDatabaseName* parameter and to specify a DAG member, you use the *MailboxServerName* parameter. When run interactively in the console, the script performs the redundancy check only once, and outputs the CurrentState (red or green) on the screen.

Like other scripts and cmdlets, CheckDatabaseRedundancy.ps1 can also be run in monitoring mode and generate events by adding the *MonitoringContext* parameter. The scheduled task created by Exchange runs the script in monitoring mode. This mode also enables the script to be invoked by a monitoring solution, such as Microsoft System Center Operations Manager (SCOM). In monitoring mode, the script generates red alert and green alert events into the local server's Application event log. A red alert event (event ID 4113) is generated only if the database has been "red" for 20 minutes more (in

duration, not consecutive) in the hour-long run of the script, and a green alert event (event ID 4114) when the database has been "green" for 10 consecutive minutes. By default, once a red alert event is generated, it will continue to be reported every 15 minutes.

In addition, the script has some other useful options. For example, you can add the *ShowDetailedErrors* parameter to get greater detail about any errors that occur, and you can add the *Verbose* parameter for additional troubleshooting information. The script also includes a *SendSummaryMailTos* parameter which can be used to send a summary report by email to a list of specified email addresses when the script has finished running. This enables administrators to quickly look at hourly reports to see if any redundancy issues have occurred. If you do use the email functionality, you'll need to include the *SummaryMailFrom* parameter whenever you use the *SendSummaryMailTos* parameter.

Microsoft recommends running this script regularly, as part of your normal monitoring operations, using either the automated scheduled task, or a monitoring system such as SCOM. To ensure you don't have lengthy periods in which database redundancy is compromised, run the script every 60 minutes. The script includes a parameter called *TerminateAfterDurationSecs*, which when set to -1 or 0 when executing the script, can be used to run the script for an infinite amount of time.

If you're not running a monitoring solution such as SCOM, we recommend you allow the automatically created scheduled task to automate and schedule script execution.

There are known issues in the Windows Server 2008 SP2 Task Scheduler that may cause Task Scheduler to crash when you have scheduled a long-running task. These issues do not exist in Windows Server 2008 R2; so if possible, run the script from Windows Server 2008 R2. If you can't run the script from Windows Server 2008 R2, and you're running it from Windows Server 2008 SP2, we recommend two modifications. First, instead of running the script with its built-in transient suppression of 60 minutes, run the script every 5 minutes by using the following parameters:

```
CheckDatabaseRedundancy.ps1 -MonitoringContext -SleepDurationBetweenIterationsSec
```

Second, if possible, use SCOM to define the transient suppression behavior (e.g., if 3 red alert events are logged within a 20 minute period, generate an alert; and if a green alert event is logged, change the CurrentState to green).

If the Database One Copy Alert scheduled task is altered or removed, you can delete and re-schedule by running the following command:

```
schtasks /create /TN "Check Database Redundancy" /TR "Powershell.exe -NonInteract
```

Replace the parameters in the above script with the script parameters you want to use. Additional parameters for the script are also described in the script.

When using the schtasks command line tool to create a scheduled task, the /TR option is limited to 261 characters. The above example exceeds that limit. If the parameters and paths you use cause the /TR option to exceed 261 characters then you must manually create the scheduled task using the Task Scheduler applet on the Administrative Tools menu. Alternatively, you can copy and paste the following XML into Notepad, edit it appropriately, save it as an XML file and import it using the Task Scheduler applet.

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"
  <RegistrationInfo>
    <Date>2010-05-11T15:55:47</Date>
    <Author>administrator</Author>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
```

```
      <Repetition>
        <Interval>PT1H</Interval>
        <StopAtDurationEnd>false</StopAtDurationEnd>
      </Repetition>
      <StartBoundary>2010-05-11T15:55:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <UserId>SYSTEM</UserId>
      <RunLevel>HighestAvailable</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>Powershell.exe</Command>
      <Arguments>-NonInteractive -WindowStyle Hidden -command 'C:\Program Files\M
    </Exec>
  </Actions>
</Task>
```

Return to top

1.10.4.4 Switchovers and Failovers

Switchovers and Failovers

Exchange Server 2010 > High Availability and Site Resilience > Managing High Availability and Site Resilience >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-28*

Switchovers and failovers are the two forms of outages in Microsoft Exchange Server 2010. A *switchover* is a scheduled outage of a database or server that's explicitly initiated by an administrator, typically in preparation for performing a maintenance operation. Switchovers involve an administrator moving the active mailbox database copy to another server in the database availability group (DAG).

A *failover* refers to unexpected events that result in the unavailability of services, data, or both. A failover involves the system automatically recovering from the failure by activating

a passive mailbox database copy to make it the active mailbox database copy.

The high availability platform in Exchange 2010 is designed to handle both switchovers and failovers.

Looking for management tasks related to high availability and site resilience? See Managing High Availability and Site Resilience.

Switchovers

There are three types of switchovers in Exchange 2010:

- Database switchovers
- Server switchovers
- Datacenter switchovers

Database Switchovers

A *database switchover* is the process by which an individual active database is switched over to another database copy (a passive copy), and that database copy is made the new active database copy. Database switchovers can happen both within and across datacenters. A database switchover can be performed by using the Exchange Management Console (EMC) or the Exchange Management Shell. Regardless of which interface is used, the switchover process is the same:

1. The administrator initiates a database switchover to move the current active mailbox database copy to another server. The switchover can be initiated by using the Move-ActiveMailboxDatabase cmdlet or by using the Activate a Database Copy wizard.
2. The client used for the task makes an RPC call to the Microsoft Exchange Replication service on a DAG member.
3. If the DAG member doesn't hold the Primary Active Manager (PAM) role, the DAG member refers the task to the PAM.
4. The task makes an RPC call to the Microsoft Exchange Replication service on the PAM.
5. The PAM reads and updates the database location information that's stored in the cluster database for the DAG.
6. The PAM contacts the Microsoft Exchange Replication service on the DAG member whose passive copy is being activated as the new active mailbox database copy.
7. The Microsoft Exchange Replication service on the target server queries the Microsoft Exchange Replication services on all other DAG members to determine the best log source for the database copy.
8. The database is dismounted from the current server and the Microsoft Exchange Replication service on the target server copies the remaining logs to the target server.
9. The Microsoft Exchange Replication service on the target server requests a database mount.
10. The Microsoft Exchange Information Store service on the target server replays the log files and mounts the database.
11. Any error codes are returned to the Microsoft Exchange Replication service on the target server.
12. The PAM updates the database copy state information in the cluster database for the DAG.
13. Any error codes are returned by the Microsoft Exchange Replication service on the target server to the Microsoft Exchange Replication service on the PAM.
14. The Microsoft Exchange Replication service on the PAM returns any errors to the administrative interface where the task was called.
15. Remote PowerShell returns the results of the operation to the calling administrative interface.

For detailed steps about how to perform a database switchover, see Move the Active Mailbox Database.

Server Switchovers

A server switchover is the process by which all active databases on a DAG member are activated on one or more other DAG members. Like database switchovers, a server switchover can occur both within a datacenter and across datacenters, and it can be initiated by using both the EMC and the Shell. Regardless of which interface is used, the switchover process is the same:

1. The administrator initiates a server switchover to move all current active mailbox database copies to one or more other servers. The switchover can be initiated by using the Move-ActiveMailboxDatabase cmdlet, or by using the Switchover Server UI.
2. The task performs the same steps described earlier in this topic for database switchovers (Steps 2 through 4) for each of the active databases on the current server.
3. The PAM reads and updates the database location information that's stored in the cluster database for the DAG.
4. The PAM contacts the Microsoft Exchange Replication service on each DAG member that has a passive copy being activated.
5. The Microsoft Exchange Replication service on the target servers query the Microsoft Exchange Replication services on all other DAG members to determine the best log source for the database copy.
6. The database is dismounted from the current server and the Microsoft Exchange Replication service on each target server copies the remaining logs.
7. The Microsoft Exchange Replication service on each target server requests a database mount.
8. The Microsoft Exchange Information Store service on each target server replays the log files and mounts the database.
9. Any error codes are returned to the Microsoft Exchange Replication service on the target server.
10. The PAM updates the database copy state information in the cluster database for the DAG.
11. Any error codes are returned by the Microsoft Exchange Replication service on the target server to the Microsoft Exchange Replication service on the PAM.
12. The Microsoft Exchange Replication service on the PAM returns any errors to the administrative interface where the task was called.
13. Remote PowerShell returns the results of the operation to the calling administrative interface.

For detailed steps about how to perform a server switchover, see Perform a Server Switchover.

Datacenter Switchovers

A datacenter or site failure is managed differently from the types of failures that can cause a server or database failover. In a high availability configuration, automatic recovery is initiated by the system, and the failure typically leaves the messaging system in a fully functional state. By contrast, a datacenter failure is considered to be a disaster recovery event, and as such, recovery must be manually performed and completed for the client service to be restored and for the outage to end. The process you perform is called a *datacenter switchover*. As with many disaster recovery scenarios, prior planning and preparation for a datacenter switchover can simplify your recovery process and reduce the duration of your outage.

For more information about datacenter switchovers, including detailed steps for performing a datacenter switchover, see Datacenter Switchovers.

Failovers

A failover is an automatic activation process that can occur at either the database or server level. Failovers occur in response to a failure that affects an individual database (for example, an isolated storage loss) or an entire server (for example, a motherboard failure or a loss of power).

DAGs and mailbox database copies provide full redundancy (and therefore rapid recovery) of both the data and the services that provide access to the data. The following table lists the expected recovery actions for a variety of failures. Some failures require the administrator to initiate the recovery, and other failures are automatically handled by the system.

Description	Automatic activation	Automatic repair action	State during repair: Active	State during repair: Passive	Repair actions	Comments
Extensible Storage Engine (ESE) soft database failure: The drives storing the database are returning errors on some reads (for example, a -1018 error).	Possible short outage. Possible automatic failover.	Automatic patching of bad page.	Manual switchover, automatic failover, or online repair.	Failed	RAID rebuild, database and database copy repair, restore and run recovery then page patching, or page patching from copy.	There may be other soft database failure codes. Doesn't include NTFS file system block failures. If failover or switchover is performed, host server is updated.
ESE "*semi-soft*" database failure: The drives storing the database are returning errors on some writes.	Short outage during automatic failover.	Automatic volume/ disk rebuilt after possible drive replacement.	Dismounted if can't be recovered.	Failed	RAID rebuild may solve the problem. Copy and repair, restore and run recovery, or volume/ disk rebuilt after possible replacement.	An ESE semi-soft write error means some writes are successful. Doesn't include an NTFS block failure.

ESE "semi-soft" log failure: The drives storing the log data are returning non-recovered errors on some reads or writes.	Short outage during automatic failover.	Automatic volume/ disk rebuilt after possible drive replacement.	Dismounted if can't be recovered.	Failed	RAID rebuild may solve the problem. Copy and repair, restore and run recovery, or volume/ disk rebuilt after possible replacement.	An ESE semi-soft read/write error means some reads/ writes are successful. If the database fails, automated recovery will occur before log data recovery processing starts.
ESE software error or resource exhaustion: An error where ESE terminates instance (for example, Event ID 1022, checkpoint depth too deep).	Short outage during automatic failover.	None.	Dismounted if can't be recovered.	Failed	Fix underlying resource issue.	This failure could be the surfaced error of other cases.
NTFS block failures: The drives storing the database or logs experiences a read or write error to an NTFS control structure.	Short outage during automatic failover.	Volume completely rebuilt after possible drive replacement.	Dismounted if can't be recovered.	Failed	RAID rebuild may solve the problem. NTFS utilities may solve the NTFS problems. Exchange recovery may be required.	This is more likely to occur when RAID isn't in use. If this impacts the active log volume, some recent log files will be lost. Doesn't include errors automatically corrected by NTFS or its underlying software or hardware

						stack.
Database or log drive failure: A drive storing the database or logs has completely failed and is inaccessible.	Short outage during automatic failover.	Drive reformatted or replaced, followed by complete volume rebuild.	Dismounted if can't be recovered.	Failed	Drive replacement followed by possible RAID rebuild. Drive replacement followed by complete volume rebuild. Complete volume rebuild.	Not applicable.
Database or log volume failure: The volume fails due to NTFS or lower level volume issues.	Short outage during automatic failover.	Drive reformatted or replaced.	Dismounted if can't be recovered.	Failed	Drive replacement followed by possible RAID rebuild. Drive replacement followed by complete volume rebuild. Complete volume rebuild.	Not applicable.
Database or log volume out of space: The NTFS file system with the database or log files is out of space.	Automatic failover if other copy isn't in similar state.	None.	Dismounted.	Failed	Run full or incremental backups, manually delete logs, let time pass, resume database copy, or repair failed	Not applicable.

					database copy.	
Administrator dismounts the wrong database.	If automatic failover isn't blocked by the administrator, there will be a short outage. If automatic failover is prevented, there will be an outage until the database is mounted.	None.	Dismounted.	Not applicable	Administrator corrects the error.	Not applicable.
Administrator suspends the wrong database copy.	Depending on configuration and impacted copy, auto recovery may be prevented.	None.	Not applicable.	Suspended	Administrator corrects the error.	Not applicable.
Administrator dismounts a database for storage, NTFS, or volume maintenance.	If automatic failover isn't blocked by the administrator, there will be a short outage. If automatic failover is blocked, there will be an outage until the administrator	None.	Dismounted.	Not applicable	Administrator completes the task.	Not applicable.

	completes the task.					
Administrator suspends a database copy for storage, NTFS, or volume maintenance.	Depending on configuration and impacted copy, auto recovery may be prevented.	None.	Not applicable.	Suspended	Administrator completes the actions.	Not applicable.
Administrator dismounts a database for offline database maintenance.	Outage until repaired.	None.	Dismounted.	Suspended	Administrator completes the actions.	Active and passive database copies are diverged. Administrator must suspend copies.
Storage area network (SAN), disk, or storage controller failure.	Short outage during automatic failover.	None.	Dismounted.	Any	Repair hardware.	A passive database copy will be in the state that existed at the time when the system failed.
Server hardware maintenance.	Short outage during automatic failover (unless blocked by an administrator).	None.	Dismounted.	Any	Complete actions.	A passive database copy will be in the state that existed at the time when the system was shut down.
Server software maintenance.	Short outage during automatic failover (unless blocked by an administrator).	None.	Dismounted.	Any	Complete actions.	A passive database copy will be in the state that existed at the time when the system was shut down.

Microsoft Exchange Information Store service is stopped or paused by an administrator.	None.	None.	Dismounted.	Any	Restart the Microsoft Exchange Information Store service.	A passive database copy will be in the state that existed at the time when the service was stopped.
Microsoft Exchange Information Store service fails; operating system is still running.	Short outage during automatic failover.	Service Control Manager restarts the Microsoft Exchange Information Store service.	Dismounted.	Any	Manually or automatically restart the Microsoft Exchange Information Store service.	A passive database copy will be in the state that existed when the Microsoft Exchange Information Store service failed.
Partial Microsoft Exchange Information Store service failure; some part of the Exchange store stops functioning, but it's not identified as completely failed.	Possible short outage during automatic failover.	None.	Mounted and partially functional.	Any, but may be only partially functional	Restart server, operating system, or Microsoft Exchange Information Store service.	Not applicable.
Server failure: The server fails for one of the following reasons: • Complete power failure • Unrecovered failure of the processor chip, motherboard, or backplane • Operating system stop error • Operating system stops responding • Complete communication failure	Short outage during automatic failover.	Restart computer.	Dismounted.	Any	Restore power, change operating system settings, change hardware settings, replace hardware, restart operating system, service operating system, service hardware, or repair communication problems.	Not applicable.

DAG experiences a quorum failure.	Outage until repaired.	None.	Dismounted.	Any	Repair failed quorum, assign new quorum, or restore the network that's causing quorum failure.	A passive database copy will be in the state that existed at the time when the system failed.
MAPI network communication failure: The server is no longer available on the MAPI network.	Short outage during automatic failover; must be lossless.	None. Communication continues to be attempted.	Dismounted.	Any	Fix communication problem by correcting hardware or software issues.	Not applicable.
Replication network communication failure: The server can't receive heartbeats, log copies, or seed through the failed replication network.	Possible short copying or seeding outage while the workload is switched to other network.	None. Communication continues to be attempted.	None.	Any	Fix communication problem by correcting hardware or software issues.	Resiliency impacted by failure.
Multiple network communication failure: The server can't receive heartbeats, log copies, or seed through multiple networks.	Short outage during automatic failover; must be lossless.	None. Communication continues to be attempted.	Dismounted.	Any	Fix communication problem by correcting hardware or software issues.	At least one network is still functional.
Partial failure of one or more networks: Networks experience high error rates.	Failure not detected; no action.	None.	Mounted, but possible performance issues.	Any	Fix communication problem by correcting hardware or software issues.	Network experiences higher than normal error rates.
Undetected operating	None.	None.	Any.	Any	Restart or	Hang isn't detected

system hang: Operating system stops responding but it's not detected by monitoring or clustering.					terminate the resources that aren't responding.	so no action is taken. Some functionality may be operational.
Operating system drive experiences a failure.	Short outage during automatic failover.	None.	Dismounted.	Any	Replace drive and rebuild server or rebuild volume by using RAID.	Not applicable.
Operating system drive out of space.	Short outage during automatic failover.	None.	Dismounted.	Any	Manually free space on the volume.	Not applicable.
Drive containing Exchange binaries experiences a volume or drive failure.	Short outage during automatic failover.	None.	Dismounted.	Any	Replace drive and reinstall application or rebuild volume by using RAID.	Not applicable.
Drive containing the Exchange binaries is out of space.	Short outage during automatic failover.	None.	Dismounted.	Any	Manually free space on the volume.	Not applicable.
Invalid new log detected: The log sequence is disrupted by an existing file.	Short outage during automatic failover; assume other copies don't have the same problem.	None.	Dismounted.	Failed	Remove disruptive logs after determining source.	The disruptive logs shouldn't replicate.
Continuous replication detects invalid log: Replay detects an inappropriate log during copy or replay.	Not applicable.	Discard log.	Not applicable.	Failed	Discard invalid log; move impacting log stream.	Not applicable.

Database Failovers

A database failover occurs when a database copy that was active is no longer able to remain active. The following occurs as part of a database failover:

1. The database failure is detected by the Microsoft Exchange Information Store service.
2. The Microsoft Exchange Information Store service writes failure events to the crimson channel event log.
3. The Active Manager on the server that contains the failed database detects the failure events.
4. The Active Manager requests the database copy status from the other servers that hold a copy of the database.
5. The other servers return the requested database copy status to the requesting Active Manager.
6. The PAM initiates a move of the active database to another server in the DAG using a best copy selection algorithm.
7. The PAM updates the database mount location in the cluster database to refer to the selected server.
8. The PAM sends a request to the Active Manager on the selected server to become the database master.
9. The Active Manager on the selected server requests that the Microsoft Exchange Replication service attempt to copy the last logs from the previous server and set the mountable flag for the database.
10. The Microsoft Exchange Replication service copies the logs from the server that previously had the active copy of the database.
11. The Active Manager reads the maximum log generation number from the cluster database.
12. The Microsoft Exchange Information Store service mounts the new active database copy.

Server Failovers

A server failover occurs when the DAG member is no longer able to service the MAPI network, or when the Cluster service on a DAG member is no longer able to contact the remaining DAG members. The following occurs as part of a server failover:

1. The Cluster service on the PAM sends a notification to the PAM for one of two conditions:
   1.a. **Node Down** The server is reachable but is unable to participate in DAG operations.
   1.b. **MAPI Network Down** The server can't be contacted over the MAPI network and therefore can't participate in DAG operations.
2. If the server is reachable, the PAM contacts the Active Manager on the affected server and requests that all databases be immediately dismounted.
3. For each affected database copy:
   3.a. The PAM requests the database copy status from all servers in the DAG.
   3.b. The PAM receives a response from all reachable and active DAG members.
   3.c. The PAM tries to determine the best log source among all responding servers by querying the most recent log generation number from each of the responders.
   3.d. Each of the servers responds with the log generation number.
4. The PAM retrieves the current search index catalog status from the cluster database.
5. Based on the log generation number and catalog health of each database copy, the PAM selects the best copies to activate.
6. The PAM updates the mounted location of the database in the cluster database.
7. The PAM initiates database failover by communicating with the Active Manager on one or more other servers.
8. The Active Manager on the selected servers requests that the Microsoft Exchange Replication service attempt to copy the last logs from the previous server and set the mountable flag.
9. When the database is mountable, the Active Manager on the servers mounts the databases.

For more information about Active Manager's best copy selection process, see Understanding Active Manager.

1.10.4.4.1 Datacenter Switchovers

Datacenter Switchovers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-14*

By combining the native site resilience capabilities in Microsoft Exchange Server 2010 Service Pack 1 (SP1) with proper planning, a second datacenter can be rapidly activated to serve the failed datacenter's clients. A datacenter or site failure is managed differently from the types of failures that can cause a server or database failover. In a high availability configuration, automatic recovery is initiated by the system, and the failure typically leaves the messaging system in a fully functional state. By contrast, a datacenter failure is considered to be a disaster recovery event, and recovery must be manually performed and completed for the client service to be restored, and for the outage to end. The process you perform is referred to as a *datacenter switchover*. As with many disaster recovery scenarios, prior planning and preparation for a datacenter switchover can simplify the recovery process and reduce the duration of the outage.

There are four basic steps that you complete to perform a datacenter switchover, after making the initial decision to activate the second datacenter:

1. **Terminate a partially running datacenter** This step involves terminating Mailbox and Unified Messaging services in the primary datacenter, if any services are still running. This is particularly important for the Mailbox server role because it uses an active/passive high availability model. If services in a partially failed datacenter aren't stopped, it's possible for problems from the partially failed datacenter to negatively affect the services during a switchover back to the primary datacenter.

   Important:

   If network or Active Directory infrastructure reliability has been compromised as a result of the primary datacenter failure, we recommend that all messaging services be off until these dependencies are restored to healthy service.

2. **Validate and confirm the prerequisites for the second datacenter** This step can be performed in parallel with step 1 because validation of the health of the infrastructure dependences in the second datacenter is largely independent of the first datacenter services. Each organization typically requires its own method for performing this step. For example, you may decide to complete this step by reviewing health information collected and filtered by an infrastructure monitoring application, or by using a tool that's unique to your organization's infrastructure. This is a critical step, because activating the second datacenter when its infrastructure is unhealthy and unstable is likely to yield poor results.
3. **Activate the Mailbox servers** This step begins the process of activating the second datacenter. This step can be performed in parallel with step 4 because the Microsoft Exchange services can handle database outages and recover. Activating the Mailbox servers involves a process of marking the failed servers from the primary datacenter as unavailable followed by activation of the servers in the second datacenter. The activation process for

Mailbox servers depends on whether the DAG is in database activation coordination (DAC) mode. For more information about database activation coordination mode, see Understanding Datacenter Activation Coordination Mode.
If the DAG is in DAC mode, you can use the Exchange site resilience cmdlets to terminate a partially failed datacenter (if necessary) and activate the Mailbox servers. For example, in DAC mode, this step is performed by using the Stop-DatabaseAvailabilityGroup cmdlet. In some cases, the servers must be marked as unavailable twice (once in each datacenter). Next, the Restore-DatabaseAvailabilityGroup cmdlet is run to restore the remaining members of the database availability group (DAG) in the second datacenter by reducing the DAG members to those that are still operational, thereby reestablishing quorum. If the DAG isn't in DAC mode, you must use the Windows Failover Cluster tools to activate the Mailbox servers. After either process is complete, the database copies that were previously passive in the second datacenter can become active and be mounted. At this point, Mailbox server recovery is complete.

4. **Activate the other server roles** This involves using the URL mapping information and the Domain Name System (DNS) change methodology to perform all required DNS updates. The mapping information describes what DNS changes to perform. The amount of time required to complete the update depends on the methodology used and the Time to Live (TTL) settings on the DNS record (and whether the deployment's infrastructure honors the TTL).

Users should start to have access to messaging services sometime after steps 3 and 4 are completed. Steps 3 and 4 are described in greater detail later in this topic.

Looking for management tasks related to high availability and site resilience? See Managing High Availability and Site Resilience.

Contents

Terminating a Partially Failed Datacenter

If any DAG members in the failed datacenter are still running, they should be terminated.

When the DAG is in DAC mode, the specific actions to terminate any surviving DAG members in the primary datacenter are as follows:

1. The DAG members in the primary datacenter must be marked as stopped in the primary datacenter. *Stopped* is a state of Active Manager that prevents databases from mounting, and Active Manager on each server in the failed datacenter is put into this state by using the Stop-DatabaseAvailabilityGroup cmdlet. The *ActiveDirectorySite* parameter of this cmdlet can be used to mark all of the servers in the primary datacenter as stopped with a single command. This step may not be possible depending on the failure. This step should be taken if the state of the datacenter permits it. The **Stop-DatabaseAvailabilityGroup** cmdlet should be run against all servers in the primary datacenter. If the Mailbox server is unavailable but Active Directory is

operating in the primary datacenter, the **Stop-DatabaseAvailabilityGroup** command with the *ConfigurationOnly* parameter must be run against all servers in this state in the primary datacenter, or the Mailbox server must be turned off. Failure to either turn off the Mailbox servers in the failed datacenter or to successfully perform the **Stop-DatabaseAvailabilityGroup** command against the servers will create the potential for split-brain syndrome to occur across the two datacenters. You may need to individually turn off computers through power management devices to satisfy this requirement.

2. The second datacenter must now be updated to represent which primary datacenter servers are stopped. This is done by running the same **Stop-DatabaseAvailabilityGroup** command with the *ConfigurationOnly* parameter using the same *ActiveDirectorySite* parameter and specifying the name of the Active Directory site in the failed primary datacenter. The purpose of this step is to inform the servers in the second datacenter about which mailbox servers are available to use when restoring service.

When the DAG isn't in DAC mode, the specific actions to terminate any surviving DAG members in the primary datacenter are as follows:

1. The DAG members in the primary datacenter must be forcibly evicted from the DAG's underlying cluster by running the following commands on each member:

```
net stop clussvc
cluster <DAGName> node <DAGMemberName> /forcecleanup
```

2. The DAG members in the second datacenter must now be restarted and then used to complete the eviction process from the second datacenter. Stop the Cluster service on each DAG member in the second datacenter by running the following command on each member:

```
net stop clussvc
```

3. On a DAG member in the second datacenter, force a quorum start of the Cluster service by running the following command:

```
net start clussvc /forcequorum
```

4. Open the Failover Cluster Management tool and connect to the DAG's underlying cluster. Expand the cluster, and then expand **Nodes**. Right-click each node in the primary datacenter, select **More Actions**, and then select **Evict**. When you're done evicting the DAG members in the primary datacenter, close the Failover Cluster Management tool.

If any Unified Messaging servers are in use in the failed datacenter, they must be disabled to prevent call routing to the failed datacenter. You can disable a Unified Messaging server by using the Disable-UMServer cmdlet (for example, `Disable-UMServer UM01`). Alternatively, if you are using a Voice over IP (VoIP) gateway, you can also remove the Unified Messaging server entries from the VoIP gateway, or change the DNS records for the failed servers to point to the IP address of the Unified Messaging servers in the second datacenter if your VoIP gateway is configured to route calls using DNS.

Return to top

Activating Mailbox Servers

The steps needed to activate Mailbox servers during a datacenter switchover also depend on whether the DAG is in DAC mode. Before activating the DAG members in the second datacenter, we recommend that you validate that the infrastructure services in the second datacenter are ready for messaging service activation.

When the DAG is in DAC mode, the steps to complete activation of the mailbox servers in

the second datacenter are as follows:

1. The Cluster service must be stopped on each DAG member in the second datacenter. You can use the **Stop-Service** cmdlet to stop the service (for example, `Stop-Service ClusSvc`), or use `net stop clussvc` from an elevated command prompt.
2. The Mailbox servers in the standby datacenter are then activated by using the Restore-DatabaseAvailabilityGroup cmdlet. The Active Directory site of the standby datacenter is passed to the **Restore-DatabaseAvailabilityGroup** cmdlet to identify which servers to use to restore service and to configure the DAG to use an alternate witness server. If the alternate witness server wasn't previously configured, you can configure it by using the *AlternateWitnessServer* and *AlternateWitnessDirectory* parameters of the Restore-DatabaseAvailabilityGroup cmdlet. If this command succeeds, the quorum criteria are shrunk to the servers in the standby datacenter. If the number of servers in that datacenter is an even number, the DAG will switch to using the alternate witness server as identified by the setting on the DAG object.
3. The databases can now be activated. Depending on the specific configuration used by the organization, this may not be automatic. If the servers in the standby datacenter have an activation blocked setting, the system won't do an automatic failover from the primary datacenter to the standby datacenter of any database. If no failover restrictions are present for any of the database copies in the standby datacenter, the system will activate copies in the second datacenter assuming they are healthy. If databases are configured with an activation blocked setting that requires explicit manual action, there are two choices for action:
   3.a. Clear the setting that blocks activation. This will make the system return to its default behavior, which is to activate any available copy.
   3.b. Leave the setting unchanged and use the Move-ActiveMailboxDatabase cmdlet to complete the database activation in the second datacenter. To complete this step using the **Move-ActiveMailboxDatabase** cmdlet when activation blocked is set, you must explicitly identify the target of the move.
4. The last step is to review all error and warning messages from the tasks. Any indicated warnings should be followed up and corrected. The task design model for these commands is to only fail if they can't achieve the fundamental goal of their design. For example, the **Restore-DatabaseAvailabilityGroup** cmdlet will fail if it can't shrink the quorum of the DAG to allow a server in the second datacenter to be restarted for servicing without causing a quorum outage. However, each task's output is also used to identify the issues that require administrator follow-up. You're strongly encouraged to save all task output and review it for follow-up actions.

When the DAG isn't in DAC mode, the steps to complete activation of the mailbox servers in the second datacenter are as follows:

1. The quorum must be modified based on the number of DAG members in the second datacenter.
   1.a. If there's an odd number of DAG members, change the DAG quorum model from a Node a File Share Majority to a Node Majority quorum by running the following command:

```
cluster <DAGName> /quorum /nodemajority
```

   1.b. If there's an even number of DAG members, reconfigure the witness server and directory by running the following command in the Exchange Management Shell:

```
Set-DatabaseAvailabilityGroup <DAGName> -WitnessServer <Ser
```

2. Start the Cluster service on any remaining DAG members in the second

datacenter by running the following command:

```
net start clussvc
```

3. Perform server switchovers to activate the mailbox databases in the DAG by running the following command for each DAG member:

```
Move-ActiveMailboxDatabase -Server <DAGMemberinPrimarySite> -ActivateO
```

4. Mount the mailbox databases on each DAG member in the second site by running the following command:

```
Get-MailboxDatabase <DAGMemberinSecondSite> | Mount-Database
```

5. Because public folder databases don't use continuous replication and instead rely on public folder replication for high availability, the behavior for Outlook clients reconnecting to a public folder database after a datacenter switchover depends on a site-resilient public folder architecture and the health and currency of your public folder databases. To re-establish public folder connectivity for Outlook clients, simply change the default public folder for the mailbox database to point to a public folder database in the second site. For detailed steps about how to change the default public folder database for a mailbox database, see Change the Default Public Folder Database for a Mailbox Database.

Return to top

Activating Other Server Roles

The steps necessary to activate non-Mailbox server roles depend on the specific server and its configuration. The activation process for each of the server roles is described in the following sections.

Activating Client Access Servers

Clients connect to service endpoints (for example Outlook Web App, Autodiscover, Exchange ActiveSync, Outlook Anywhere, POP3, IMAP4, and the RPC Client Access array) to access Exchange services and data. Therefore, activating Client Access servers involves changing the mapping of the DNS records for these service endpoints from IP addresses in the primary datacenter to the IP addresses in the second datacenter that are configured as the new service endpoints. Depending on your DNS configuration, the DNS records that need to be modified may or may not be in the same DNS zone.

Clients will then automatically connect to the new service endpoints in one of two ways:

- Clients will continue to try to connect, and should automatically connect after the TTL has expired for the original DNS entry, and after the entry is expired from the client's DNS cache. Users can also run the `ipconfig /flushdns` command from a command prompt to manually clear their DNS cache.
- Clients starting or restarting will perform a DNS lookup on startup and will get the new IP address for the service endpoint, which will be a Client Access server or array in the second datacenter.

Assuming that all appropriate configuration changes have been completed to define and configure the services in the second datacenter to function as they were in the primary datacenter, and assuming that the established DNS configuration is correct, no further changes should be needed to activate Client Access servers.

Activating Hub Transport Servers

Clients and other servers that submit messages to Hub Transport servers typically identify those servers using DNS. Activating Hub Transport servers involves changing DNS records to point to the IP addresses of the Hub Transport servers in the second datacenter. Clients and sending servers will then automatically connect to the Hub Transport servers in the second datacenter in one of two ways:

- Clients will continue to try to connect, and should automatically connect after

the TTL has expired for the original DNS entry, and after the entry is expired from the client's DNS cache. Users can also run the `ipconfig /flushdns` command from a command prompt to manually clear their DNS cache.
- Clients starting or restarting will perform a DNS lookup on startup and will get the new IP address for the SMTP endpoint, which will be a Hub Transport server in the second datacenter.

Assuming that all appropriate configuration changes have been completed to define and configure the services in the second datacenter to function as they were in the primary datacenter, and assuming that the established DNS configuration is correct, no further changes should be needed to activate Hub Transport servers.

Activating Unified Messaging Servers

Unified Messaging (UM) servers connect to an organization's PBX system and phone lines. The logical connection between the PBX system and the Unified Messaging server is provided by an IP gateway. IP gateways include high availability functionality and are able to switch between multiple Unified Messaging servers when a failure is detected.

If there are Unified Messaging servers in the second datacenter that were in a disabled state because they are dedicated to the site resilience solution, they can be enabled by using the Enable-UMServer cmdlet (for example, `Enable-UMServer UM04`).

Assuming the IP gateways are associated with Unified Messaging servers by using DNS servers, activating Unified Messaging servers therefore involves changing DNS records to point to the new IP addresses that will be configured for the Unified Messaging servers in the second datacenter. After the TTL and DNS cache entries have expired, clients and IP gateways won't be able to connect to the Microsoft Exchange Unified Messaging service. Assuming that all appropriate configuration changes have been completed to define and configure the services in the second datacenter to function as they were in the primary datacenter, and assuming that the established DNS configuration is correct, no further changes should be needed to activate Unified Messaging servers.

If the IP gateway in use doesn't support the use of DNS names to resolve the Unified Messaging servers, additional configuration steps will be necessary to manually point the IP gateway to the IP addresses of the Unified Messaging servers in the second datacenter.

Activating Edge Transport Servers

The steps to activate the Edge Transport server role will vary, depending on the specific configuration. Edge Transport servers in two datacenters can be configured in either an active/passive or an active/active configuration. In an active/passive configuration, the Edge Transport server in the second datacenter is idle until the second datacenter is activated. In an active/active configuration, Edge Transport servers in both datacenters are delivering mail at all times.

In an active/active configuration, no steps are necessary to activate the second datacenter's Edge Transport servers because they are already running. In an active/passive configuration, the DNS MX resource record for each SMTP domain needs to be updated as part of the switchover from the primary datacenter to the standby datacenter. Although the active/active configuration provides a simple datacenter switchover solution, it has the drawback of requiring careful load monitoring to make sure that after the datacenter switchover, the Edge Transport servers in the second datacenter can provide sufficient capacity to support the increased load now flowing through it, as a result of the Edge Transport servers in the primary datacenter being unavailable.

Even with an active/active configuration, it may be appropriate to update the MX resource records for your Edge Transport servers during a datacenter switchover. Allowing the MX resource record for the failed datacenter to continue to point at the failed datacenter means that when the datacenter starts recovering, it could start experiencing connection attempts to its Edge Transport servers. This could happen while the Edge Transport

services are in an unstable state (for example, because dependent services in the datacenter are being restored).

Assuming the DNS records are under the control of the organization, activating Edge Transport servers involves updating the MX resource record for each SMTP domain hosted by the server.

Note:
If the MX resource record used by your organization isn't hosted by a DNS server under your organization's control, you might consider referencing a CNAME record in the MX resource record and using a CNAME record under the organization's control that can then be updated.

DNS updates enable incoming traffic, and outgoing traffic is handled by the activation of the mailbox databases in a site that has functioning Edge Transport servers:

- When incoming SMTP connections are initiated using the updated name resolution information, SMTP clients will connect to the Edge Transport servers in the second datacenter. Traffic will be appropriately routed by the Edge Transport server, and no further changes are required.
- When outgoing SMTP connections are initiated, they will try the locally available Edge Transport server, and those messages will be queued or immediately sent based on the status of the receiving server.

Return to top

Restoring Service to the Primary Datacenter

Generally, datacenter failures are either temporary or permanent. With a permanent failure, such as an event that has caused the permanent destruction of a primary datacenter, there's no expectation that the primary datacenter will be activated. However, with a temporary failure (for example, an extended power loss or extensive but repairable damage), there's an expectation that the primary datacenter will eventually be restored to full service.

The process of restoring service to a previously failed datacenter is referred to as a *switchback*. The steps used to perform a datacenter switchback are similar to the steps used to perform a datacenter switchover. A significant distinction is that datacenter switchbacks are scheduled, and the duration of the outage is often much shorter.

It's important that switchback not be performed until the infrastructure dependencies for Exchange have been reactivated, are functioning and stable, and have been validated. If these dependencies aren't available or healthy, it's likely that the switchback process will cause a longer than necessary outage, and it's possible the process could fail altogether.

Mailbox Server Role Switchback

The Mailbox server role should be the first role that's switched back to the primary datacenter. The following steps detail the Mailbox server role switchback process:

1. As part of the datacenter switchover process, the Mailbox servers in the primary datacenter were put into a stopped state. When the environment (such as primary datacenter, Exchange dependencies, and wide area network (WAN) connectivity) is ready, the first step is to put the Mailbox servers in the restored primary datacenter into a started state and incorporate them into the DAG. The way in which this is done depends on whether the DAG is in DAC mode.
   1.a. If the DAG is in DAC mode, you can reincorporate the DAG members in the primary site by using the Start-DatabaseAvailabilityGroup cmdlet. Then, to

make sure that the proper quorum model is being used by the DAG, run the Set-DatabaseAvailabilityGroup cmdlet against the DAG without specifying any parameters.

1.b.If the DAG isn't in DAC mode, you can reincorporate the DAG members by using the Add-DatabaseAvailabilityGroupServer cmdlet.

2. After the Mailbox servers in the primary datacenter have been incorporated into the DAG, they will need some time to synchronize their database copies. Depending on the nature of the failure, the length of the outage, and actions taken by an administrator during the outage, this may require reseeding the database copies. For example, if during the outage, you remove the database copies from the failed primary datacenter to allow log file truncation to occur for the surviving active copies in the second datacenter, reseeding will be required. Each database can individually proceed from this point forward. After a replicated database copy in the primary datacenter is healthy, it can proceed to the next step.

Note:

This process doesn't require that all databases be moved at the same time. You are encouraged to move the majority of your organization's databases at one time, but some databases many linger in the second datacenter if there are issues associated with the database copies in the primary datacenter.

3. After a majority of the databases are in a healthy state in the primary datacenter, the switchback outage can be scheduled. When the scheduled time arrives, the following steps must be taken:

3.a.During the datacenter switchover process, the DAG was configured to use an alternate witness server. The DAG must be reconfigured to use a witness server in the primary datacenter. If you are using the same witness server and witness directory that was used prior to the primary datacenter outage, you can run the `Set-DatabaseAvailabilityGroup -Identity DAGName` command. If you plan on using a witness server or witness directory that is different from the original witness server and directory, use the Set-DatabaseAvailabilityGroup command to configure the witness server and witness directory parameters with the appropriate values.

3.b.The databases being reactivated in the primary datacenter should be dismounted in the second datacenter. You can use the Dismount-Database cmdlet to dismount the databases.

3.c.After the databases have been dismounted, the Client Access server URLs should be moved from the second datacenter to the primary datacenter. This is accomplished by changing the DNS record for the URLs to point to the Client Access server or array in the primary datacenter. This will result in the system acting as though a database failover has occurred for each database being moved.

Important:

Don't proceed to the next step until the Client Access server URLs have been moved and the DNS TTL and cache entries have expired. Activating the databases in the primary datacenter prior to moving the Client Access server URLs to the primary datacenter will result in an invalid configuration (for example, a mounted database that has no Client Access servers in its Active Directory site).

3.d.Because each database in the primary datacenter is in a healthy state, it can be activated in the primary datacenter by performing database switchovers. This is accomplished by using the Move-ActiveMailboxDatabase cmdlet for each database that will be activated.

3.e.After each database is moved to the primary datacenter, it can be mounted by using the Mount-Database cmdlet.

After one or more databases are active and mounted in the primary datacenter, switchback procedures for the other server roles can be performed.

Other Server Role Switchback

As part of the switchover process, the internal and external DNS records used by clients, other servers, and IP gateways to resolve the service endpoints for Client Access, Hub Transport, Edge Transport, and Unified Messaging servers were modified to point to the corresponding endpoints in the second datacenter. The switchback process for the other server roles involves modifying those records to point to the restored service endpoints in the primary datacenter.

As with the DNS changes that were made during the switchover to the second datacenter, clients, servers, and IP gateways will continue to try to connect, and should automatically connect after the TTL has expired for the original DNS entry, and after the entry is expired from their DNS cache.

Reestablishing Site Resilience

After switchback to the primary datacenter is completed successfully, you can reestablish site resilience for the primary datacenter by verifying the health and status of each mailbox database copy in the second datacenter. In addition, if any database copies in the second datacenter were originally blocked for activation, you can reconfigure those settings at this time.

Return to top

1.10.4.4.2 Perform a Server Switchover

Perform a Server Switchover

High Availability and Site Resilience > Managing High Availability and Site Resilience > Switchovers and Failovers >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A server switchover is a task that you perform to move all active mailbox database copies from their current Mailbox server to one or more other Mailbox servers in a database availability group (DAG). This task is performed as part of preparation for a scheduled outage for the current Mailbox server.

Use the EMC to perform a server switchover

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Mailbox database copies" entry in the High Availability Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Mailbox**.
2. In the result pane, select the Mailbox server you want.
3. In the action pane, select **Switchover Server**.
4. In the **Switchover server database copies** dialog box, do one of the following:
   4.a. Accept the default setting of **Automatically choose a target server** (in which case, the system automatically selects the best Mailbox server for

each database being switched over), and then click **OK**.

4.b.Click **Use the specified server as the target for switchover**, click **Browse** to select a Mailbox server, and then click **OK**.

Use the Shell to perform a server switchover

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the"Mailbox database copies" entry in the High Availability Permissions topic.

This example performs a server switchover for the server MBX1. The system automatically selects the best Mailbox server for each active database on MBX1.

```
Move-ActiveMailboxDatabase -Server MBX1
```

This example performs a server switchover of the Mailbox server MBX4. When the command completes, MBX5 hosts the active copy of the databases that were previously active on MBX4. Because the *MountDialOverride* parameter isn't specified, MBX5 mounts the databases using a database auto mount dial setting of *Lossless*.

```
Move-ActiveMailboxDatabase -Server MBX4 -ActivateOnServer MBX5
```

For detailed syntax and parameter information, see Move-ActiveMailboxDatabase.

1.10.4.5 Installing Update Rollups on Database Availability Group Members

Installing Update Rollups on Database Availability Group Members

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-14*

It's relatively straightforward to install Microsoft Exchange Server 2010 update rollups on a server that's a member of a database availability group (DAG).

Microsoft Update offers released update rollups to Mailbox servers that are part of DAG. However, we recommend that you download the update rollups from the Microsoft Download Center and then install them manually. When you install an update rollup on a server that's a DAG member, several services will be stopped during the installation, including all Exchange services and the Windows Cluster service.

The general process for installing update rollups on a DAG member is as follows:

- Run the StartDagServerMaintenance.ps1 script to put the DAG member into maintenance mode and prepare it for the update rollup installation.
- Install the update rollup.
- Run the StopDagServerMaintenance.ps1 script to take the DAG member out of maintenance mode and put it back into production.
- Optionally rebalance the DAG by using the RedistributeActiveDatabases.ps1 script.

This process can also be used to install operating system updates from Microsoft Update, as well.

You can download the latest update rollup for Exchange 2010 from the Microsoft Download Center.

Install a Update Rollup on a Database Availability Group Member

To update all DAG members, perform the following procedures on each DAG member, one at a time.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Database availability groups" entry in the High Availability Permissions topic.

Run the StartDagServerMaintenance.ps1 script on the server being updated

Run the following command in the Exchange Management Shell from the Scripts directory:

```
.\StartDagServerMaintenance.ps1 <ServerName>
```

For more information about the StartDagServerMaintenance.ps1 script, see Managing Database Availability Groups.

Install the update rollup

1. Close all Exchange management tools.
2. Right-click the Exchange update rollup file (.msp file) you downloaded, and then select **Apply**.
3. On the **Welcome** page, click **Next**.
4. On the **License Terms** page, review the license terms, select **I accept the License Terms**, and then click **Next**.
5. On the **Completion** page, click **Finish**.

Run the StopDagServerMaintenance.ps1 script

Run the following command in the Shell from the Scripts directory:

```
.\StopDagServerMaintenance.ps1  <ServerName>
```

For more information about the StopDagServerMaintenance.ps1 script, see Managing Database Availability Groups.

Re-balance the DAG, as needed

Run the following command in the Shell from the Scripts directory to optionally balance the DAG by Activation Preference and to produce a report when balancing is complete:

```
.\ RedistributeActiveDatabases.ps1 -DagName <DAGName>
-BalanceDbsByActivationPreference -ShowFinalDatabaseDistribution
```

For more information about the RedistributeActiveDatabases.ps1 script, see Managing Database Availability Groups.

1.10.5 Understanding Backup, Restore and Disaster Recovery

Understanding Backup, Restore and Disaster Recovery

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-01*

Microsoft Exchange Server 2010 features a new, unified platform for high availability and site resilience that makes deploying redundant, highly available mailbox databases quicker and easier. But even the most extreme forms of redundancy and fault tolerance can't protect you against every possible failure or disaster. Ensuring there's sufficient protection for the critical data in your Exchange organization is a necessary operational task for all organizations.

As part of your data protection planning, it's important that you understand the ways in which data can be protected, and to determine of those ways, which best suits your organization's needs. Data protection planning is a complex process that relies on many decisions that you make during the planning phase of your deployment.

Contents

Supported Backup Technologies

Microsoft Exchange Server 2007 and Exchange Server 2003 include two different options for data backup and recovery: Extensible Storage Engine (ESE) streaming backup APIs and support for the Volume Shadow Copy Service (VSS) backup APIs. Exchange 2010 no longer supports the ESE streaming APIs for backup and restore of program files or data. Instead, Exchange 2010 supports only VSS-based backups.

Exchange 2010 includes a plug-in for Windows Server Backup that enables you to make VSS-based backups of Exchange data. You can use Windows Server Backup to back up and restore your Exchange databases. To back up and restore Exchange 2010, you must use an Exchange-aware application that supports the VSS writer for Exchange 2010, such as Windows Server Backup (with the VSS plug-in), Microsoft System Center Data Protection Manager, or a third-party Exchange-aware VSS-based application. Be aware of these limitations when using VSS for backup and restore of Exchange data:

- The VSS plug-in that ships with Exchange 2010 can be used to back up volumes containing active mailbox database copies or standalone (non-replicated) mailbox databases only. It can't be used to back up volumes containing passive mailbox database copies. To back up passive mailbox database copies, you need either Microsoft System Center Data Protection Manager or a third-party Exchange-aware VSS-based application.
- Passive mailbox database copies are backed up using a separate VSS writer in

the Microsoft Exchange Replication service. The Microsoft Exchange Replication service VSS Writer doesn't support restores. Although you can back up a passive mailbox database copy using Microsoft System Center Data Protection Manager or a third-party Exchange-aware VSS-based application, you can't perform a VSS restore directly to a passive mailbox database copy. However, you can perform a VSS restore to an alternate location, suspend replication to the passive copy, and then copy the database and log files from the alternate location to the location of the passive database copy in the file system.

For detailed steps to back up and restore Exchange data using Windows Server Backup, see Using Windows Server Backup to Back Up and Restore Exchange Data.

Return to top

Server Recovery

Almost all of the configuration settings for Mailbox, Client Access, Hub Transport, and Unified Messaging server roles are stored in Active Directory. As with previous versions of Exchange, Exchange 2010 includes a Setup parameter for recovering lost servers. This parameter, */m:RecoverServer*, is used to rebuild and re-create a lost server by using the settings and configuration information stored in Active Directory.

For detailed steps to perform a server recovery of a lost Exchange 2010 server, see Recover an Exchange Server. For detailed steps to recover a lost server that's a member of a database availability group, see Recover a Database Availability Group Member Server.

Return to top

Recovery Database

A recovery database is an Exchange 2010 feature that replaces the recovery storage group (RSG) found in previous versions of Exchange. A recovery database is a special kind of mailbox database that allows you to mount a restored mailbox database and extract data from the restored database as part of a recovery operation. You can use the Restore-Mailbox cmdlet to extract data from a recovery database. After extraction, the data can be exported to a folder or merged into an existing mailbox. Recovery databases enable you to recover data from a backup or copy of a database without disturbing user access to current data.

Before you can use a recovery database, there are certain requirements that must be met. A recovery database can be used for Exchange 2010 mailbox databases only. Mailbox databases from previous versions of Exchange aren't supported. In addition, the target mailbox used for data merges and extraction must be in the same Active Directory forest as the database mounted in the recovery database.

For more information, see Recovery Databases. For detailed steps to create a recovery database, see Create a Recovery Database. For detailed steps to use a recovery database, see Restore Data Using a Recovery Database.

Return to top

Database Portability

Database portability is a feature that enables an Exchange 2010 mailbox database to be moved to and mounted on any other Exchange 2010 Mailbox server in the same organization. By using database portability, reliability is improved by removing several

error-prone, manual steps from the recovery processes. In addition, database portability reduces the overall recovery times for various failure scenarios.

For more information, see Database Portability. For detailed steps to use database portability, see Move a Mailbox Database Using Database Portability.

Return to top

Dial Tone Portability

Dial tone portability is a feature that provides a limited business continuity solution for failures that affect a mailbox database, a server, or an entire site. Dial tone portability enables a user to have a temporary mailbox for sending and receiving e-mail while the original mailbox is being restored or repaired. The temporary mailbox can be on the same Exchange 2010 Mailbox server or on any other Exchange 2010 Mailbox server in your organization. This allows an alternative server to host the mailboxes of users who were previously on a server that's no longer available. Clients that support Autodiscover, such as Microsoft Outlook 2010 or Office Outlook 2007, are automatically redirected to the new server without having to manually update the user's desktop profile. After the user's original mailbox data has been restored, an administrator can merge a user's recovered mailbox and the user's dial tone mailbox into a single, up-to-date mailbox.

The process for using dial tone portability is called a *dial tone recovery*. A dial tone recovery involves creating an empty database on a Mailbox server to replace a failed database. This empty database, referred to as a *dial tone database*, allows users to send and receive e-mail while the failed database is recovered. After the failed database is recovered, the dial done database and the recovered database are swapped, and then the data from the dial tone database is merged into the recovered database.

For more information, see Dial Tone Portability. For detailed steps to perform a dial tone recovery, see Perform a Dial Tone Recovery.

Return to top

Exchange Native Data Protection

Exchange 2010 includes several new features and core changes that, when deployed and configured correctly, can provide native data protection that eliminates the need to make traditional backups of your data. Using the high availability features built into Exchange 2010 to minimize downtime and data loss in the event of a disaster can also reduce the total cost of ownership of the messaging system. By combining these features with other built-in features, such as Legal Hold, organizations can reduce or eliminate their dependency on traditional point-in-time backups and reduce the associated costs.

In addition to determining whether Exchange 2010 enables you to move away from traditional point-in-time backups, we also recommend that you evaluate the cost of your current backup infrastructure. Consider the cost of end-user downtime and data loss when attempting to recover from a disaster using your existing backup infrastructure. Also, include hardware, installation, and license costs, as well as the management cost associated with recovering data and maintaining the backups. Depending on the requirements of your organization, it is quite likely that a pure Exchange 2010 environment with at least three mailbox database copies will provide lower total cost of ownership than one with backups.

Backups are typically used for the following scenarios, and there are Exchange 2010 features to meet each of these needs in an efficient and cost effective manner.

- **Disaster recovery** In the event of a hardware or software failure, multiple database copies in a database availability group (DAG) enable high availability

with fast failover with no data loss. This eliminates the end-user downtime and resulting lost productivity that's a significant cost of recovering from a past point-in-time backup to disk or tape. DAGs can be extended to multiple sites and can provide resilience against datacenter failures.

- **Recovery of accidentally deleted items** Historically, in a situation where a user deleted items that later needed to be recovered, it involved finding the backup media on which the data that needed to be recovered was stored, and then somehow obtaining the desired items and providing them to the user. With the new Recoverable Items Folder in Exchange 2010 and the Hold Policy that can be applied to it, it's possible to retain all deleted and modified data for a specified period of time, so recovery of these items is easier and faster. This reduces the burden on Exchange administrators and the IT help desk by enabling end users to recover accidentally deleted items themselves, thereby reducing the complexity and administrative costs associated with single item recovery. For more information, see Messaging Policy and Compliance, Understanding Recoverable Items, and Understanding Retention Tags and Retention Policies.
- **Long-term data storage** Sometimes, backups also serve an archival purpose, and typically tape is used to preserve point-in-time snapshots of data for extended periods of time as governed by compliance requirements. The new archiving, multiple-mailbox search, and message retention features in Exchange 2010 provide a mechanism to efficiently preserve data in an end-user accessible manner for extended periods of time. This eliminates expensive restores from tape, and increases end-user productivity by enabling rich clients such as Microsoft Outlook and Outlook Web App access to older data. For more information see Understanding Personal Archives, Understanding Multi-Mailbox Search, and Understanding Retention Tags and Retention Policies.
- **Point-in-time database snapshot** If a past point-in-time copy of mailbox data is a requirement for your organization, Exchange provides the ability to create a lagged copy in a DAG environment. This can be useful in the rare event that there's a logical corruption that replicates across the databases in the DAG, resulting in a need to return to a previous point in time. It may also be useful if an administrator accidentally deletes mailboxes or user data. Recovery from a lagged copy can be faster than restoring from a backup because lagged copies don't require a time-consuming copy process from the backup server to the Exchange server. This can significantly lower total cost of ownership by reducing end-user downtime.

Log Truncation without Backups

One of the functions performed at the end of a successful full or incremental backup is the truncation of transaction log files that are no longer needed for database recovery. If backups are not being taken, then log truncation will not occur. To prevent a buildup of log files, you enable circular logging for your replicated databases. When you combine circular logging with continuous replication, you have a new type of circular logging called continuous replication circular logging (CRCL), which is different from ESE circular logging. Whereas ESE circular logging is performed and managed by the Microsoft Exchange Information Store service, CRCL is performed and managed by the Microsoft Exchange Replication Service. When enabled, ESE circular logging does not generate additional log files and instead overwrites the current log file when needed. However, in a continuous replication environment, log files are needed for log shipping and replay. As a result, when you enable CRCL, the current log file is not overwritten and closed log files are generated for the log shipping and replay process.

Specifically, the Microsoft Exchange Replication Service manages CRCL so that log continuity is maintained and logs are not deleted if they are still needed for replication. The Microsoft Exchange Replication Service and the Microsoft Exchange Information Store service communicate by using remote procedure calls (RPCs) regarding which log files can be deleted.

For truncation to occur on highly available (non-lagged) mailbox database copies, the answer must be "Yes" to the following questions:

- Has the log file been backed up, or is CRCL enabled?
- Is the log file below the checkpoint?
- Do the other non-lagged copies of the database agree with deletion?
- Has the log file been inspected by all lagged copies of the database?

For truncation to occur on lagged database copies, the answer must be "Yes" to the following questions:

- Is the log file below the checkpoint?
- Is the log file older than ReplayLagTime + TruncationLagTime?
- Is the log file deleted on the active copy of the database?

For information about how to enable and disable circular logging, see Configure Mailbox Database Properties.

Considerations for Implementing Exchange Native Data Protection

There are technical reasons and several issues that you should consider before using the features built into Exchange 2010 as a replacement for traditional backups. The following list includes some of these considerations, although the list isn't exhaustive. There may also be special considerations or considerations unique to your organization. Consider the following issues:

- How many copies of the database will be deployed? We strongly recommend deploying a minimum of three (non-lagged) copies of a mailbox database before eliminating traditional forms of protection for the database, such as RAID or traditional VSS-based backups.
- Your recovery time objective and recovery point objective goals should be clearly defined, and you should establish that using a combined set of built-in features in lieu of traditional backups enables you to meet these goals.
- You should determine how many copies of each database are needed to cover the various failure scenarios against which your system is designed to protect.
- If you eliminate the use of a DAG or some of its members, does that capture sufficient costs to support a traditional backup solution? If so, does that solution improve your recovery time objective or recovery point objective service level agreements (SLAs)?
- Can you afford to lose a point-in-time copy if the DAG member hosting the copy experiences a failure that affects the copy or the integrity of the copy?
- Exchange 2010 allows you to deploy larger mailboxes, and the recommended maximum mailbox database size has been increased from 200 gigabytes (GB) in Exchange 2007 to 2 terabytes (when two or more highly available mailbox database copies are being used). Based on the larger mailboxes that most organizations are likely to deploy, what will your recovery point objective be if you have to replay a large number of log files when activating a database copy or a lagged database copy?
- How will you detect and prevent logical corruption in an active database copy from replicating to the passive copies of the database? What is your recovery plan for this situation? How frequently has this scenario occurred in the past? If logical corruption occurs frequently in your organization, we recommend that you factor that scenario into your design by using one or more lagged copies, with a sufficient replay lag window to allow you to detect and act on logical corruption when it occurs, but before that corruption is replicated to other database copies.

Return to top

1.10.5.1 Using Windows Server Backup to Back Up and Restore Exchange Data

Using Windows Server Backup to Back Up and Restore Exchange Data

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-01*

Microsoft Exchange Server 2010 includes a plug-in for Windows Server Backup that enables you to create Volume Shadow Copy Service (VSS)-based backups of Exchange data. You can use Windows Server Backup to back up and restore your Exchange databases. A thorough understanding of what needs to be backed up, where to store backups, and how to restore backups is key to being an effective Exchange administrator. For more information about what needs to be backed up in Exchange 2010, see Understanding Backup, Restore and Disaster Recovery.

The new plug-in is delivered in the form of an executable called WSBExchange.exe, which is configured to run as a service named Microsoft Exchange Server Extension for Windows Server Backup (the short name for this service is WSBExchange). The plug-in is automatically installed on all Exchange 2010 Mailbox servers and configured by default for manual startup. The plug-in enables Windows Server Backup to create Exchange-aware VSS backups.

Note:

To use the plug-in, you must have the Windows Server Backup feature installed. However, you shouldn't install the Windows Server Backup command-line tools. These tools require an older version of the Windows PowerShell command-line interface, which isn't compatible with Exchange 2010. When you install Windows Server Backup, the command-line tool WBAdmin.exe is also installed. This command-line tool can be run from the Windows command prompt (cmd.exe).

For detailed steps about how to back up an Exchange server using Windows Server Backup, see Use Windows Server Backup to Perform a Backup of Exchange.

For detailed steps about how to restore data from a backup taken with Windows Server Backup, see Use Windows Server Backup to Restore a Backup of Exchange.

Before using Windows Server Backup to back up Exchange data, we recommend that you familiarize yourself with the following features and options for the plug-in:

- Backups are VSS-based only. You can't create streaming Extensible Storage Engine (ESE) backups using Windows Server Backup with or without the plug-in.
- Backups taken with Windows Server Backup occur at volume level. To back up a database and its log stream, you must back up the entire volume containing the database and logs. You can't back up any data without backing up the entire volume containing the data.
- The backup must be run locally on the server being backed up, and you can't use the plug-in to take remote VSS backups. There is no remote administration of Windows Server Backup or the plug-in. You can, however, use Remote Desktop Services or Terminal Services to remotely manage backups.
- The backup can be created on a local drive or on a remote network share.
- Only full backups can be taken. Log truncation will occur only after a successful completion of a full backup of a volume or folders containing an Exchange database.
- When restoring data, it's possible to restore only Exchange data. This data can be restored to its original location or to an alternate location. If you

restore the data to its original location, Windows Server Backup and the plug-in automatically handle the recovery process, including dismounting any existing databases and replaying logs into the recovered database.
- The restore process doesn't directly support the recovery database (RDB). However, if you restore to an alternate location, you can then manually move the restored data from the alternate location into an RDB, if needed.
- When restoring Exchange data, all backed up databases must be restored together. You can't restore a single database.

Using Windows Server Backup on Database Availability Group Members

If a server hosting the data being backed up is a member of a database availability group (DAG) and hosts both active and passive database copies, you must disable the Microsoft Exchange Replication service VSS writer. If the Microsoft Exchange Replication service VSS writer is enabled, the backup operation will fail.

To disable the Microsoft Exchange Replication service VSS writer, perform the following steps:

1. Log on to the server by using an account that has local administrator access, and then start Registry Editor (regedit).

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

2. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\ExchangeServer\v14\Replay\Parameters.
3. Add a new DWORD value named **EnableVSSWriter**, and set its value to **0**.
4. Exit Registry Editor and then restart the Microsoft Exchange Replication service.

Important:

If you later want to use a different a backup solution to back up passive database copies on a server that has the Microsoft Exchange Replication service VSS writer disabled, you need to remove the preceding registry key and then restart the Microsoft Exchange Replication service.

1.10.5.1.1 Use Windows Server Backup to Perform a Backup of Exchange

Use Windows Server Backup to Perform a Backup of Exchange

High Availability and Site Resilience > Understanding Backup, Restore and Disaster Recovery > Using Windows Server Backup to Back Up and Restore Exchange Data >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Microsoft Exchange Server 2010 includes a plug-in for Windows Server Backup that allows you to make Volume Shadow Copy Service (VSS)-based backups of Exchange data. You can use Windows Server Backup to back up and restore your Exchange databases.

During the backup operation, a consistency check of the Exchange data files is run to make sure that the files are in a good state and can be used for recovery. If the consistency check succeeds, Exchange data is available for recovery from that backup. If

the consistency check fails, the Exchange data isn't available for recovery. Windows Server Backup runs the consistency check on the snapshot taken for the backup. As a result, before copying files from the snapshot to backup media, the consistency of the backup is known, and the user is notified of the consistency check results.

Prerequisites

- This procedure can only be performed locally on a computer running Exchange 2010 on the Windows Server 2008 or Windows Server 2008 R2 operating system.
- The Windows Server Backup feature must be installed on the local computer.
- If a server hosting the data being backed up is a member of a database availability group (DAG) and hosts both active and passive database copies, you must disable the Microsoft Exchange Replication service VSS writer. If the Microsoft Exchange Replication service VSS writer is enabled, the backup operation will fail. For detailed steps, see Using Windows Server Backup to Back Up and Restore Exchange Data.

Use Windows Server Backup to perform a backup of Exchange

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox recovery" entry in the Mailbox Permissions topic.

1. Start Windows Server Backup.
2. In the **Actions** pane, click **Backup Once**. The Backup Once wizard appears.
3. On the **Backup options** page, select **Different options**, and then click **Next**.
4. On the **Select backup configuration** page, select the type of backup that you want, and then click **Next**:
   4.a. Select **Full server (recommended)** to back up all volumes on the server.
   4.b. Select **Custom** to specify which volumes should be included in the backup. If you select this option, the **Select backup items** page appears. Select the volumes to be backed up, and then click **Next**.

   Note:
   By default, volumes that contain operating system components or applications are included in the backup and can't be excluded.
5. On the **Specify destination type** page, select the location where you want to store the backup, and then click **Next**. If **Remote shared folder** is selected, the **Specify remote folder** page appears. Specify a UNC path for the backup files, and then do one of the following to configure access control settings:
   5.a. Select **Do not inherit** if you want the backup to be accessible only by a set of specified user credentials, and then click **Next**. Type a user name and password for a user account that has write permissions on the computer that is hosting the remote folder, and then click **OK**.
   5.b. Select **Inherit** if you want the backup to be accessible by everyone who has access to the remote folder, and then click **Next**.
6. On the **Specify advanced options** page, select **VSS full backup**, and then click **Next**.
7. On the **Confirmation** page, review the backup settings, and then click **Backup**.
8. On the **Backup progress** page, you can view the status and progress of the backup operation.
9. Click **Close** when the backup operation has completed.

Use Windows Server Backup to Restore a Backup of Exchange

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-12*

Microsoft Exchange Server 2010 includes a plug-in for Windows Server Backup that enables you to make Volume Shadow Copy Service (VSS)-based backups of Exchange data. You can use Windows Server Backup to back up and restore your Exchange databases.

Prerequisites

- This procedure can only be performed locally on a computer running Exchange 2010 on the Windows Server 2008 or Windows Server 2008 R2 operating system.
- When you restore a database to its original location, the database can remain in a dirty shutdown state and be mountable by the system. When you restore to an alternative location (such as the recovery database), the database must be in a clean shutdown state. You can bring a database into a clean shutdown state by using Exchange Server Database Utilities (Eseutil.exe).

Use Windows Server Backup to restore a backup of Exchange

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox recovery" entry in the Mailbox Permissions topic.

1. Start Windows Server Backup.
2. In the **Actions** pane, click **Recover**. The Recovery wizard appears.
3. On the **Getting Started** page, do either of the following:
   3.a. If the data being recovered was backed up from the server on which Windows Server Backup is running, select **This server (ServerName)**, and then click **Next**.
   3.b. If the data being recovered wasn't from the server on which Windows Server Backup is running, or if the backup being recovered is located on another computer, select **Another server**, and then click **Next**. On the **Specify location type** page, select **Local drives** or **Remote shared folder**, and then click **Next**. If you select **Local drives**, select the drive containing the backup on the **Select backup location** page, and then click **Next**. If you select **Remote shared folder**, enter the UNC path for the backup data on the **Specify remote folder** page, and then click **Next**.
4. On the **Select backup date** page, select the date and time of the backup that you want to recover, and then click **Next**.
5. On the **Select recovery type** page, select **Applications**, and then click **Next**.
6. On the **Select application** page, verify that Exchange is selected in the **Applications** field. Click **View Details** to view the application components of the backups. If the backup that you're recovering is the most recent, the **Do not perform a roll-forward recovery of the application database** check box is displayed. Select this check box if you want to prevent Windows Server Backup from rolling forward the database being recovered. Click **Next**.
7. On the **Specify recovery options** page, select where you want to recover the data, and then click **Next**:
   7.a. Select **Recover to original location** to recover backed up data to its original location. If you use this option, you can't set a single database or

multiple databases; all backed up databases are restored to their original location.

7.b.Select **Recover to another location** to restore databases and files to a specified location. Click **Browse** to specify the alternative location. If you use this option, you can restore databases to a custom location. After being restored, the data files can then be moved to a recovery database, and then manually returned to their original location. When you restore databases to an alternative location, the restored databases are in a dirty shutdown state.

8. On the **Confirmation** page, review the recovery settings, and then click **Recover**.
9. On the **Recovery progress** page, you can view the status and progress of the recovery operation.
10. Click **Close** when the recovery operation has completed.

1.10.5.2 Recover an Exchange Server

Recover an Exchange Server

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-22*

You can recover a lost server by using the **Setup /m:RecoverServer** switch in Microsoft Exchange Server 2010. Most of the settings for a computer running Exchange 2010 are stored in Active Directory. The */m:RecoverServer* switch rebuilds an Exchange server with the same name by using the settings and other information stored in Active Directory.

Recovering a lost Exchange server is often accomplished by using new hardware. However, you can also use an existing server.

This topic shows you how to recover a lost Exchange 2010 server that isn't a member of a database availability group (DAG). For detailed steps about how to recover a server that was a member of a DAG, see Recover a Database Availability Group Member Server.

Note:

If Exchange is installed in a location other than the default location, you must use the **/TargetDir** switch to specify the location of the Exchange binary files. If you don't use the **/TargetDir** switch, the Exchange files are installed in the default location (%programfiles%\Microsoft\Exchange Server\V14).
To determine the install location, follow these steps:

1. Open ADSIEDIT.MSC or LDP.EXE.
2. Navigate to the following location:
   CN=ExServerName,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=ExOrg Name,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=DomainName,CN=Com
3. Right-click the Exchange server object, and then click **Properties**.
4. Locate the **msExchInstallPath** attribute. This attribute stores the current installation path.

Prerequisites

- The server on which recovery is being performed must be running the same

operating system as the lost server. For example, you can't recover a server that was running Exchange 2010 and Windows Server 2008 on a server running Windows Server 2008 R2, or vice versa.
- The same disk drive letters on the failed server for mounted databases must exist on the server on which you're running recovery.
- The server on which recovery is being performed should have the same performance characteristics and hardware configuration as the lost server.
- The following procedure can be run on an Exchange 2010 server that has the Client Access, Hub Transport, Mailbox, or Unified Messaging server roles installed. You can't use **Setup /m:RecoverServer** to recover an Edge Transport server. For information about preserving Edge Transport server settings and applying saved settings to an Edge Transport server, see Understanding Edge Transport Server Cloned Configuration.

Recover a Lost Exchange Server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Exchange infrastructure permissions" section in the Exchange and Shell Infrastructure Permissions topic.

1. Reset the computer account for the lost server. For detailed steps, see Reset a Computer Account.
2. Install the proper operating system and name the new server with the same name as the lost server. Recovery won't succeed if the server on which recovery is being performed doesn't have the same name as the lost server.
3. Join the server to the same domain as the lost server.
4. Install the necessary prerequisites and operating system components. For details, see Exchange 2010 System Requirements and Exchange 2010 Prerequisites.
5. Log on to the server being recovered and open a command prompt.
6. Navigate to the Exchange 2010 installation files, and run the following command:

```
Setup /m:RecoverServer
```

7. After Setup has completed, but before the recovered server is put into production, reconfigure any custom settings that were previously present on the server.

1.10.5.3 Recovery Databases

Recovery Databases

Exchange Server 2010 > High Availability and Site Resilience > Understanding Backup, Restore and Disaster Recovery >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-03-06*

A recovery database (RDB) is a special kind of mailbox database that allows you to mount a restored mailbox database and extract data from the restored database as part of a recovery operation. You can use the Restore-Mailbox cmdlet to extract data from an RDB. After extraction, the data can be exported to a folder or merged into an existing mailbox. RDBs enable you to recover data from a backup or copy of a database without disturbing user access to current data.

Microsoft Exchange Server 2010 supports the ability to restore data directly to a recovery

database. Mounting the recovered data as a recovery database allows the administrator to restore individual mailboxes or individual items in a mailbox. Restoring to a recovery database can be accomplished in two ways:

- If a recovery database already exists, the application can dismount the database, restore the data onto the recovery database and log files, and then remount the database.
- The database and log files can be restored to any disk location. Exchange analyzes the restored data and replays the transaction logs to bring the databases up to date, and then a recovery database can be configured to point to already recovered database files.

Difference between a Mailbox Database and a Recovery Database

RDBs are different from standard mailbox databases in several respects:

- An RDB is created by using the Exchange Management Shell.
- Mail can't be sent to or from an RDB. All client protocol access to an RDB (including SMTP, POP3, and IMAP4) is blocked. This design prevents using an RDB to insert mail into or remove mail from the messaging system.
- Client MAPI access using Microsoft Office Outlook or Outlook Web App is blocked. MAPI access is supported for an RDB, but only by recovery tools and applications. Both the mailbox GUID and the database GUID must be specified when using MAPI to log into a mailbox in an RDB.
- Mailboxes in an RDB can't be connected to user accounts. To allow a user to access the data in a mailbox in an RDB, the mailbox must be merged into an existing mailbox, or exported to a folder.
- System and mailbox management policies aren't applied. This design prevents items in an RDB from being deleted by the system during the recovery process.
- Online maintenance isn't performed for RDBs.
- Circular logging can't be enabled for RDBs.
- An RDB is used for recovering only mailbox database data. You can't use an RDB to recover public folder data.
- Only one RDB can be mounted at any time on a Mailbox server. The use of an RDB doesn't count against the 100 database limit per Mailbox server.
- You can't create mailbox database copies of an RDB.
- An RDB can be used as a target for restore operations, but not backup operations.
- A recovered database mounted as an RDB isn't tied to the original mailbox in any way.

Using a Recovery Database

Before you can use an RDB, there are certain requirements that must be met. An RDB can be used for Exchange 2010 mailbox databases only. Mailbox databases from previous versions of Exchange aren't supported. In addition, the target mailbox used for data merges and extraction must be in the same Active Directory forest as the database mounted in the RDB.

An RDB can be used to recover data in several situations, such as:

- **Same server dial tone recovery** You can perform a recovery from an RDB after the original database has been restored from backup, as part of a dial tone recovery operation.
- **Alternate server dial tone recovery** You can use an alternate server to host the dial tone database, and then later recover data from an RDB after the original database has been restored from backup.
- **Mailbox recovery** You can recover an individual mailbox from backup when

the deleted mailbox retention period has elapsed. You then extract data from the restored mailbox and copy it to a target folder or merge it with another mailbox.

- **Specific item recovery** You can restore from backup data that has been deleted or purged from a mailbox.

Note:

Folder access control lists (ACLs) aren't preserved when recovering content into an active mailbox. Because the recovery process typically involves recovering mailbox data and merging the content back into the original database, there should be no need to recover or copy ACLs.

An RDB is designed for mailbox database recovery under the following conditions and scenarios:

- The logical information about the original database and the mailboxes in that database remains intact and unchanged in Active Directory.
- You need to recover a single mailbox or a single database. Recovery scenarios include:
  - Recovering or repairing a database while a dial tone database is in use, with the goal of merging the two databases.
  - Recovering a database on a server other than the original server for that database. If needed, you can then merge the recovered data back to the original server.
  - Recovering deleted items that users previously deleted from their mailbox, after the deleted item retention period has expired.

An RDB cannot be used when you have to recover public folder content. In addition, RDBs are generally not designed for scenarios in which you have to restore entire servers, when you have to restore multiple databases, or when you're in an emergency situation that requires changing or rebuilding your Active Directory topology.

For detailed steps about how to create an RDB, see Create a Recovery Database. For detailed steps about how to use an RDB, see Restore Data Using a Recovery Database.

1.10.5.3.1 Create a Recovery Database

Create a Recovery Database

High Availability and Site Resilience > Understanding Backup, Restore and Disaster Recovery > Recovery Databases >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use a recovery database, which is a special kind of mailbox database, to mount a restored mailbox database and extract data from the restored database as part of a recovery operation. After you create a recovery database, you can move a recovered or restored mailbox database into the recovery database, and then use the Restore-Mailbox cmdlet to extract data from the recovered database. After extraction, the data can then be exported to a folder or merged into an existing mailbox. Using recovery databases, you can recover data from a backup or copy of a database without disrupting user access to current data.

Looking for other management tasks related to recovery databases? Check out Recovery Databases.

Use the Shell to create a recovery database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox recovery" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to create a recovery database.

This example creates the recovery database RDB1 on the Mailbox server MBX2.

```
New-MailboxDatabase -Recovery -Name RDB1 -Server MBX2
```

This example creates the recovery database RDB2 on the Mailbox server MBX1 using a custom path for the database file and log folder.

```
New-MailboxDatabase -Recovery -Name RDB2 -Server MBX1 -EdbFilePath "C:\Recovery\R
```

For detailed syntax and parameter information, see New-MailboxDatabase.

Other Tasks

After you create a recovery database, you may also want to restore data using a recovery database. For detailed steps, see Restore Data Using a Recovery Database.

1.10.5.3.2 Restore Data Using a Recovery Database

Restore Data Using a Recovery Database

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-01-22*

A recovery database (RDB) is a special kind of mailbox database that allows you to mount a restored mailbox database and extract data from the restored database as part of a recovery operation. After you've created an RDB, you can restore a mailbox database into the RDB by using your backup application (or if you have the database and its log files in the file system, by copying them to the RDB file structure). Then you can use the New-MailboxRestoreRequest cmdlet to extract data from the recovered database. After being extracted, the data can then be exported to a folder or merged into an existing mailbox. RDBs allow you to recover data from a backup or copy of a database without disrupting user access to current data.

Looking for other management tasks related to RDBs? Check out Recovery Databases.

Prerequisites

- An RDB must be created. For detailed steps, see Create a Recovery Database.
- The database and log files containing the recovered data must be restored or copied into the RDB folder structure that was created when the RDB was created.
- The database must be in a clean shutdown state. Because an RDB is an

alternate restore location for all databases, all restored databases will be in a dirty shutdown state. You can use **Eseutil /R** to put the database in a clean shutdown state.

Use the Shell to recover data using a recovery database

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox recovery" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to restore data using an RDB.

This example restores the source mailbox that has the MailboxGUID 1d20855f-fd54-4681-98e6-e249f7326ddd on mailbox database DB1 to the target mailbox with the alias Scott.

```
New-MailboxRestoreRequest -SouceDatabase DB1 -SourceStoreMailbox 1d20855f-fd54-46
```

This example restores the content of the source mailbox that has the display name Scott Schnoll on mailbox database DB1 to the archive mailbox for scott@contoso.com.

```
New-MailboxRestoreRequest -SourceDatabase DB1 -SourceStoreMailbox "Scott Schnoll"
```

For detailed syntax and parameter information, see New-MailboxRestoreRequest.

1.10.5.4 Database Portability

Database Portability

Exchange Server 2010 > High Availability and Site Resilience > Understanding Backup, Restore and Disaster Recovery >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-09*

Database portability is a feature that enables a Microsoft Exchange Server 2010 mailbox database to be moved to or mounted on any other Mailbox server in the same organization. By using database portability, reliability is improved by removing several error-prone, manual steps from the recovery processes. In addition, database portability reduces the overall recovery times for various failure scenarios.

Note:

Database portability is for Exchange 2010 mailbox databases only. Public folder databases aren't portable. This is because replication between public folder databases is controlled by each database being linked to and accessed through a specific server. The preferred way to move public folder data between servers is to use public folder replication to replicate it to a different server. If you instead simply copy a public folder database to a different server, it will no longer replicate with other databases.

Mailbox databases from previous versions of Exchange can't be moved to a Mailbox server running Exchange 2010.

For information about how to perform a database recovery using the database portability feature, see Move a Mailbox Database Using Database Portability.

Move a Mailbox Database Using Database Portability

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use database portability to move a Microsoft Exchange Server 2010 mailbox database between Exchange 2010 Mailbox servers in the same organization. This can help reduce overall recovery times for various failure scenarios. To learn more, see Database Portability.

Note:
Database portability in Exchange 2010 can be used only for Exchange 2010 mailbox databases. It can't be used for public folder databases or mailbox databases from previous versions of Microsoft Exchange.

Use the Shell to move user mailboxes to a recovered or dial tone database using database portability

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox recovery" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to move user mailboxes to a recovered or dial tone database using database portability.

1. Verify that the database is in a Clean Shutdown state. If the database isn't in a Clean Shutdown state, perform a soft recovery.

   Note:
   When you perform a soft recovery, any uncommitted log files are committed to the database. If you don't have all of the required log files, you can't complete the soft recovery process. Proceed to step 2.

   To commit all uncommitted log files to the database, from a command prompt, run the following command.

   ```
   ESEUTIL /R <Enn>
   ```

   Note:
   <*Enn*> specifies the log file prefix for the database into which you intend to replay the log files. The log file prefix specified by <*Enn*> is a required parameter for Eseutil /r.

2. Create a database on the new server, as shown in this example.

   ```
   New-MailboxDatabase -Name DB1 -Server MBX1 -EdbFilePath C:\Databases\D
   ```

   Note:
   To create a database, see Create a Mailbox Database.

3. Set the *This database can be over written by restore* attribute using the following syntax.

   ```
   Set-MailboxDatabase <Database Name> -AllowFileRestore:$true
   ```

4. Move the database files (.edb file, log files, and Exchange Search catalog) to the appropriate location. The database files need to be present and in the

correct location for recovery operations to succeed.

5. Mount the database using the following syntax.

```
Mount-Database <Database Name>
```

6. After the database is mounted, modify the user account settings with the Set-Mailbox cmdlet so that the account points to the mailbox on the new mailbox server. To move all of the users from the old database to the new database, use the following syntax.

```
Get-Mailbox -Database <SourceDatabase> |where {$_.ObjectClass -NotMatc
```

After Active Directory replication is complete, all users can access their mailboxes on the new Exchange server. Clients can connect to the new server as follows:

- Microsoft Outlook 2010, Office Outlook 2007, and Windows Mobile 6.1 and later clients are redirected via the Autodiscover service.
- Outlook Web App users are automatically redirected to the new server.
- Older Outlook clients need to be manually configured to point to the new server, if the server name has changed.

1.10.5.5 Dial Tone Portability

Dial Tone Portability

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-26*

Dial tone portability is a feature of Microsoft Exchange Server 2010 that provides a limited business continuity solution for failures that affect a mailbox database, a server, or an entire site. Dial tone portability enables users to have a temporary mailbox for sending and receiving e-mail while their original mailbox is being restored or repaired. The temporary mailbox can be on the same Exchange 2010 Mailbox server or on any other Exchange 2010 Mailbox server in your organization. This allows an alternative server to host the mailboxes of users who were previously on a server that is no longer available. Clients that support Autodiscover, such as Microsoft Office Outlook 2007, are automatically redirected to the new server without having to manually update the user's desktop profile. After the user's original mailbox data has been restored, an administrator can merge a user's recovered mailbox and the user's dial tone mailbox into a single, up-to-date mailbox.

The process for using dial tone portability is called a *dial tone recovery*. A dial tone recovery involves creating an empty database on a Mailbox server to replace a failed database. This empty database, referred to as a *dial tone database*, allows users to send and receive e-mail messages while the failed database is recovered.

There are three options for performing a dial tone recovery:

- **Dial tone recovery on the server with the failed database** If the server hosting the failed database is still functional, we recommend that you perform a dial tone recovery on that server. This means less downtime because you don't need to move database files between servers. In addition, you won't need to reconfigure messaging profiles for clients that don't support Autodiscover.
- **Dial tone recovery using an alternate server for the dial tone database** If a

server fails and needs to be rebuilt, the most efficient way to give users basic mail functionality is to create a dial tone database on another server, and use database portability to move the users' mailbox configuration to that new server. Because this process involves moving the dial tone database back to the original (recovered) server, this option adds more time to the overall recovery process. In addition, this process is more complex than performing a dial tone recovery on the original server. When performing this process, the server hosting the dial tone database must have sufficient resources to support the added load of the additional users. In addition, if the user's client doesn't support Autodiscover, their messaging profile will need to be reconfigured to point to the dial tone server.

- **Dial tone recovery using and staying on an alternate server for the dial tone database** This is similar to the preceding option, except that you don't revert back to the original server. This option is recommended for situations in which it isn't possible or feasible to recover the failed server. In this scenario, users typically remain on an alternate server after the recovery operation has completed. When performing this process, the server hosting the dial tone database must have sufficient resources to support the added load of the additional users. In addition, if the user's client doesn't support Autodiscover, their messaging profile will need to be reconfigured to point to the dial tone server.

All three options follow the same basic steps:

1. **Create an empty dial tone database to replace the failed database**
   This new database will allow users who had mailboxes on the failed database to send and receive new messages. Dial tone portability allows you to point a user to a different database without moving the mailbox. If you created the dial tone database on a different server than the server that housed the failed database, you need to move the mailbox configuration to that new server.
2. **Restore the old database**
   Use the backup and recovery software you typically use to restore the failed database. If there is no backup of the failed database, recover the failed database using other means if possible. If you're using the same server for dial tone recovery, you need to restore the database to a recovery database (RDB).
3. **Swap the dial tone database with the restored database**
   After the failed database is restored, swap it with the dial tone database. This gives the users the ability to send and receive e-mail and access all the data in the restored database. If users were moved to a dial tone database on another server, you need to move the mailbox configuration back to the original server.
4. **Merge the databases**
   To get the data from the dial tone database into the restored database, you merge the data using the Restore-Mailbox cmdlet.

For detailed steps about how to perform a dial tone recovery, see Perform a Dial Tone Recovery.

1.10.5.5.1 Perform a Dial Tone Recovery

Perform a Dial Tone Recovery

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Using dial tone portability, users can have a temporary mailbox for sending and receiving e-mail while their original mailbox is being restored or repaired. The temporary mailbox can be on the same Exchange 2010 Mailbox server or on any other Exchange 2010 Mailbox server in your organization. The process for using dial tone portability is called a dial tone recovery, which involves creating an empty database on a Mailbox server to replace a failed database. To learn more, see Dial Tone Portability.

Prerequisites

You must have fewer than the maximum number of databases deployed to create a dial tone database. Exchange 2010 Standard Edition supports a maximum of 5 databases per server. Exchange 2010 Enterprise Edition supports a maximum of 100 databases per server.

Use the Shell to perform a dial tone recovery on a single server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox recovery" entry in the Mailbox Permissions topic.

Note:

You can't use the EMC to perform a dial tone recovery on a single server.

1. Make sure that any existing files for the database being recovered are preserved in case they're needed later for further recovery operations.
2. Use the New-MailboxDatabase cmdlet to create a dial tone database, as shown in this example.

```
New-MailboxDatabase -Name DTDB1 -EdbFilePath D:\DialTone\DTDB1.EDB
```

3. Use the Set-Mailbox cmdlet to rehome the user mailboxes hosted on the database being recovered, as shown in this example.

```
Get-Mailbox -Database DB1 | Set-Mailbox -Database DTDB1
```

4. Use the Mount-Database cmdlet to mount the database so client computers can access the database and send and receive messages, as shown in this example.

```
Mount-Database -Identity DTDB1
```

5. Create a recovery database (RDB) and restore or copy the database and log files containing the data you want to recover into the RDB. For detailed steps, see Create a Recovery Database.
6. After the data is copied to the RDB, but before mounting the restored database, copy any log files from the failed database to the recovery database log folder so they can be played against the restored database.
7. Mount the RDB, and then use the Dismount-Database cmdlet to dismount it, as shown in this example.

```
Mount-Database -Identity RDB1
Dismount-Database -Identity RDB1
```

8. After the RDB is dismounted, move the current database and log files within the RDB folder to a safe location. This is done in preparation for swapping the recovered database with the dial tone database.
9. Dismount the dial tone database, as shown in this example. Note that your end users will experience an interruption in service when you dismount this database.

```
Dismount-Database -Identity DTDB1
```

10. Move the database and log files from the dial tone database folder into the RDB folder.
11. Move the database and log files from the safe location containing the recovered database into the dial tone database folder, and then mount the database, as shown in this example.

```
Mount-Database -Identity DTDB1
```

This ends the service interruption for your end users. They will be able to access their original production database and send and receive messages.

12. Mount the RDB, as shown in this example.

```
Mount-Database -Identity RDB1
```

13. Use the Get-Mailbox and Restore-Mailbox cmdlets to export the data from the RDB and import it into the recovered database, as shown in this example. This will import all the messages sent and received using the dial tone database into the production database.

```
Get-Mailbox -Database DTDB1 | Restore-Mailbox -RecoveryDatabase RDB1
```

14. After the restore operation is complete, you can dismount and remove the RDB, as shown in this example.

```
Dismount-Database -Identity RDB1
Remove-MailboxDatabase -Identity RDB1
```

For detailed syntax and parameter information, see the following topics:

- New-MailboxDatabase
- Get-Mailbox
- Set-Mailbox
- Mount-Database
- Dismount-Database
- Remove-MailboxDatabase

1.11 Messaging Policy and Compliance

Messaging Policy and Compliance

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-21*

Planning for Compliance

Learn about factors you must consider when planning for compliance.

Create a Message Classification

Message classifications allow your organization to comply with e-mail policies and regulatory responsibilities. When a message is classified, the message contains specific metadata that describes the intended use or audience of the message.

Transport Rules

Transport rules allow you to apply messaging policies to e-mail messages that flow through the transport pipeline on Hub Transport and Edge Transport servers. Transport rules help you to comply with messaging policies, secure messages, and protect messaging systems.

Information Rights Management

Information Rights Management (IRM) allows your organization and your users to apply persistent protection to messages so that access is restricted to authorized users and actions (such as forwarding, copying, and printing message content).

Journaling

Journaling can help your organization respond to legal, regulatory, and organizational compliance requirements by recording inbound and outbound e-mail communications. When planning for messaging retention and compliance, it's important to understand journaling, how it fits in your organization's compliance policies, and how Microsoft Exchange Server 2010 helps you secure journaled messages.

Messaging Records Management

Messaging records management (MRM) makes it easier to retain the messages needed to comply with company policy, government regulations, or legal needs. MRM also helps remove older content that has no legal or business value. This is accomplished through the use of retention policies or managed folders.

Discovery

Discovery consists of Multi-Mailbox Search, a tool that allows authorized discovery managers, legal professionals, and Human Resource professionals to perform mailbox searches across the Exchange 2010 organization for messages matching specified criteria.

Litigation Hold

Litigation hold allows you to preserve messages for an extended period and protect them from permanent deletion. It also maintains the version history for items modified while litigation hold is enabled for a mailbox.

Archiving

Personal archives allow you to gain control of your organization's messaging data by eliminating the need for .pst files. Personal archives also allow users to store their messages in an archive mailbox that's accessible by using Microsoft Outlook 2010 and Microsoft Office Outlook Web App.

Mailbox Audit Logging

Mailbox audit logging allows you to audit mailbox access by mailbox owners, delegates, and administrators. You can also use audit logging to audit actions such as deletions and access to messages and folders.

1.11.1 Planning for Compliance

Planning for Compliance

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-09*

Microsoft Exchange Server 2010 is designed to help users meet compliance requirements. Exchange 2010 offers you several features that help you capture, protect, modify, retain, and discover e-mail messages in a user mailbox as the messages flow in, through, and out of your organization.

The following list provides several examples of the areas where compliance features in Exchange 2010 can help you become compliant or respond to future discovery requirements:

- **Data retention policies** Many organizations are required to keep data for a specific time and then remove that data to protect privacy. To learn more, see Understanding Messaging Records Management.
- **Privacy and confidentiality requirements** Every day organizations transmit sensitive and confidential information through e-mail, both to and from individuals and the organization itself. These organizations have to protect the privacy of individuals and the confidentiality of communications. To learn more, see Understanding Information Rights Management.
- **Ethical walls** Organizations that work with securities and other financial information are frequently required to prohibit communication between specific groups in their own organization. To learn more, see Understanding Ethical Walls.
- **Discovery requests** Organizations are sometimes subject to litigation. As part of this process, litigants can request information from each other. Because most business communication occurs over e-mail, complying with discovery requests requires the ability to search mailbox content, including e-mail messages and attachments. To learn more, see Understanding Multi-Mailbox Search.

Why is Compliance Important?

Every organization should consider compliance. Every day organizations are required to produce evidence for litigation or to provide documentation to regulatory agencies to prove they're complying with regulations.

Organizations that consider compliance when they plan their information technology infrastructures, including their e-mail infrastructures, can supply the required documentation on demand with less effort. They can also comply with other regulatory requirements more easily.

On the other hand, organizations that don't consider compliance up-front may find themselves sorting through millions of e-mail messages manually, wasting time and money. Organizations can also be held legally responsible for not complying with laws or regulatory requirements.

Although your organization may have never been subject to litigation or may not be required to follow regulatory requirements, there's a good chance that you handle private and confidential information that may be regulated by laws or regulations in your country or region. It's important that you understand the laws and regulations that apply to your organization and take proactive steps to make sure that you comply with them.

For a list of some of the laws and regulations that may apply to your organization, see Understanding Journaling.

Discussing Compliance in Your Organization

It's important to understand the requirements and obligations that may apply to your organization. If you haven't discussed compliance in your organization, the deployment of Exchange 2010 can be a catalyst for these conversations. Speak with your organization's management and legal representatives to understand the answers to the following questions:

- Do we handle customer data?
- Do we have established policies that protect customer data?
- Do we transmit confidential organizational information through e-mail?
- Do we control who can view confidential information and where it can be sent?
- Have we established policies and procedures that help us respond to legal

requests for information?
- Are there laws or regulations that prohibit communication between specific groups in our organization?
- Are there laws or regulations that require us to remove data after a specific time?

This list presents some of the questions that many organizations must answer. The list isn't definitive. It provides examples to help you consider some of the issues that may apply to your organization. Your organization may have other issues to consider.

If you already have a solid compliance policy in your organization, talk with your compliance officers and management to help them understand how your organization can use Exchange 2010 as a compliance tool.

1.11.2 Message Classifications

Message Classifications

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-01*

Understanding Message Classifications

Learn about message classifications and how they can help you implement your organization's messaging policies.

Managing Message Classifications

Learn about managing message classifications in your Exchange organization.

1.11.2.1 Understanding Message Classifications

Understanding Message Classifications

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-06*

Message classifications are a Microsoft Exchange Server 2010 and Microsoft Office Outlook 2007 feature intended to help organizations comply with their e-mail policies and regulatory responsibilities. When a message is *classified*, the message contains specific metadata that describes the intended use or audience of the message. Outlook 2007 or Microsoft Office Outlook Web App may act on this metadata by displaying a user-friendly description of the classification to senders and receivers of a classified message. In Exchange 2010, the Microsoft Exchange Transport service may act on the metadata if there's a transport rule that meets specific criteria that you have configured.

The following list provides a brief description of some of the message classification fields that you can set:

- **Display name** This property specifies the display name for the message classification instance. The display name appears in the **Permission** menu in Outlook 2007 and Outlook Web App and is used by Outlook and Outlook Web App users to select the appropriate message classification before a message

is sent. The display name is also displayed in the recipient description that appears in the InfoBar in an Outlook message. The parameter name for this property is *DisplayName*.

- **Sender description** This property explains to the sender what the message classification is intended to achieve. The text that you enter for this field is used by Outlook and Outlook Web App users to select the appropriate message classification before a message is sent. The parameter name for this property is *SenderDescription*.
- **Recipient description** This property explains to the recipient what the message classification was intended to achieve. The text that you enter for this field is viewed by Outlook and Outlook Web App users when they receive a message that has this message classification. The parameter name for this property is *RecipientDescription*.
- **Locale** This field specifies a culture code to create a locale-specific version of the message classification. For more information about the locale field, see "Localizing Message Classification Instances for Different Languages and Locales" later in this topic. The parameter name for this property is *Locale*.

After Outlook 2007 is enabled to accept the default message classifications, users can apply message classification to messages that they send. Senders see the sender description in the InfoBar in Outlook 2007. By using the Exchange Management Shell, you can customize the sender description for each message classification and locale.

Note:
Outlook Web App requires no special configuration to display or use message classifications.

Three message classifications are enabled in Exchange 2010 by default:

- **Attachment Removed** This classification notifies recipients when attachments have been removed from the message.
- **Originator Requested Alternate Recipient Mail** This classification notifies recipients that the message has been redirected from delivery to the original addressed recipient.
- **Partner Mail** This classification notifies recipients that the message was encrypted and delivered through a secure connector.

Note:
Users can't add these classifications to messages.

In the initial installation of Exchange 2010, all message classifications are informational only. They aren't associated with any transport rules and only provide additional information about a message to the message recipients. By default, in Exchange 2010, the Microsoft Exchange Transport service doesn't take any special action on the message.

However, you can create transport rules based on message classifications. For example, you can configure a transport rule that checks all incoming messages for a specific message classification and direct that these messages be delivered to a designated recipient. For more information, see Create a Transport Rule.

Message classifications can be logically separated into two classes based on how they are attached to a specific message:

- A message classification can be manually added by the sender of a message before the message is sent.
- A message classification can be added as the result of a rule. For example, when the Attachment Filter agent removes an attachment from a message, the Attachment Removed message classification is attached to the message. When the sender receives the message, Outlook 2007 displays an explanation of why the attachment was removed in the recipient description in the InfoBar. As the Exchange administrator, you can customize the recipient description.

Looking for management tasks related to message classifications? See Managing Message Classifications.

Contents

Localizing Message Classification Instances for Different Languages and Locales

In some scenarios, your business needs may dictate using different languages for message classifications for different groups of users, regions, or locales where your business operates. After you create the default message classification instance, you can create more than one message classification instance for different languages.

You can also use a message classification instance to change the content of the sender description and recipient description to reflect differences in regulatory requirements for different jurisdictions. If a message classification for the locale of the recipient exists in Active Directory, Exchange will attach the localized message classification to the message.

For example, health care-related companies that operate in the United States and in Europe may have to comply with Health Insurance Portability and Accountability Act (HIPAA) regulations in the United States but not in Europe. Therefore, the display of message classifications that are HIPAA-specific should only be enabled for employees operating in the United States. You can set Read permission on classifications so that only appropriate users can view specific message classifications.

Each localized version of a specific message classification is a new message classification instance. The *Locale* parameter defines the locale for a particular message classification instance. The *Locale* parameter takes a data type of **CultureInfo**. When you create a localized version of a message classification, you will reference the default instance of the message classification and create a localized instance of the existing message classification.

For an example of a localized message classification and more information about how to create localized versions of message classifications, see Create Localized Versions of Message Classifications.

Return to top

Precedence and Retention of the Message Classification

By default, a message classification travels with a message for the life of the message until it leaves the organization. Therefore, if a sender sets a message classification on a

specific message, the message will retain the message classification as long as other rules don't remove it.

Each message classification can be assigned a relative priority to other message classifications. This sets the precedence on a specified classification and how it's displayed to the recipient in Outlook. The message classification with the highest precedence is shown first, and subsequent classifications with lesser precedence are displayed in the appropriate order thereafter. You set precedence by using the *DisplayPrecedence* parameter on the **Set-MessageClassification** cmdlet in the Shell.

For each message classification, you can specify whether the message classification is retained when a recipient replies to or forwards the message. You can specify whether a classification is retained by setting the *RetainClassificationEnabled* parameter on the **Set-MessageClassification** cmdlet in the Shell.

For more information, see Set-MessageClassification.

Return to top

Providing Read Access to Message Classifications

When you create a message classification and enable the computer on which Outlook runs, the new message classification will be present in the **Permission** menu of Outlook and Outlook Web App.

You can control read access for the message classifications presented in the **Permission** menu of Outlook 2007 if you configure the message classifications that you export into the Classifications.xml file. For more information about how to create and use the Classifications.xml file, see Deploy Message Classifications for Outlook 2007.

You can control read access for the message classifications presented in the **Permission** menu of Outlook Web App if you configure the Read permission on the message classification object. By default, all message classifications are created with Read permission for any authenticated user when you grant Read permission to authenticated users on the message classification object in Active Directory.

It's important to understand that the Read permission set on the message classification object doesn't control whether the sender can use the message classification. Read permission on the message classification only controls whether the message classification is displayed in the **Permission** menu in Outlook Web App. Outlook 2007 users can send message classifications even if the user doesn't have read access to the message classification. Advanced users can still send classified messages by editing the Classifications.xml file installed on their computer to enable message classifications Outlook 2007.

Return to top

Message Classifications in Transport Rules

After you create a message classification instance, you can associate a transport rule with the message classification. You use the Shell to create a transport rule and add the message classification as a condition. For information about how to use the Shell to create transport rules, see Create a Transport Rule.

Return to top

Managing and Deploying Message Classifications

Before Outlook 2007 users can set and view message classifications, you must deploy the message classification configuration files and create an Outlook registry key on the end-users' computers. The Outlook message classification templates are .xml files that you must generate after you create and configure the message classifications.

You manage all message classifications by using the message classification cmdlets in the Shell. You can bind message classifications to transport rules by using the Shell or the Exchange Management Console (EMC).

For more information, see Deploy Message Classifications for Outlook 2007.

Return to top

1.11.2.1.1 Understanding Attorney-Client Privileged Communication

Understanding Attorney-Client Privileged Communication

Messaging Policy and Compliance > Message Classifications > Understanding Message Classifications >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-20*

In Microsoft Exchange Server 2010, you can use message classifications and transport rules to comply with your organization's messaging policies. For example, a message classification for attorney-client privileged communication could be used to identify messages that should be considered confidential and that contain privileged information that should only be shared between an attorney and their client. This topic provides an overview about this scenario for an Exchange organization.

For more detailed information about deploying an attorney-client privileged message classification, see Deploy an Attorney-Client Privileged Message Classification. Looking for other management tasks related to message classifications? See Managing Message Classifications.

Contents

Attorney-Client Privileged Communication Concepts

The *attorney-client privilege* is a legal doctrine that is intended to protect the confidentiality of communication between an attorney and his or her client. By assuring confidential communication, lawyers and their clients will feel free to discuss sensitive legal matters thoroughly. Communication that meets the legal tests that define the privilege is

considered confidential. Disclosure of that communication can't be compelled by anyone if the client doesn't want the communication disclosed.

To qualify as an attorney-client privileged communication, in general, communication must meet all the following criteria:

- It must be between an attorney and a client.
- It must be for the purpose of seeking or providing legal advice.
- It must be intended to be confidential. Confidentiality must be strictly maintained.

Note:

The rules related to the doctrine of attorney-client privilege may vary by jurisdiction. The information contained in this topic isn't intended to define the privilege or how to ensure protection. This topic is intended to highlight features that may help you in your attempts to improve protection for attorney-client privileged communication that occurs by e-mail using Exchange 2010. The declaration of attorney-client privilege on a message doesn't guarantee that the contents of the message can't be disclosed.

Enabling Attorney-Client Privileged Communication with Exchange 2010

To use the attorney-client privilege when you communicate with an attorney by using e-mail, you typically must declare that your message is intended to be privileged communication between you and your attorney. You must also take reasonable steps to make sure that only your attorney is addressed on the message. The following are examples of requirements that an organization may apply to messages that it wants to preserve under the attorney-client privilege:

- An attorney should be on the To line of the message.
- No recipients outside the organization should be present on the message.
- The subject or body of the message should contain the text "Attorney Client Privileged" or similar wording that clearly specifies that the message is intended as attorney-client privileged communication.
- The message shouldn't be forwarded except by the attorney or at the direction of the attorney.
- The message should be rights-protected.

In earlier versions of Exchange Server, recipients and senders had to manually apply organizational requirements, such as attorney-client privilege requirements, to their messages. In the following circumstances, recipients and senders might unintentionally omit a step or mistakenly forward a privileged message to an external recipient:

- They didn't fully understand complex policies and related procedures.
- They were unaware of these policies and procedures.

By inadvertently violating organizational or regulatory requirements for attorney-client privileged communications, senders and recipients may unknowingly waive the attorney-client privilege. In Exchange 2010, message classifications and transport rules help reduce the possibility of such user errors by alerting users that special handling requirements may be needed for specific message classifications.

Attorney-Client Privileged Message Classification

A custom attorney-client privileged message classification in an Exchange 2010 organization can help reduce the burden on senders and recipients by helping ensure that their messages meet the attorney-client privilege policy requirements adopted by the organization. This classification can be used to display a user-friendly description of the

attorney-client privileged classification to the senders and recipients of the message. It can also include specific instructions about how the message should be handled to maintain the attorney-client privilege.

In addition to displaying specific instructions to the sender and recipients of the message, Exchange 2010 can also enforce the attorney-client privilege requirements when the message enters the transport pipeline. In a typical scenario, you can use transport rules on the Hub Transport server to identify messages to which the attorney-client privileged message classification has been applied. If the classification has been applied, the transport rules can check whether the message meets the organization's list of attorney-client privilege requirements. If the message doesn't meet the requirements, the message may be returned to the sender.

It's important to remember that applying an attorney-client privileged message classification doesn't prevent the recipient from misusing the message by default. This misuse could be any action taken by the recipient that is prohibited by your organization's classification policy, such as printing, forwarding, or copying the message. To prevent these actions, you should apply Information Rights Management (IRM) protection rules to enforce your organizational compliance requirements.

1.11.2.2 Managing Message Classifications

Managing Message Classifications

Exchange Server 2010 > Messaging Policy and Compliance > Message Classifications >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-01*

Create a Message Classification

Create Localized Versions of Message Classifications

Deploy Message Classifications for Outlook 2007

Deploy an Attorney-Client Privileged Message Classification

1.11.2.2.1 Create a Message Classification

Create a Message Classification

Messaging Policy and Compliance > Message Classifications > Managing Message Classifications >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

This topic provides information about how to create a new message classification. For more information about message classifications, see Understanding Message Classifications.

Looking for other management tasks related to message classifications? Check out Managing Message Classifications.

Caution:
Before you create or modify message classifications in your production environment, we recommend that you use a test environment to understand how message classifications work. Before you modify message classifications, test them in a production environment.

Use the Shell to create a message classification

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Message classifications" entry in the Transport Permissions topic.

Note:
You can't use the Exchange Management Console to create a message classification.

To create a new message classification instance, you must use the **New-MessageClassification** cmdlet in the Exchange Management Shell. The **New-MessageClassification** cmdlet requires four parameters to create a new message classification:

- *DisplayName*
- *Locale*
- *Name*
- *SenderDescription*

You should also consider setting a value for the optional *RecipientDescription* parameter so that recipients are provided with a detailed description about the intent of the classification and how they should handle the message.

This example creates a new message classification with only the required classification parameters:

```
New-MessageClassification -Name NewMessageClassification -DisplayName "New Messag
```

This example creates a new message classification that includes the *RecipientDescription* parameter with the required classification parameters:

```
New-MessageClassification -Name NewMessageClassification -DisplayName "New Messag
```

Other Tasks

After creating a new message classification, you may also want to:

Create Localized Versions of Message Classifications

1.11.2.2.2 Create Localized Versions of Message Classifications

Create Localized Versions of Message Classifications

Messaging Policy and Compliance > Message Classifications > Managing Message Classifications >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use the Shell to create localized versions of message classifications in Microsoft

Exchange Server 2010.

Use the Shell to create localized versions of message classifications

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Message classifications" entry in the Transport Permissions topic.

Note:
You can't use the EMC to create localized versions of message classifications.

This example creates a Spanish - Spain ("es-ES") version of an existing message classification.

```
New-MessageClassification Example -Locale es-ES -DisplayName "España Example" -Se
```

For detailed syntax and parameter information, see New-MessageClassification.

1.11.2.2.3 Deploy Message Classifications for Outlook 2007

Deploy Message Classifications for Outlook 2007

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Office Outlook 2007 requires a local file (Classifications.xml) that contains definitions of the message classifications that Microsoft Exchange Server 2010 supports before Outlook users can apply message classifications to their messages. You must also create a registry key that enables message classification and references the Classifications.xml file on the Outlook user's computer.

Looking for other management tasks related to message classifications? Check out Managing Message Classifications.

Use Registry Editor to create a registry key for message classifications on Outlook 2007 clients

The following registry key and related registry settings must be created on all Outlook 2007 computers from which users who have mailboxes hosted on Exchange 2010 send message classifications.

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Policy]
"AdminClassificationPath"="c:\\Classifications.xml"
"EnableClassifications"=dword:00000001
"TrustClassifications"=dword:00000001
```

Note:
The `Policy` key isn't present by default and therefore must be created.

Caution:
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

The following table provides details about each registry value you need to use.

Registry values

Registry value	Description
AdminClassificationPath	You must change the path to refer to the location where you will copy the Classifications.xml file. Although you can use a network share, we recommend that the path is a location on the local computer for any computer running Outlook in cached mode so that Outlook can read the instructions and enable message composition even when offline.
EnableClassifications	You can enable and disable message classification functionality for the specified user. To enable message classification functionality, set this DWORD value to 00000001. To disable message classification functionality, set this DWORD value to 00000000.
TrustClassifications	You can qualify the assertions made on classified messages when the messages are sent to users who have mailboxes on Exchange Server 2003. You should enable TrustClassifications only for users who have mailboxes on Exchange 2010. To enable TrustClassifications, set this DWORD value to 00000001. Outlook also supports message classifications between users on Exchange 2003. Because Exchange 2003 doesn't support or recognize message classifications, the content and validity of the message classifications can't be guaranteed. Therefore, disabling TrustClassifications prepends the text **The sender claims:** to the message classification to protect users from incorrectly assuming that their organization has processed the classification. To disable TrustClassifications, set this DWORD value to 00000000.

The message classifications in the Classifications.xml file are the only message classifications that will be available to Outlook users when they send messages. However, the message classifications in the Classifications.xml file don't restrict the set of classifications that a user can receive.

For example, a user can receive an e-mail message with a message classification that isn't present in his or her version of the Classifications.xml file. If the user forwards the message classification, the message retains its classification, assuming that the *RetainClassificationEnabled* parameter on the originating message classification instance was set to `$True`, even though the recipient who forwards the message doesn't have the specific message classification in the local Classifications.xml file.

Use a script to create a Classifications.xml file for Outlook 2007 clients

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Message classifications" entry in the Transport Permissions topic.

1. Open the Shell and run the following script from the Program Files\Microsoft\Exchange Server\V14\Scripts directory:
   ./Export-OutlookClassification.ps1 > c:\exports\Classifications.xml

   Note:
   This script will export all message classifications into the Classifications.xml file. If you don't want all classifications in the XML file, you must manually remove them by removing the specific <Classification> element from Classification.xml.

2. After you export the appropriate message classifications, you must copy the resulting Classifications.xml file onto the end-users' computers to the *AdminClassificationPath* path that you specified in the registry setting discussed earlier in this topic. You must restart Outlook so that the Classifications.xml file is picked up by Outlook.

Other Tasks

After deploying message classifications to Outlook 2007 clients, you may also want to create a message classification. For detailed steps, see Create a Message Classification.

1.11.2.2.4 Deploy an Attorney-Client Privileged Message Classification

Deploy an Attorney-Client Privileged Message Classification

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

By default, Exchange 2010 includes three default message classifications: Attachment Removed, Originator Requested Alternate Recipient Mail, and Partner Mail. For new Exchange 2010 installations, you'll need to create a new message classification for Attorney-Client Privileged communication.

If your organization is transitioning from Exchange Server 2007, you don't need to create the Attorney-Client Privileged message classification. It's included in the Exchange 2007 default classifications and therefore available to servers that have been upgraded from Exchange 2007 to Exchange 2010. However, this classification must exist in each Active Directory forest for users in that forest to see the classification.

You can review existing message classifications by running the following command in the Exchange Management Shell.

```
Get-MessageClassification | Format-Table
```

For more information about attorney-client privileged communication, see Understanding Attorney-Client Privileged Communication.

Step 1: Create the Attorney-Client Privileged message classification

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Message classifications" entry in the Transport Permissions topic.

To create a new message classification instance, you must use the **New-MessageClassification** cmdlet in the Exchange Management Shell.

Run the following command to create the Attorney-Client Privileged message classification:

```
New-MessageClassification -Name AttorneyClientPrivileged -DisplayName "Attorney-C
```

Note:

For more information about creating new message classifications, see Create a Message Classification

Step 2: Deploy the Attorney-Client Privileged message classification to all Outlook 2007 Clients

This step requires that you modify the registry. You must have local administrator permissions on the client you want to update.

Caution:

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Outlook 2007 requires a local file (Classifications.xml) that contains definitions of the message classifications that Exchange 2010 supports before Outlook users can apply message classifications to their messages. The Exchange administrator must also create a new registry key that enables message classifications and references the Classifications.xml file on the Outlook user's computer.

Create the following registry key and related registry settings on all computers from which users who have mailboxes hosted on Exchange 2010 send message classifications.

```
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Policy
"AdminClassificationPath"="c:\\Classifications.xml"
"EnableClassifications"=dword:00000001
"TrustClassifications"=dword:00000001
```

Note:

The Policy key is not present by default and therefore must be created. For more detailed information about how to deploy message classifications to clients, see Deploy Message

Classifications for Outlook 2007. Changes to message classifications are immediately available in Outlook Web App.

Step 3: Export message classifications from Exchange 2010 and copy Classifications.xml file to all Outlook 2007 clients

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Message classifications" entry in the Transport Permissions topic.

1. Open the Exchange Management Shell and run the following script from the \Program Files\Microsoft\Exchange Server\V14\Scripts directory.

```
./Export-OutlookClassification.ps1 > c:\exports\Classifications.xml
```

Note:
This script will export all message classifications into Classifications.xml. If you don't want all classifications in the XML file, you must manually remove them by removing the specific <Classification> element from Classifications.xml.

2. Copy the resulting Classifications.xml file onto the end user's computers to the AdminClassificationPath that you specified in the registry setting that was discussed in Step 2 earlier. You must restart Outlook so that the Classifications.xml file is picked up by Outlook.

Note:
Whenever new classifications are added to your Exchange organization, the new classifications should be added to the Classifications.xml file on each client. The Classifications.xml file can be exported from Exchange 2010 and copied to all Outlook clients again, or it can be manually updated for each client computer.

Step 4: Create a Transport Rule that checks messages for the Attorney-Client Privileged classification and enforces the addition of a legal disclaimer

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

Transport rules let you apply messaging policies to e-mail messages that flow through the transport pipeline on Hub and Edge Transport servers. For more information about Transport Rules, see the following topics:

- Understanding Transport Rules
- Create a Transport Rule

For this scenario, we will create a new transport rule that appends a legal disclaimer to all messages sent from internal users to external recipients for messages that have the Attorney-Client Privileged classification. (Although we will create this transport rule for the Hub Transport servers in the organization using the Exchange Management Shell, the Exchange Management Console can also be used to create a transport rule.)

Run the following command to create a transport rule that appends a legal disclaimer to all messages that have the Attorney-Client privileged classification:

```
New-TransportRule -Name "Attorney-Client Privilege Disclaimer" -Enabled $true -Fr
```

Note:
The rule parameters and action used here are for illustration only. Review all the available transport rule predicates and actions to determine which ones meet your organization's requirements.

1.11.3 Transport Rules

Transport Rules

Exchange Server 2010 > Messaging Policy and Compliance >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

Understanding Transport Rules

Learn about transport rules and how they can help you implement your organization's messaging policies.

Understanding How Transport Rules Are Applied

Learn how transport rules are applied in different scenarios.

Transport Rule Predicates

Learn about the transport rule predicates and properties available on Hub Transport and Edge Transport servers that are running Microsoft Exchange Server 2010.

Transport Rule Actions

Learn about the transport rule actions and properties available on Exchange 2010 Hub Transport and Edge Transport servers.

Regular Expressions in Transport Rules

Learn how you can use regular expressions to match text patterns in messages and supported attachments.

Understanding Disclaimers

Learn about adding disclaimers and personal signatures to e-mail messages.

Understanding Ethical Walls

Learn about ethical walls and how to use transport rules to implement them.

Managing Transport Rules

Learn about managing transport rules in your Exchange organization.

Transport Rules: End-to-End Tasks

Learn how to implement transport rules in specific scenarios.

Using Exchange Hosted Services

Transport messaging policies are enhanced by or are also available as a service from Microsoft Exchange Hosted Services.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

1.11.3.1 Understanding Transport Rules

Understanding Transport Rules

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-26*

Many organizations today are required by law, regulatory requirements, or company policies to apply messaging policies that limit the interaction between recipients and senders, both inside and outside the organization. In addition to limiting interactions among individuals, departmental groups inside the organization, and entities outside the organization, some organizations are also subject to the following messaging policy requirements:

- Preventing inappropriate content from entering or leaving the organization
- Filtering confidential organization information
- Tracking or archiving messages that are sent to or received from specific individuals
- Redirecting inbound and outbound messages for inspection before delivery
- Applying disclaimers to messages as they pass through the organization

Transport rules let you apply messaging policies to e-mail messages that flow through the transport pipeline on Hub Transport and Edge Transport servers. These rules allow information technology (IT) administrators to comply with messaging policies, secure messages, protect messaging systems, and prevent information leakage.

In Microsoft Exchange Server 2010, transport rules have been enhanced with additional predicates and actions. Additional functionality has been integrated with transport rules, such as rights protection.

Looking for management tasks related to managing transport rules? See Managing Transport Rules.

Contents

Transport Rule Components

Transport rules consist of the following components:

- **Conditions** Transport rule conditions are used to identify messages to which a transport rule action should be applied. Conditions consist of one or more predicates that specify the parts of a message that should be examined. Some predicates examine message fields or headers, such as To, From, or Cc. Other predicates examine message characteristics such as message subject, body, attachments, message size, and message classification. Most predicates require that you specify a comparison operator, such as equals, doesn't equal, or contains, and a value to match.
  For a complete list of transport rule predicates available to Hub Transport and Edge Transport servers, see Transport Rule Predicates. The list of predicates is also available in the New Transport Rule wizard in the Exchange Management Console (EMC), and can be retrieved by using the Get-TransportRulePredicate cmdlet in the Exchange Management Shell.
- **Exceptions** Exceptions are based on the same predicates used to build transport rule conditions. However, unlike conditions, exceptions identify messages to which transport rule actions shouldn't be applied. Exceptions override conditions and prevent actions from being applied to an e-mail message, even if the message matches all configured conditions.
- **Actions** Actions are applied to messages that match the conditions and don't match any exception defined in the transport rule. Transport rules have many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers and personalized signatures in the message body.
  To view a complete list of transport rule actions available on Hub Transport and Edge Transport servers, see Transport Rule Actions. The list of transport rule actions can also be viewed in the New Transport Rule wizard in the EMC, and can be retrieved by using the Get-TransportRuleAction cmdlet in the Shell.

Return to top

Rules Agents

Transport rules are applied on Hub Transport and Edge Transport servers by transport agents. On the Hub Transport server, rules are applied by the Transport Rules agent. On the Edge Transport server, this is the job of the Edge Rules agent. Although similar in functionality, both agents have some differences in the predicates and actions available, the transport event on which each agent fires, and the priority of each agent relative to other transport agents enabled on that transport server.

Transport Rules Agent

The Transport Rules agent processes transport rules on Hub Transport servers. It fires on the **OnRoutedMessage** transport event. All messages in an Exchange 2010 organization are touched by at least one Hub Transport server. This includes:

- Messages to and from users in the same Active Directory site, including users with mailboxes on the same Mailbox server.
- Messages to and from users in different Active Directory sites.
- Messages to and from users in the Exchange organization and external users.

Transport rules configured on Hub Transport servers are stored in Active Directory, making them accessible to all Hub Transport servers in the organization as the configuration is replicated to all domain controllers across the Active Directory forest. This allows Exchange to consistently apply a single set of rules across the entire organization. Each Hub Transport server queries Active Directory to retrieve the organization's current

transport rule configuration and then applies the rules to messages it handles.

Important:
Transport rules are an Exchange feature. They can't prevent users from communicating in other ways, such as networked file shares, newsgroups, and forums, or e-mail services that don't deliver messages to an Exchange organization.

Important:
Replication of transport rules across an organization is dependent on Active Directory replication. Replication time between Active Directory domain controllers varies depending on the number of Active Directory sites in the organization, slow links, and other factors outside the control of Exchange. When deploying transport rules, consider replication delays.

For more information about Active Directory replication, see Active Directory Replication Technologies.

Edge Rules Agent

The Edge Rules agent processes transport rules on Edge Transport servers. It fires on the **EndOfData** transport event. The Edge Transport server, which serves as an e-mail gateway to and from external messaging systems, is the ideal place to apply messaging hygiene and policy to inbound Internet e-mail. Rules applied by the Edge Rules agent can reduce the total number of messages delivered to and processed by Hub Transport servers, and ultimately delivered to recipients. The agent can also help remove any harmful or objectionable message content. The following list provides some examples of how the Edge Rules agent can help you protect your organization.

- **Virus outbreaks** Thousands of new viruses, worms, and other types of malicious code are created each year. There's generally a lag between when such malware is noticed or reported, identified by antivirus software providers, an update created for the antivirus software, and then sent to customers. This causes a gap in protection during which an infected message can enter an organization undetected.
- **Denial of service attacks** Individuals who want to harm organizations may use denial of service (DoS) attacks, which can potentially result in deterioration, unavailability, or an outage of network services such as e-mail.

The Edge Rules agent is designed to help mitigate the impact of each of these risks.

Outbound Internet e-mail can also be subjected to similar policy-based scrutiny, and harmful or objectionable content can be prevented from leaving the organization. Additionally, message content can be checked to prevent sensitive information from being leaked outside the organization.

Transport rules configured on Edge Transport servers are stored in Active Directory Lightweight Directory Services (AD LDS), formerly known as Active Directory Application Mode (ADAM), on each Edge Transport server. Rules configured on one Edge Transport server aren't automatically replicated to other Edge Transport servers in your organization, with or without the use of EdgeSync. Depending on your requirements, you may want to configure each Edge Transport server with identical transport rules, or you may want to configure different transport rules on different Edge Transport servers that address the unique e-mail message traffic patterns of each server. To duplicate rule configuration, you can use the Export-TransportRuleCollection and Import-TransportRuleCollection cmdlets.

Return to top

Using Exchange Hosted Services

Transport messaging policies are enhanced by or are also available as a service from Microsoft Exchange Hosted Services.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

Return to top

1.11.3.2 Understanding How Transport Rules Are Applied

Understanding How Transport Rules Are Applied

Exchange Server 2010 > Messaging Policy and Compliance > Transport Rules >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-25*

In Microsoft Exchange Server 2010, transport rules allow you to apply messaging policies to messages in the transport pipeline. Actions such as redirecting a message or adding recipients, rights-protecting messages, and rejecting or silently deleting a message can be taken on messages that match the conditions and none of the exceptions defined in the rule.

Given the scope and potential impact of transport rules on messages, it's important to understand how transport rules work. To learn more about transport rules, see Understanding Transport Rules. For a comprehensive list of transport rule predicates and actions available on the Hub Transport server and Edge Transport server, see Transport Rule Predicates and Transport Rule Actions.

Looking for management tasks related to managing transport rules? Check out Managing Transport Rules.

Contents

Transport Rule Scope

Although the procedures used to create and modify transport rules on each server role are the same, the scope of transport rules on each server role is very different.

Transport rule scope

Transport component	Hub Transport server role	Edge Transport server role
Agent	Transport Rules agent	Edge Rules agent
Transport event	**OnRoutedMessage**	**EndOfData**
Rule storage	Active Directory domain controllers	Active Directory Lightweight Directory Services (AD LDS) (local)
Rule replication	Active Directory replication	No automated replication between Edge Transport servers
Rule scope	Entire Exchange organization	Local to each Edge Transport server
Message types	All messages except system messages	All messages
Lookup distribution group membership	Yes	No
Lookup Active Directory attributes	Yes	No
Inspect or modify Information Rights Management (IRM)-protected message content	Yes (requires transport decryption)	No

Rule Storage and Replication

The transport rules you create on a Hub Transport server are stored in Active Directory and are available after Active Directory replication on all Hub Transport servers in your Exchange 2010 organization. This allows you to apply a consistent set of rules across the entire Exchange organization.

Transport rules created on an Edge Transport server are stored in the local instance of AD LDS. No automated replication of configuration information or transport rules occurs between two Edge Transport servers. You can use distinct sets of transport rules on different Edge Transport servers. For example, if an organization uses a different set of Edge Transport servers for inbound and outbound messages to and from the Internet, different rules can be used on these servers. Rules created on the Edge Transport server apply only to messages that pass through that server. However, if applying the same set of transport rules on all Edge Transport servers is a requirement, you can also clone the Edge Transport server configuration, or export transport rules from one Edge Transport server and import it to other Edge Transport servers. For more details, see Understanding Edge Transport Server Cloned Configuration and Export and Import Transport Rules.

Message Types

On Edge Transport servers, rules apply to all messages. On Hub Transport servers, rules are applied to messages that meet the following criteria:

- **Messages sent by anonymous senders** Transport rules are applied to all messages received from anonymous senders. E-mail received from the Internet falls under this category.
- **Messages sent between authenticated users** Transport rules are applied to the following types of messages sent between authenticated users:
  - **Interpersonal messages** Interpersonal messages that contain a single rich

text format (RTF), HTML, or plain text message body or a multipart or alternative set of message bodies.

- **Encrypted e-mail messages** Messages that are encrypted using S/MIME. Transport rules can access envelope headers contained in encrypted messages and process messages based on predicates that inspect them. Rules with predicates that require inspection of message content, or actions that modify content, can't be processed.
- **Protected messages** Messages that are protected by applying an Active Directory Rights Management Services (AD RMS) rights policy template. With transport decryption enabled, the Transport Rules agent on a Hub Transport server can access the content of protected messages. Messages must be published using an AD RMS cluster in the same Active Directory forest as the Exchange 2010 server. With transport decryption disabled, the agent can't access message content and treats the message as an encrypted message.
- **Clear-signed messages** Messages that have been signed but not encrypted.
- **Unified messaging e-mail messages** Messages that are created or processed by the Unified Messaging server role, such as voice mail, fax, missed call notifications, and messages created or forwarded by using Microsoft Outlook Voice Access.
- **Read reports** Reports that are generated in response to read receipt requests by senders. Read reports have a message class of `IPM.Note*.MdnRead` or `IPM.Note*.MdnNotRead`.

Return to top

Transport Rule Replication

Transport rules configured on Hub Transport servers are applied to all messages handled by the Hub Transport servers in the Exchange 2010 organization. When a transport rule is created or an existing transport rule is modified or deleted on one Hub Transport server, the change is replicated to all Active Directory domain controllers in the organization. All the Hub Transport servers in the organization then read the new configuration from the Active Directory servers and apply the new or modified transport rules. By replicating transport rules across the organization, Exchange 2010 enables you to apply a consistent set of rules across the organization.

Important:

Replication of transport rules across an organization depends on Active Directory replication. Replication time between Active Directory domain controllers varies depending on the number of sites in the organization, slow links, and other factors outside the control of Exchange. When you configure transport rules in your organization, make sure that you consider replication delays. For more information about Active Directory replication, see Active Directory Replication Technologies.

Important:

Each Hub Transport server maintains a recipient cache that's used to look up recipient and distribution list information. The recipient cache reduces the number of requests that each Hub Transport server must make to an Active Directory domain controller. The recipient cache updates every four hours. You can't modify the recipient cache update interval. Therefore, changes to transport rule recipients, such as the addition or removal of distribution list members, may not be applied to transport rules until the recipient cache is updated. To force an immediate update of the recipient cache, you must stop and start the Microsoft Exchange Transport service. You must do this for each Hub Transport server where you want to forcibly update the recipient cache.

Note:

Each time the Hub Transport server retrieves a new transport rule configuration, an event is logged in the Security log in Event Viewer.

Transport rules configured on Edge Transport servers are applied only to the local server on which the transport rule was created. New transport rules and changes to existing transport rules affect only messages that pass through that specific Edge Transport server. If you have more than one Edge Transport server and you want to apply a consistent set of rules across all Edge Transport servers, you must either manually configure each server or export the transport rules from one server and import them into all other Edge Transport servers.

Return to top

Order in Which Transport Rules Are Applied

Transport rules are applied in the following order:

1. **Message scope** The first check performed by rules agents is whether a message falls within the scope of the agent. Transport rules aren't applied to all types of messages.
2. **Priority** For messages that fall within the scope of the rules agent, the agent starts processing rules based on rule priority in ascending order. Rules with lower priority are applied first. Transport rule priority values range from 0 to n–1, where n is the total number of transport rules. Only enabled rules are applied, regardless of priority. You can change the priority of rules using the Exchange Management Console or the Exchange Management Shell.
3. **Conditions** Transport rule conditions are made up of predicates.
4. **Rule with no conditions** A rule with no predicates and no exceptions is applied to all messages.
5. **Rule with multiple predicates** For a rule's action to be applied to a message, it must match all of the predicates selected in the rule. For example, if a rule uses the predicates **from a member of distribution list**, and **when the Subject field contains specific words**, the message must match both predicates. It must be sent by a member of the distribution list specified, and the message subject must contain the word specified.
6. **Predicate with multiple values** If one predicate allows entering multiple values, the message must match any value specified for that predicate. For example, if an e-mail message has the subject **Stock price information**, and the `SubjectContains` condition on a transport rule is configured to match the words **Contoso** and **stock**, the condition is satisfied because the subject contains at least one of the values of the condition.
7. **Exceptions** A rule isn't applied to messages that match any of the exceptions defined in the rule. Note, this is exactly opposite of how the rules agent treats predicates. For example, if the exceptions **except when the message is from people** and **except when the message contains specific words** are selected, the message fails to match the rule condition if the message is sent from any of the specified senders, or if the message contains any of the specified words.
8. **Actions** Messages that match the rules conditions get all actions specified in the rule applied to them. For example, if the actions **prepend the subject with string** and **Blind carbon copy (Bcc) the message to addresses** are selected, both actions are applied to the message. The message will get the specified string prefixed to the message subject, and the recipients specified will be added as Bcc recipients.

Note:

Some actions, such as the **Delete the message without notifying anyone** action, prevent subsequent rules from being applied to a message.

Return to top

Transport Rules and Group Membership

When you define a transport rule using a predicate that expands membership of a distribution group, the resulting list of recipients is cached by the Hub Transport server that applies the rule. This is known as the *Expanded Groups Cache* and is also used by the Journaling agent for evaluating group membership for journal rules. By default, the Expanded Groups Cache stores group membership for four hours. Recipients returned by the recipient filter of a dynamic distribution group are also stored. The Expanded Groups Cache makes repeated round-trips to Active Directory and the resulting network traffic from resolving group memberships unnecessary.

In Exchange 2010, this interval and other parameters related to the Expanded Groups Cache are configurable. You can lower the cache expiration interval, or disable caching altogether, to ensure group memberships are refreshed more frequently. You must plan for the corresponding increase in load on your Active Directory domain controllers for distribution group expansion queries. You can also clear the cache on a Hub Transport server by restarting the Microsoft Exchange Transport service on that server. You must do this on each Hub Transport server where you want to clear the cache. When creating, testing, and troubleshooting transport rules that use predicates based on distribution group membership, you must also consider the impact of Expanded Groups Cache.

Note:

The Expanded Groups Cache isn't used by the categorizer to resolve recipients for message delivery.

Return to top

1.11.3.3 Transport Rule Predicates

Transport Rule Predicates

Exchange Server 2010 > Messaging Policy and Compliance > Transport Rules >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-22*

In Microsoft Exchange Server 2010, predicates are used to create conditions and exceptions in a transport rule. Transport rules can be applied to e-mail messages routed through Hub Transport and Edge Transport servers. Some predicates are available on both transport server roles, and some are exclusive to just one transport server role.

Contents

Predicates and Predicate Properties

Transport rule conditions and exceptions consist of one or more predicates. Predicates instruct the Transport Rules agent on a Hub Transport server (or the Edge Rules agent on an Edge Transport server) to examine a specific part of an e-mail message, such as sender, recipients, subject, other message headers, and message body, to determine whether the rule should be applied to that message. As such, predicates act as building blocks for conditions and exceptions.

To determine whether a transport rule should be applied to a message, most predicates have one or more properties for which you must specify a value. The Transport Rules agent inspects message properties for specified values. For example, the **HasClassification** predicate requires that you specify one or more message classifications for the classification property. Some predicates don't have properties. For example, the **HasNoClassification** predicate simply inspects whether a message has a classification, and therefore doesn't require any values.

To assign a value to a predicate, you must determine the predicate property or properties in the case of predicates that require more than one property. In the Exchange Management Console (EMC), you can specify predicate values in the **Edit the rule description by clicking an underlined value** box of the New Transport Rule or Edit Transport Rule wizards. In the Exchange Management Shell the properties are available as parameters of the New-TransportRule and Set-TransportRule cmdlets. Property values are specified after the property name.

Note:

In Exchange 2010, you don't need to instantiate predicates and actions by using the Get-TransportRulePredicate and Get-TransportRuleAction cmdlets. These cmdlets only allow you to list the predicates and actions available for use on the Hub Transport and Edge Transport servers on which the cmdlets are executed. The **New-TransportRule** and **Set-TransportRule** cmdlets have all the predicates and actions available as parameters, allowing you to create or modify a transport rule using a single command.

Because some predicates examine specific fields within an e-mail message (such as the message header fields), you must set two predicate properties. When you use a predicate to inspect message headers, one predicate property specifies the header to examine, such as To, From, Received, or Content-Type. You must also specify a value for the second property. Predicates that require a second property are listed in Table 1 and Table 2, with the second property listed in the **Second predicate property** column.

Return to top

Predicates Available on Hub Transport Servers

Table 1 lists the predicates available on a Hub Transport server, and provides the following information about each predicate:

- The **Predicate** column lists the predicate as it appears in the New Transport Rule and Edit Transport Rule wizards in the EMC.
- The **Predicate name** column lists the predicate name as returned by the Get-TransportRulePredicate cmdlet.
- The **Predicate property** and **Second predicate property** columns list the property types. Most property types accept specific values. Refer to Table 3 to determine valid values for a property type.

Note:

Each predicate listed in Table 1 also has an equivalent exception that can be selected

from the **Exceptions** page of the New Transport Rule and Edit Transport Rule wizards. In the Shell, the predicates that can be used as exceptions start with **ExceptIf**. For example, for the **FromMemberOf** predicate, the parameter that can be used as an exception in transport rule cmdlets is called *ExceptIfFromMemberOf*.
The same predicate object contains the logic for use in a transport rule condition and exception. Therefore, when you use the **Get-TransportRulePredicate** cmdlet to list predicates, exceptions aren't listed as separate predicates.

Table 1 Predicates available on Hub Transport servers

No	Predicate	Predicate name	Predicate property	Second predicate property	Description
1	**from people**	From	Addresses	Not applicable	From matches messages sent by the specified mailboxes, mail-enabled users, or contacts. **Note:** You can't specify a distribution group by using this predicate. If you need to create a rule that takes action on messages sent to a distribution group, use the "when any of the recipients in the To field is people" (AnyOfToHeader) predicate instead. The AnyOfToHeader predicate compares the actual values of the headers in the message. This differs from the SentTo type of predicates that compare the resolved set of recipients, including recipients found from group

					expansions.
2	**from a member of distribution list**	FromMemberOf	Addresses	Not applicable	`FromMemberOf` matches messages where the sender is a member of the specified distribution group.
3	**from users that are inside or outside the organization**	FromScope	FromUserScope	Not applicable	`FromScope` matches messages that are sent by senders within the specified scope.
4	**sent to people**	SentTo	Addresses	Not applicable	`SentTo` matches messages where one of the recipients is the specified mailbox, mail-enabled user, or contact. The specified recipients can be listed in the **To**, **Cc**, or **Bcc** fields. **Note:** You can't specify a distribution group by using this predicate. If you need to create a rule that takes action on messages sent to a distribution group, use the "when any of the recipients in the To field is people" (AnyOfToHeader) predicate instead. The AnyOfToHeader predicate compares the

					actual values of the headers in the message. This differs from the SentTo type of predicates that compare the resolved set of recipients, including recipients found from group expansions.
5	**sent to a member of distribution list**	SentToMemberOf	Addresses	Not applicable	`SentToMemberOf` matches messages that contain recipients who are members of the specified distribution group. The recipients can be listed in the **To**, **Cc**, or **Bcc** fields.
6	**sent to users that are inside or outside the organization, or partners**	SentToScope	ToUserScope	Not applicable	`SentToScope` matches messages that are sent to recipients within the specified scope.
7	**between members of distribution list and distribution list**	BetweenMemberOf	Addresses (`BetweenMemberOf1`)	Addresses (`BetweenMemberOf2`)	`BetweenMemberOf` matches messages that are sent between members of two distribution groups.
8	**when the manager of any sender is people**	ManagerIs	EvaluatedUser (`ManagerForEvaluatedUser`)	Addresses (`ManagerAddresses`)	`ManagerIs` matches messages where the specified user's (sender or recipient) manager exists in the list of specified addresses.
9	**when the**	ManagementR	ManagementR	Not applicable	`ManagementRe`

	sender is the manager of a recipient	elationship	elationship (SenderManagementRelationship)		lationship matches messages where the sender has the specified management relationship with a recipient.
10	**if the sender and recipient's AD Attribute are Evaluation**	ADAttributeComparison	ADAttribute (ADComparisonAttribute)	Evaluation (ADComparisonOperator)	ADAttributeComparison matches messages where the sender's specified Active Directory attribute matches or doesn't match (as specified in the **Evaluation** property) the same attribute of any recipient.
11	**when a recipient's address contains specific words**	RecipientAddressContainsWords	Words	Not applicable	RecipientAddressContainsWords matches messages where a recipient's address contains any of the specified words.
12	**when a recipient's address contains text patterns**	RecipientAddressMatchesPatterns	Patterns	Not applicable	RecipientAddressMatchesPatterns matches messages where a recipient's address matches a specified regular expression.
13	**when a recipient's properties contains specific words**	RecipientAttributeContains	Words* (RecipientADAttributeContainsWords)	Not applicable	RecipientAttributeContains matches messages where the specified attribute of a recipient

					contains a specified string.
14	**when a recipient's properties contains text patterns**	RecipientAttributeMatches	Patterns* (RecipientADAttributeMatchesPatterns)	Not applicable	RecipientAttributeMatches matches messages where the specified attribute of a recipient matches a regular expression.
15	**when any of the recipients in the To field is people**	AnyOfToHeader	Addresses	Not applicable	AnyOfToHeader matches messages where the **To** field includes any of the specified recipients.
16	**when any of the recipients in the "To" field is a member of distribution list**	AnyOfToHeaderMemberOf	Addresses	Not applicable	AnyOfToHeaderMemberOf matches messages where the **To** field contains a recipient who is a member of the specified distribution group.
17	**when any of the recipients in the Cc field is people**	AnyOfCcHeader	Addresses	Addresses	AnyOfCcHeader matches messages where the **Cc** field includes any of the specified recipients.
18	**when any of the recipients in the Cc field is member of distribution list**	AnyOfCcHeaderMemberOf	Addresses	Not applicable	AnyOfCcHeaderMemberOf matches messages where the **Cc** field contains a recipient who is a member of the specified distribution group.
19	**when any of the recipients in the To or Cc fields is**	AnyOfToCcHeader	Addresses	Not applicable	AnyOfToCcHeader matches messages where the **To**

	people				or **Cc** fields include any of the specified recipients.
20	**when any of the recipients in the To or CC fields is a member of a distribution list**	AnyOfToCcHeaderMemberOf	Addresses	Not applicable	`AnyOfToCcHeaderMemberOf` matches messages where the **To** or **Cc** fields contains a recipient who is a member of the specified distribution group.
21	**marked with classification**	HasClassification	Classification	Not applicable	`HasClassification` matches messages that have the specified classification.
22	**when the Subject field contains specific words**	SubjectContains	Words	Not applicable	`SubjectContains` matches messages that have the specified words in the **Subject** field.
23	**when the Subject field or message body contains specific words**	SubjectOrBodyContains	Words	Not applicable	`SubjectOrBodyContains` matches messages that have the specified words in the **Subject** field or message body.
24	**when the message header contains specific words**	HeaderContains	MessageHeader (`HeaderContainsMessageHeader`)	Words (`HeaderContainsWords`)	`HeaderContains` matches messages where the specified message header contains the specified value.
25	**when the From address contains specific words**	FromAddressContains	Words (`FromAddressContainsWords`)	Not applicable	`FromAddressContains` matches messages that contain the specified words in the **From** field.

26	**when the Subject field contains text patterns**	SubjectMatches	Patterns (SubjectMatchesPatterns)	Not applicable	SubjectMatches matches messages where text patterns in the **Subject** field match a specified regular expression.
27	**when the Subject field or the message body contains text patterns**	SubjectOrBodyMatches	Patterns (SubjectOrBodyMatchesPatterns)	Not applicable	SubjectOrBodyMatches matches messages where text patterns in the **Subject** field or message body match a specified regular expression.
28	**when the message header matches text patterns**	HeaderMatches	MessageHeader (HeaderMatchesMessageHeader)	Patterns (HeaderMatchesPatterns)	HeaderMatches matches messages where the specified message header contains a text pattern that matches a specified regular expression.
29	**when the From address matches text patterns**	FromAddressMatches	Patterns (FromAddressMatchesPatterns)	Not applicable	FromAddressMatches matches messages that contain text patterns in the **From** field that match a specified regular expression.
30	**when any attachment file name matches text patterns**	AttachmentNameMatches	Patterns (AttachmentNameMatchesPatterns)	Not applicable	AttachmentNameMatches matches messages that contain text patterns in an attachment that matches a specified regular

					expression.
31	**with a spam confidence level (SCL) rating that is greater than or equal to limit**	SCLOver	SclValue	Not applicable	`SCLOver` matches messages that are assigned a spam confidence level (SCL) matching or exceeding the specified value.
32	**when the size of any attachment is greater than or equal to limit**	AttachmentSizeOver	Size	Not applicable	`AttachmentSizeOver` matches messages that contain attachments larger than the specified value.
33	**marked with importance**	WithImportance	Importance	Not applicable	`WithImportance` matches messages marked with the specified priority.
34	**if the message is Message Type**	MessageTypeMatches	MessageType	Not applicable	`MessageTypeMatches` matches messages of the specified type.
35	**when the sender's properties contain specific words**	SenderAttributeContains	Words* (`SenderADAttributeContainsWords`)	Not applicable	`SenderAttributeContains` matches messages where the specified attribute of the sender matches a specified string.
36	**when the sender's properties match text patterns**	SenderAttributeMatches	Patterns (`SenderADAttributeMatchesPatterns`)	Not applicable	`SenderAttributeMatches` matches messages where the specified attribute of the sender contains text patterns that match a specified regular expression.

37	**not marked with a message classification**	HasNoClassifications	Not applicable	Not applicable	`HasNoClassifications` matches messages that don't have a message classification.
38	**when an attachment's content contains words**	AttachmentContainsWords	Words	Not applicable	`AttachmentContainsWords` matches messages with attachments that contain a specified string.
39	**when an attachment's content matches text patterns**	AttachmentMatchesPatterns	Patterns	Not applicable	`AttachmentMatchesPatterns` matches messages with attachments that contain a text pattern that matches a specified regular expression.
40	**when an attachment is unsupported**	AttachmentIsUnsupported	Not applicable	Not applicable	`AttachmentIsUnsupported` matches messages with attachments that aren't supported.

Return to top

Predicates Available on Edge Transport Servers

Table 2 lists the predicates available on Edge Transport servers.

Note:

Each predicate listed in Table 1 also has an equivalent exception that can be selected from the **Exceptions** page of the New Transport Rule and Edit Transport Rule wizards. In the Shell, the predicates that can be used as exceptions start with `ExceptIf`. For example, for the `FromMemberOf` predicate, the parameter that can be used as an exception in transport rule cmdlets is called *ExceptIfFromMemberOf*.
The same predicate object contains the logic for use in a transport rule condition and exception. Therefore, when you use the **Get-TransportRulePredicate** cmdlet to list predicates, exceptions aren't listed as separate predicates.

Predicates available on Edge Transport servers

No	Predicate	Predicate name	Predicate property	Second predicate property	Description

1	**when the subject field contains specific words**	SubjectContains	Words	Not applicable	`SubjectContains` matches messages that contain the specified words in the **Subject** field.
2	**when the subject field or message body contains specific words**	SubjectOrBodyContains	Words	Not applicable	`SubjectOrBodyContains` matches messages that contain the specified words in the **Subject** field or message body.
3	**when the message header contains specific words**	HeaderContains	MessageHeader	Words	`HeaderContains` matches messages where the value of the specified message header contains the specified words.
4	**when the From address contains specific words**	FromAddressContains	Words	Not applicable	`FromAddressContains` matches messages that contain the specified words in the **From** field.
5	**when any recipient address contains specific words**	AnyOfRecipientAddressContainsWords	Words	Not applicable	`AnyOfRecipientAddressContains` matches messages that contain the specified words in the **To**, **Cc**, or **Bcc** fields of the message.
6	**when the Subject field matches text patterns**	SubjectMatches	Patterns	Not applicable	`SubjectMatches` matches messages where text patterns in the **Subject** field match a specified regular

					expression.
7	**when the Subject field or the message body matches text patterns**	SubjectOrBodyMatches	Patterns	Not applicable	`SubjectOrBodyMatches` matches messages where text patterns in the **Subject** field or message body match a specified regular expression.
8	**when the message header matches text patterns**	HeaderMatches	MessageHeader	Patterns	`HeaderMatches` matches messages where the specified message header field contains text patterns that match a specified regular expression.
9	**when the From address matches text patterns**	FromAddressMatches	Patterns	Not applicable	`FromAddressMatches` matches messages that contain text patterns in the **From** field of the messages that match a specified regular expression.
10	**when any recipient address matches text patterns**	AnyOfRecipientAddressMatches	Patterns	Not applicable	`AnyOfRecipientAddressMatches` matches messages where text patterns in the **To**, **Cc**, or **Bcc** fields of the message match a specified regular expression.
11	**with a spam confidence**	SCLOver	SclValue	Not applicable	`SclOver` matches

	level (SCL) rating that is greater than or equal to limit				messages with an SCL that's equal to or greater than the value specified.
12	**when the size of any attachment is greater than or equal to limit**	AttachmentSizeOver	Size	Not applicable	`AttachmentSizeOver` matches messages that contain attachments larger than the specified value.
13	**From users that are inside or outside the organization**	FromScope	Scope	Not applicable	`FromScope` matches messages that are sent from the specified scope.

Return to top

Predicate Properties

The following table lists the property types used in transport rule predicates.

Table 3 Property types used in transport rule predicates

Predicate	Name	Description
ADAttribute	One of the Active Directory attributes available for use	The `ADAttribute` predicate accepts the name of one of the following Active Directory attributes available for use with this property type in transport rules: • `DisplayName` • `FirstName` • `Initials` • `LastName` • `Office` • `PhoneNumber` • `OtherPhoneNumber` • `Email` • `Street` • `POBox` • `City` • `State` • `ZipCode` • `Country` • `UserLogonName` • `HomePhoneNumber` • `OtherHomePhoneNumber`

		• PagerNumber • MobileNumber • FaxNumber • OtherFaxNumber • Notes • Title • Department • Company • Manager • CustomAttribute1 - CutomAttribute15 When you use the Shell to create a transport rule consisting of the RecipientAddressContains or RecipientAddressMatches predicates, you must specify an attribute name from the preceding list followed by a colon (:) and the word or text pattern you want to match in the specified attribute. The entire notation should be enclosed in quotation marks ("). For example, to specify the attribute City and the values San Francisco or Palo Alto, you must use City:San Francisco, Palo Alto. You can also specify multiple Active Directory attributes and value pairs. For example, "City:San Francisco, Palo Alto","Department:Sales, Finance". In this case, the recipient's City attribute should contain either San Francisco or Palo Alto, and the Department attribute should contain either Sales or Finance.
Addresses and Addresses2	Array of Active Directory mailbox, contact, or distribution group objects	The Addresses and Addresses2 predicates accept a single mailbox, contact, mail-enabled user, or distribution group object.
Classification	Message classification object	The Classification predicate accepts a message classification object. To specify a message classification object, you must use the Get-MessageClassification cmdlet. For example, use the following command to search for messages with the ExCompanyInternal classification and prepend the message subject with

		CompanyInternal. `New-TransportRule "Rule Name" -HasClassification @(Get-MessageClassification ExCompanyInternal).Identity -PrependSubject "CompanyInternal"`
EvaluatedUser	Single value of `Sender` or `Recipient`	The `ManagementRelationship` predicate accepts an `EvaluatedUser` value for the `ManagerForEvaluatedUser` property. It instructs the Transport Rules agent whether the predicate should inspect a message's sender or the recipient.
Evaluation	Single value of `Equal` or `NotEqual`	The `ADAttributeComparison` predicate accepts a value of type `Evaluation` for the `ADComparisonOperator` property. This allows you to compare the specified Active Directory attribute values for the sender and recipient.

FromUserScope	Single value of `InOrganization` or `NotInOrganization`	The `FromScope` predicate accepts a scope value of type `FromUserScope`. This specifies whether the message is sent by a sender who is considered to be inside the organization. The following values can be used:
		• **InOrganization** A sender is considered to be inside the organization if either of the following conditions is true:
		  • The sender is a mailbox, mail-enabled user, distribution group, or public folder that exists in the organization's Active Directory.
		  • The domain of the sender is an accepted domain in the Exchange organization, but isn't an `ExternalRelay` domain. Also, the message must be sent or received by using an authenticated connection.

		Note: To determine whether mail contacts are considered to be inside or outside the organization, the domain part of the sender's address is compared with the configured accepted domains. For more information, see Understanding Accepted Domains • **NotInOrganization** A sender is considered to be outside the organization if the sender's domain isn't an accepted domain in the Exchange organization and is an `ExternalRelay` domain.
Importance	Single value of `High`, `Low`, or `Normal`	The `Importance` predicate accepts the message priority.
ManagementRelationship	Single value of `Manager` or `DirectReport`	The `ManagementRelationship` predicate specifies the relationship between two evaluated users, for example the sender and the recipient. The evaluated user's Active Directory information is located to determine the manager and direct reports.
MessageHeader	Single string	The `MessageHeader` predicate accepts a string that can be used to specify the SMTP message header to examine. This property is used together with the `Words` or `Patterns` properties, which specify the value of the header field to match. You don't need to add a colon (`:`) in the header name.
MessageType	Single message type name	The `MessageType` predicate accepts one of the following message types: • OOF • AutoAccept • AutoForward • Encrypted • Calendaring • PermissionControlled • Voicemail • RSS • Signed • ApprovalRequest • ReadReceipt
Patterns	Array or regular expressions	The `Patterns` predicate accepts a regular expression that can be

		used to match text that follows an identifiable pattern. Enclose the expression in quotation marks ("). For more information, see Regular Expressions in Transport Rules.
SclValue	Single integer	The `SclValue` predicate accepts an integer that can be used to match the spam confidence level (SCL) assigned to a message. SCL values range from -1 through 9.
Size	Single integer with quantifier such as KB or MB	The `Size` predicate accepts an integer that specifies the size of an e-mail attachment. When using the EMC, the value specified is in kilobytes. When using the Shell, you can enter an integer value qualified by one of the following units: • B (bytes) • KB (kilobytes) • MB (megabytes) • GB (gigabytes) For example, `20MB`
ToUserScope	One of the following values: • `InOrganization` • `NotInOrganization` • `ExternalPartner` • `ExternalNonPartner`	The `SentToScope` predicate accepts a scope value of type `ToUserScope`. The `InOrganization` and `NotInOrganization` values are evaluated similar to the `FromUserScope` property, but in the context of the recipient. The following is a description of the other possible values: • **ExternalPartner** These domains are configured to send mail to an external domain by using Domain Secure security • **ExternalNonPartner** These represent all other domains that aren't considered `ExternalPartner` domains.
Words	Array of strings	The `Words` property accepts one string or an array of strings. It's used in all predicates that inspect different parts of a message for specific words or strings. In Exchange 2010, only instances of the word without a prefix or suffix are matched. For example, if you specify the word "contoso",

		the rule will fire only if an exact match is found. The following variations where the word appears as a suffix, a prefix, or between other characters (other than the space character) aren't considered an exact match: • Acontoso • Contosoa • Acontosob The property isn't case-sensitive. The asterisk (*) is treated as a literal character, and not used as a wildcard character.

Return to top

1.11.3.4 Transport Rule Actions

Transport Rule Actions

Exchange Server 2010 > Messaging Policy and Compliance > Transport Rules >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-22*

Transport rule actions instruct the rules agent to take the specified action on messages that match all the predicates in a condition, and don't match any of the exceptions. In Microsoft Exchange Server 2010, both the Hub Transport server and Edge Transport server can apply transport rules to e-mail messages routed by them. Some actions are available on both transport server roles, and some are exclusive to either role.

Each action affects e-mail messages in a unique way. For example, an action can cause an e-mail message to be redirected to another address or to be deleted. Each action consists of the action itself, its action property, and the value of the property.

To assign a value to an action, you must determine the available action property for a specific action. For example, you must use the `Address` action property together with the `RedirectMessage` action. (For information about the action properties available for use with Hub Transport servers and Edge Transport servers, see the tables later in this topic.)

Some actions require that you set two or more action properties, because some actions modify specific fields within sections of an e-mail message, such as the message header fields. When you specify an action to modify a message header, one action property specifies the specific header field to modify, and a second action property specifies the new value of the message header. In these cases, you must also specify a value for the second action property, as shown later in this topic in the **Additional action property** table column in either Actions Available on a Hub Transport Server or Actions Available on an Edge Transport Server, depending on the server role. For example, you can configure an action to modify the **X-Test-Message-Source** header field to a specific string, such as `contoso.com`.

You can use either the Exchange Management Console or the Exchange Management Shell to create or modify a transport rule. For relevant procedures, see Transport Rules.

Contents

Actions Available on a Hub Transport Server

The following table lists the actions that can be used with transport rules on a server running Exchange 2010 that has the Hub Transport server role installed. The transport rule action LogEvent isn't available on Exchange 2010 Hub Transport servers.

Transport rule actions available on Hub Transport servers

Supported rule action	Action name	First action property	Additional action property	Description
prepend the subject with string	PrependSubject	Prefix	Not applicable	PrependSubject prepends a string to the start of the Subject field of the message.
apply message classification	ApplyClassification	Classification	Not applicable	ApplyClassification applies a message classification to the e-mail message. For more information, see Understanding Message Classifications.
append disclaimer text and fallback to action if unable to apply	ApplyHtmlDisclaimer	ApplyHtmlDisclaimerLocation	ApplyHtmlDisclaimerText, ApplyHtmlDisclaimerFallbackAction	ApplyHtmlDisclaimer applies an HTML disclaimer to the message. For more information, see Understanding Disclaimers.
rights protect message with RMS template	RightsProtectMessage	RMSTemplateIdentity	Not applicable	RightsProtectMessage applies the specified Rights Management Services (RMS) template to the

				message. For more information, see Understanding Transport Protection Rules.
set the spam confidence level to value	SetScl	SclValue	Not applicable	SetScl sets the spam confidence level (SCL) on an e-mail message. For more information, see Understanding Spam Confidence Level Threshold.
set header with value	SetHeader	MessageHeader	HeaderValue	SetHeader creates a new message header field or modifies an existing message header field.
remove header	RemoveHeader	MessageHeader	Not applicable	RemoveHeader removes the specified message header field from a message.
add a recipient in the To field addresses	AddToRecipient	Addresses	Not applicable	AddToRecipient adds one or more recipients to the To field of the message. The original recipients can see the additional address.
copy the message to addresses	CopyTo	Addresses	Not applicable	CopyTo adds one or more recipients to the carbon copy (Cc) field of the message. The original recipients can see the Cc address.
Blind carbon copy (Bcc) the message to addresses	BlindCopyTo	Addresses	Not applicable	BlindCopyTo adds one or more recipients as blind carbon copy (Bcc) recipients. The original recipients aren't notified and can't see the Bcc addresses.
add the sender's	AddManagerAsR	AddedRecipien	Not applicable	AddManagerAsRe

manager as a specific recipient type	ecipientType	tType		cipientType adds the sender's manager, if defined in the manager attribute in Active Directory, as the specified recipient type.
forward the message to addresses for moderation	ModerateMessageByUser	Addresses	Not applicable	ModerateMessageByUser forwards the message to the specified moderators as an attachment wrapped in an approval request. For more information, see Understanding Moderated Transport.
forward the message to the sender's manager for moderation	ModerateMessageByManager	Not applicable	Not applicable	ModeratedMessageByManager forwards the message to the sender's manager for moderation, if the manager attribute is populated in Active Directory. **Important:** If the sender's manager attribute isn't populated in Active Directory, the message is delivered to recipients without moderation. This action doesn't require any action properties.
redirect the message to addresses	RedirectMessage	Addresses	Not applicable	RedirectMessage redirects the e-mail message to one or more recipients specified by the administrator. The message isn't delivered to the original recipients, and no notification is sent to the

				sender or the original recipients.
send rejection message to sender with enhanced status code	RejectMessage	RejectReason	EnhancedStatusCode	RejectMessage deletes the e-mail message and sends a non-delivery receipt to the sender. The recipient doesn't receive the message or notification.
Delete the message without notifying anyone	DeleteMessage	Not applicable	Not applicable	DeleteMessage deletes the e-mail message without sending a notification to either the recipient or the sender.

Return to top

Actions Available on an Edge Transport Server

The following table lists the actions that can be used with transport rules on Exchange 2010 Edge Transport servers.

Transport rule actions available on Edge Transport servers

Supported rule action	Action name	First action property	Additional action property	Description
log an event with message	LogEvent	EventMessage	Not applicable	LogEvent inserts an event into the Application log of the local computer.
prepend the subject with string	PrependSubject	Prefix	Not applicable	PrependSubject prepends a string to the start of the e-mail message subject field.
set the spam confidence level to value	SetScl	SclValue	Not applicable	SetScl configures the SCL on an e-mail message.
set header with value	SetHeader	MessageHeader	HeaderValue	SetHeader creates a new message header field or modifies an existing message header field.

remove header	RemoveHeader	MessageHeader	Not applicable	RemoveHeader removes the specified message header field from an e-mail message.
add a recipient in the To field addresses	AddToRecipient	Addresses	Not applicable	AddToRecipient adds one or more e-mail addresses to the To address list of the e-mail message. The original recipients can see the additional address.
copy the message to addresses	CopyTo	Addresses	Not applicable	CopyTo adds one or more e-mail addresses to the Cc field of the e-mail message. The original recipients can see the original address.
Blind carbon copy (Bcc) the message to addresses	BlindCopyTo	Addresses	Not applicable	BlindCopyTo adds one or more e-mail addresses to the Bcc address list of the e-mail message. The original recipients aren't notified and can't see the additional address.
drop connection	Disconnect	Not applicable	Not applicable	Disconnect ends the connection between the sending server and the Edge Transport server without generating an NDR message.
redirect the message to addresses	RedirectMessage	Addresses	Not applicable	RedirectMessage redirects the e-mail message to one or more e-mail addresses specified by the administrator. The message isn't delivered to the original recipient, and no notification

				is provided to the recipient or the sender.
Put message in spam quarantine mailbox	`Quarantine`	Not applicable	Not applicable	`Quarantine` redirects the e-mail message to the spam quarantine mailbox configured by using the *QuarantineMailbox* parameter on the **Set-ContentFilterConfig** cmdlet. **Important:** The *QuarantineMailbox* parameter on the **Set-ContentFilterConfig** cmdlet must be populated, and the specified mailbox must exist before you configure the **Put message in spam quarantine mailbox** action. If the *QuarantineMailbox* parameter isn't populated or if the quarantine mailbox doesn't exist, messages sent to the quarantine mailbox will be lost and an NDR will be generated. For more information about the spam quarantine mailbox, see Understanding Spam Quarantine.
reject the message with status code and response	`SmtpRejectMessage`	`StatusCode`	`RejectReason`	`SmtpRejectMessage` deletes the e-mail message and sends a notification to the sender. The recipients don't

				receive the message or notification. This action enables you to specify a specific delivery status notification (DSN) code. For more information about DSNs, see Managing Delivery Status Notifications.
Delete the message without notifying anyone	DeleteMessage	Not applicable	Not applicable	DeleteMessage deletes the e-mail message without sending a notification to either the recipient or the sender.

Return to top

Action Properties for Transport Rules on a Hub Transport or an Edge Transport Server

The following table lists the action properties used by transport rules actions on Exchange 2010 Hub Transport or Edge Transport servers.

Action properties for transport rules on a Hub Transport server or an Edge Transport server

Action property	Expected format	Description
AddedRecipientType	One of the following values: • **To** • **Cc** • **Bcc** • **Redirect**	AddedRecipientType accepts a single value: • To, Cc, and Bcc values are self-explanatory and correspond to the addressing fields of e-mail messages. • Redirect delivers the message only to the specified recipient. The message isn't delivered to any of the original recipients.
Addresses	• **Edge Transport server** Array of SMTP addresses • **Hub Transport server**	On an Edge Transport server, Addresses accepts an array of SMTP addresses that are each enclosed in quotation marks (").

	Array of Active Directory mailbox, contact, mail-enabled user, or distribution group objects	On a Hub Transport server, `Addresses` accepts an array of mailbox, contact, mail-enabled user, or distribution group objects.
`Classification`	Single message classification object	`Classification` accepts a single message classification object. To specify a message classification object, use the Get-MessageClassification cmdlet. For more information about message classifications, see Understanding Message Classifications.
`DisclaimerLocation`	One of the following values: • Append • Prepend	`DisclaimerLocation` specifies where the disclaimer is inserted into the e-mail message: • `Append` (default) adds the disclaimer at the bottom of the message thread. • `Prepend` puts the disclaimer at the start of the newest e-mail message.
`EnhancedStatusCode`	Single DSN code of `5.7.1`, or any value from `5.7.10` through `5.7.999`	`EnhancedStatusCode` specifies the DSN code and related DSN message to display to the senders of messages rejected by the `RejectMessage` transport rule action. The DSN message associated with the specified DSN status code is displayed in the user information portion of the NDR displayed to the sender. The specified DSN code must be an existing default DSN code or a customized DSN status code that you can create by using the **New-SystemMessage** cmdlet.
`EventMessage`	Single string	`EventMessage` accepts a single string displayed in an event log, which is added to the application event log on the local computer.
`FallbackAction`	Single value with the choices of `Wrap`, `Ignore`, or `Reject`	`FallbackAction` specifies what the transport rule should do if a disclaimer can't be applied to an e-mail message such as when a message is encrypted. The default fallback action is `Wrap`. Enclose the value in quotation marks ("). The following list shows each fallback action and its description:

		• **Wrap** If the disclaimer can't be inserted into the original message, Exchange encloses, or *wraps*, the original message in a new message envelope. Then the disclaimer is inserted into the new message. **Important:** If an original message is wrapped in a new message envelope, subsequent transport rules are applied to the new message envelope, and not to the original message. Therefore, you must configure transport rules with disclaimer actions that wrap original messages in a new message body after you configure other transport rules. **Note:** If the original message can't be wrapped in a new message envelope, the original message isn't delivered. The sender of the message receives an NDR that explains why the message wasn't delivered. • **Ignore** If the disclaimer can't be inserted into the original message, Exchange lets the original message continue unmodified. No disclaimer is added. • **Reject** If the disclaimer can't be inserted into the original message, Exchange doesn't deliver the message. The sender of the message receives an NDR that explains why

		the message wasn't delivered.
HeaderValue	Single string	HeaderValue accepts a single string that's applied to the header specified by using the MessageHeader action property. Enclose the string in quotation marks (").
MessageHeader	Single string	MessageHeader accepts a string that specifies which MessageHeader to add or modify. The string that's specified by using the HeaderValue action property is inserted into the header that's specified by MessageHeader. Enclose the string in quotation marks (").
Prefix	Single string	Prefix accepts a string that's prepended to the subject of the e-mail message. Enclose the string in quotation marks ("). To prevent the string that's specified with the Prefix transport rule action from being added to the subject every time that a reply to the message encounters the transport rule, add the SubjectContains exception to the transport rule. The SubjectContains exception should contain the string that you specified with the Prefix transport rule action. If you add the SubjectContains exception to the transport rule, the transport rule doesn't add another instance of the Prefix string to the subject if the Prefix string already appears in the subject.
RejectReason	Single string	RejectReason accepts a string that's used to populate the administrator information portion of the NDR returned to the e-mail sender if an e-mail message is rejected. Enclose the string in quotation marks (").
RMSTemplateIdentity	RMS Template identity	RMSTemplateIdentity accepts an RMS Template identity. You can get a list of RMS templates available on an Active Directory RMS server in the Active Directory forest using the **Get-**

		RMSTemplate cmdlet.
`SclValue`	Single integer	`SclValue` accepts a single integer from 0 through 9, which is used to configure the SCL of the e-mail message. Enclose the integer in quotation marks (").

Return to top

For More Information

Understanding Transport Rules

Transport Rule Predicates

Configure a Disclaimer

Regular Expressions in Transport Rules

1.11.3.5 Regular Expressions in Transport Rules

Regular Expressions in Transport Rules

Exchange Server 2010 > Messaging Policy and Compliance > Transport Rules >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-11-21*

You can use regular expressions in Microsoft Exchange Server 2010 transport rule predicates to match text patterns in different parts of a message (such as message headers, sender, recipients, message subject, and body). Predicates are used by conditions and exceptions to determine whether a configured action should be applied to an e-mail message.

Looking for management tasks related to transport rules? See Managing Transport Rules.

Contents

Simple Expressions vs. Regular Expressions

To understand regular expressions, you must first understand simple expressions. A *simple expression* is a specific value that you want to match exactly in a message. Predicates using simple expressions match specific words or strings. An example of a simple expression is the title of a document that your organization doesn't want to be distributed outside the organization, such as Yearly Sales Forecast.doc. A piece of data in

an e-mail message must exactly match a simple expression to satisfy a condition or exception in transport rules.

A *regular expression* is a concise and flexible notation for finding patterns of text in a message. The notation consists of two basic character types:

- **Literal characters** Text that must exist in the target string. These are normal characters, as typed.
- **Metacharacters** One or more special characters that aren't interpreted literally. These indicate how the text can vary in the target string.

You can use regular expressions to quickly parse e-mail messages to find specific text patterns. This enables you to detect messages with specific types of content, such as social security numbers (SSNs), patent numbers, and phone numbers.

You can't reasonably match this data with a simple expression because a simple expression requires that you enter every possible variation of the value that you want to detect. In many cases, using simple expressions for such applications becomes a logistical challenge, and matching a large number of simple expressions in message content can be resource-intensive. Using regular expressions is generally more efficient. Instead of specifying all possible variations, you can configure the transport rule predicate to search for a text pattern.

Regular Expressions in Exchange 2010

In the Exchange Management Shell, you can use regular expressions in any predicate that accepts the **Patterns** predicate property. In the Exchange Management Console, you can use regular expressions with any condition or exception that contains the words **with text patterns**. For more information about predicates, see Transport Rule Predicates.

Caution:

You must carefully test the regular expressions that you construct to make sure that they yield the expected results. An incorrectly configured regular expression could yield unexpected matches and cause unwanted transport rule behavior. This may result in undesirable actions being taken on messages and message content, potentially resulting in data loss when actions such as rejecting or bouncing a message are used. Also, complex regular expressions may affect mail transport performance. Test your regular expressions in a test environment before you implement them in production.

The following table lists the pattern strings that you can use to create a pattern-matching regular expression in Exchange 2010.

Pattern strings

Pattern string	Description
\S	The \S pattern string matches any single character that's not a space.
\s	The \s pattern string matches any single white-space character.
\D	The \D pattern string matches any non-numeric digit.
\d	The \d pattern string matches any single numeric digit.
\w	The \w pattern string matches any single Unicode character categorized as a letter or decimal digit.

\W	The \W pattern string matches any single Unicode character not categorized as a letter or a decimal digit.
|	The pipe (|) character performs an **OR** function.
*	The asterisk (*) character matches zero or more instances of the previous character. For example, ab*c matches the following strings: ac, abc, abbbbc.
( )	Parentheses act as grouping delimiters. For example, a(bc)* matches the following strings: a, abc, abcbc, abcbcbc, and so on.
\	A backslash is used as an escaping character before a special character. Special characters are characters used in pattern strings: • Backslash (\ ) • Pipe (|) • Asterisk (*) • Opening parenthesis (( ) • Closing parenthesis ( )) • Caret (^) • Dollar sign ($) For example, if you want to match a string that contains (525), you would type \(525\).
^	The caret (^) character indicates that the pattern string that follows the caret must exist at the start of the text string being matched. For example, ^fred@contoso matches fred@contoso.com and fred@contoso.co.uk but not alfred@contoso.com.
$	The dollar sign ($) character indicates that the preceding pattern string must exist at the end of the text string being matched. For example, contoso.com$ matches adam@contoso.com and kim@research.contoso.com, but doesn't match kim@contoso.com.au.

Constructing Regular Expressions

By using the preceding table, you can construct a regular expression that matches the pattern of the data that you want to match. Working from left to right, examine each character or group of characters in the data that you want to match. Read the description of each pattern string to determine how it's applied to the data that you're matching. Then, determine which pattern string in the table represents that character or group of characters, and add that pattern string to the regular expression. When finished, you have a fully constructed regular expression.

This example of a regular expression matches North American telephone numbers in the formats 425 555-0100 and 425.555.0100.

```
425(\s|.)\d\d\d(-|.)\d\d\d\d
```

You can expand on this example by adding the telephone format (425) 555-0100, which

uses parentheses around the area code. This example of a regular expression matches all three telephone number formats.

\d\d\d((\s|.|-|\)|\)\s)\d\d\d(\s|.|-)\d\d\d\d

You can analyze the previous example as follows:

- **\d\d\d** This portion requires that exactly three numeric digits appear first.
- **((\s|.|-|\)|\)\s)** This portion requires that a space, a period, or a hyphen exists after the three-digit number. Each character-matching string is contained in the grouping delimiters and is separated by the pipe character. This means that only one of the specified characters inside the grouping delimiters can exist in this location in the string being matched. For the separation between area code and the next three digits, it also looks for a close parenthesis, or close parenthesis and space.
- **\d\d\d** This portion requires that exactly three numeric digits appear next.
- **(\s|.|-)** This portion requires that a space, a period, or a hyphen exists after the three-digit number.
- **\d\d\d\d** This portion requires that exactly four numeric digits appear next.

The above regular expression will match the following sample values:

- (425)555.0100
- 425 555 0100
- 425. 555-0100
- (425) 555-0100
- 425-555-0100
- (425) 555-0100

Creating a Transport Rule That Uses a Regular Expression

This example creates a transport rule in the Shell that uses regular expressions to match SSNs in the subject of an e-mail message.

```
New-TransportRule -Name "Social Security Number Block Rule" -SubjectOrBodyMatches
```

This example lets you view the new transport rule.

```
Get-TransportRule "Social Security Number Block Rule" | Format-List
```


1.11.3.6 Understanding Disclaimers

Understanding Disclaimers

Exchange Server 2010 > Messaging Policy and Compliance > Transport Rules >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-22*

Microsoft Exchange Server 2010 includes the ability to add HTML or text disclaimers to e-mail messages that are processed on Hub Transport servers. Disclaimers are typically used to provide legal information, warnings about unknown or unverified e-mail senders, or for other reasons as determined by an organization.

Here's an example of an e-mail disclaimer:

IMPORTANT NOTICE: This e-mail message is intended to be received only by persons entitled to receive the confidential information it may contain. E-mail messages to clients of Contoso may contain information that is confidential and legally privileged. Please do not read, copy, forward, or store this message unless you are an intended recipient of it. If you have received this message in error, please forward it to the sender and delete it completely from your computer system.

Another example of a disclaimer is the use of e-mail signatures. Many organizations require that uniform signatures be applied to e-mail. Details such as the sender's name, title, department, company, location, and contact details may be required in signatures. In addition, organizations may require insertion of logos and other branding elements in signatures.

For details about how to create a disclaimer, see Configure a Disclaimer.

Targeting Disclaimers

Exchange 2010 lets you target disclaimers (assign specific disclaimers to specific e-mail messages) based on conditions and exceptions that are defined in transport rules created on Hub Transport servers. Transport rules give you the flexibility to assign specific disclaimers to e-mail messages based on business needs. For example, you could specify different disclaimers for internal and external messages or for messages sent by users in a specific departments or offices. However, when configuring multiple transport rules to apply disclaimers, carefully consider the transport rule conditions you use and avoid applying multiple disclaimers to the same message. For information about the transport rule predicates you can use to target the disclaimer, see Transport Rule Predicates.

Here are examples of business conditions that might require that you use unique disclaimers:

- Different legal requirements in different countries or regions.
- Different business or regulatory requirements in different countries or regions.
- Different languages.
- Potentially unsafe e-mail messages that are sent to internal users.

Customizing Disclaimers

When you create a disclaimer, you can modify the appearance, position, and behavior of the disclaimer within the e-mail message. You can customize disclaimers by using the following elements:

- Disclaimer text
- HTML tags and in-line CSS Styles
- Using Images in Disclaimers
- Using Active Directory Attributes in Disclaimers and Personalized Signatures
- Use of a separator line
- Placement of the disclaimer
- Behavior with messages that can't be modified

Disclaimer Text

The disclaimer text is the text that's inserted into a message. Exchange 2010 inserts disclaimers into e-mail messages by using the same message format as the original message. For example, if a message is created in HTML, the disclaimer is added in HTML. If the message is created as plain text, HTML tags are stripped from the disclaimer text before it's added to the plain text message.

Important:

In Exchange 2010, the maximum length of disclaimer text is 5,000 characters. This includes any HTML tags and inline Cascading Style Sheets (CSS) styles.

HTML Tags and Inline CSS Styles

Exchange 2010 disclaimer text can include HTML tags. This allows you to create messages with the rich styling functionality available in HTML. Additionally, HTML tags can include inline Cascading Style Sheets (CSS). Messages sent in the HTML format can display the rich disclaimer messages.

Note:
You can also configure a transport rule with text-only disclaimers by not using any HTML tags.

Using Images in Disclaimers

In Exchange 2010, you can add images to an HTML disclaimer by using the IMG tag. For example:

```
<IMG src="http://myserver.mydomain.com/images/companylogo.gif">
```

Note:
Images added by using IMG tags aren't embedded in the message. Images should be located on a Web server that's accessible to the e-mail client.

When determining whether to use IMG tags in a disclaimer, keep in mind that Outlook Web Access, Outlook Web App, and Outlook 2007 and later blocks external Web content (including images) by default. Users may need to perform a specific action if they want to view the blocked external content. Therefore, images added to HTML disclaimers by using the IMG tag may not be visible by default. We recommend that you test disclaimers with IMG tags in the e-mail clients your recipients are likely to use to make sure it meets your requirements.

Using Active Directory Attributes in Disclaimers and Personalized Signatures

In Exchange 2010, you can add Active Directory attributes (such as DisplayName, FirstName, LastName, Department, and Company) to disclaimers and personalized signatures. When a disclaimer rule is triggered, the attribute names are replaced by corresponding values from the sender's Active Directory user account. To use attributes in a disclaimer or personalized signature, you must enclose it in two percent signs (%%). For example, to use the **DisplayName** attribute, you must use %%DisplayName%%.

For a complete list of attributes that can be used in disclaimers and personalized signatures, see the description for the ADAttribute property in Transport Rule Predicates.

Use of a Separator Line

You may want to clearly identify in an e-mail message where a disclaimer starts or ends and where the original message content starts or ends. In Exchange 2010, you can use the HTML tag <HR> to create a separator line. You can also use inline CSS styles in HTML tags to add lines or borders around the HTML disclaimer message.

Placement of the Disclaimer

When configuring a transport rule to add a disclaimer, Exchange lets you decide whether to prepend or append the disclaimer to the message. When you prepend the disclaimer to the message, the disclaimer is inserted before the text of the newest message. When you append the disclaimer to the message, the disclaimer is inserted at the bottom of the message thread. Exchange doesn't check whether previous disclaimers have been added.

The following is an example of disclaimer text used to create a HTML disclaimer with an IMG tag and embedded CSS:

```
<div style="font-size:9pt;  font-family: 'Calibri',sans-serif;">
%%displayname%%</br>
%%title%%</br>
%%company%%</br>
%%street%%</br>
%%city%%, %%state%% %%zipcode%%</div>
```

```
 </br>
<div style="background-color:#D5EAFF; border:1px dotted #003333; padding:.8em; ">
<div><img alt="Fabrikam"  src="http://fabrikam.com/images/fabrikamlogo.png"></div
<span style="font-size:12pt;  font-family: 'Cambria','times new roman','garamond'
<p style="font-size:8pt; line-height:10pt; font-family: 'Cambria','times roman',s
<span style="padding-top:10px; font-weight:bold; color:#CC0000; font-size:10pt; f
</div>
```

Note:
The preceding HTML disclaimer is used as an example. It isn't intended for use as-is.

Behavior of the Disclaimer with Messages That Can't Be Modified

Some messages, such as encrypted messages, prevent Exchange from modifying the content of the original message. Exchange allows you to control how your organization handles these messages. When you create a disclaimer, you can decide whether to wrap a message that can't be modified in a message envelope that contains the disclaimer, reject the message if a disclaimer can't be added, or ignore the disclaimer action and deliver the message without a disclaimer.

The following list describes each fallback action:

- **Wrap** If the disclaimer can't be inserted into the original message, Exchange encloses, or "wraps," the original message in a new message envelope. Then the disclaimer is inserted into the new message.

  Important:
  If an original message is wrapped in a new message envelope, subsequent transport rules are applied to the new message envelope, not to the original message. Therefore, you must configure transport rules with disclaimer actions that wrap original messages in a new message body after you configure other transport rules.

  Note:
  If the original message can't be wrapped in a new message envelope, the original message is not delivered. The sender of the message receives a non-delivery report (NDR) that explains why the message was not delivered.

- **Reject** If the disclaimer can't be inserted into the original message, Exchange doesn't deliver the message. The sender of the message receives an NDR that explains why the message wasn't delivered.
- **Ignore** If the disclaimer can't be inserted into the original message, Exchange delivers the original message unmodified. No disclaimer is added.

Using Exchange Hosted Services

Transport messaging policies are enhanced by or are also available as a service from Microsoft Exchange Hosted Services.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

1.11.3.7 Understanding Ethical Walls

Understanding Ethical Walls

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-30*

An *ethical wall* is a zone of non-communication between distinct departments of a business or organization. This zone is established to help prevent conflicts of interest that might result in the inappropriate release of sensitive information .

An ethical wall typically spans multiple methods of communication, such as telephone, e-mail, postal mail, and direct person-to-person communication. To make sure that no communication occurs between those regulated by an ethical wall, some organizations go so far as to put whole departments on separate floors or buildings and to require that employees use separate entrances.

One example of where an ethical wall could be used is in an investment organization where brokers aren't allowed to talk to market researchers who may have information that isn't available to the general public. Because market researchers may have confidential information that might influence a broker, regulatory requirements frequently state that those two groups must be prevented from communicating in any way.

How Does Exchange 2010 Help You Implement Ethical Walls?

Exchange 2010 uses transport rules configured on Hub Transport servers. Correctly configured transport rules support ethical walls by helping to prevent e-mail messages from being sent between specific groups of recipients within your organization.

Important:

Exchange 2010 includes features that may help you prevent breaches of an ethical wall. However, Exchange 2010 doesn't prevent individuals from using other methods of communication, such as private e-mail accounts located outside the Exchange organization, network file shares, or phone calls, to share information. Consider Exchange 2010 transport rules as part of an overall suite of tools or processes that you deploy throughout your organization to help enforce an ethical wall policy.

Transport rules are applied by Hub Transport servers across your whole organization. Because all the messages that flow into or out of the Exchange 2010 organization or that are sent within the organization pass through Hub Transport servers, you can consistently apply transport rules to every message.

It doesn't matter whether both the sender's mailbox and the recipient's mailbox reside in the same mailbox database, on the same Mailbox server, or whether their mailboxes are in separate sites. When the sender sends the message to the recipient, the message passes through the Hub Transport server where transport rules are applied.

In a typical configuration, when a sender tries to send a message to a recipient who is on the other side of an ethical wall, Exchange 2010 rejects the message and returns a non-delivery report (NDR) to the sender. By default, the NDR informs the sender that his or her message couldn't be delivered because of policy restrictions. However, you can easily modify the NDR by customizing the delivery status notification (DSN) code and message that are used in the NDR. This capability enables you to provide the sender with specific instructions or hypertext links that relate directly to the policies or regulations that prevented delivery.

For more information about how to customize DSN codes and messages that are used in transport rules and NDRs, see Associate a DSN Message with a Transport Rule.

Implementing an Ethical Wall

The most common method of implementing an ethical wall is to make each affected mailbox a member of one of two distribution groups and then configure the transport rule to reject any messages sent between members of those two distribution groups. Before you use transport rules to implement ethical walls, consider the following important practices:

- **Route messages through a Hub Transport server** For transport rules to be applied to e-mail messages, a route must exist that enables the message to enter and leave a server that applies transport rules. Also, the message must not be subject to an administrator-configured transport restriction that prevents delivery of the message. If a transport restriction prevents delivery of a message, the Transport Rules agent can't act on that message. Also, Transport Rules agent events are logged.
- **Define an appropriate scope** Ethical walls can block all messages if you don't define an appropriate scope. When you create a transport rule to enforce an ethical wall, you must specify conditions to define which recipients and senders to prohibit from sending messages to each other. If you don't specify any conditions, you must specify exceptions to narrow the scope of the transport rule. If you don't specify conditions or exceptions, the transport rule will block all messages sent to or from recipients or senders in your organization.
- **Test transport rules in a test environment first** Before you modify existing transport rules or create new transport rules in your production environment, we recommend that you use a test environment to make sure that the modifications or new rules perform as you intend.

For More Information

Configure an Ethical Wall

Understanding Transport Rules

Understanding How Transport Rules Are Applied

1.11.3.8 Managing Transport Rules

Managing Transport Rules

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-04-16*

Create a Transport Rule

Modify a Transport Rule

View a Transport Rule

Enable or Disable a Transport Rule

Remove a Transport Rule

Export and Import Transport Rules

1.11.3.8.1 Create a Transport Rule

Create a Transport Rule

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Transport rules can be created on a Hub Transport or an Edge Transport server. Both server roles have many common predicates and actions, but some predicates and actions are exclusive to each transport server role. This topic describes how to create a transport rule by using either the EMC or the Shell.

Looking for other management tasks related to transport rules? Check out Managing Transport Rules.

Caution:
Before you create or modify transport rules in your production environment, we recommend that you use a test environment to understand how transport rules work. Test all rules before creating them in a production environment.

Important:
For transport rules to be applied to e-mail messages, a route must exist that enables the message to enter and leave a server that applies transport rules. Also, the message must not be subject to an administrator-configured transport restriction that prevents its delivery. If a transport restriction prevents delivery of a message, the Transport Rules agent can't act on that message, and no Transport Rules agent events are logged.

What Do You Want to Do?

- Use the EMC to create a transport rule
- Use the Shell to create a transport rule

Use the EMC to create a transport rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

1. Navigate to **Organization Configuration > Hub Transport**.
2. In the result pane, click the **Transport Rules** tab.
3. In the action pane, click **New Transport Rule**.
4. On the **Introduction** page, complete the following fields:
   - 4.a. **Name** Type a name for the transport rule.
   - 4.b. **Comment** (optional) You can use this field to describe the rule's functionality and relevant details such as a change request or trouble ticket number, date, and name of administrator. Text in the comments field has no impact on rule functionality.
   - 4.c. **Enable Rule** New rules are enabled by default. If you want the rule to be created in a disabled state, clear the check box.

5. On the **Conditions** page, complete the following fields:
   5.a. In the **Step 1. Select condition(s)** box, select all the conditions that you want to apply to this rule.

   Important:
   If you want this rule to be applied to all e-mail messages, don't select any conditions in this step.

   5.b. If you selected conditions in the Select Conditions box, in the **Step 2. Edit the rule description by clicking an underlined value** box, click each blue underlined word.
   5.c. When you click a blue underlined word, a new window opens to prompt you for the values to apply to the condition. Select the values that you want to apply, or type the values manually. If the window requires that you manually add values to a list, type a value. Then click **Add**. Repeat this process until you have entered all the values, and then click **OK** to close the window.
   5.d. Repeat the previous step for each condition that you selected. After you configure all the conditions, click **Next**.
6. On the **Actions** page, complete the following fields:
   6.a. In the **Step 1. Select actions** box, select all the actions that you want to apply to this rule.
   6.b. In the **Step 2. Edit the rule description by clicking an underlined value** box, click each blue underlined word.
   6.c. In the new window that appears, select the items that you want to apply, or type the values manually, and then click **OK** to close the window.
   6.d. Repeat the previous step for each action that you selected. After you configure all the actions, click **Next**.
7. On the **Exceptions** page, complete the following fields:
   7.a. In the **Step 1. Select exceptions if necessary** box, select all the exceptions that you want to apply to this rule. You don't have to select any exceptions.
   7.b. If you selected exceptions in the previous step, in the **Step 2. Edit the rule description by clicking an underlined value** box, click each blue underlined word.
   7.c. When you click a blue underlined word, a new window opens to prompt you to select the items that you want to add, or to type the values manually. When you have finished, click **OK** to close the window.
   7.d. Repeat the previous step for each exception that you selected. After you configure all the exceptions, click **Next**.

8. On the **Create Rule** page, review the **Configuration Summary**. If you're satisfied with the configuration of the new rule, click **New**.

9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   9.a. A status of **Completed** indicates that the wizard completed the task successfully.
   9.b. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a transport rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

This example creates a new transport rule that prepends "`Sales DG:`" to messages sent from outside the organization to the DG-Sales distribution group.

```
New-TransportRule -Name "Rule1-SalesList" -FromScope NotInOrganization -SentTo "D
```

Note:
The rule parameters and action used in the above procedure are for illustration only. Review all the available transport rule predicates and actions to determine which ones meet your requirements.

For More Information

Understanding Transport Rules

Transport Rule Predicates

Transport Rule Actions

Transport Rules

1.11.3.8.2 Modify a Transport Rule

Modify a Transport Rule

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can modify existing transport rules when you want to make changes to messaging policy.

Caution:
Before you modify transport rules in your production environment, we recommend that you use a test environment to understand how transport rules work, and test all rules before creating them in a production environment.

Important:
For transport rules to be applied to e-mail messages, a route must exist that enables the message to enter and leave a server that applies transport rules. Also, the message must not be subject to an administrator-configured transport restriction that prevents delivery of the message. If a transport restriction prevents delivery of a message, the Transport Rules agent can't act on that message, and no Transport Rules agent events are logged.

Looking for other management tasks related to transport rules? Check out Managing Transport Rules.

Prerequisites

- A transport rule has been created.

What Do You Want to Do?

- Use the EMC to modify a transport rule
- Use the Shell to modify a transport rule

Use the EMC to modify a transport rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, expand the forest you want and navigate to **Organization Configuration > Hub Transport**.
2. In the result pane, click the **Transport Rules** tab, and then select the transport rule you want to modify.
3. In the action pane, click **Edit Rule.**
4. On the **Introduction** page, modify the **Name** or the **Comment** field as required.
5. On the **Conditions** page, modify the conditions listed in **Step 1: Select condition(s):** by either clearing the check boxes for existing selected conditions or by selecting new conditions as required.
6. On the **Actions** page, modify the rule actions by either clearing the check boxes for existing actions or by selecting a new action as required.
7. On the **Exceptions** page, modify the exceptions by either clearing the check boxes for existing exceptions or by selecting new exceptions as required.
8. On the **Update Rule** page, review the changes displayed in the **Configuration Summary**. If you're satisfied with the configuration, click **Update**. If you want to make a revision, click **Back**.
9. On the **Completion** page, click **Finish**.

Use the Shell to modify a transport rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

This command modifies a transport rule so that it's applied to messages sent to recipients outside the Exchange organization.

```
Set-TransportRule -Identity GlobalDislciamer -SentToScope NotInOrganization
```

For detailed syntax and parameter information, see Set-TransportRule.

Other Tasks

After you modify a transport rule, you may also want to:

- Enable or Disable a Transport Rule
- View a Transport Rule
- Remove a Transport Rule

For More Information

Overview of Transport Rules

Understanding How Transport Rules Are Applied

View a Transport Rule

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

When managing transport rules, you may want to enumerate all rules or view the properties of a rule, such as the predicates and their values used to form conditions and exceptions, or the actions the rules apply.

When you view transport rules on a Hub Transport server, you can view any transport rule that is configured in the Exchange organization, except transport rules that are configured on Edge Transport servers. If you view transport rules on an Edge Transport server, you can only view the transport rules on the local computer. To view transport rules on another Edge Transport server, you must open the Exchange Management Console on that computer.

Looking for other management tasks related to transport rules? Check out Managing Transport Rules.

Prerequisites

One or more transport rules exist on a Hub Transport or an Edge Transport server.

What Do You Want to Do?

- Use the EMC to view transport rules
- Use the shell to view transport rules

Use the EMC to view transport rules

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

Note:

The procedure for viewing a transport rule on a Hub Transport server is slightly different from the procedure for viewing a transport rule on an Edge Transport server.

Use the EMC to view transport rules on a Hub Transport server

1. Open the EMC on the Hub Transport server.
2. In the console tree, click **Organization Configuration**, and then click **Hub Transport**.
3. In the result pane, on the **Transport Rules** tab, right-click the rule that you want to view, and then click **Edit Rule**.
4. Click **Next** to navigate through the Transport Rule wizard to view the configuration of the transport rule.
5. Click **Cancel** when you're finished viewing the transport rule and haven't made any changes.

Use the EMC to view transport rules on an Edge Transport server

1. Open the EMC on the Edge Transport server that contains the transport rule that you want to view.
2. In the console tree, click **Edge Transport**.

3. In the result pane, on the **Transport Rules** tab, right-click the rule that you want to view, and then click **Edit Rule**.
4. Click **Next** to navigate through the Transport Rule wizard to view the configuration of the transport rule.
5. Click **Cancel** when you're finished viewing the transport rule and haven't made any changes.

Use the Shell to view transport rules

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

In the Shell, you can view a summary list of all transport rules that are configured on all Hub Transport servers or on the local Edge Transport server, or you can view the detailed configuration of a single transport rule.

Use the Shell to view a summary list of all transport rules

You can view a summary list of all transport rules configured on all Hub Transport servers or an Edge Transport server by using the following command:

```
Get-Transport Rule
```

Use the Shell to view properties of a single transport rule

To view the detailed configuration of a transport rule in the Shell, you must pipe the output of the **Get-TransportRule** command to the **Format-List** command by using the following command:

```
Get-Transport Rule <transport rule GUID or name> | Format-List
```

For more information about pipelining, see Pipelining. For more information about how to work with the information that is returned by a command, see Working with Command Output.

Other Tasks

After you view transport rules, you may also want to:

- Create a Transport Rule
- Enable or Disable a Transport Rule
- Remove a Transport Rule

For More Information

Understanding Transport Rules

Transport Rule Predicates

Transport Rule Actions

1.11.3.8.4 Enable or Disable a Transport Rule

Enable or Disable a Transport Rule

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The Transport Rule agent must be enabled before you can apply transport rules to e-mail messages that enter and leave a Hub Transport server. The Edge Rule agent must be enabled before you can apply transport rules to messages that enter and leave the Edge Transport server. You can run the **Get-TransportAgent** cmdlet on both the Hub Transport server and Edge Transport server to determine whether the Transport Rule agent or Edge Rule agent is running on the respective server role.

To temporarily stop the Rules agent on a Hub Transport server or the Edge Transport server from executing a transport rule, you can disable the rule.

When you enable or disable transport rules on a Hub Transport server, the modified transport rule is replicated across the Exchange 2007 organization to all the Hub Transport servers. When you enable or disable transport rules on an Edge Transport server, the modified transport rule is modified only on the local Edge Transport server.

Looking for other management tasks related to transport rules? Check out Managing Transport Rules.

Prerequisites

One or more transport rules must exist.

Disable a Transport Rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

Use the EMC to disable a transport rule on a Hub Transport server

1. Open EMC on the Hub Transport server on which you want to disable a transport rule.
2. In the console tree, click **Organization Configuration**, and then click **Hub Transport**.
3. In the result pane, click the **Transport Rules** tab.
4. Right-click the transport rule that you want to disable. Click **Disable Rule**.

Use the EMC to disable a transport rule on an Edge Transport server

1. Open the EMC on the Edge Transport server on which you want to disable a transport rule.
2. In the console tree, click **Edge Transport**.
3. In the result pane, click the **Transport Rules** tab.
4. Right-click the transport rule that you want to disable. Click **Disable Rule**.

Use the Shell to disable a transport rule

Run the following command:

```
Disable-TransportRule "TR-Project Hamilton"
```

Enable a Transport Rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

Use the EMC to enable a transport rule on a Hub Transport server

1. Open EMC on the Hub Transport server on which you want to enable a transport rule.
2. In the console tree, click **Organization Configuration**, and then click **Hub Transport**.
3. In the result pane, click the **Transport Rules** tab.
4. Right-click the transport rule that you want to enable. Click **Enable Rule**.

Use the EMC to enable a transport rule on an Edge Transport server

1. Open the EMC on the Edge Transport server on which you want to enable a transport rule.
2. In the console tree, click **Edge Transport**.
3. In the result pane, click the **Transport Rules** tab.
4. Right-click the transport rule that you want to enable. Click **Enable Rule**.

Use the Shell to enable a transport rule

Run the following command:

```
Enable-TransportRule "TR-Project Hamilton"
```

Other Tasks

After you disable or enable a transport rule, you may also want to:

- View a Transport Rule
- Modify a Transport Rule
- Remove a Transport Rule
- Create a Transport Rule

1.11.3.8.5 Remove a Transport Rule

Remove a Transport Rule

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-13*

Transport rules are used to apply messaging policies to messages routed by a Hub Transport or an Edge Transport server. Rules can be disabled if they aren't immediately required. Rules that are no longer required can be removed permanently using the following procedures.

Important:

If you remove a transport rule from a Hub Transport server, the rule is removed from Active Directory. It's no longer available to any Hub Transport server in the Exchange 2010 organization. Edge Transport servers store transport rules in the Active Directory Lightweight Directory Services (AD LDS) instance locally, and the transport rules are managed on the Edge Transport server.

Prerequisites

A transport rule has been created on a Hub Transport server or an Edge Transport server.

What Do You Want to Do?

- Use the EMC to remove a transport rule
- Use the Shell to remove a transport rule

Use the EMC to remove a transport rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

Remove a transport rule on a Hub Transport server

1. Open the EMC on the Hub Transport server.
2. In the console tree, click **Organization Configuration**, and then click **Hub Transport**.
3. On the **Transport Rules** tab, right-click the rule that you want to remove, and then click **Remove**.
4. Click **Yes** if you're sure that you want to remove the transport rule.

Remove a transport rule on an Edge Transport server

1. Open the EMC on the Edge Transport server that contains the transport rule that you want to remove.
2. In the console tree, click **Edge Transport**.
3. On the **Transport Rules** tab, right-click the rule that you want to remove, and then click **Remove**.
4. Click **Yes** if you're sure that you want to remove the transport rule. The transport rule that you select is removed from the Active Directory Lightweight Directory Services instance on that Edge Transport server.

Important:

If you have more than one Edge Transport server deployed, you may need to remove the rule on all of them.

Use the Shell to remove a transport rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

When using the Shell, the process to remove a transport rule from the Hub Transport and the Edge Transport server is identical.

1. Run the following command to see how transport rules will be affected without making any modifications:

```
Remove-TransportRule "Messages From DG-Sales" -WhatIf
```

Note:

Use the *WhatIf* parameter to verify that the results of the operation are what you expect. For more information about the *WhatIf* parameter, see WhatIf, Confirm, and ValidateOnly Switches.

2. Run the following command to remove the transport rule:

```
Remove-TransportRule "Messages From DG-Sales"
```

Other Tasks

After you remove a transport rule, you may also want to:

- View a Transport Rule
- Create a Transport Rule

For More Information

Understanding Transport Rules

Transport Rule Predicates

Transport Rule Actions

Managing Transport Rules

Transport Rules: End-to-End Tasks

1.11.3.8.6 Export and Import Transport Rules

Export and Import Transport Rules

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You may need to export and import the transport rule collection from one transport server running Microsoft Exchange Server 2010 or Exchange Server 2007 to another transport server in the following scenarios:

- **Duplicate transport rule configuration on Edge Transport servers** Make sure all Edge Transport servers or a set of Edge Transport servers apply the same transport rules. Hub Transport servers store their configuration in Active Directory. The configuration is replicated to all domain controllers in the organization. Edge Transport servers store their configuration in the local instance of Active Directory Lightweight Directory Services (AD LDS), which is not automatically replicated.
  Depending on your Exchange deployment and message routing topology, you may want to have different sets of Edge Transport servers use different transport rules. For example, you may want to apply different rules on the Edge Transport servers that receive inbound e-mail than the ones on the Edge Transport servers that send outbound e-mail. If you want all Edge Transport servers in your organization to apply the same set of transport rules, you can use this procedure to duplicate the transport rule configuration.
  If you want to replicate the entire Exchange configuration from one Edge Transport server to another, we recommend that you use a cloned configuration. This configuration includes the configuration of transport rules on an Edge Transport server. For more information about how to clone Edge Transport servers, see Understanding Edge Transport Server Cloned Configuration.

  Important:
  If you expect frequent changes to the transport rule configuration on Edge Transport servers, we recommend that you designate one Edge Transport server as a source server and perform modifications on that server. Configure

the other Edge Transport servers to automatically update their transport rule configuration from the source Edge Transport server by using a Shell script that performs the procedures later in this topic. For more information about how to run scripts in the Shell, see Scripting with the Exchange Management Shell.

- **During coexistence with Exchange 2007 Hub Transport servers** Exchange 2010 includes many new transport rule predicates and actions, and changes to some predicates and actions found in Exchange 2007. When you install the first Exchange 2010 server in your Exchange 2007 organization, Exchange Setup creates a container in Active Directory to hold Exchange 2010 rules, resulting in rules for both versions being stored in different locations. Any existing transport rules from Exchange 2007 are converted, and a copy is stored in the Exchange 2010 container. After setup, the Exchange organization has the same set of transport rules for both Exchange server versions.
  Subsequently, if you make any changes to the transport rule configuration on Exchange 2007 or Exchange 2010, both versions will have a different set of rules. To ensure both Exchange server versions have the same transport rules and to apply the same messaging policies, make sure that any changes you make to the transport rule configuration on Exchange 2007 are also made to the Exchange 2010 configuration. This procedure helps you export rules from Exchange 2007 and import them in Exchange 2010.

  Important:
  To export Exchange 2007 transport rules to an Exchange 2010 server, you must run the **Export-TransportRuleCollection** cmdlet on an Exchange 2010 server. The **Export-TransportRuleCollection** cmdlet includes the option to export Exchange 2007 rules.
  When you import Exchange 2007 transport rules to an Exchange 2007 server, you must run the **Import-TransportRuleCollection** cmdlet on an Exchange 2007 server.
  You can't export Exchange 2010 rules and import them to an Exchange 2007 server.

Looking for other management tasks related to transport rules? Check out Managing Transport Rules.

Use the Shell to export Exchange 2010 transport rules from a Hub Transport or an Edge Transport server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to export Exchange 2010 transport rules from a Hub Transport or an Edge Transport server.

The procedure to export Exchange 2010 transport rules is the same for both Hub Transport and Edge Transport servers. On the Hub Transport server, you may want to export transport rules to be imported on an Exchange 2010 Hub Transport server during coexistence. Or you may want to export transport rules for backup purposes.

On Edge Transport servers, you may want to export transport rules to duplicate them on another Edge Transport server, or to back up the transport rules on that Edge Transport server.

This example exports transport rules on an Exchange 2010 Hub Transport or Edge Transport server. Rule data is exported to the variable $file, and then written to the Exchange2010TransportRules.xml file in the C:\MyDocs folder.

```
$file = Export-TransportRuleCollection
Set-Content -Path "C:\MyDocs\Exchange2010TransportRules.xml" -Value $file.FileDat
```

For detailed syntax and parameter information, see Export-TransportRuleCollection.

Use the Shell to export Exchange 2007 transport rules from an Exchange 2010 Hub Transport server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the EMC to export Exchange 2007 transport rules from an Exchange 2010 Hub Transport server.

You may need to export Exchange 2007 transport rules to import them to an Exchange 2010 Hub Transport server during a period of coexistence when you have both Exchange versions in your organization. When you set up the first Exchange 2010 server in your Exchange 2007 organization, Exchange Setup copies the rules from the Exchange 2007 transport rule container to the Exchange 2010 container. You need to perform this procedure only if you have made changes to transport rules on an Exchange 2007 server, and need to make the same changes to the Exchange 2010 server to make sure both servers have the same transport rules.

This example exports legacy transport rules created in Exchange 2007. Run the command from an Exchange 2010 Hub Transport server.

```
$ file = Export-TransportRuleCollection -ExportLegacyRules
Set-Content -Path "C:\MyDocs\LegacyRules.xml" -Value $file.FileData -Encoding Byt
```

For detailed syntax and parameter information, see Export-TransportRuleCollection.

Use the Shell to import transport rules on an Exchange 2010 Hub Transport or Edge Transport server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the EMC to import transport rules on an Exchange 2010 Hub Transport or Edge Transport server.

Use this procedure to import Exchange 2010 or Exchange 2007 transport rules on an Exchange 2010 Hub Transport or Edge Transport server. Both the server roles use the same procedure and cmdlet to import transport rules.

Caution:
Importing a transport rule collection from a .xml file removes or overwrites all preexisting transport rules defined for the Transport Rules agent. Make sure that you have a backup of your current transport rule collection before you import and overwrite the transport rules.
On Hub Transport servers, the **Import-TransportRuleCollection** cmdlet overwrites all transport rules configured in the Exchange 2010 organization, except for transport rules on Edge Transport servers. On Edge Transport servers, this command overwrites transport rules configured on the local computer only.

Important:
Although similar in concept and implementation, the Hub Transport and Edge Transport server roles use different transport rule predicates and actions designed to meet different requirements. You shouldn't import transport rules exported from an Edge Transport server from either Exchange version to a Hub Transport server of either version. Similarly, you shouldn't import rules exported from a Hub Transport server from either Exchange version to an Edge Transport server of either version.

This example imports transport rules from the ExportedRules.xml file.

```
[Byte[]]$Data = Get-Content -Path "C:\MyDocs\ExportedRules.xml" -Encoding Byte -R
Import-TransportRuleCollection -FileData $Data
```

For detailed syntax and parameter information, see Import-TransportRuleCollection.

1.11.3.9 Transport Rules: End-to-End Tasks

Transport Rules: End-to-End Tasks

Exchange Server 2010 > Messaging Policy and Compliance > Transport Rules >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-11*

Transport rules provide many predicates and actions that you can use to implement your organization's messaging policies and messaging hygiene. These are listed in Transport Rule Predicates and Transport Rule Actions.

Depending on your organization's requirements, you can use transport rules to accomplish a wide range of tasks. This section contains information about the following scenarios made possible by transport rules:

- Configure a Catch-All Mailbox
- Configure a Disclaimer
- Configure an Ethical Wall
- Configure a Transport Rule for Messages That Have a Blank Subject
- Associate a DSN Message with a Transport Rule

Looking for general management tasks related to transport rules? For topics about basic management functionality, such as how to create, modify, enable, disable, and remove transport rules, see Managing Transport Rules.

Configure a Catch-All Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can configure transport rules on Edge Transport servers to copy or redirect messages received by your organization to the *catch-all mailbox*. A catch-all mailbox is typically a mailbox in your organization used to collect all the e-mail messages sent to your organization. Depending on your preferences, the catch-all mailbox may receive all messages or only messages sent to mailboxes that don't exist.

To configure a catch-all mailbox, you must perform the following steps:

1. Create a mailbox.
2. Disable recipient filtering.
3. Configure a transport rule to copy or redirect messages to the catch-all mailbox.

Looking for other management tasks related to mailboxes? Check out Managing Mailbox Servers.

Prerequisites

Before you disable recipient filtering (as required in step 2), you should understand the benefits of running the Recipient Filter agent and understand what features depend on it. For more information about the Recipient Filter agent and how it helps reduce the effect of spam, denial of service attacks (DoS), and other threats, see Understanding Recipient Filtering.

Note:

Recipients are resolved before messages pass through the Transport Rules agent on Hub Transport servers. Therefore, transport rules on Hub Transport servers can't be used to copy or redirect messages to a catch-all mailbox.

Step 1: Create a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "User mailboxes" entry in the Mailbox Permissions topic.

You must create a mailbox to receive the messages that are copied or redirected to it by transport rules. Because the messages delivered to the new mailbox may contain sensitive information, restrict access to the mailbox.

1. Create the catch-all mailbox. For details, see Create a Mailbox.
2. Complete one or both of the following, depending on the volume of messages delivered to the mailbox:
   - Increase the mailbox quota limits. For more information, see Configure Storage Quotas for a Mailbox.
   - Configure messaging records management (MRM) to automatically remove messages from the mailbox that are older than a configured age. For more information, see Create a Retention Tag and Create Managed Content Settings.
3. After you create the mailbox, note the SMTP address assigned to the mailbox.

Step 2: Disable recipient filtering

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Anti-spam features" and "Anti-spam features – Edge Transport" entry in the Transport Permissions topic.

You must disable recipient filtering on each Edge Transport server that you want to configure transport rules to copy or redirect messages to a catch-all mailbox. You must do this because messages pass through the Recipient Filter agent before passing through the Edge Rule agent, and the Recipient Filter agent will reject messages addressed to mailboxes that don't exist.

Use the EMC on an Edge Transport server to disable recipient filtering

1. Open the EMC on the Edge Transport server where you want to create the transport rule.
2. In the console tree, click **Edge Transport**.
3. In the work pane, click the **Anti-spam** tab, and then select **Recipient Filtering**.
4. In the action pane, click **Disable**.

Use the Shell on an Edge Transport server to disable recipient filtering

This example disables recipient filtering.

```
Set-RecipientFilterConfig -Enabled $false
```

For detailed syntax and parameter information, see Set-RecipientFilterConfig.

Step 3: Configure a transport rule to copy or redirect messages to the catch-all mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

After you create a mailbox to accept messages and you disable recipient filtering, you must create a transport rule to copy or redirect messages to the catch-all mailbox. You must configure this transport rule on each Edge Transport server on which you want to copy or redirect messages.

Your organization's requirements should determine whether you copy messages to the catch-all mailbox or redirect messages to the catch-all mailbox. The differences between the two actions are as follows:

- When a message is copied to the catch-all mailbox (using the Cc line or Bcc line text box), the message also continues to the original recipient. If the original recipient doesn't exist, the sender receives a non-delivery report (NDR).
- When a message is redirected to the catch-all mailbox, the message doesn't continue to the original recipient. The message is sent only to the catch-all mailbox. If the original recipient doesn't exist, the sender doesn't receive an NDR.

You should also configure the **except when the text patterns appears in any recipient address** exception to avoid copying or redirecting messages to the catch-all mailbox for SMTP addresses that already exist in your organization. This exception uses regular expressions to prevent the transport rule from copying or redirecting messages to the

catch-all mailbox if the SMTP address exists in your organization. You must manually configure the exception with the SMTP addresses in your organization and enclose each SMTP address with the ^ and $ pattern strings.

For more information about regular expressions, see Regular Expressions in Transport Rules.

Important:
A message sent to your organization won't be copied or redirected to the catch-all mailbox if one or more SMTP addresses are included in the message recipients and are configured on the transport rule exception. This is true even if one or more of the SMTP addresses on the message doesn't exist in your organization.

Use the EMC to configure a transport rule to copy or redirect a message to the catch-all mailbox

1. Open the EMC on the Edge Transport server on which you want to create the transport rule.
2. In the console tree, click **Edge Transport**.
3. In the result pane, click the **Transport Rules** tab, and then in the **Actions** pane, click **New Transport Rule**.
4. In the **Name** field of the Transport Rule wizard, type the name of the transport rule.
5. If you have notes for this rule, in the **Comments** field, type the notes.
6. If you want the rule to be created in a disabled state, clear the **Enable Rule** check box. Otherwise, leave the **Enable Rule** check box selected. Click **Next**.
7. In the **Step 1. Select Condition(s)** box, select the **from users that are inside or outside the organization** check box.
8. In the **Step 2. Edit the rule description by clicking an underlined value** box, click **inside the organization**.
9. In the **From scope** list, select **Outside the organization**, and then click **OK**.
10. If you want to add conditions, do so now. After you configure all the conditions, click **Next**.
11. In the **Step 1. Select Action(s)** box, select **copy the message to addresses** if you want to copy messages to the catch-all mailbox. Select **redirect the message to addresses** if you want to redirect messages to the catch-all mailbox. Don't select both actions in the same transport rule.
12. In the **Step 2. Edit the rule description by clicking an underlined value** box, click **addresses**.
13. In the **Specify recipients** dialog box, type the SMTP address of the catch-all mailbox in the **E-mail addresses of recipients** box, click **Add**, and then click **OK**.
14. If you want to configure additional actions, do so now. After you configure all the actions, click **Next**.
15. In the **Step 1. Select Exceptions if necessary** box, select the **except when any recipient address matches text patterns** check box.
16. In the **Step 2. Edit the rule description by clicking an underlined value** box, click **text patterns**.
17. In the **Text patterns** box, type the SMTP addresses of existing mailboxes in your organization. Enclose each SMTP address with the ^ and $ pattern strings. For example, if the SMTP address is david@contoso.com, enter: **^david@contoso.com$**. After you enter each SMTP address, click **Add**. When you have finished, click **OK** to close the window.
18. If you want to configure additional exceptions, do so now. After you configure all the exceptions, click **Next**.
19. Review the **Configuration Summary**. If the configuration of the new rule is satisfactory, click **New**, and then click **Finish**.

Use the Shell to configure a transport rule to copy or redirect a message to the catch-all mailbox

Before you begin, you must be familiar with how to create a transport rule using the Shell. For more information, see "Use the Shell to create a transport rule" in Create a Transport Rule.

To configure a transport rule to copy or redirect messages to a catch-all mailbox, you must configure the transport rule condition that directs the transport rule to apply the action only to messages sent from senders outside the organization. To do this, use the FromScope transport rule predicate together with the New-TransportRule cmdlet.

The following example configures a transport rule to copy messages from senders outside the organization to the catch-all mailbox:

```
New-TransportRule -Name "Catch-all Mailbox" -FromScope
NotInOrganization -Actions RedirectMessage <Catch_All_Mailbox _Address>
```

Use the Shell to configure the transport rule condition to copy messages to a catch-all mailbox on an Edge Transport server

This example configures the transport rule condition to:

- Select messages only from senders outside the organization.
- Copy a message to the catch-all mailbox.
- Specify the SMTP address of the catch-all mailbox.
- Avoid copying messages sent to SMTP addresses that exist in your organization.
- Create a transport rule that copies messages to a catch-all mailbox.

```
New-TransportRule -Name "Copy messages to catch-all mailbox" -FromScope
NotInOrganization -CopyTo "catch-all@contoso.com" -
ExceptIfAnyOfRecipientAddressMatchesPatterns "^david@contoso.com$",
"^brian@contoso.com$"
```

For detailed syntax and parameter information, see Get-TransportRulePredicate, Get-TransportRuleAction, or New-TransportRule.

Use the Shell to redirect messages to a catch-all mailbox on an Edge Transport server

This example configures the transport rule condition to:

- Select messages only from senders outside the organization.
- Copy a message to the catch-all mailbox.
- Specify the SMTP address of the catch-all mailbox.
- Avoid redirecting messages sent to SMTP addresses that exist in your organization.
- Create a transport rule that redirects messages to a catch-all mailbox.

```
New-TransportRule -Name "Redirect messages to catch-all mailbox" -
FromScope NotInOrganization -RedirectMessage "catch-all@contoso.com" -
ExceptIfAnyOfRecipientAddressMatchesPatterns "^david@contoso.com$",
"^brian@contoso.com$"
```

For detailed syntax and parameter information, see Get-TransportRulePredicate, Get-TransportRuleAction, or New-TransportRule.

1.11.3.9.2 Configure a Disclaimer

Configure a Disclaimer

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Disclaimers are statements, generally of a legal nature, added to e-mail messages that enter or leave a Microsoft Exchange Server 2010 organization. It's possible to apply multiple disclaimers to a single e-mail message. If a message matches more than one transport rule, and a disclaimer action is configured on each transport rule, the transport rule applies each disclaimer action to the message.

The procedure that you use to create a disclaimer is the same procedure used to create a transport rule. This is because a disclaimer is a configurable action available to transport rules on a Hub Transport server.

As with transport rules, when you create a new disclaimer, you can configure conditions and exceptions to control which e-mail messages receive the disclaimer. If you want the disclaimer to apply to all e-mail messages that enter and leave the Exchange 2010 organization, don't configure any conditions or exceptions.

Important:

For transport rules to be applied to e-mail messages, a route must exist that enables the message to enter and leave a server that applies transport rules. Also, the message must not be subject to an administrator-configured transport restriction that prevents delivery of the message. If a transport restriction prevents delivery of a message, the Transport Rules agent can't act on that message, and no Transport Rules agent events are logged.

Caution:

To apply disclaimers, you must create or modify a transport rule. Before you modify or create transport rules in your production environment, use a test environment to test rules thoroughly. The following procedures aren't intended to be run in a production environment without modification to support your organization.

Looking for other management tasks related to transport rules? Check out Managing Transport Rules.

Prerequisites

To apply Exchange 2010 transport rules, all Hub Transport servers in the organization should be running Exchange 2010.

Use the EMC to Configure a Disclaimer

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

1. Navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **Transport Rules** tab.
3. In the action pane, click **New Transport Rule**. On the **Introduction** page, complete the following fields:
   - **Name** Type a name for the transport rule.
   - **Comment** (Optional) Comments can be used to describe rule functionality and relevant details such as a change request or trouble ticket number, date, and name of an administrator. Text in the comments field has no effect on rule functionality.
   - **Enable Rule** New rules are enabled by default. If you want the rule to be created in a disabled state, clear the check box.
4. On the **Conditions** page, complete the following fields:
   - In the **Step 1. Select Condition(s)** field, select all the conditions that you

want to apply to this rule.

Important:
If you want this rule to be applied to all e-mail messages, don't select any conditions in this step.

- In the **Step 2. Edit the rule description by clicking an underlined value** field, for each condition selected in the **Select Conditions** box, click each blue, underlined word.
- When you click a blue, underlined word, a window opens to prompt you for the values to apply to the condition. Select the values that you want to apply, or type the values manually. If the window requires that you manually add values to a list, type a value. Then click **Add**. Repeat this process until you have entered all the values, and then click **OK** to close the window.
- Repeat the previous step for each condition that you selected. After you configure all the conditions, click **Next**.

5. On the **Actions** page, complete the following fields:
   - In the **Step 1. Select actions** field, select the **append disclaimer text and fallback to action if unable to apply** check box.
   - In the **Step 2. Edit the rule description by clicking an underlined value** field, complete the following fields:
     - Click **disclaimer text**. In the **Specify disclaimer text** dialog box, type the plaintext or HTML disclaimer text that you want to add to messages.
     - (Optional) To change the position of the disclaimer in messages, click **append**. From the **Select position** dialog box, select **prepend**.
     - (Optional) To change the fallback action, click **wrap**. In the **Select fallback action** dialog box, select the desired fallback action.
6. On the **Exceptions** page, complete the following fields:
   - In the **Step 1. Select exceptions if necessary** box, select all the exceptions that you want applied to this rule. You aren't required to select any exceptions.
   - If you selected exceptions in the previous step, in the **Step 2. Edit the rule description by clicking an underlined value** box, click each blue, underlined word.
   - When you click a blue, underlined word, a window opens to prompt you to select the items that you want to add, or to type the values manually. After you finish, click **OK** to close the window.
   - Repeat the previous step for each exception that you selected. After you configure all the exceptions, click **Next**.

Note:
If you don't apply an exception to this transport rule and all the transport rule conditions are met, a disclaimer is added to every message. The **append disclaimer text and fallback to action if unable to apply** action doesn't verify that a disclaimer has already been applied to a message. To avoid having a disclaimer text added repeatedly to messages that meet the conditions of this transport rule, add the **except when the Subject field or message body contains specific words** exception, and then edit the **specific words** value to include text that's unique to the disclaimer you created.

7. On the **Create Rule** page, review the **Configuration Summary**. If you're satisfied with the configuration of the new rule, click **New**.

8. On the **Completion** page, click **Finish**. A status of **Completed** indicates that the wizard completed the task successfully. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an

explanation, and then click **Back** to make any additional changes.

Use the Shell to Configure a Disclaimer

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

This example creates a transport rule to apply a disclaimer to all messages sent outside the organization. The disclaimer is appended to messages, and the fallback action is set to wrap.

```
New-TransportRule -Name ExternalDisclaimer -Enabled $true -SentToScope 'NotInOrga
```

For detailed parameter and syntax information, see New-TransportRule.

Other Tasks

After you configure a disclaimer, you may also want to:

- View a Transport Rule
- Enable or Disable a Transport Rule
- Remove a Transport Rule

1.11.3.9.3 Configure an Ethical Wall

Configure an Ethical Wall

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-12-11*

An *ethical wall* is a zone of non-communication between distinct departments of a business or organization that is established to prevent conflicts of interest that might result in the inappropriate release of sensitive information. You can use Microsoft Exchange Server 2010 to configure ethical walls that comply with your organization's compliance policies and with regulations and laws that apply to your organization. For more information about ethical walls, see Understanding Ethical Walls.

To create an ethical wall, use the same procedure that you use to create a transport rule. When you implement an ethical wall by creating a transport rule, you can configure conditions and exceptions to control which e-mail messages the ethical wall blocks.

Caution:

Before you create or modify transport rules in your production environment, we recommend that you use a test environment to understand how transport rules work. Test all rules before you create them in a production environment.
Ethical walls block all messages if you don't define an appropriate scope. When you create a transport rule to enforce an ethical wall, you must specify conditions to define which recipients and senders are prohibited from sending messages to each other. If you don't specify any conditions, you must specify exceptions to narrow the scope of the transport rule. If you don't specify conditions or exceptions, the transport rule blocks all messages sent to or from recipients and senders in your organization.

Prerequisites

Although you are not required to use an Exchange 2010 Hub Transport server, you must route e-mail messages through an Exchange 2010 Hub Transport server to apply transport rules to the messages.

Use the EMC to create an ethical wall

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the action pane, click **New Transport Rule**.
3. On the **Introduction** page, complete the following fields:
   - **Name** Enter a name for the transport rule.
   - **Comment** [optional] Type any notes for the rule.
   - **Enable Rule** If you want the rule to be created in a disabled state, clear this check box.
4. On the **Conditions** page, complete the following steps:
   - In the **Step 1. Select condition(s)** box, select all the conditions that you want to apply to this rule.

     Note:
     The **between members of distribution list and distribution list** condition is well suited for transport rules that enforce ethical walls.

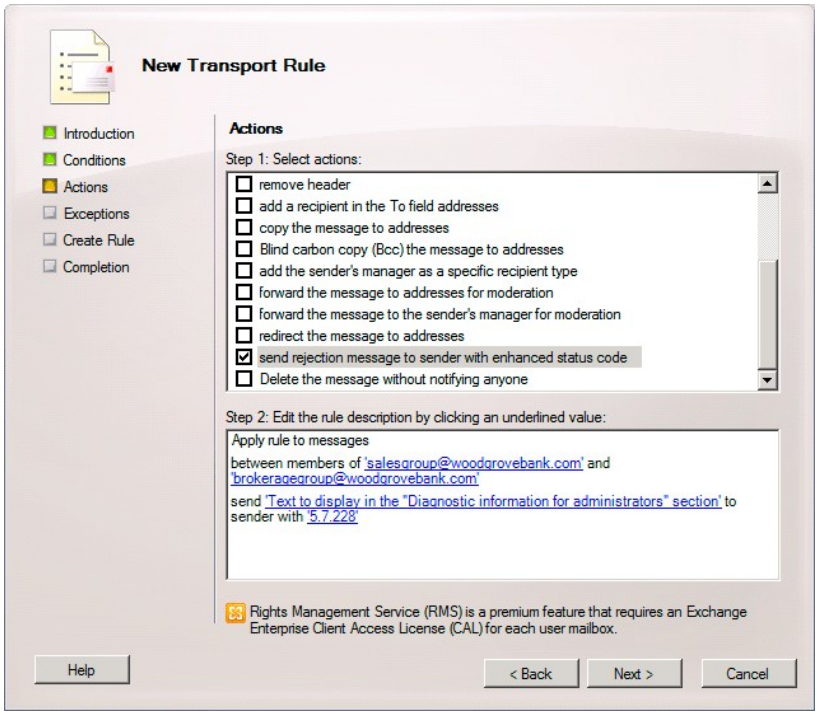
   - If you selected conditions in the previous step, click each blue underlined word in the **Step 2. Edit the rule description by clicking an underlined value** box.

     Note:
     When you click a blue underlined word, you are prompted for the values to apply to the condition. Select the values that you want to apply, or type the values manually. If the prompt window requires that you manually add values to a list, enter a value, and then click **Add**. Repeat this process until you have entered all the values, and then click **OK** to close the window.

   - Repeat the previous step for each condition that you selected. After you configure all the conditions, click **Next**.
5. On the **Actions** page, complete the following steps:
   - In the **Step 1. Select actions** box, click **send rejection message to sender with enhanced status code**. This transport rule action deletes the message and returns a non-delivery report (NDR) to the sender of the message.
   - In the **Step 2. Edit the rule description by clicking an underlined value** box, follow these steps:
     5..a.Click **rejection message**.
     5..b.In the **Specify rejection message** dialog box, enter the text to display in the **Diagnostic information for administrators** section of the NDR that's sent to the sender of the rejected message. When you're finished, click **OK**.
     5..c.Click **enhanced status code**.
     5..d.In the **Specify Enhanced Status Code** dialog box, enter the delivery status notification (DSN) code you want to display in the **Diagnostic information for administrators** section of the NDR that's sent to the sender of the rejected message. Valid enhanced status code values are 5.7.1 and any value from 5.7.10 through 5.7.999. When you're

finished, click **OK**.

Note:
For more information about how Exchange 2010 associates a DSN code with a transport rule, see Associate a DSN Message with a Transport Rule.



- If you want to add more actions, repeat the previous step, and select the transport rule actions that you want to apply. After you configure all the actions, click **Next**.

6. On the **Exceptions** page, complete the following optional steps:
   - In the **Step 1. Select exceptions if necessary** box, select all the exceptions that you want to apply to this rule. You aren't required to select any exceptions.
   - If you selected exceptions, in the **Step 2. Edit the rule description by clicking an underlined value** box, click each blue underlined word.

     Note:
     When you click a blue underlined word, you are prompted to select the items that you want to add or to type the values manually. When you're finished, click **OK** to close the window.Repeat the previous step for each exception that you selected.

   - After you configure all the exceptions, click **Next**.
7. On the **Create Rule** page, review the **Configuration Summary**. If you're satisfied with the configuration of the new rule, click **New**, and then click **Finish**.

Use the Shell to create an ethical wall

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

In this example, Woodgrove Bank wants to prevent members of its Brokerage group and

the Sales group from communicating. The bank decides to implement an ethical wall between the two groups by using a transport rule.

Predicate The `BetweenMemberOf` transport rule predicate is used to prohibit the members of the Brokerage Group distribution group and the Sales Group distribution group from communicating with each other. The `BetweenMemberOf` transport rule predicate is well suited for transport rules that enforce ethical walls. For more information about transport rule predicates, see Transport Rule Predicates.

Exception Woodgrove Bank wants to create an exception to this policy that allows members of the Executive Group distribution group to communicate with one other. Members may belong to either of the two groups,. The `ExceptIfFromMemberOf` predicate is used to implement this exception.

Action The `RejectMessage` transport rule action is used to block messages that are sent to a prohibited recipient. When the `RejectMessage` transport rule action is applied to a message, an NDR is returned to the sender of the message, and the message itself is deleted. You can configure the user information text and the DSN code and message that are displayed in the administrator section of the NDR.

You can modify the text that's displayed to the sender in the **Diagnostic information for administrators** section of the NDR. This text can provide helpful information to enable the administrator to understand why the message was rejected.

DSN Codes By default, the `RejectMessage` transport rule action uses the enhanced status code `5.7.1`. You can modify the DSN code returned by specifying a custom DSN code. A custom DSN code must be associated with a custom DSN message. The DSN message appears in the user information section of the NDR. You can specify a custom DSN code to be able to provide the sender more detailed information. You can also refer the sender to an internal or public Web page that contains more information about the specific policy or regulation.

The following example specifies a new, unused, custom DSN code in the **RejectMessageEnhancedStatusCode** property.

```
New-TransportRule "Sample Ethical Wall" -Enabled $true -BetweenMemberOf1 Brokerag
```

This example then creates the custom DSN code and specifies the text that should be displayed when a message is returned with that DSN code.

```
New-SystemMessage -DsnCode 5.7.228 -Internal $true -Language En -Text "A message
```

For more information about which values are accepted and about how Exchange 2010 associates a DSN code with a transport rule, see Associate a DSN Message with a Transport Rule.

For detailed syntax and parameter information, see New-TransportRule and New-SystemMessage.

1.11.3.9.4 Configure a Transport Rule for Messages That Have a Blank Subject

Configure a Transport Rule for Messages That Have a Blank Subject

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Transport rules perform specified actions on messages based on message properties such as sender, recipients, message scope, message subject, and message body. Creating a transport rule for messages that have a blank subject line requires the use of regular expressions.

Caution:

Before you configure new transport rules in your production environment, use a test environment to learn how to create transport rules and test them thoroughly. The following procedures aren't intended to be run in a production environment without modification to support your organization.

Important:

For transport rules to be applied to e-mail messages, a route must exist that enables the message to enter and leave a server that applies transport rules. Also, the message must not be subject to an administrator-configured transport restriction that prevents delivery of the message. If a transport restriction prevents delivery of a message, the Transport Rules agent can't act on that message, and no Transport Rules agent events are logged.

The ^$ Regular Expression

To detect messages that have blank subject lines, the following procedures use the ^$ regular expression. This regular expression consists of two pattern strings, ^ and $. Pattern strings are used in regular expressions to match patterns in text that can vary. When the ^ and $ pattern strings are used in this order, the transport rule condition matches only the exact string that's between the two pattern strings. Because there's no string between the ^ and $ pattern strings in the ^$ regular expression, it matches only an empty string, such as a blank subject line.

For more information about regular expressions, see Regular Expressions in Transport Rules.

The RejectMessage Transport Rule Action

The `RejectMessage` transport rule action is used to reject messages and provide an enhanced status code for the rejection. In this example, the `RejectMessage` transport rule action is used to reject a message and return a non-delivery report (NDR). The `RejectMessage` transport rule action is available only on Hub Transport servers.

You can modify the text that's displayed to the sender in the **Diagnostic information for administrators** section of the NDR. This text can provide helpful information to enable you to understand why the message was rejected.

You can also modify the delivery status notification (DSN) code and message that appears in the user information section of the NDR by specifying a customized DSN code. A customized DSN code is associated with a customized DSN message. It's useful to specify this code so that you can refer the user to an HTML link to a specific policy or regulation. By default, the NDR associated with the 5.7.1 DSN code is sent.

For example, if you want to refer users to the Information Technology department if their message is rejected, you can specify a new, unused, customized DSN code in the **EnhancedStatusCode** property. After you specify a new customized DSN code, if the customized DSN code isn't already defined, you must use the **New-SystemMessage** cmdlet to create the DSN code and specify the text that should be displayed when that DSN code is referenced. For an example of how to do this, see Use the Shell to create a

transport rule for messages that have a blank subject later in this topic.

Note:
The `RejectReason` transport rule action is available only on Hub Transport servers. If you want to reject messages that have a blank subject line on Edge Transport servers, you must use the `SmtpRejectMessage` transport rule action. You can only specify the DSN code when you use the `SmtpRejectMessage` transport rule action. You can't specify an alternative message to display to the user or administrator.
For more information about the `SmtpRejectMessage` transport rule action, see "Actions Available on an Edge Transport Server" in Transport Rule Actions.

For more information about what values are accepted and how Microsoft Exchange Server 2010 associates a DSN code with a transport rule, see Associate a DSN Message with a Transport Rule.

Use the EMC to create a transport rule for messages that have a blank subject

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

1. Open the New Transport Rule wizard. Depending on whether you're performing this procedure on a Hub Transport or Edge Transport server, use the following navigation:
   - Hub Transport servers: In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
   - Edge Transport servers: In the console tree, click **Edge Transport**.
2. In the action pane, click **New Transport Rule**.
3. On the **Introduction** page, complete the following fields:
   - **Name** Type the name for the transport rule.
   - **Comments** (optional) You can use this field to describe the rule's functionality and relevant details. Text in the comments field has no impact on rule functionality.
   - **Enable Rule** New rules are enabled by default. If you want the rule to be created in a disabled state, clear this check box.
4. On the **Conditions** page, complete the following fields:
   - In the **Step 1. Select condition(s)** box, select the **when the Subject field matches text patterns** condition.
   - In the **Step 2. Edit the rule description by clicking an underlined value** box, click the blue underlined **text patterns**.
   - In the **Specify text patterns** dialog box, type **^$**, and then click **Add**. Click **OK** to close the dialog box, and then click **Next**.
5. On the **Actions** page, complete the following fields:
   - In the **Step 1. Select actions** box, select all the actions that you want to apply to this rule. You must select at least one action to create a transport rule.
   - In the **Step 2. Edit the rule description by clicking an underlined value** box, click each blue underlined word.
   - In the new dialog box that appears, select the items that you want to apply, or type the values manually, and then click **OK** to close the dialog box.
   - Repeat the previous step for each action that you selected. After you configure all the actions, click **Next**.
6. On the **Exceptions** page, complete the following fields:
   - In the **Step 1. Select exceptions if necessary** box, select all the exceptions that you want to apply to this rule. You don't have to select any

exceptions.
- If you selected exceptions in the previous step, in the **Step 2. Edit the rule description by clicking an underlined value** box, click each blue underlined word.
- In the new dialog box that appears, select the items that you want to apply, or type the values manually, and then click **OK** to close the dialog box.
- Repeat the previous step for each exception that you selected. After you configure all the exceptions, click **Next**.

7. On the **Create Rule** page, review the **Configuration Summary**. If you're satisfied with the configuration of the new rule, click **New**.
8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a transport rule for messages that have a blank subject

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

This example creates the transport rule Blank Line Rule to reject messages that have a blank subject. The rule uses the enhanced status code 5.7.1 and includes the explanatory text "The message has a blank subject field."

```
New-TransportRule -Name "Blank Line Rule" -Enabled $true -SubjectMatchesPatterns
```

This example creates the transport rule Blank Line Rule to reject messages that have a blank subject on a Hub Transport server. The rule uses the customized DSN code 5.7.228 and includes the explanatory text "Messages must have a subject in the subject line or they are rejected."

Note:

When using a customized DSN code, you must define the DSN code and customized message using the **New-SystemMessage** cmdlet. For more information, see Associate a DSN Message with a Transport Rule.

```
New-TransportRule -Name "Blank Line Rule" -Enabled $true -SubjectMatchesPatterns
```

This example creates a customized DSN code and message.

```
New-SystemMessage -DsnCode 5.7.228 -Internal $True -Language En -Text "This messa
```

For detailed syntax and parameter information, see New-TransportRule or New-SystemMessage.

Associate a DSN Message with a Transport Rule

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 allows you to use a transport rule to reject messages based on conditions specified in the rule. The `RejectMessage` transport rule action is used to reject messages. When a message is rejected, a non-delivery report (NDR) is returned to the sender and the original message is deleted. When you create a transport rule on an Exchange 2010 Hub Transport server to reject messages, Exchange 2010 allows you to specify a delivery status notification (DSN) code, also known as an enhanced status code, and a rejection message.

For more information about transport rules, see Understanding Transport Rules.

Exchange 2010 also lets you customize the contents of the NDR that is returned to the sender by creating a custom DSN message. The custom content can contain information that you want to send to the recipient of the NDR, such as policy information and specific troubleshooting or contact information. For more information about how to customize DSN messages, see Managing Delivery Status Notifications.

The RejectMessage Transport Rule Action

To reject messages and specify a DSN message by using a transport rule, you must create the rule on a Hub Transport server. In the Shell, the transport rule action is known by the `RejectMessage` identifier. The same action is displayed using the descriptive string **send rejection message to sender with enhanced status code** in the EMC. The `RejectMessage` action lets you specify the following properties:

- **Enhanced Status Code** The enhanced status code you specify is displayed in the **Diagnostic information for administrators** section of the NDR. The value that's specified with this property can be 5.7.1, or any value from 5.7.10 through 5.7.999, inclusively. Enhanced status codes are also associated with a descriptive message that's displayed in the user information section of the NDR. If you use the Shell to create a transport rule, you must use the `RejectMessageEnhancedStatusCode` parameter to specify the enhanced status code.
- **Reject Reason** The text that's specified in this property is displayed in the **Diagnostic information for administrators** section of the NDR. If you use the Shell to create the rule, you can use the `RejectMessageReasonText` parameter to specify the reject reason.

Note:

If you use the Shell to create a transport rule that uses the `RejectMessage` action, you can create the rule without specifying the rejection message. If you don't specify the rejection message, the following default rejection message is used: `Delivery not authorized, message refused`. If you use the New Transport Rule wizard in EMC to create the rule, you must specify both the rejection message and the enhanced status code.

When you create a new transport rule with the `RejectMessage` transport rule action, Exchange 2010 searches the DSN message list for a DSN code that matches the value that is specified in the `RejectMessageEnhancedStatusCode` property of the transport rule. If a matching DSN code is found, Exchange 2010 automatically associates that DSN message with the transport rule action. If no matching DSN code is found, Exchange 2010

displays the following warning when you create the transport rule: `No custom DSN text is configured for the enhanced status code '5.7.xxx'. You can use the New-SystemMessage cmdlet to customize DSNs.`

Note:

If you specify a DSN code other than 5.7.1, you must create a custom DSN message to associate with that DSN code. If a matching DSN code doesn't exist, Exchange 2010 uses the 5.7.0 DSN code.

Use the EMC to create a transport rule to reject messages and provide a custom DSN code

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

1. On the **Conditions** page, select the **between members of distribution list and distribution list** condition, and then select the distribution groups that you want the transport rule to be applied to. For example, the following figure shows that the Sales Group distribution group and Brokerage Group distribution group have been selected for use with the condition.

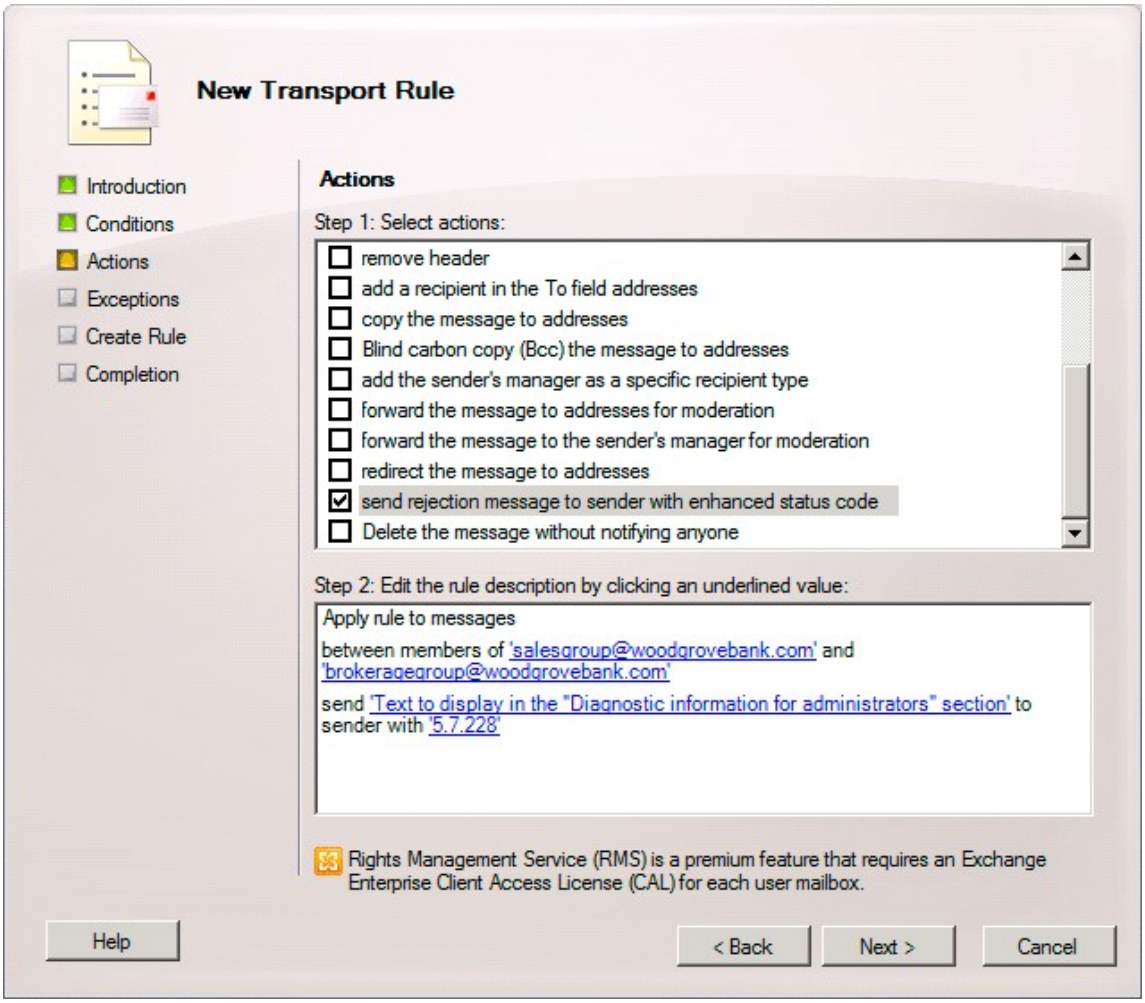
   Note:

   The **between members of distribution list and distribution list** predicate used in step 1 is an example. You can use any condition to suit your requirements.

2. On the **Actions** page, select the **send rejection message to sender with enhanced status code** action, and then type the text for the rejection message. To provide a helpful DSN message that explains why the message was rejected, specify a custom DSN code. For example, the following figure specifies that the rejection message **Text to display in the "Diagnostic information for administrators" section** will be included in the rejection message and will also include the custom DSN code 5.7.228. This code is associated with a new custom DSN message that's created by the command shown in DSN Message Association later in this topic.

Note:

You can check whether a custom DSN message already exists for a particular DSN code. Use the Get-SystemMessage cmdlet to list all custom DSN messages. You can also list standard DSN codes and the associated DSN messages by using the **Get-SystemMessage** cmdlet with the *Original* switch



For more information about how to create transport rules and how to configure an ethical wall, see the following topics:

- Create a Transport Rule
- Configure an Ethical Wall

Use the Shell to create a transport rule to reject messages and provide a custom DSN code

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

This example creates the transport rule SalesBrokerageEthicalWall to reject messages between the Sales and Brokerage distribution groups and use the custom DSN code 5.7.228 in the rejection response.

Note:

The `BetweenMemberOf` predicate used in this procedure is an example. You can use any condition to suit your requirements.

```
New-TransportRule SalesBrokerageEthicalWall -BetweenMemberOf1 "Sales" -BetweenMem
```

For detailed syntax and parameter information, see New-TransportRule.

Custom DSN Message Association

You use the New-SystemMessage cmdlet to create a custom DSN message for a DSN code. After the custom DSN message is created, Exchange 2010 automatically uses it when rejecting a message with the specified DSN code. If you specify the same custom DSN code in multiple transport rules, the DSN message is inserted in the NDRs that are generated by those transport rules.

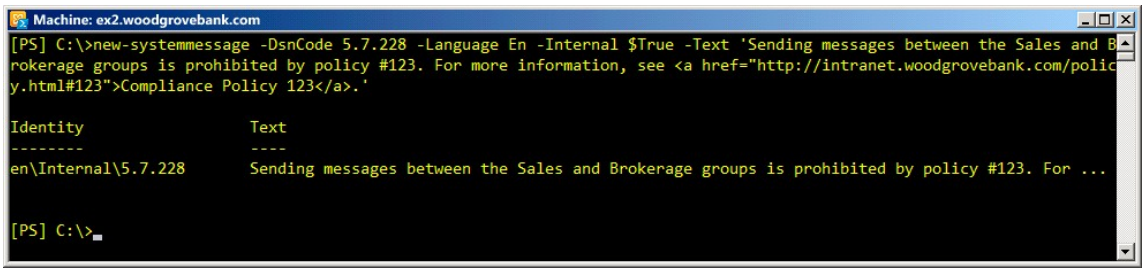
Note:

If you want to change the default text associated with the 5.7.1 DSN code, you must create a new custom DSN message by using the **New-SystemMessage** cmdlet. However, if you do this, the new text will be displayed any time that the 5.7.1 DSN code is used, including for messages that are rejected by other components of Exchange transport. Therefore, we recommend that you create a new DSN code for specific transport rule actions.

This example creates a custom DSN message with the DSN code 5.7.228. The DSN message is created in English. The message also includes a link to an internal Web site, which can provide more details about the organization's messaging policies.

```
New-SystemMessage -DsnCode 5.7.228 -Language En -Internal $True -Text 'Sending me
```

The following figure shows the result of entering the preceding command in the Shell.



Note:

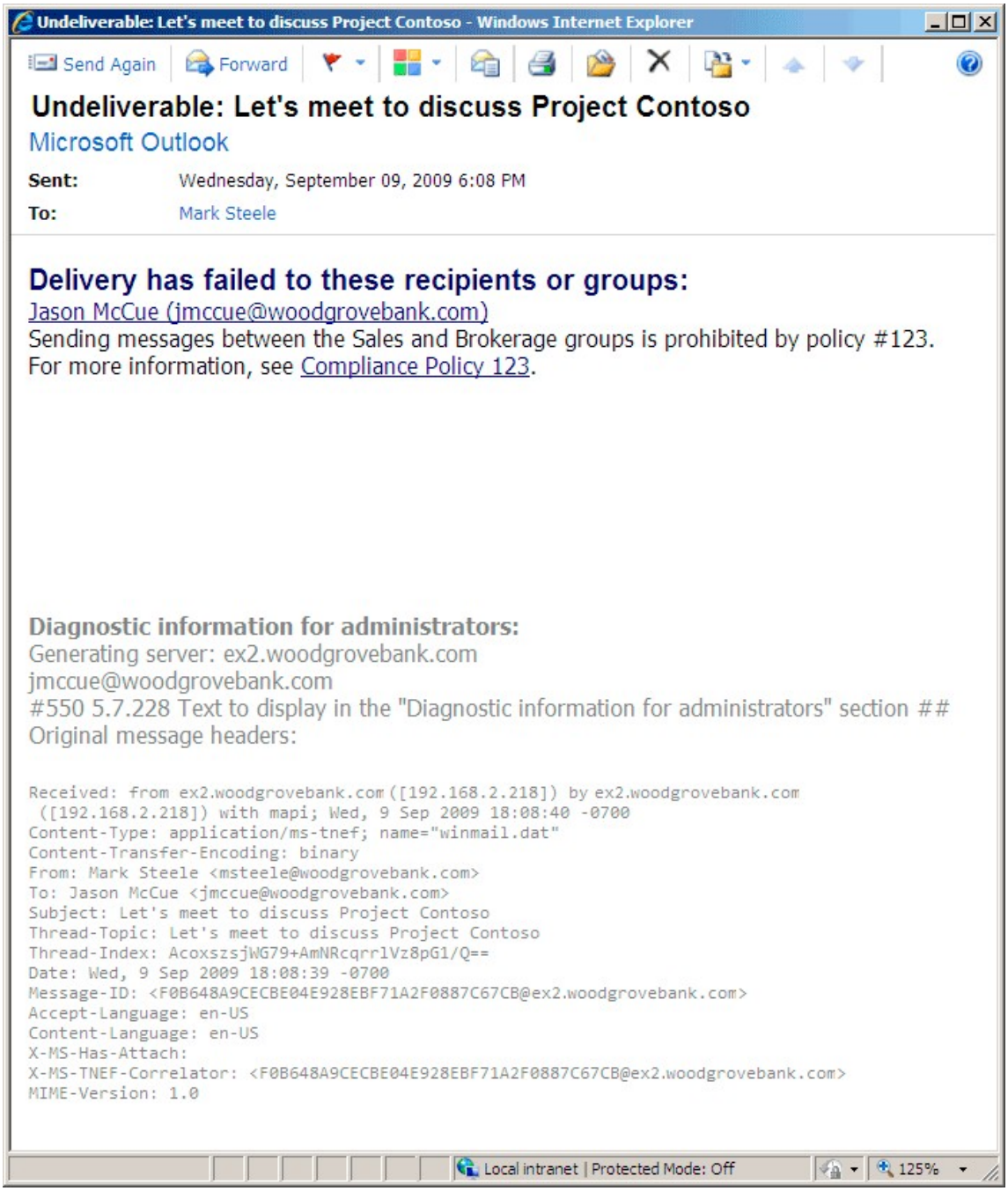
You can create custom DSN messages in additional languages and also remove the English versions of DSN messages completely. For a list of supported languages that you can use with DSN messages, see Supported Locales for Use with System Messages.

Example of an NDR with a Custom DSN Message

After you've created a custom DSN message for the DSN code you specified in the `RejectMessage` transport rule action, Exchange 2010 can use the custom DSN code and message in NDRs to senders whose messages are blocked by that transport rule.

For example, the following figure shows an NDR that was sent to Mark Steele who is a member of the Brokerage Group distribution group. He received the NDR because he tried to send a message to Jason McCue, who is a member of the Sales Group distribution group. A transport rule was created to enforce an ethical wall between the Brokerage Group and Sales Group. This transport rule prevents members of these groups from sending messages to each other.

The DSN message in the following figure also shows the link to the relevant corporate compliance policy. By clicking this link, Mark can read the policy that prohibits communication between the two groups.



1.11.4 Information Rights Management

Information Rights Management

Exchange Server 2010 > Messaging Policy and Compliance >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-08-10*

Understanding Information Rights Management

Learn about Information Rights Management (IRM), and how it helps you to protect sensitive messaging content.

Understanding Transport Protection Rules

Learn how you can automatically apply IRM-protection to messages based on your organization's messaging policy and content inspection.

Understanding Outlook Protection Rules

Learn how you can automatically apply IRM protection to messages in Outlook 2010 based on recipient, department, or message scope.

Understanding Transport Decryption

Learn how Exchange 2010 helps you apply messaging policies by decrypted IRM-protected content.

Understanding Journal Report Decryption

Learn how Exchange 2010 helps you comply with regulations by journaling IRM-protected messages.

Understanding Information Rights Management in Outlook Web App

Learn how Exchange 2010 allows your users to use IRM in Outlook Web App to read IRM-protected messages and apply IRM protection to messages they send.

Understanding Information Rights Management in Exchange ActiveSync

Learn how Exchange 2010 SP1 provides protocol-level support for Exchange ActiveSync, allowing users of supported mobile devices to create and access IRM-protected messages.

Understanding Information Rights Management Logging

Learn how Exchange 2010 SP1 provides logging of IRM operations between the Exchange and AD RMS servers in your organization.

Managing Information Rights Management

Learn how to manage Exchange 2010 IRM features.

1.11.4.1 Understanding Information Rights Management

Understanding Information Rights Management

Exchange Server 2010 > Messaging Policy and Compliance > Information Rights Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-30*

Every day, information workers use e-mail to exchange sensitive information such as financial reports and data, legal contracts, confidential product information, sales reports

and projections, competitive analysis, research and patent information, and customer and employee information. Because people can now access their e-mail from just about anywhere, mailboxes have transformed into repositories containing large amounts of potentially sensitive information. As a result, information leakage can be a serious threat to organizations. To help prevent information leakage, Microsoft Exchange Server 2010 includes the Information Rights Management (IRM) features, which provide persistent online and offline protection of e-mail messages and attachments.

Contents

What is Information Leakage?

Leakage of potentially sensitive information can be costly for an organization and have wide-ranging impact on the organization and its business, employees, customers, and partners. Local and industry regulations increasingly govern how certain types of information are stored, transmitted, and secured. To avoid violating applicable regulations, organizations must protect themselves against intentional, inadvertent, or accidental information leakage.

The following are some consequences resulting from information leakage:

- **Financial damage** Depending on the size, industry, and local regulations, information leakage may result in financial impact due to loss of business or due to fines and punitive damages imposed by courts or regulatory authorities. Public companies may also risk losing market capitalization due to adverse media coverage.
- **Damage to image and credibility** Information leakage can damage an organization's image and credibility with customers. Moreover, depending on the nature of communication, leaked e-mail messages can potentially be a source of embarrassment for the sender and the organization.
- **Loss of competitive advantage** One of the most serious threats from information leakage is the loss of competitive advantage in business. Disclosure of strategic plans or disclosure of merger and acquisition information can potentially lead to loss of revenue or market capitalization. Other threats include loss of research information, analytical data, and other intellectual property.

Return to top

Traditional Solutions to Information Leakage

Although traditional solutions to information leakage may protect initial access to data, they often don't provide constant protection. The following table lists some traditional solutions and their limitations.

Traditional solutions

Solution	Description	Limitations
Transport Layer Security (TLS)	TLS is an Internet standard protocol used to secure communications over a network by means of encryption. In a messaging environment, TLS is used to secure server/server and client/server communications. By default, Exchange 2010 uses TLS for all internal message transfers. Opportunistic TLS is also enabled by default for sessions with external hosts. Exchange first attempts to use TLS encryption for the session, but if a TLS connection can't be established with the destination server, Exchange uses SMTP. You can also configure domain security to enforce mutual TLS with external organizations. For more information, see Understanding Domain Security.	TLS only protects the SMTP session between two SMTP hosts. In other words, TLS protects information in motion, and it doesn't provide protection at the message-level or for information at rest. Unless the messages are encrypted using another method, messages in the sender's and recipients' mailboxes remain unprotected. For e-mail sent outside the organization, you can require TLS only for the first hop. After a remote SMTP host outside your organization receives the message, it can relay it to another SMTP host over an unencrypted session. Because TLS is a transport layer technology, it can't provide control over what the recipient does with the message.
E-mail encryption	Users can use technologies such as S/MIME to encrypt messages.	Users decide whether a message gets encrypted. There are additional costs of a public key infrastructure (PKI) deployment, with the accompanying overhead of certificate management for users and protection of private keys. After a message is decrypted, there's no control over what the recipient can do with the information. Decrypted information can be copied, printed, or forwarded. By default, saved attachments aren't protected. Messages encrypted using

		technologies such as S/MIME can't be accessed by your organization. The organization can't inspect message content, and therefore can't enforce messaging policies, scan messages for viruses or malicious content, or take any other action that requires accessing the content.

Finally, traditional solutions often lack enforcement tools that apply uniform messaging policies to prevent information leakage. For example, a user sends a message containing sensitive information and marks it as **Company Confidential** and **Do Not Forward**. After the message is delivered to the recipient, the sender or the organization no longer has control over the information. The recipient can willfully or inadvertently forward the message (using features such as automatic forwarding rules) to external e-mail accounts, subjecting your organization to substantial information leakage risks.

Return to top

IRM in Exchange 2010

Warning:

The IRM feature in Exchange 2010 is not compatible with AD RMS Cryptographic Mode 2. If the Exchange 2010 IRM features are critical for your organization, we recommend that you do not switch your AD RMS clusters to Cryptographic Mode 2.

In Exchange 2010, you can use IRM features to apply persistent protection to messages and attachments. IRM uses Active Directory Rights Management Services (AD RMS), an information protection technology in Windows Server 2008. With the IRM features in Exchange 2010, your organization and your users can control the rights recipients have for e-mail. IRM also helps allow or restrict recipient actions such as forwarding a message to other recipients, printing a message or attachment, or extracting message or attachment content by copying and pasting. IRM protection can be applied by users in Microsoft Outlook or Microsoft Office Outlook Web App, or it can be based on your organization's messaging policies and applied using transport protection rules or Outlook protection rules. Unlike other e-mail encryption solutions, IRM also allows your organization to decrypt protected content to enforce policy compliance.

AD RMS uses extensible rights markup language (XrML)-based certificates and licenses to certify computers and users, and to protect content. When content such as a document or a message is protected using AD RMS, an XrML license containing the rights that authorized users have to the content is attached. To access IRM-protected content, AD RMS-enabled applications must procure a use license for the authorized user from the AD RMS cluster.

Note:

In Exchange 2010, the Prelicensing agent attaches a use license to messages protected using the AD RMS cluster in your organization. For more details, see Prelicensing later in this topic.

Applications used to create content must be RMS-enabled to apply persistent protection to content using AD RMS. Microsoft Office applications, such as Word, Excel, PowerPoint

and Outlook are RMS-enabled and can be used to create and consume protected content.

IRM helps you do the following:

- Prevent an authorized recipient of IRM-protected content from forwarding, modifying, printing, faxing, saving, or cutting and pasting the content.
- Protect supported attachment file formats with the same level of protection as the message.
- Support expiration of IRM-protected messages and attachments so they can no longer be viewed after the specified period.
- Prevent IRM-protected content from being copied using the Snipping Tool in Microsoft Windows.

However, IRM can't prevent information from being copied using the following methods:

- Third-party screen capture programs
- Use of imaging devices such as cameras to photograph IRM-protected content displayed on the screen
- Users remembering or manually transcribing the information

To learn more about AD RMS, see Active Directory Rights Management Services.

AD RMS Rights Policy Templates

AD RMS uses XrML-based rights policy templates to allow compatible IRM-enabled applications to apply consistent protection policies. In Windows Server 2008, the AD RMS server exposes a Web service that can be used to enumerate and acquire templates. Exchange 2010 ships with the Do Not Forward template. When the Do Not Forward template is applied to a message, only the recipients addressed in the message can decrypt the message. The recipients can't forward the message, copy content from the message, or print the message. You can create additional RMS templates on the AD RMS server in your organization to meet your IRM protection requirements.

IRM protection is applied by applying an AD RMS rights policy template. Using policy templates, you can control permissions that recipients have on a message. Actions such as replying, replying to all, forwarding, extracting information from a message, saving a message, or printing a message can be controlled by applying the appropriate rights policy template to the message.

For more information about rights policy templates, see AD RMS Policy Template Considerations.

For more information about creating AD RMS rights policy templates, see AD RMS Rights Policy Templates Deployment Step-by-Step Guide.

Return to top

Applying IRM Protection to Messages

In Exchange 2010, IRM protection can be applied to messages using the following methods:

- **Manually by Outlook users** Your Outlook users can IRM-protect messages with the AD RMS rights policy templates available to them. This process uses the IRM functionality in Outlook, and not Exchange. However, you can use Exchange to access messages, and you can take actions (such as applying transport rules) to enforce your organization's messaging policy. For more information about using IRM in Outlook, see Introduction to using IRM for e-mail messages.
- **Manually by Outlook Web App users** When you enable IRM in Outlook Web App, users can IRM-protect messages they send, and view IRM-protected messages they receive. In Exchange 2010 Service Pack 1 (SP1), Outlook Web

App users can also view IRM-protected attachments using Web-Ready Document Viewing. For more information about IRM in Outlook Web App, see Understanding Information Rights Management in Outlook Web App.

- **Manually by Windows Mobile and Exchange ActiveSync device users** In the release to manufacturing (RTM) version of Exchange 2010, users of Windows Mobile devices can view and create IRM-protected messages. This requires users to connect their supported Windows Mobile devices to a computer and activate them for IRM. In Exchange 2010 SP1, you can enable IRM in Microsoft Exchange ActiveSync to allow users of Exchange ActiveSync devices (including Windows Mobile devices) to view, reply to, forward, and create IRM-protected messages. For more information about IRM in Exchange ActiveSync, see Understanding Information Rights Management in Exchange ActiveSync.
- **Automatically in Outlook 2010** You can create Outlook protection rules to automatically IRM-protect messages in Outlook 2010. Outlook protection rules are deployed automatically to Outlook 2010 clients, and IRM-protection is applied by Outlook 2010 when the user is composing a message. For more information about Outlook protection rules, see Understanding Outlook Protection Rules.
- **Automatically on Hub Transport servers** You can create transport protection rules to automatically IRM-protect messages on Exchange 2010 Hub Transport servers. For more information about transport protection rules, see Understanding Transport Protection Rules.

Note:
IRM protection isn't applied again to messages that are already IRM-protected. For example, if a user IRM-protects a message in Outlook or Outlook Web App, IRM protection isn't applied to the message using a transport protection rule.

Return to top

Scenarios for IRM Protection

Scenarios for IRM protection are described in the following table.

Scenarios for IRM protection

Sending IRM-protected messages	Supported	Requirements
Within the same on-premises Exchange 2010 deployment	Yes	For requirements, see IRM Requirements later in this topic.
Between different forests in an on-premises deployment	Yes	For requirements, see Configuring AD RMS to Integrate with Exchange Server 2010 Across Multiple Forests.
Between an on-premises Exchange 2010 deployment and a cloud-based Exchange 2010 organization	Yes	• Use an on-premises AD RMS server. • Export the trusted publishing domain from your on-premises AD RMS server. • Import the trusted publishing domain in your cloud-based organization.
To external recipients	No	Exchange 2010 doesn't include a solution for sending IRM-protected

		messages to external recipients in a non-federated organization. AD RMS offers solutions using trust policies. You can configure a trust policy between your AD RMS cluster and Windows Live ID. For messages sent between two organizations, you can create a federated trust between the two Active Directory forests using Active Directory Federation Services (AD FS). To learn more, see Understanding AD RMS Trust Policies.

Return to top

Decrypting IRM-Protected Messages to Enforce Messaging Policies

To enforce messaging policies and for regulatory compliance, you must be able to access encrypted message content. To meet eDiscovery requirements due to litigation, regulatory audits, or internal investigations, you must also be able to search encrypted messages. To help with these tasks, Exchange 2010 includes the following IRM features:

- **Transport decryption** To apply messaging policies, transport agents such as the Transport Rules agent should have access to message content. Transport decryption allows transport agents installed on Exchange 2010 servers to access message content. For more information, see Understanding Transport Decryption.
- **Journal report decryption** To meet compliance or business requirements, organizations can use journaling to preserve messaging content. The Journaling agent creates a journal report for messages subject to journaling and includes metadata about the message in the report. The original message is attached to the journal report. If the message in a journal report is IRM-protected, journal report decryption attaches a cleartext copy of the message to the journal report. For more information, see Understanding Journal Report Decryption.
- **IRM decryption for Exchange Search** With IRM decryption for Exchange Search, Exchange Search can index content in IRM-protected messages. When a discovery manager users Multi-Mailbox Search to perform a discovery search, IRM-protected messages that have been indexed are returned in search results. For more information, see Understanding Exchange Search. For more information about Multi-Mailbox Search, see Understanding Multi-Mailbox Search.

  Note:
  In Exchange 2010 SP1, members of the Discovery Management role group can access IRM-protected messages returned by a discovery search and residing in a discovery mailbox. To enable this functionality, use the *EDiscoverySuperUserEnabled* parameter with Set-IRMConfiguration cmdlet. For more information, see Configure IRM for Exchange Search and Discovery.

To enable these decryption features, Exchange servers must have access to the message. This is accomplished by adding the Federation mailbox, a system mailbox created by Exchange Setup, to the super users group on the AD RMS server. For details, see Add the Federation Mailbox to the AD RMS Super Users Group.

Return to top

Prelicensing

To view IRM-protected messages and attachments, Exchange 2010 automatically attaches a prelicense to protected messages. This prevents the client from having to make repeated trips to the AD RMS server to retrieve a use license, and enables offline viewing of IRM-protected messages and attachments. Prelicensing also allows IRM-protected messages to be viewed in Outlook Web App. When you enable IRM features, prelicensing is enabled by default.

Return to top

IRM Agents

In Exchange 2010, IRM functionality is enabled on Hub Transport servers using transport agents. IRM agents are installed by Exchange Setup on a Hub Transport server. You can't control IRM agents using the management tasks for transport agents.

Note:

In Exchange 2010, IRM agents are built-in agents. Built-in agents aren't included in the list of agents returned by the **Get-TransportAgent** cmdlet. For more information, see Understanding Transport Agents.

The following table lists the IRM agents implemented on Hub Transport servers.

IRM agents on Hub Transport servers

Agent	Event	Function
RMS Decryption agent	OnEndOfData (SMTP) and OnSubmittedMessage	Decrypts messages to allow access to transport agents.
Transport Rules agent	OnRoutedMessage	Flags messages that match rule conditions in a transport protection rule to be IRM-protected by the RMS Encryption agent.
RMS Encryption agent	OnRoutedMessage	Applies IRM protection to messages flagged by the Transport Rules agent and re-encrypts transport decrypted messages.
Prelicensing agent	OnRoutedMessage	Attaches a prelicense to IRM-protected messages.
Journal Report Decryption agent	OnCategorizedMessage	Decrypts IRM-protected messages attached to journal reports and embeds cleartext versions along with the original encrypted messages.

For more information about transport agents, see Understanding Transport Agents.

Return to top

IRM Requirements

To implement IRM in your Exchange 2010 organization, your deployment must meet the requirements described in the following table.

IRM requirements

Server	Requirements

AD RMS cluster	• **Operating system** Windows Server 2008 R2 or Windows Server 2008 SP2 with the hotfix Active Directory Rights Management Services role in Windows Server 2008 is required.
	• **Service connection point** Exchange 2010 and AD RMS-aware applications use the service connection point registered in Active Directory to discover an AD RMS cluster and URLs. AD RMS allows you to register the service connection point from within AD RMS Setup. If the account used to set up AD RMS isn't a member of the Enterprise Admins security group, service connection point registration can be performed after setup is complete. There is only one service connection point for AD RMS in an Active Directory forest.
	• **Permissions** Read and Execute permissions to the AD RMS server certification pipeline (`ServerCertification.asmx` file on AD RMS servers) must be assigned to the following:
	  • Exchange Servers group or individual Exchange servers
	  • AD RMS Service group on AD RMS servers
	By default, the ServerCertification.asmx file is located in the `\inetpub\wwwroot\_wmcs\certification\` folder on AD RMS servers. For details, see Set Permissions on the AD RMS Server Certification Pipeline.
	• **AD RMS super users** To enable transport decryption, journal report decryption, IRM in Outlook Web App, and IRM for Exchange Search, you must add the Federation mailbox, a system mailbox created by Exchange 2010 Setup, to the super users group on the AD RMS cluster. For details, see Add the Federation Mailbox to the AD RMS Super Users Group.

Exchange	• Exchange 2010 is required. • The hotfix FIX: ArgumentNullException exception error message when a .NET Framework 2.0 SP2-based application tries to process a response with zero-

	length content to an asynchronous ASP.NET Web service request: "Value cannot be null" is recommended for Microsoft .NET Framework 2.0 SP2.
Outlook	• Users can IRM-protect messages in Outlook. Beginning with Outlook 2003, AD RMS templates for IRM-protecting messages is supported. • Outlook protection rules are an Exchange 2010 and Outlook 2010 feature. Previous versions of Outlook don't support this feature.
Exchange ActiveSync	• Devices supporting Exchange ActiveSync protocol version 14.1, including Windows Mobile devices, can support IRM in Exchange ActiveSync. The mobile e-mail application on a device must support the **RightsManagementInformation** tag defined in Exchange ActiveSync protocol version 14.1. In Exchange 2010 SP1, IRM in Exchange ActiveSync allows users with supported devices to view, reply to, forward, and create IRM-protected messages without requiring the user to connect the device to a computer and activate it for IRM. For details, see Understanding Information Rights Management in Exchange ActiveSync.

Note:

AD RMS cluster is the term used for an AD RMS deployment in an organization, including a single server deployment. AD RMS is a Web service. It doesn't require that you set up a Windows Server 2008 failover cluster. For high availability and load-balancing, you can deploy multiple AD RMS servers in the cluster and use Network Load Balancing.

Important:

In a production environment, installing AD RMS and Exchange on the same server isn't supported.

Exchange 2010 IRM features support Microsoft Office file formats. You can extend IRM protection to other file formats by deploying custom protectors. For more information about custom protectors, see Information Protection and Control Partners in Independent Software Vendors.

Return to top

Configuring and Testing IRM

You must use the Exchange Management Shell to configure IRM features in Exchange 2010. To configure individual IRM features, use the Set-IRMConfiguration cmdlet. You can enable or disable IRM for internal messages, transport decryption, journal report decryption, Exchange Search, and Outlook Web App. For more information about configuring IRM features, see Managing Information Rights Management.

After you set up an Exchange 2010 server, you can use the Test-IRMConfiguration cmdlet to perform end-to-end tests of your IRM deployment. These tests are useful to verify IRM functionality immediately after initial IRM configuration and on an ongoing basis. The cmdlet performs the following tests:

- Inspects IRM configuration for your Exchange 2010 organization.
- Checks the AD RMS server for version and hotfix information.
- Verifies whether an Exchange server can be activated for RMS by retrieving a Rights Account Certificate (RAC) and client licensor certificate.
- Acquires AD RMS rights policy templates from the AD RMS server.
- Verifies that the specified sender can send IRM-protected messages.
- Retrieves a super user use license for the specified recipient.
- Acquires a prelicense for the specified recipient.

Return to top

1.11.4.2 Understanding Transport Protection Rules

Understanding Transport Protection Rules

Exchange Server 2010 > Messaging Policy and Compliance > Information Rights Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-21*

E-mail messages and attachments increasingly contain business critical information such as product specifications, business strategy documents, and financial data, or personally identifiable information (PII) such as contact details, social security numbers, credit card numbers, and employee records. There are a number of industry-specific and local regulations in many parts of the world that govern the collection, storage, and disclosure of PII.

To help protect sensitive information, organizations create messaging policies that provide guidelines about how to handle this information. In Exchange Server 2010, you can use transport protection rules to implement these messaging policies by inspecting message content, encrypting sensitive e-mail content, and using rights management to control access to the content.

Looking for management tasks related to managing IRM? See Managing Information Rights Management.

Transport Protection Rules and AD RMS

Transport protection rules allow you to use transport rules to IRM-protect messages by applying an Active Directory Rights Management Services (AD RMS) rights policy template.

Note:

AD RMS is an information protection technology that works with Rights Management Service (RMS)-enabled applications and clients to protect sensitive information online and offline. To use IRM protection in an on-premise Exchange deployment, Exchange 2010 requires an on-premise deployment of the Windows Server 2008 operating system AD RMS.

AD RMS uses XML-based policy templates to allow compatible IRM-enabled applications to apply consistent protection policies. In Windows Server 2008, the AD RMS server exposes a Web service that can be used to enumerate and acquire templates. Exchange 2010 ships with the Do Not Forward template.

When the Do Not Forward template is applied to a message, only the recipients addressed in the message can decrypt the message. The recipients can't forward the message to anyone else, copy content from the message, or print the message.

Additional RMS templates can be created in the on-premises AD RMS deployment to meet rights protection requirements in your organization.

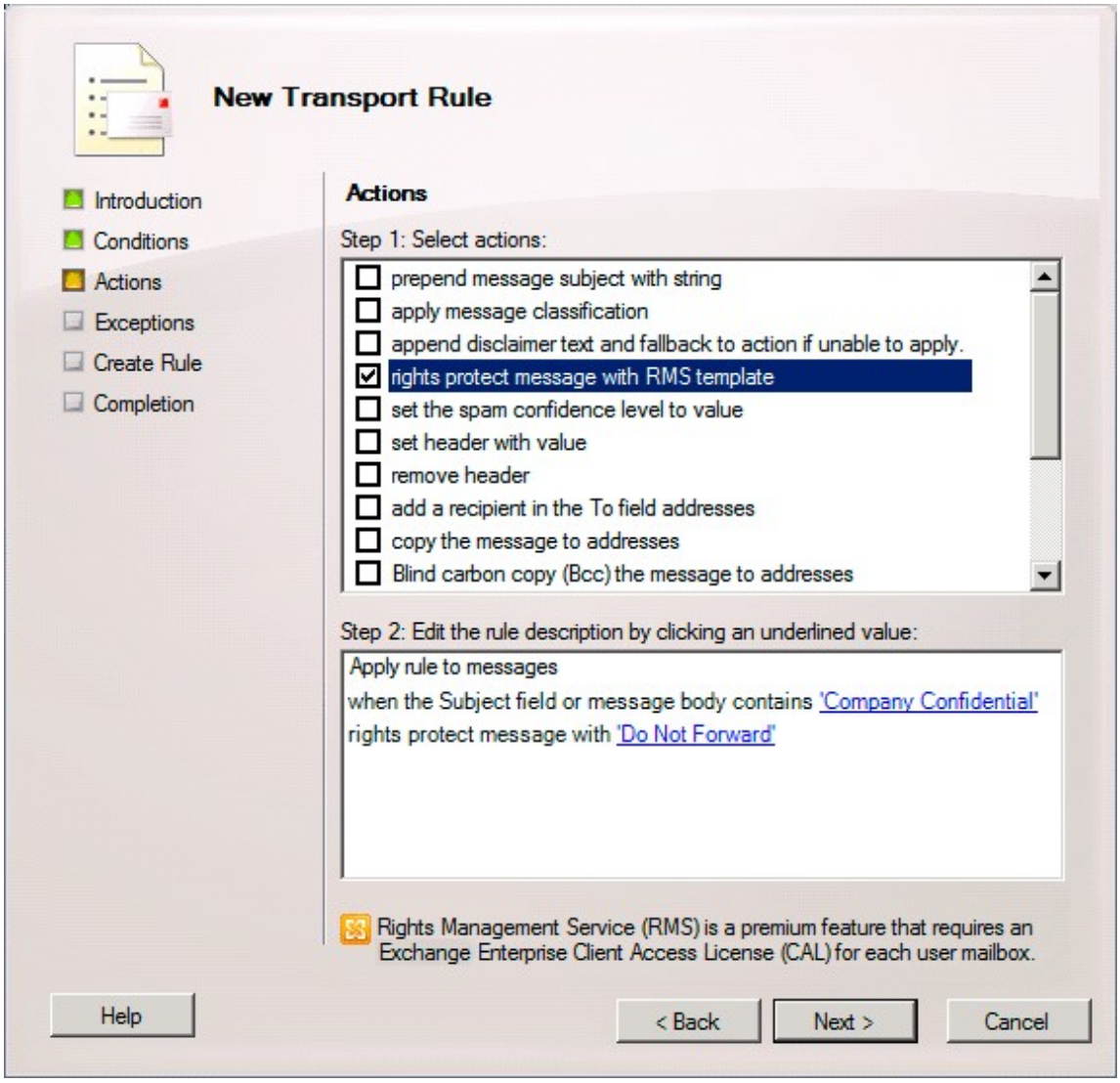
Important:

If a rights policy template is removed from the AD RMS server, you must modify any transport protection rules that use the removed template. If a transport protection rule continues to use a rights policy template that's been removed, the AD RMS server will fail to license the content to any of the recipients, and a non-delivery report (NDR) will be delivered to the sender.
In Windows Server 2008, rights policy templates can be archived instead of deleted. Archived templates can still be used to license content, but when you create or modify a transport protection rule, archived templates aren't included in the list of templates.

For more information about creating AD RMS templates, see AD RMS Rights Policy Templates Deployment Step-by-Step Guide.

Automatic Protection Using Transport Protection Rules

Messages containing business critical information or PII can be identified by using a combination of transport rule conditions, including regular expressions to identify text patterns such as social security numbers. Organizations require different levels of protection for sensitive information. Some information may be restricted to employees, contractors, or partners; while other information may be restricted only to full-time employees. The desired level of protection can be applied to messages by applying an appropriate rights policy template. For example, users may mark messages or e-mail attachments as Company Confidential. As illustrated in the following figure, you can create a transport protection rule to inspect message content for the words "Company Confidential", and automatically IRM-protect the message.



For more information about creating transport rules to enforce rights protection, see Create a Transport Protection Rule.

Persistent Protection of E-Mail Attachments

Users send business critical information and PII in e-mail attachments using common Microsoft Office file formats such as Microsoft Office Word, Excel, and PowerPoint. All of these file formats support persistent protection via IRM, and you can make sure that the business critical information and PII in these documents are properly protected. Transport protection rules apply the same protection to e-mail messages and attachments in supported file formats.

Transport Rules Agent and Encryption Agent

When you use transport protection rules to IRM-protect messages based on rule conditions, the Transport Rules agent on the Hub Transport server inspects messages. If they meet all the conditions and none of the exceptions, it flags the message to be IRM-protected. The Encryption agent, a built-in transport agent that fires on the **OnRoutedMessage** event, actually applies IRM protection to the message. The Encryption agent acts on messages only if IRM is enabled for internal messages. For more information about enabling IRM, see Enable or Disable IRM for Internal Messages.

When the transport service is restarted, and it processes the first message that requires IRM encryption, the Encryption agent must be able to reach an AD RMS server in the organization. For subsequent messages, the agent doesn't need to contact the AD RMS server. Upon failure to encrypt a message due to transient conditions, Exchange retries the message three times at 10-minute intervals. After three retries, if the message can't be encrypted, it isn't delivered to recipients. An NDR is sent to the sender. We recommend that you plan your AD RMS deployment for high availability to make sure message flow isn't impacted.

When planning to use transport protection rules, you must consider the type of information you want to protect and plan on creating rules accordingly. In Exchange 2010, transport rules have a large number of predicates that allow you to inspect message content, including supported attachments, message headers, sender and recipient addresses, their Active Directory attributes such as department, distribution group membership, and management relationships of the sender with recipients. For more details about transport rule predicates available in Exchange 2010, see Transport Rule Predicates.

You must also consider the messaging traffic in your organization, and the number of messages that will be protected using transport protection rules. Applying IRM protection to a large number of messages requires more resources on the Hub Transport server. Additionally, protecting a large number of messages or all messages also impacts the client experience, particularly for Microsoft Outlook users.

1.11.4.3 Understanding Outlook Protection Rules

Understanding Outlook Protection Rules

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-13*

Information workers exchange sensitive information such as financial reports and data, customer and employee information, and confidential product information and specifications, by e-mail everyday. In Microsoft Exchange Server 2010, Microsoft Outlook, and Microsoft Office Outlook Web App, users can apply Information Rights Management (IRM) protection to messages by applying an Active Directory Rights Management Services (AD RMS) rights policy template. This requires an AD RMS deployment in the organization. For more information about AD RMS, see Active Directory Rights Management Services.

However, when left to the discretion of users, messages may be sent in clear text without IRM protection. In organizations that use e-mail as a hosted service, there's a risk of information leakage as a message leaves the client and is routed and stored outside the boundaries of an organization. Although e-mail hosting companies may have well-defined procedures and checks to help mitigate the risk of information leakage, after a message leaves the boundary of an organization, the organization loses control of the information. Outlook protection rules can help protect against this type of information leakage.

Looking for management tasks related to managing IRM? See Managing Information Rights Management.

Automatic IRM Protection in Outlook 2010

In Exchange 2010, Outlook protection rules help your organization protect against the risk of information leakage by automatically applying IRM-protection to messages in

Outlook 2010. Messages are IRM-protected before they leave the Outlook client. This protection is also applied to any attachments using supported file formats.

When you create Outlook protection rules on an Exchange 2010 server, the rules are automatically distributed to Outlook 2010 by using Exchange Web Services. For Outlook 2010 to apply the rule, the AD RMS rights policy template you specify must be available on users' computers.

Important:

If a rights policy template is removed from the AD RMS server, you must modify any Outlook protection rules that use the removed template. If an Outlook protection rule continues to use a rights policy template that's been removed, and transport decryption is enabled in the organization, the Decryption agent will fail to decrypt the message protected with a template that's no longer available. If transport decryption is configured as mandatory, the Hub Transport server will reject the message and send a non-delivery report (NDR) to the sender. For more details about transport decryption, see Understanding Transport Decryption. For more details about AD RMS rights policy templates, see AD RMS Policy Template Considerations.
In Windows Server 2008, rights policy templates can be archived instead of deleted. Archived templates can still be used to license content, but when you create or modify an Outlook protection rule, archived templates aren't included in the list of templates.

Outlook protection rules are similar to transport protection rules. Both are applied based on message conditions, and both protect messages by applying an AD RMS rights protection template. However, transport protection rules are applied on the Hub Transport server by the Transport Rules agent. Outlook protection rules are applied in Outlook 2010, before the message leaves the user's computer. Messages protected by an Outlook protection rule enter the transport pipeline with IRM protection already applied. Additionally, messages protected with an Outlook protection rule are also saved in an encrypted format in the Sent Items folder of the sender's mailbox.

Note:

If transport decryption is enabled in your Exchange organization, messages that are IRM-protected by an Outlook protection rule using the AD RMS server in your organization can be decrypted by the Decryption agent on Hub Transport servers. Message content can be inspected by the Transport Rules agent and other transport agents installed on the Hub Transport server. For more details about transport decryption, see Understanding Transport Decryption.

When you use transport protection rules, users have no indication of whether a message is going to be automatically protected on the Hub Transport server. When an Outlook protection rule is applied to a message in Outlook 2010, users know if a message will be IRM-protected. If required, users can also select a different rights policy template.

Creating Outlook Protection Rules

To create Outlook protection rules, you must use the New-OutlookProtectionRule cmdlet in the Exchange Management Shell. For detailed instructions, see Create an Outlook Protection Rule.

When creating a rule, you can specify whether the user can override it, either by removing IRM-protection or by applying a different AD RMS rights policy template than the one specified in the rule. If a user overrides the IRM protection applied by an Outlook protection rule, Outlook 2010 inserts the `X-MS-Outlook-Client-Rule-Overridden` header in the message, which allows you to determine that the rule was overridden by the user.

Predicates in Outlook Protection Rules

Outlook protection rules allow you to use three predicates to automatically apply IRM protection in Outlook 2010:

- **FromDepartment** The *FromDepartment* predicate looks up the sender's department attribute in Active Directory and automatically IRM-protects the message if the sender's department matches the department specified in the rule. For example, you can create an Outlook protection rule to automatically protect all messages sent by the Research department.
- **SentTo** Your organization may need to protect messages sent to certain sensitive recipients, such as the All Company or Finance distribution groups. Using the *SentTo* predicate, you can create an Outlook protection rule to automatically IRM-protect messages sent to specified recipients.
- **SentToScope** The *SentToScope* predicate allows you to create an Outlook protection rule to automatically IRM-protect messages sent inside or outside the organization. For example, you can use the *SentToScope* predicate with the *FromDepartment* predicate to IRM-protect messages sent by a particular department to internal users.

1.11.4.4 Understanding Transport Decryption

Understanding Transport Decryption

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-06-28*

In Microsoft Exchange Server 2010, Microsoft Outlook 2010, and Microsoft Office Outlook Web App, users can use Information Rights Management (IRM) to protect their messages. You can create Outlook protection rules to automatically apply IRM protection to messages before they're sent from an Outlook 2010 client. You can also create transport protection rules to apply IRM protection to messages in transit that match the rule conditions. Transport decryption allows access to IRM-protected messaging content to enforce messaging policies.

Looking for management tasks related to managing IRM? See Managing Information Rights Management.

Limitations of Other Encryption Solutions

If it's critical that your organization protects sensitive information, including high business impact (HBI) information and personally identifiable information (PII), consider encrypting e-mail messages and attachments. E-mail encryption solutions such as S/MIME have been available for a long time. These encryption solutions have seen varying degrees of adoption in organizations of different types. However, such solutions present the following challenges:

- **Inability to apply messaging policies** Organizations also face compliance requirements that require inspection of messaging content to make sure it adheres to messaging policies. However, messages encrypted with most client-based encryption solutions, including S/MIME, prevent content inspection on the server. Without content inspection, an organization can't validate that all messages sent or received by its users comply with messaging policies. For

example, to comply with a legal regulation, you've configured a transport rule to detect PII, such as a social security number, and automatically apply a disclaimer to the message. If the message is encrypted, the Transport Rules agent on the Hub Transport server can't access message content, and therefore won't apply the disclaimer. This results in a violation of the policy.

- **Decreased security** Antivirus software is unable to scan encrypted message content, further exposing an organization to risk from malicious content such as viruses and worms. Encrypted messages are generally considered to be trusted by most users, thereby increasing the likelihood of a virus spreading throughout your organization. For example, you've configured an Outlook protection rule to automatically apply IRM protection to all messages sent to the All Employees distribution list with the Company Confidential rights management service (RMS) template. A user's workstation is infected with a virus that propagates by automatically using Reply All to reply to messages. If the message carrying the virus is encrypted, the antivirus scanner can't scan the message.
- **Impact to custom transport agents** Many organizations develop custom transport agents for different purposes, such as meeting additional processing requirements for compliance, security, or custom message routing. Custom transport agents developed by an organization to inspect or modify messages are unable to process encrypted messages. If the custom transport agents developed by your organization can't access message content, message encryption may prevent your organization from meeting the goals for which the custom transport agents are developed.

Using Transport Decryption for Encrypted Content

In Exchange 2010, IRM features address these challenges. If messages are IRM-protected, transport decryption allows you to decrypt them in transit. IRM-protected messages are decrypted by the Decryption agent, a compliance-focused transport agent.

Note:

In Exchange 2010, the Decryption agent is a built-in agent. Built-in agents aren't included in the list of agents returned by the **Get-TransportAgent** cmdlet. For more details, see Understanding Transport Agents.

The Decryption agent decrypts the following types of IRM-protected messages:

1. Messages IRM-protected by the user in Outlook Web App.
2. Messages IRM-protected by the user in Outlook 2010.
3. Messages IRM-protected automatically by Outlook protection rules in Outlook 2010.

Important:

Only messages IRM-protected by the AD RMS server in your organization are decrypted by the Decryption agent.

Note:

Messages protected in-transit using transport protection rules aren't required to be decrypted by the Decryption agent. The Decryption agent fires on the **OnEndOfData** and **OnSubmit** transport events. Transport protection rules are applied by the Transport Rules agent, which fires on the **OnRoutedMessage** event, and IRM-protection is applied by the Encryption agent on the **OnRoutedMessage** event. For more information about transport agents and a list of SMTP events on which they can be registered, see Understanding Transport Agents.

Transport decryption is performed on the first Exchange 2010 Hub Transport server that handles a message in an Active Directory forest. If a message is transferred to a Hub Transport server in another Active Directory forest, the message is decrypted again. After

decryption, unencrypted content is available to other transport agents on that server. For example, the Transport Rules agent on a Hub Transport server can inspect message content and apply transport rules. Any actions specified in the rule, such as applying a disclaimer or modifying the message in any other way, can be taken on the unencrypted message. Third-party transport agents, such as antivirus scanners, can scan the message for viruses and malware. After other transport agents have inspected the message and possibly made modifications to it, it's encrypted again with the same user rights that it had before being decrypted by the Decryption agent. The same message isn't decrypted again by other Hub Transport servers in the organization.

Messages decrypted by the Decryption agent don't leave the Hub Transport server without being encrypted again. If a transient error is returned when decrypting or encrypting the message, the Hub Transport server retries the operation twice. After the third failure, the error is treated as a permanent error. If any permanent errors occur, including when transient errors are treated as permanent errors after retries, the Hub Transport server treats them as follows:

- If the permanent error occurs during decryption, a non-delivery report (NDR) is sent only if transport decryption is set to `Mandatory`, and the encrypted message is sent with the NDR. For more details about the configuration options available for transport decryption, see Configuring Transport Decryption later in this topic.
- If the permanent error occurs during re-encryption, an NDR is always sent without the decrypted message.

Important:

Any custom or third-party agents installed on a Hub Transport server have access to the decrypted message. You must consider the behavior of such transport agents. We recommend that you test all custom and third-party transport agents thoroughly before you deploy them in a production environment.
After a message is decrypted by the Decryption agent, if a transport agent creates a new message and embeds (attaches) the original message to the new one, only the new message is protected. The original message, which becomes an attachment to the new message, doesn't get re-encrypted. A recipient receiving such a message can open the attached message and take actions such as forwarding or replying, which would bypass rights enforcement.

Configuring Transport Decryption

Transport decryption is configured by using the Set-IRMConfiguration cmdlet in the Exchange Management Shell. However, before you configure transport decryption, you must provide Exchange 2010 servers the right to decrypt content protected by your AD RMS server. This is done by adding the Federation mailbox to the super users group configured on the AD RMS cluster in your organization.

Important:

In cross-forest AD RMS deployments where you have an AD RMS cluster deployed in each forest, you must add the Federation mailbox to the super users group on the AD RMS cluster in each forest to allow an Exchange 2010 Hub Transport server to decrypt the messages protected against each AD RMS cluster.

For details, see Add the Federation Mailbox to the AD RMS Super Users Group.

Exchange 2010 allows two different settings when enabling transport decryption:

- **Mandatory** When transport decryption is set to `Mandatory`, the Decryption agent rejects the message and returns an NDR to the sender if a permanent error is returned when decrypting a message. If your organization doesn't want a message to be delivered if it can't be successfully decrypted and actions such as antivirus scanning and transport rules are applied, you must choose this setting.

- **Optional** When transport decryption is set to Optional, the Decryption agent uses a best-effort approach. Messages that can be decrypted are decrypted, but messages with a permanent error on decryption are also delivered. If your organization prioritizes message delivery over messaging policy, you must use this setting.

For more information about configuring transport decryption, see Enable or Disable Transport Decryption.

1.11.4.5 Understanding Journal Report Decryption

Understanding Journal Report Decryption

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-06-17*

In Microsoft Exchange Server 2010, Information Rights Management (IRM) allows Microsoft Outlook 2010 and Microsoft Office Outlook Web App users to protect their messages. You can create Outlook protection rules to automatically apply IRM-protection to messages before they're sent from an Outlook 2010 client. You can also create transport protection rules to apply IRM protection to messages in transit that match the rule conditions.

To learn about Outlook protection rules, see Understanding Outlook Protection Rules.

Limitations of Standard Encryption Solutions

If your organization encrypts messages by using traditional solutions such as S/MIME, your records managers won't be able to inspect or search the encrypted content. Archiving encrypted messages that contain inaccessible and unsearchable content may not meet business, regulatory, or compliance requirements. When faced with an electronic discovery (eDiscovery) request, an inability to decrypt, search, and present content from encrypted messages can be a challenge, and failure to do so may expose your organization to legal and financial risks.

Also, your organization's messaging policies may require journaled messages to be decrypted so the content can be accessible to eDiscovery tools, automated processes, or records managers who access a journaling mailbox. Journal report decryption in Exchange 2010 can help you meet these requirements.

To learn more about journaling, see Understanding Journaling and Understanding Journal Reports.

Journal Report Decryption

Journal report decryption allows you to save a clear-text copy of IRM-protected messages in journal reports, along with the original, IRM-protected message. If the IRM-protected message contains any supported attachments that were protected by the Active Directory Rights Management Services (AD RMS) cluster in your organization, the attachments are also decrypted.

Important:

To use journal report decryption, you must have an Exchange Enterprise client access

license (CAL). Journal report decryption only supports premium journaling.

Decryption is performed by the Journal Report Decryption agent, a compliance-focused transport agent. The Journal Report Decryption agent fires on the **OnCategorizedMessage** event. Messages protected in-transit using transport protection rules are already encrypted by the Encryption agent, which fires on the **OnRoutedMessage** event, before they get to the Journal Report Decryption agent. The Journal Report Decryption agent decrypts these messages.

Note:
In Exchange 2010, the Journal Report Decryption agent is a built-in agent. Built-in agents aren't included in the list of agents returned by the **Get-TransportAgent** cmdlet. For more details, see Understanding Transport Agents.

The agent decrypts the following types of IRM-protected messages:

1. Messages that were IRM-protected by the user in Outlook Web App.
2. Messages that were IRM-protected by the user in Outlook 2010.
3. Messages that were IRM-protected automatically in Outlook 2010 by using Outlook protection rules.
4. Messages that were IRM-protected automatically in transit by using transport protection rules.

Important:
Only messages that were IRM-protected by the AD RMS server in your organization are decrypted by the Journal Report Decryption agent. The agent doesn't decrypt an attachment if it isn't protected at the same time as the message (and therefore doesn't have the same use license), or if an IRM-protected file is attached to an unprotected message.

Configuring Journal Report Decryption

Journal report decryption is configuredb using the Set-IRMConfiguration cmdlet in the Exchange Management Shell. However, before you configure journal report decryption, you must assign Exchange 2010 servers the permissions to decrypt content that's IRM-protected by your AD RMS server. To do this, you add the Federation mailbox to the super users group configured on your organization's AD RMS cluster. For details, see Add the Federation Mailbox to the AD RMS Super Users Group.

Important:
In cross-forest AD RMS deployments where you have an AD RMS cluster deployed in each forest, you must add the Federation mailbox to the super users group on the AD RMS cluster in each forest to allow Exchange 2010 Hub Transport servers to decrypt the messages protected against each AD RMS cluster.

For details about how to configure journal report decryption, see Enable or Disable Journal Report Decryption.

After you enable journal report decryption, the journaling mailbox may contain journal reports with sensitive information in an unencrypted form. As a best practice, we recommend that access to the journaling mailbox be monitored closely and restricted only to authorized individuals. This is a best-practice even if you're not using IRM protection for e-mail.

1.11.4.6 Understanding Information Rights Management in Outlook Web App

Understanding Information Rights Management in Outlook Web App

Exchange Server 2010 > Messaging Policy and Compliance > Information Rights Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

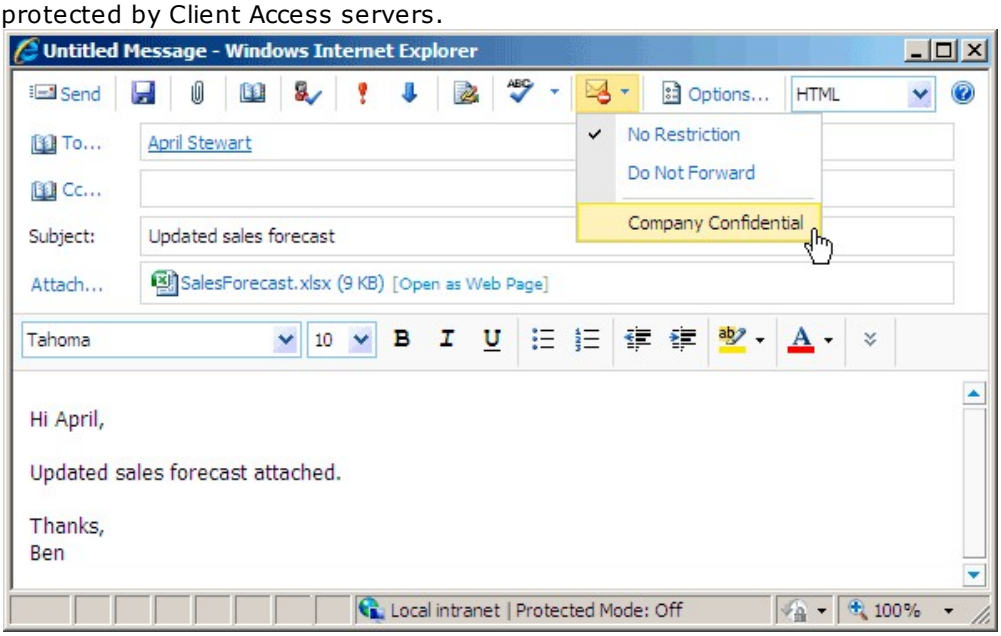
Topic Last Modified: *2010-08-10*

Information workers increasingly use e-mail to exchange sensitive information. To help secure this information, organizations can use Information Rights Management (IRM) to apply persistent protection to messaging content. Prior to Microsoft Exchange Server 2010, effective use of IRM protection was limited to Outlook clients. In Exchange Server 2007, Microsoft Outlook Web Access users were required to download the Rights Management add-in for Microsoft Internet Explorer so they could access IRM-protected content.

In Exchange 2010, IRM in Outlook Web App allows your users to access the rich IRM functionality offered by Exchange to apply persistent IRM-protection to messaging content.

The following IRM functionality is available in Outlook Web App:

- **Send IRM-protected messages** As shown in the following figure, Outlook Web App users can use the permissions drop-down list and select a rights policy template to apply to the message. This allows users to send IRM-protected messages from within Outlook Web App. Messages are IRM-protected by Client Access servers.



- **IRM-protected attachments** When users send an IRM-protected message from Outlook Web App, any files attached to the message also receive the same IRM protection and are protected by using the same rights policy template as the message. In Exchange 2010, IRM protection is applied to files associated with Microsoft Office Word, Excel, and PowerPoint, as well as .xps files and e-mail messages. IRM protection is applied to an attachment only if it's not already IRM-protected. To learn more about Active Directory Rights Management Services (AD RMS) rights policy templates, see Understanding Information Rights Management.

Note:
IRM in Outlook Web App protects only the supported file attachments mentioned in this section. Attachments that use unsupported file formats aren't protected. When Outlook Web App users protect a message and attach a file of an unsupported type, a notification is displayed informing the users that only supported file types are protected.

Important:
IRM protection can't be applied to a message that's already signed or encrypted by using S/MIME. To apply IRM protection, S/MIME signature and encryption must be removed from the message. The same applies for IRM-protected messages; users can't sign or encrypt them by using S/MIME.

- **Read IRM-protected messages** Messages protected by senders using your organization's AD RMS cluster are rendered in the preview pane in Outlook Web App. No add-ins need to be installed, and the computer doesn't need to be enrolled in the AD RMS deployment. When a user opens a message or views it in the preview pane, the message is decrypted by using the use license added by the Pre-licensing agent. After decryption, the message is displayed in the preview pane. If a pre-license isn't available, Outlook Web App requests one from the AD RMS server and then renders the message. When reading IRM-protected attachments in Outlook Web App, Web-Ready Document Viewing isn't available.

  Note:
  IRM in Outlook Web App can't prevent users from taking screen captures by using Print Screen functionality in the way Outlook and other Office applications do. This impacts the EXTRACT right, which prevents message content from being copied, if specified in the AD RMS rights policy template.

- **Cross-browser, multiple platform IRM support** IRM in Outlook Web App offers cross-browser, multiple platform IRM support. IRM in Outlook Web App is supported in all browsers supported by Exchange 2010, including on Apple Macintosh and Linux operating systems. To learn more about supported browsers and operating systems, see Outlook Web App Supported Browsers.
- **WebReady Document Viewing** In Exchange 2010 SP1, users can view supported IRM-protected attachments by using WebReady Document Viewing. This allows users to view supported attachments without having to download the attachment use the associated application. To learn more about WebReady Document Viewing, including the supported file formats, see Understanding File and Data Access for Outlook Web App.

Looking for management tasks related to managing IRM? See Managing Information Rights Management.

Enabling IRM in Outlook Web App

To enable IRM in Outlook Web App, you must add the Federation mailbox, a system mailbox created by Exchange 2010 Setup, to the super users group in AD RMS. For details, see Add the Federation Mailbox to the AD RMS Super Users Group. This allows Exchange 2010 servers to access IRM-protected messages.

You must also enable IRM in Outlook Web App by using the Set-IRMConfiguration cmdlet in the Exchange Management Shell. This enables IRM in Outlook Web App for your Exchange 2010 organization. You can disable or enable IRM in Outlook Web App for an Outlook Web App virtual directory. You can also control IRM in Outlook Web App at the following levels of granularity:

- **Per-Outlook Web App virtual directory** To enable or disable IRM in Outlook Web App for an Outlook Web App virtual directory, use the **Set-OWAVirtualDirectory** cmdlet and set the *IRMEnabled* parameter to `$false` or `$true` (default). This allows you to disable IRM in Outlook Web App for one virtual directory on an Exchange 2010 Client Access server, while keeping it enabled on another virtual directory on a different Client Access server.
- **Per-Outlook Web App mailbox policy** To enable or disable IRM in Outlook Web App for an Outlook Web App mailbox policy, use the **Set-OWAMailboxPolicy** cmdlet and set the *IRMEnabled* parameter to `$false` or `$true` (default). This allows you to enable IRM in Outlook Web App for one set of users and disable it for another set of users by assigning them a different

Outlook Web App mailbox policy.

For more information, see Enable or Disable Information Rights Management on Client Access Servers.

1.11.4.7 Understanding Information Rights Management in Exchange ActiveSync

Understanding Information Rights Management in Exchange ActiveSync

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-07-14*

Information workers often use e-mail to exchange sensitive information. To help secure this information, organizations can use Information Rights Management (IRM) to apply persistent protection to messaging content. Because mobile devices are increasingly being used to access e-mail, it's important that your mobile device users be able to create and consume IRM-protected content.

Contents

Looking for management tasks related to IRM? See Managing Information Rights Management.

Differences Between Mobile IRM Protection in Exchange 2010 RTM and Exchange 2010 SP1

To enable IRM protection for mobile devices in the release to manufacturing (RTM) version of Microsoft Exchange Server 2010, the following requirements must be met:

- The mobile devices must be running Windows Mobile 6.0 or later.
- The Active Directory Rights Management Services (AD RMS) administrator must allow Read permissions and Read and Execute permissions on the mobile certification pipeline (using the MobileDeviceCertification.asmx file in the Inetpub\wwwroot_wmcs\Certification folder on the AD RMS server). For more information, see Enable Certification of Mobile Devices.
- Users must connect the device to a computer and activate it for IRM using one of the following methods:
  - Using the Windows Mobile Device Center on computers running the Windows 7 or Windows Vista operating systems
  - Using the Microsoft ActiveSync client application on computers running the Windows XP operating system

In Exchange 2010 Service Pack 1 (SP1), IRM in Microsoft Exchange ActiveSync allows your users to access rich IRM functionality on any supported Exchange ActiveSync device without having to configure AD RMS permissions or connect the device to a computer and activate it for IRM. Also, the mobile device doesn't need to be running Windows. Exchange ActiveSync is licensed by Microsoft to mobile device manufacturers, original equipment manufacturers (OEMs), and others. For a list of current Exchange ActiveSync licensees, see Exchange ActiveSync Protocol.

Using IRM in Exchange ActiveSync, mobile device users can:

- Create IRM-protected messages.
- Read IRM-protected messages.
- Reply to and forward IRM-protected messages.

Return to top

Requirements

The following requirements apply:

- The Client Access servers in your organization must be running Exchange 2010 SP1.
- An AD RMS server must be deployed in your organization.
- IRM must be enabled for internal messages. This is a prerequisite for all IRM features in Exchange 2010. For details, see Enable or Disable IRM for Internal Messages.
- IRM must be enabled in the Exchange ActiveSync mailbox policy. You can enable or disable IRM for different sets of users using different Exchange ActiveSync mailbox policies.
- Devices that support Exchange ActiveSync protocol version 14.1, including Windows phones, can support IRM in Exchange ActiveSync. The device's mobile e-mail application must support the RightsManagementInformation tag defined in Exchange ActiveSync version 14.1.

Return to top

Security

When you enable IRM in Exchange ActiveSync, the Client Access server decrypts IRM-protected messages before providing the messages for access by the supported mobile device. Upon synchronization, IRM-protected messages reside on the mobile device in an unencrypted format. IRM protection is enforced by the IRM-capable e-mail client application on the mobile device.

IRM in Exchange ActiveSync doesn't decrypt IRM-protected attachments on the Client Access server. Access to IRM-protected files is enforced by the application used to create or view the file. For example, on a Windows phone, IRM protection for Microsoft Office files is enforced by Microsoft Office Mobile. To access IRM-protected Office files, users must connect the device to a computer and activate Office Mobile with the RMS server.

When enabling IRM in Exchange ActiveSync, we recommend using the Exchange ActiveSync policy settings shown in the following table to help secure mobile devices.

Exchange ActiveSync policy settings

Setting	Configure using the New Exchange ActiveSync Mailbox Policy wizard	Configure using the New-ActiveSyncMailboxPolicy cmdlet

Require that the user enter a password to access information on their mobile device.	Select the **Require password** check box.	Set the *DevicePasswordEnabled* parameter to `$true`.
Enable encryption for the mobile device.	Select the **Require password** check box, and then select the **Require encryption on device** check box.	Set the *RequireDeviceEncryption* parameter to `$true`. **Important:** When you set the *RequireDeviceEncryption* parameter to `$true`, mobile devices that don't support device encryption will be unable to connect.
Don't allow non-provisionable mobile devices to synchronize with the Exchange server.	Clear the **Allow non-provisionable devices** check box.	Set the *AllowNonProvisionableDevices* parameter to `$false`.

To learn more, see Understanding Exchange ActiveSync Mailbox Policies.

Return to top

Enabling IRM in Exchange ActiveSync

To enable IRM in Exchange ActiveSync, perform the following tasks:

1. Add the Federation mailbox (a system mailbox created by Exchange 2010 Setup) to the super users group in AD RMS. This allows Exchange 2010 servers to access IRM-protected messages. For details, see Add the Federation Mailbox to the AD RMS Super Users Group.
2. Use the Set-IRMConfiguration cmdlet in the Exchange Management Shell to enable IRM on the Client Access server. This enables IRM in Exchange ActiveSync and IRM in Microsoft Office Outlook Web App for your organization. For details, see Enable or Disable Information Rights Management on Client Access Servers.

Return to top

1.11.4.8 Understanding Information Rights Management Logging

Understanding Information Rights Management Logging

Exchange Server 2010 > Messaging Policy and Compliance > Information Rights Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-01*

In Microsoft Exchange Server 2010 Service Pack 1 (SP1), Information Rights Management (IRM) operations performed on Exchange 2010 Mailbox, Client Access, Hub Transport, and Unified Messaging servers are logged in IRM logs. IRM logs help you monitor and troubleshoot interactions between the Rights Management Services (RMS) client on an Exchange 2010 SP1 server and the Active Directory Rights Management Services (AD RMS) cluster in your organization.

To learn about IRM, see Understanding Information Rights Management.

Contents

Looking for management tasks related to IRM? See Managing Information Rights Management.

Structure of IRM Logs

By default, IRM logs are located in C:\Program Files\Microsoft\Exchange Server\V14\Logging\IRMLogs.

The naming convention for IRM log files is *<Process>*_*<Process identifier* or *IIS AppPool identifier>*_IRMLOG*yyyymmdd-nnnn*.log, where:

- *<Process>* = process that creates the log file. For example, on Hub Transport servers, this will be EdgeTransport.
- *<Process identifier* or *IIS AppPool identifier>* = numerical ID of the process.
- *yyyymmdd* = Coordinated Universal Time (UTC) date when the log file was created.
- *nnnn* = instance number, which starts at 1 for each day.

An example IRM log file name is EdgeTransport_1056_IRMLOG20101201-1.log.

The following table shows the logs generated on different server roles.

Logs on server roles

Server role	IRM log file name	Description
Hub Transport	EdgeTransport_*<Process identifier>*_IRMLOG*yyyymmdd-nnnn*.log	This log is used to record all RMS transactions made by the transport pipeline on Hub Transport servers (for example, transport protection rules and journal report decryption). The process identifier (PID) of the edgetransport.exe process is used to generate the log file name.
Mailbox	msftefd_*<Process identifier>*_IRMLOG*yyyymmdd-nnnn*.log	This log is used to record all RMS transactions that occur during search and index requests. Exchange 2010 Mailbox servers use the msftefd.exe process for content indexing. The PID of the msftefd.exe process is used to generate the log file name.

Client Access	w3wp_MSExchangeOWAAppOol_IRMLOG*yyyymmdd-nnnn*.log	This log is used to record all transactions for IRM in Microsoft Office Outlook Web App.
All Exchange 2010 server roles except Edge Transport	w3wp_MSExchangePowerShellAppPool_IRMLOG*yyyymmdd-nnnn*.log	This log is used to record all IRM RMS transactions issued from Windows PowerShell, for example, when issuing the **Test-IRMConfiguration** cmdlet.

Return to top

Logging Process

Information is written to the log file until the file size reaches its maximum specified value. When the maximum size is reached, a log file that has an incremental instance number is created. This process is repeated throughout the day. Circular logging deletes the oldest log files when the IRM log directory reaches its maximum specified size or when a log file reaches the maximum age specified in the IRM logging configuration on each server.

Return to top

Information Written to IRM Logs

IRM log files are text files that contain data in comma-separated value (CSV) format. Each IRM log has a header that contains the following information:

- **#Software** Name of the software that created the IRM log file. Typically, the value is `Microsoft Exchange Server`.
- **#Version** Version number of the software that created the IRM log file.
- **#Log-type** Log type value, which is `Rms Client Manager Log`.
- **#Date** The UTC date and time when the log file was created. The UTC date and time is represented in the ISO 8601 date-time format: *yyyy-mm-dd*T*hh*:*mm*:*ss.fff*Z, where:
  - yyyy = year
  - *mm* = month
  - *dd* = day
  - T = time designator used to show the start of the time component
  - *hh* = hour
  - *mm* = minute
  - *ss* = second
  - *fff* = fractions of a second
  - Z = Zulu, which is another way to denote UTC
- **#Fields** Comma-delimited field names used in IRM log files.
  The IRM log stores each RMS transaction event on a single line, organized in comma-separated fields. The following table lists the fields in IRM logs for all server roles that have IRM features enabled.

Fields used in IRM logs

Field	Description
Date-time	Lists the UTC timestamp.
Feature	Lists the RMS client feature used. Valid values include: • `RacClc`

	• Template • Prelicense • UseLicense • Signature verification • ServerInfo
Event-Type	Lists the event type. Valid values include: • Acquire An RMS license or template is requested. • Success An RMS license or template is acquired successfully. • Exception An error has occurred. • Queued A request is pending.
Tenant-Id	Reserved for internal Microsoft use.
Server-url	Lists the RMS server URL accessed during the operation.
Context	Used by the calling process to tie multiple RMS transactions together. Valid values include: • MessageID: <Actual message ID> • MailboxGuid: <Mailbox GUID> • AttachmentFileName: <File name>
Transaction-id	Identifies a unique transaction. All events that occur during one transaction have the same transaction ID.

Return to top

Managing IRM Logs

On each server role that has IRM features enabled, IRM logging is enabled by default. For each server role, you can modify the following IRM log configuration by using the server role's corresponding **Set** cmdlet. For example, to configure IRM logging on a Mailbox server, you use the **Set-MailboxServer** cmdlet.

Configuration parameters for IRM logs

Parameter	Description
IrmLogEnabled	Enables logging of IRM transactions. IRM logging is enabled by default. To disable IRM logging for a server role, set the parameter to $false.
IrmLogMaxAge	Specifies the maximum age for an IRM log file. Files older than the specified age are deleted. The default value is 30.00:00:00 (30 days).
IrmLogMaxDirectorySize	Specifies the maximum size of all IRM logs in the connectivity log directory. When a directory reaches its maximum file size, the server deletes the oldest log files first. The default value is 250 MB.

IrmLogMaxFileSize	Specifies the maximum file size for a single log file. When a file reaches the specified size, a log file is created, and the instance number is incremented. The default value is 10 MB.
IrmLogPath	Specifies the IRM log location. The default path is C:\Program Files\Microsoft\Exchange Server\V14\Logging\IRMLogs.

For detailed syntax and parameter information, see the following topics:

- Set-MailboxServer
- Set-ClientAccessServer
- Set-TransportServer
- Set-UMServer

Return to top

1.11.4.9 Managing Information Rights Management

Managing Information Rights Management

Exchange Server 2010 > Messaging Policy and Compliance > Information Rights Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-28*

1.11.4.9.1 Enable or Disable IRM for Internal Messages

Enable or Disable IRM for Internal Messages

Messaging Policy and Compliance > Information Rights Management > Managing Information Rights Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2010, Information Rights Management (IRM) is enabled by default for internal messages. This allows you to create transport protection rules and Microsoft Outlook protection rules to IRM-protect messages in transport and on Microsoft Outlook 2010 clients. Enabling IRM for internal messages is a prerequisite for all other IRM features in Exchange 2010, such as transport decryption, journal rule decryption, IRM in Microsoft Office Outlook Web App, and IRM in Microsoft Exchange ActiveSync.

Looking for other management tasks related to IRM? Check out Managing Information Rights Management.

Use the Shell to enable IRM for internal messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to enable IRM for internal messages.

This example enables IRM for internal messages for the Exchange organization.

```
Set-IRMConfiguration -InternalLicensingEnabled $true
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

Use the Shell to disable IRM for internal messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to disable IRM for internal messages.

Caution:
Disabling IRM for internal messages disables all IRM features in the Exchange organization. The client-side IRM features in Outlook, for example, the ability to read, reply to, forward, and create IRM-protected messages using an Active Directory Rights Management Services (AD RMS) server, aren't affected.

This example disables IRM for internal messages for the Exchange organization.

```
Set-IRMConfiguration -InternalLicensingEnabled $false
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

1.11.4.9.2 Create a Transport Protection Rule

Create a Transport Protection Rule

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use transport protection rules to apply persistent rights protection to messages based on message properties such as sender, recipient, message subject, and content.

Caution:
Before you create transport rules in your production environment, use a test environment to learn how to create transport rules and test them thoroughly. The transport rules created in this topic are examples. You can create transport rules by using the appropriate transport rule predicates and values based on your requirements.

Important:
If you configure transport protection rules to protect messages using Information Rights Management (IRM), and you also use journaling, consider enabling journal report decryption to allow the Journaling agent to save an unencrypted copy of the message in the journal report. For more information, see Understanding Journal Report Decryption.

Looking for other management tasks related to IRM? Check out Managing Information Rights Management.

Prerequisites

A server running Active Directory Rights Management Services (AD RMS) is available in your organization.

Important:
After you create a transport protection rule, if the rule can't be applied to messages because an AD RMS server is unavailable, messages will be queued on Hub Transport servers. Depending on the volume of these messages, additional disk space may be consumed on Hub Transport servers. Exchange will attempt to IRM-protect the message three times. After these attempts, if the AD RMS server is unreachable or the message can't be IRM-protected, a non-delivery report (NDR) is sent to the sender.

Use the EMC to create a transport protection rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the action pane, click **New Transport Rule**.
3. On the **Introduction** page, complete the following fields:
   - **Name** Type a name for the transport rule.
   - **Comments** (optional) You can use this field to describe the rule's functionality, and relevant details such as a change request or trouble ticket number, date, and name of the administrator. Text in this field has no impact on rule functionality.
   - **Enabled** New rules are enabled by default. If you want the rule to be

created in a disabled state, clear the check box.

4. On the **Conditions** page, complete the following fields:
   - In the **Step 1. Select Condition(s)** box, select all the conditions that you want to apply to this rule.

     Important:
     If you don't select any conditions when creating a transport protection rule, all messages handled by servers running Microsoft Exchange Server 2010 with Hub Transport servers installed in your organization are IRM-protected. IRM-protecting all messages requires more resources. Therefore, we recommend that you plan your Hub Transport servers and AD RMS deployment accordingly.

   - If you selected conditions in the **Select Conditions** box, in the **Step 2. Edit the rule description by clicking an underlined value** box, click each blue underlined word.
   - When you click a blue underlined word, a window opens to prompt you for the values to apply to the condition. Select the values that you want to apply, or type the values manually. If the window requires that you manually add values to a list, type a value, and then click **Add**. Repeat this process until you have entered all the values, and then click **OK** to close the window.
   - Repeat the previous step for each condition that you selected. After you configure all the conditions, click **Next**.
5. On the **Actions** page, complete the following fields:
   - In the **Step 1. Select actions** box, select **rights protect message with RMS template**.
   - In the **Step 2: Edit the rule description by clicking an underlined value** box, click the underlined words **RMS template**.
   - In the **Select RMS template** dialog box, select an available RMS template, and then click **OK**.
6. (Optional) On the **Exceptions** page, select an exception you want to use, and then type the appropriate value if required.
7. On the **Create Rule** page, review the **Configuration Summary** to make sure the predicates and values used in the conditions and any exceptions appear as expected. Make sure the RMS template selected is the one you intend to use.
8. Click **New** to create the transport rule.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a transport protection rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Transport rules" entry in the Messaging Policy and Compliance Permissions topic.

To create a transport protection rule, you must have rights management templates created in your AD RMS deployment. This example retrieves the available templates from your AD RMS cluster.

```
Get-RMSTemplate | fl
```

This example creates the transport protection rule Protect-BusinessCriticalProject. The rule IRM-protects messages that contain the phrase "Business Critical" in the Subject field with the **Do Not Forward** template.

Note:

The `SubjectContainsWords` value is used in this example. You can use any combination of transport rule values to form the conditions and exceptions for the rule.

```
New-TransportRule -Name "Protect-BusinessCriticalProject" -SubjectContainsWords "
```

For detailed syntax and parameter information, see Get-RMSTemplate and New-TransportRule.

Other Tasks

After you create a transport protection rule, you may also want to:

- Enable or Disable a Transport Rule
- Enable or Disable Transport Decryption
- Enable or Disable Journal Report Decryption

1.11.4.9.3 Create an Outlook Protection Rule

Create an Outlook Protection Rule

Messaging Policy and Compliance > Information Rights Management > Managing Information Rights Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Using Microsoft Outlook protection rules, you can protect messages with Information Rights Management (IRM) by applying an Active Directory Rights Management Services (AD RMS) template in Outlook 2010 before the messages are sent.

Important:

If you configure Outlook protection rules to IRM-protect messages, consider enabling transport decryption to allow transport agents, including the Transport Rules agent, to decrypt and access the message. If you use journaling, you should also consider enabling journal report decryption to allow the Journaling agent to save an unencrypted copy of the message in the journal report. For more information, see Understanding Journal Report Decryption.

Looking for other management tasks related to IRM? Check out Managing Information Rights Management.

Prerequisites

You must have an AD RMS server deployed in the same Active Directory forest as your server running Microsoft Exchange Server 2010.

Use the Shell to create an Outlook protection rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to create Outlook protection rules.

This example creates the Outlook protection rule Project Contoso. The rule protects messages sent to the ContosoPMs distribution group with the AD RMS template Business Critical.

```
New-OutlookProtectionRule -Name "Project Contoso" -SentTo "DL-ContosoPMs@contoso.
```

Note:
When you use the `SentTo` predicate for an Outlook protection rule and specify a distribution group, only messages addressed to the distribution group in the To, Cc, or Bcc fields are IRM-protected. IRM protection isn't applied to messages addressed to individual members of the distribution group.

You can also use the `FromDepartment` and `SentToScope` predicates to apply IRM protection to messages sent from users in the specified department or messages sent to the specified scope (`InOrganization` for internal messages, `All` for all recipients).

For detailed syntax and parameter information, see New-OutlookProtectionRule.

Other Tasks

After you create an Outlook protection rule, you may also want to:

- Remove an Outlook Protection Rule
- Enable or Disable Transport Decryption
- Enable or Disable Journal Report Decryption

1.11.4.9.4 Remove an Outlook Protection Rule

Remove an Outlook Protection Rule

Messaging Policy and Compliance > Information Rights Management > Managing Information Rights Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Using Microsoft Outlook protection rules, you can protect messages with Information Rights Management (IRM) by applying an Active Directory Rights Management Services (AD RMS) template in Outlook 2010 before the messages are sent. To prevent an Outlook protection rule from being applied, you can disable the rule. Removing an Outlook protection rule removes the rule definition from Active Directory.

Looking for other management tasks related to IRM? Check out Managing Information Rights Management.

Use the Shell to remove an Outlook protection rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to remove Outlook protection rules.

This example removes the Outlook protection rule OPR-DG-Finance.

```
Remove-OutlookProtectionRule -Identity "OPR-DG-Finance"
```

For detailed syntax and parameter information, see Remove-OutlookProtectionRule.

Use the Shell to remove all Outlook protection rules

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to remove Outlook protection rules.

This example removes all Outlook protection rules in the Exchange organization.

```
Get-OutlookProtectionRule | Remove-OutlookProtectionRule
```

For detailed syntax and parameter information, see Get-OutlookProtectionRule and Remove-OutlookProtectionRule.

Other Tasks

After you remove an Outlook protection rule, you may also want to create an Outlook protection rule. For detailed steps, see Create an Outlook Protection Rule.

1.11.4.9.5 Add the Federation Mailbox to the AD RMS Super Users Group

Add the Federation Mailbox to the AD RMS Super Users Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

For the following Microsoft Exchange Server 2010 Information Rights Management (IRM)

features to be enabled, you must add the Federation mailbox (a system mailbox created by Exchange 2010 Setup) to the super users group on your organization's Active Directory Rights Management Services (AD RMS) cluster:

- IRM in Microsoft Office Outlook Web App
- Journal report decryption
- Transport decryption

You can configure a mail-enabled distribution group as a super users group in AD RMS. Members of the distribution group are granted an owner use license when they request a license from the AD RMS cluster. This allows them to decrypt all RMS-protected content published by that cluster. Whether you use an existing distribution group or create a distribution group and configure it as the super users group in AD RMS, we recommend that you dedicate the distribution group for this purpose and configure the appropriate settings to approve, audit, and monitor membership changes.

Note:
If a super users group is already configured on an AD RMS cluster, any modifications to the distribution group membership can take up to 24 hours to be refreshed by the AD RMS cluster. This is a result of caching the group membership on the cluster.

Looking for other management tasks related to IRM? Check out Managing Information Rights Management.

Prerequisites

An AD RMS cluster is deployed in the Active Directory forest.

Use the Shell to add the Federation mailbox to a distribution group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Distribution groups" entry in the Mailbox Permissions topic.

If a distribution group has been created and configured as a super users group in the AD RMS cluster, you can add the Exchange 2010 Federation mailbox as a member of that group. If a super users group isn't configured, you must create a distribution group and add the Federation mailbox as a member.

1. Create a distribution group dedicated for use as an AD RMS super users group. For details, see Create a Distribution Group.
2. Add the user **FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042** to the new distribution group. The Federation mailbox is a system mailbox, and therefore not visible in the EMC. To add it to a distribution group, you must use the Add-DistributionGroupMember cmdlet from the Shell.
   This example adds the Federation mailbox to the ADRMSSuperUsers distribution group.

```
Add-DistributionGroupMember ADRMSSuperUsers -Member FederatedEmail.4c1
```

For detailed syntax and parameter information, see Add-DistributionGroupMember.

Use AD RMS to set up a super users group

Perform the following procedure on an AD RMS cluster. The account used to perform this procedure must be a member of the AD RMS Enterprise Administrators local group on the AD RMS server.

1. Open the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand **Security Policies**, and then click **Super Users**.
3. In the action pane, click **Enable Super Users**.
4. In the result pane, click **Change Super User Group** to open the **Super Users** property sheet.
5. In the **Super user group** box, type the e-mail address of the distribution group you created in the previous procedure, or click **Browse** to select a distribution group.

Other Tasks

After you add the Federation mailbox to the AD RMS super users group, you may also want to:

- Enable or Disable Information Rights Management on Client Access Servers
- Enable or Disable Transport Decryption
- Enable or Disable Journal Report Decryption

1.11.4.9.6 Enable or Disable Transport Decryption

Enable or Disable Transport Decryption

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Enabling transport decryption allows the Transport Rules agent on Hub Transport servers to access content in messages protected by Information Rights Management (IRM). As a result, other transport agents can access message content and possibly make changes to it. For example, the Transport Rules agent may need to inspect message content and apply transport rules (such as rules that apply a disclaimer to the message). To successfully decrypt IRM-protected messages, you must add the Federated Delivery mailbox to the super users group configured on your Active Directory Rights Management Services (AD RMS) server.

Important:

Members of the super users group are granted an owner use license when they request a license from the AD RMS cluster. This allows them to decrypt all RMS-protected content created by that AD RMS cluster.

When enabling transport decryption, you can specify the following settings:

- **Mandatory** Rejects messages that can't be decrypted and returns a non-delivery report (NDR) to the sender.
- **Optional** Uses a best-effort approach to decryption. If possible, messages are decrypted, but they're delivered even if decryption fails.

To learn more about transport decryption, see Understanding Transport Decryption.

Looking for other management tasks related to IRM? Check out Managing Information Rights Management.

Prerequisites

- An AD RMS server exists in the Active Directory forest and is accessible.
- The Federated Delivery mailbox has been added to the AD RMS super users group. For details, see Add the Federation Mailbox to the AD RMS Super Users Group.

Use the Shell to enable transport decryption

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to enable transport decryption.

This example enables transport decryption for the Microsoft Exchange Server 2010 organization. Messages that can't be decrypted are rejected, and an NDR is returned to the sender.

```
Set-IRMConfiguration -TransportDecryptionSetting Mandatory
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

Use the Shell to disable transport decryption

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to disable transport decryption.

This example disables transport decryption for the Exchange 2010 organization.

```
Set-IRMConfiguration -TransportDecryptionSetting Disabled
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

Other Tasks

After you enable or disable transport decryption, you may also want to:

- Enable or Disable Journal Report Decryption
- Enable or Disable Information Rights Management on Client Access Servers

Configure IRM for Exchange Search and Discovery

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2010, you can configure Information Rights Management (IRM) so that Exchange Search can index IRM-protected messages.

When members of the Discovery Management role group use Multi-Mailbox Search to perform a discovery search, IRM-protected messages are returned in the search results and copied to the Discovery mailbox specified in the search. Furthermore, in Exchange 2010 Service Pack 1 (SP1) and later, members of the Discovery Management role group can use Outlook Web App to access the IRM-protected messages that were copied to the Discovery mailbox as a result of the discovery search.

Note:
Members of the Discovery Management role group can't access IRM-protected messages exported from a Discovery mailbox to another mailbox or to a .pst file. IRM-protected messages in a Discovery mailbox can be accessed only by using Outlook Web App.

Looking for other management tasks related to managing IRM? Check out Managing Information Rights Management.

Prerequisites

- IRM is configured in your Exchange 2010 organization. To learn more, see Enable or Disable IRM for Internal Messages.
- The Federation mailbox is added to the Active Directory Rights Management Services (AD RMS) super users group. To learn more, see Add the Federation Mailbox to the AD RMS Super Users Group.

Use the Shell to configure IRM for Exchange Search

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to configure IRM for Exchange Search.

This example configures IRM to allow Exchange Search to index IRM-protected messages.

Note:
By default, the *SearchEnabled* parameter is set to `$true`. To disable indexing of IRM-protected messages, set it to `$false`. Disabling indexing of IRM-protected messages prevents them from being returned in search results when users search their mailbox or when discovery managers use Multi-Mailbox Search.

```
Set-IRMConfiguration -SearchEnabled $true
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

Use the Shell to configure IRM for discovery

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to configure IRM for discovery.

This example specifies that members of the Discovery Management role group can access IRM-protected messages that reside in the Discovery mailbox.

Note:
By default, the *EDiscoverySuperUserEnabled* parameter is set to `$true`. To disable access to IRM-protected messages for members of the Discovery Management role group, set it to `$false`.

```
Set-IRMConfiguration -EDiscoverySuperUserEnabled $true
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

Other Tasks

After you configure IRM for Exchange Search and discovery, you may also want to:

- Enable or Disable IRM for Internal Messages
- Enable or Disable Information Rights Management Logging

1.11.4.9.8 Enable or Disable Journal Report Decryption

Enable or Disable Journal Report Decryption

Messaging Policy and Compliance > Information Rights Management > Managing Information Rights Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Enabling journal report decryption allows the Journaling agent to attach a decrypted copy of a rights-protected message to the journal report. Before you enable Journal Report Decryption, you must add the Federated Delivery mailbox to the super users group configured on your Active Directory Rights Management Services (AD RMS) server.

Important:
Members of the super users group are granted an owner use license when they request a license from the AD RMS cluster. This allows them to decrypt all RMS-protected content created by that AD RMS cluster.

Looking for other management tasks related to Information Rights Management (IRM)? Check out Managing Information Rights Management.

Prerequisites

- An AD RMS cluster is installed in the Active Directory forest.
- The Federated Delivery mailbox has been added to an AD RMS super users group. For details, see Add the Federation Mailbox to the AD RMS Super Users Group.

Use the Shell to enable Journal Report Decryption

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to enable Journal Report Decryption.

This example enables Journal Report Decryption for the Exchange organization.

```
Set-IRMConfiguration -JournalReportDecryptionEnabled $true
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

Use the Shell to disable Journal Report Decryption

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to disable journal report decryption.

This example disables Journal Report Decryption for the Exchange organization.

```
Set-IRMConfiguration -JournalReportDecryptionEnabled $false
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

Other Tasks

After you enable Journal Report Decryption, you may also want to:

- Enable Per-Mailbox Database Journaling
- Create a Journal Rule

Enable or Disable Information Rights Management on Client Access Servers

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Enabling Information Rights Management (IRM) on Client Access servers enables the following features:

- Microsoft Office Outlook Web App
- IRM in Microsoft Exchange ActiveSync

When IRM is enabled on Client Access servers, Outlook Web App users can IRM-protect messages by applying an Active Directory Rights Management Services (AD RMS) template created on your AD RMS cluster. Outlook Web App users can also view IRM-protected messages and supported attachments. Before you enable IRM on Client Access servers, you must add the Federation mailbox to the super users group on the AD RMS cluster.

Important:

Members of the super users group are granted an owner use license when they request a license from the AD RMS cluster. This allows them to decrypt all RMS-protected content by that cluster.

You can use the **Set-IRMConfiguration** cmdlet to enable or disable IRM in Outlook Web App and IRM in Exchange ActiveSync for the entire Exchange 2010 organization.

You can also control IRM in Outlook Web App at the following levels:

- **Per-Outlook Web App virtual directory** To enable or disable IRM in Outlook Web App for an Outlook Web App virtual directory, use the **Set-OWAVirtualDirectory** cmdlet and set the *IRMEnabled* parameter to `$false` or `$true` (default). This allows you to disable IRM in Outlook Web App for one virtual directory on an Exchange 2010 Client Access server, while keeping it enabled on another virtual directory on a different Client Access server.
- **Per-Outlook Web App mailbox policy** To enable or disable IRM in Outlook Web App for an Outlook Web App mailbox policy, use the **Set-OWAMailboxPolicy** cmdlet and set the *IRMEnabled* parameter to `$false` or `$true` (default). This allows you to enable IRM in Outlook Web App for one set of users and disable it for another set of users by assigning them a different Outlook Web App mailbox policy.

You can also control IRM in Exchange ActiveSync per Microsoft ActiveSync mailbox policy. To disable or enable IRM in Exchange ActiveSync for an ActiveSync mailbox policy, use the **Set-ActiveSyncMailboxPolicy** cmdlet and set the *IRMEnabled* parameter to `$false` or `$true` (default). This allows you to enable IRM in Exchange ActiveSync for one set of users and disable it for another set of users by assigning them a different ActiveSync mailbox policy.

Note:

In the release to manufacturing (RTM) version of Microsoft Exchange Server 2010, the *OWAEnabled* parameter is used to enable or disable IRM in Outlook Web App. In Microsoft Exchange Server 2010 Service Pack 1 (SP1), the *OWAEnabled* parameter is replaced by the *ClientAccessServerEnabled* parameter, which enables or disables IRM in Outlook Web App and IRM in Exchange ActiveSync (provided that the other requirements for these features are met).

Looking for other management tasks related to rights protection? Check out Managing Information Rights Management.

Prerequisites

- An AD RMS cluster is installed in the Active Directory forest.
- The Federation mailbox has been added to the AD RMS super users group. For detailed instructions, see Add the Federation Mailbox to the AD RMS Super Users Group.
- IRM features are enabled for the organization. For detailed instructions, see Enable or Disable IRM for Internal Messages.

Use the Shell to enable IRM on Client Access servers

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to enable IRM on Client Access servers.

This example enables IRM on a Client Access server for an Exchange 2010 organization.

```
Set-IRMConfiguration -ClientAccessServerEnabled $true
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

Use the Shell to disable IRM on Client Access servers

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Rights protection" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to disable IRM on Client Access servers.

This example disables IRM on a Client Access server for an Exchange 2010 organization.

```
Set-IRMConfiguration -ClientAccessServerEnabled $false
```

For detailed syntax and parameter information, see Set-IRMConfiguration.

Other Tasks

After you enable IRM on Client Access servers, you may also want to:

- Create a Transport Protection Rule.
- View or Configure Exchange ActiveSync Mailbox Policy Properties.

Enable or Disable Information Rights Management Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Exchange 2010 Service Pack 1 (SP1), you can use Information Rights Management (IRM) logs to monitor and troubleshoot IRM operations on Mailbox, Hub Transport, Client Access, and Unified Messaging servers. IRM logging is enabled by default.

IRM logs use the following common set of parameters:

- *IrmLogEnabled* Enables or disables IRM logging. Default: $true
- *IrmLogMaxAge* Specifies the maximum age of IRM log files. Files older than the specified age are deleted. Default: 30 days.
- *IrmLogMaxDirectorySize* Specifies the maximum size of the directory that contains IRM logs. When a directory reaches its maximum file size, the server deletes the oldest log files first. Default: 250 Mb.
- *IrmLogMaxFileSize* Specifies the maximum size of each IRM log file. When a log file reaches the specified size, a new log file is created. Default: 10 MB.
- *IrmLogPath* Specifies the location of the IRM log directory. Default: `<Exchange 2010 Install path>\V14\Logging\IRMLogs`.

To configure IRM logging for each server role, use the corresponding **Set** cmdlet. For example, to configure IRM logging on a Hub Transport server, use the **Set-TransportServer** cmdlet.

Looking for other management tasks related to IRM? Check out Managing Information Rights Management.

Use the Shell to enable IRM logging on a server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Configure IRM logging" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the Exchange Management Console (EMC) to enable IRM logging on a server.

This example enables IRM log on a Hub Transport server.

```
Set-TransportServer -Identity EXCH01 -IRMLogEnabled $true
```

For detailed syntax and parameter information, see the following topics:

- Set-TransportServer
- Set-MailboxServer
- Set-ClientAccessServer
- Set-UMServer

Use the Shell to disable IRM logging on a

server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Configure IRM logging" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the Exchange Management Console (EMC) to disable IRM logging on a server.

This example disables IRM logging on a Hub Transport server.

```
Set-TransportServer -Identity EXCH01 -IRMLogEnabled $false
```

For detailed syntax and parameter information, see the following topics:

- Set-TransportServer
- Set-MailboxServer
- Set-ClientAccessServer
- Set-UMServer

1.11.5 Journaling

Journaling

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

Understanding Journaling

Learn about the compliance-focused journaling feature in Microsoft Exchange Server 2010, including standard (per-mailbox database) and premium journaling.

Understanding Journal Reports

Learn about journal reports and the information contained in them.

Understanding How to Manage Journal Reports

Learn about important considerations for configuring a journaling mailbox and an alternate journaling mailbox.

Understanding Journaling in a Mixed Exchange 2003 and Exchange 2010 Environment

Learn about journaling considerations in a mixed-mode environment with servers running Exchange 2010 and Exchange Server 2003.

Protecting Journal Reports

Learn how to protect journal reports.

Managing Journaling

Get step-by-step guidance for managing journaling in your organization.

1.11.5.1 Understanding Journaling

Understanding Journaling

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-26*

Journaling can help your organization respond to legal, regulatory, and organizational compliance requirements by recording inbound and outbound e-mail communications. When planning for messaging retention and compliance, it's important to understand journaling, how it fits in your organization's compliance policies, and how Microsoft Exchange Server 2010 helps you secure journaled messages.

Contents

Why Journaling Is Important

First, you must understand the difference between journaling and archiving:

- Journaling is the ability to record all communications, including e-mail communications, in an organization for use in the organization's e-mail retention or archival strategy. To meet an increasing number of regulatory and compliance requirements, many organizations must maintain records of communications that occur when employees perform daily business tasks.
- *Archiving* refers to backing up the data, removing it from its native environment, and storing it elsewhere, therefore reducing the strain of data storage. You may use Exchange journaling as a tool in your e-mail retention or archival strategy.

Although journaling may not be required by a specific regulation, compliance may be achieved through journaling under certain regulations. For example, corporate officers in some financial sectors may be held liable for the claims made by their employees to their customers. To verify that the claims are accurate, a corporate officer may set up a system where managers review some part of employee-to-client communications regularly. Every quarter, the managers verify compliance and approve their employees' conduct. After all managers report approval to the corporate officer, the corporate officer reports compliance, on behalf of the company, to the regulating body. In this example, e-mail messages might be one type of the employee-to-client communications that managers must review; therefore, journaling can be used to collect all e-mail messages sent by client-facing employees. Other client communication mechanisms may include faxes and telephone conversations, which may also be subject to regulation. The ability to journal all classes of data in an enterprise is a valuable functionality of the IT architecture.

The following list shows some of the more well-known U.S. and international regulations where journaling may help form part of your compliance strategies:

- Sarbanes-Oxley Act of 2002 (SOX)
- Security Exchange Commission Rule 17a-4 (SEC Rule 17 A-4)
- National Association of Securities Dealers 3010 & 3110 (NASD 3010 & 3110)
- Gramm-Leach-Bliley Act (Financial Modernization Act)
- Financial Institution Privacy Protection Act of 2001
- Financial Institution Privacy Protection Act of 2003
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act)
- European Union Data Protection Directive (EUDPD)
- Japan's Personal Information Protection Act

Return to top

Journaling Agent

In an Exchange 2010 organization, all e-mail traffic is routed by the Hub Transport server. All messages traverse at least one Hub Transport server in their lifetime. The *Journaling agent* is a compliance-focused transport agent that processes messages on Hub Transport servers. It fires on the **OnSubmittedMessage** and **OnRoutedMessage** transport events.

Note:

In Exchange 2010, the Journaling agent is a built-in agent. Built-in agents aren't included in the list of agents returned by the **Get-TransportAgent** cmdlet. For more details, see Understanding Transport Agents.

Exchange 2010 provides the following journaling options:

- **Standard journaling** Standard journaling is configured on a mailbox database. It enables the Journaling agent to journal all messages sent to and from mailboxes located on a specific mailbox database. To journal all messages to and from all recipients and senders, you must configure journaling on all mailbox databases on all Mailbox servers in the organization.
- **Premium journaling** Premium journaling enables the Journaling agent to perform more granular journaling by using journal rules. Instead of journaling all mailboxes residing on a mailbox database, you can configure journal rules to match your organization's needs by journaling individual recipients or members of distribution groups. You must have an Exchange Enterprise client access license (CAL) to use premium journaling.

When you enable standard journaling on a mailbox database, this information is saved in Active Directory and is read by the Journaling agent. Similarly, journal rules configured with premium journaling are also saved in Active Directory and applied by the Journaling agent. For more information about how to configure standard and premium journaling, see Journaling.

Return to top

Journal Rules

Here are key aspects of a journal rule that you should understand:

- Journal Rule Scope Defines which messages are journaled by the Journaling agent.
- Journal Recipients Specifies the SMTP address of the recipient you want to

journal.

- Journaling Mailbox Specifies one or more mailboxes used for collecting journal reports.

Journal Rule Scope

You can target the journal rule to Internal, External, or Global recipients. The following list describes these scopes:

- **Internal** Journal rules with the scope set to Internal target messages sent and received by recipients inside your Exchange organization.
- **External** Journal rules with the scope set to External target messages sent to recipients or received from senders outside your Exchange organization.
- **Global** Journal rules with the scope set to Global target all messages that pass through Hub Transport servers. These include messages that may have already been processed by journal rules in the Internal and External scopes.

Journal Recipients

You can implement targeted journaling rules by specifying the SMTP address of the recipient you want to journal. The recipient can be an Exchange mailbox, distribution group, or a contact. These recipients may be subject to regulatory requirements, or they may be involved in legal proceedings where e-mail messages or other communications are collected as evidence. By targeting specific recipients or groups of recipients, you can easily configure a journaling environment that matches your organization's processes and regulatory and legal requirements, and minimize storage and other costs associated with retention of large amounts of data.

All messages sent to or from the journaling recipients you specify in a journaling rule are journaled. If you specify a distribution group as the journaling recipients, all messages sent to and from members of the distribution group are journaled. If you don't specify a journaling recipient, all messages sent to or from recipients that match the journal rule scope are journaled.

Unified Messaging-Enabled Journal Recipients

Many organizations that implement journaling may also use Unified Messaging (UM) to consolidate their e-mail, voice mail, and fax infrastructure. However, you may not want the journaling process to generate journal reports for messages generated by Unified Messaging. In these cases, you can decide whether to journal voice mail messages and missed call notification messages handled by an Exchange 2010 Unified Messaging server or to skip such messages. If your organization doesn't require journaling of such messages, you can reduce the amount of hard disk space required to store journal reports by skipping such messages. When you enable or disable the journaling of voice mail messages and missed call notification messages, your change is applied to all Hub Transport servers in your organization.

Note:

Messages that contain faxes generated by a Unified Messaging server are always journaled, even if you configure a journal rule that specifies not to journal Unified Messaging voice mail and missed call notification messages.

For more information about how to enable or disable voice mail and missed call notification messages, see Managing Journaling.

Return to top

Journaling Mailbox

The journaling mailbox is used for collecting journal reports. How the journaling mailbox is configured depends on your organization's policies, regulatory requirements, and legal requirements. You can specify one journaling mailbox to collect messages for all the journal rules configured in the organization, or you can use different journaling mailboxes for different journal rules or sets of journal rules.

Important:
Journaling mailboxes contain very sensitive information. You must secure journaling mailboxes because they collect messages that are sent to and from recipients in your organization. These messages may be part of legal proceedings or may be subject to regulatory requirements. Various laws require that messages remain tamper-free before they're submitted to an investigatory authority. We recommend that you create policies that govern who can access the journaling mailboxes in your organization, limiting access to only those individuals who have a direct need to access them. Speak with your legal representatives to make sure that your journaling solution complies with all the laws and regulations that apply to your organization.

For more information about how to configure the journaling mailbox, see Managing Journaling.

For more information about how to protect journaling mailboxes, see Protecting Journal Reports.

Return to top

Journal Rule Replication

Journal rules are stored in Active Directory and applied by all Hub Transport servers in the Exchange 2010 organization. When you create, modify, or remove a journal rule on a Hub Transport server, the change is replicated to all Active Directory servers in the organization. All Hub Transport servers in the organization then retrieve the updated journal rule configuration from the Active Directory servers and apply the new or modified journal rules.

By replicating all the journal rules across the organization, Exchange 2010 enables you to provide a consistent set of journal rules across the organization. All messages that pass in or through your Exchange 2010 organization are subject to the same journal rules.

Important:
Replication of journal rules across an organization is dependant on Active Directory replication. Replication time between Active Directory domain controllers varies depending on the number of sites in the organization and the speed of links and other factors outside the control of Microsoft Exchange. Consider replication delays when you implement journal rules in your organization. For more information about Active Directory replication, see Active Directory Replication Technologies.

Important:
Each Hub Transport server caches distribution group membership to avoid repeated round trips to Active Directory. The expanded groups cache reduces the number of requests that each Hub Transport server must make to an Active Directory domain controller. By default, entries in the expanded groups cache expire in four hours. Therefore, if you specify a distribution group as the journal recipient, changes to distribution group membership may not be applied to journal rules until the expanded groups cache is updated. To force an immediate update of the recipient cache, you must stop and start the Microsoft Exchange Transport service. You must do this for each Hub Transport server where you want to forcibly update the recipient cache.

Return to top

Journal Reports

A *journal report* is the message that the Journaling agent generates when a message matches a journal rule and is to be submitted to the journaling mailbox. The original

message that matches the journal rule is included unaltered as an attachment to the journal report. The body of a journal report contains information from the original message such as the sender e-mail address, message subject, message-ID, and recipient e-mail addresses. This is also referred to as envelope journaling, and is the only journaling method supported by Exchange 2010 and Exchange 2007.

For more information about journal reports and how to manage and protect them, see the following topics:

- Understanding Journal Reports
- Protecting Journal Reports
- Understanding How to Manage Journal Reports

Journal Reports and IRM-Protected Messages

When implementing journaling in an Exchange 2010 environment, you must consider journaling reports and IRM-protected messages. IRM-protected messages will affect the search and discovery capabilities of third-party archiving systems that don't have RMS support built-in. In Exchange 2010, you can configure Journal Report Decryption to save a clear-text copy of the message in a journal report. For more information, see Understanding Journal Report Decryption.

Return to top

Interoperability with Exchange 2003 and Exchange 2007

Exchange 2010 supports journaling in a mixed Exchange 2010 and Exchange 2003 organization. Exchange 2010 can read the Exchange 2003 journaling configuration present on Exchange 2010 mailbox databases, and then journal messages to either an Exchange 2003 or Exchange 2010 journaling mailbox.

Exchange 2003 can't read the journaling configuration used by Exchange 2010. However, Exchange 2010 stamps journaled messages and journal reports with properties that Exchange 2003 can read. If a message has already been journaled by Exchange 2010 and the journal reports are sent to the same journaling mailbox, Exchange 2003 doesn't journal the message again. If a message is a journal report, Exchange 2003 treats the Exchange 2010 journal report as if it was an Exchange 2003 journal report.

For more information about journaling in a coexistence environment, see Understanding Journaling in a Mixed Exchange 2003 and Exchange 2010 Environment.

There is little difference between journaling functionality in Exchange 2010 and Exchange 2007. However, Exchange 2010 journal rules use a different format than journal rules in Exchange 2007. Exchange 2010 Setup creates a separate container in Active Directory to store Exchange 2010 journal rules. When you set up the first Exchange 2010 server in an Exchange 2007 organization, Setup creates a copy of the Exchange 2007 journal rules and stores them in the new container. When Setup finishes, the journal rules used by both versions are consistent. After Setup completes, if you change he journal rule configuration on an Exchange 2007 server, you must make the same change on an Exchange 2010 server to ensure they're consistent. You can also export journal rules from Exchange 2007 and import them on an Exchange 2010 server. For details, see Export and Import Exchange 2007 Journal Rules.

Return to top

Using Exchange Hosted Services

Journaling is enhanced by or is also available as a service from Microsoft Exchange Hosted

Services.

Exchange Hosted Services is a set of four distinct hosted services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps them satisfy retention requirements for compliance
- Hosted Encryption, which helps them encrypt data to preserve confidentiality
- Hosted Continuity, which helps them preserve access to e-mail during and after emergency situations

These services integrate with any on-premises Exchange servers that are managed in-house or Hosted Exchange e-mail services that are offered through service providers. For more information about Exchange Hosted Services, see Microsoft Exchange Hosted Services.

Return to top

1.11.5.2 Understanding Journal Reports

Understanding Journal Reports

Exchange Server 2010 > Messaging Policy and Compliance > Journaling >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-09*

Journal reports contain important message content and metadata. Understanding the structure of journal reports allows you to interpret the information in these reports.

Looking for management tasks related to managing journaling? See Managing Journaling.

Contents

Journal Reports

A *journal report* is the message generated by the Journaling agent on a Hub Transport server and delivered to the journaling mailbox. The original message is included unaltered as an attachment to the journal report. This type of journal report is called an *envelope journal report*.

Note:
Microsoft Exchange Server 2010 supports envelope journaling only.

When using standard journaling, journal reports are generated for all messages sent or received by mailboxes on a mailbox database enabled for journaling. When using premium journaling, journal reports are generated for messages that match a journal

rule.

For more information about journaling, see Understanding Journaling.

The information contained in a journal report is organized so that every value in each header field has its own line. This enables you to easily parse journal reports manually or by using an automated process, depending on your requirements.

When the Journaling agent journals a message, it tries to capture as much detail as possible about the original message. This information is very important in determining the intent of the message, its recipients, and its senders. For example, whether the recipients that are identified in the message are directly addressed in the To field, the Cc field or are included as part of a distribution list may determine the nature and extent of their involvement in the e-mail communication.

Depending on the situation, Exchange 2010 may generate more than one journal report for a single message. Whether a single message generates one journal report or multiple journal reports depends on several factors, such as message bifurcation or distribution group expansion.

Journal reports can potentially contain very sensitive information and must be protected so that they can't be viewed by unauthorized individuals. For more information about how you can protect journal reports, see Protecting Journal Reports.

For more information about managing journal reports, see Understanding How to Manage Journal Reports.

Return to top

Journal Report Fields

The following sections describe each field contained within journal reports generated by Exchange 2010. These fields are separated into basic and extended fields, as shown in the following table.

Basic and extended journal report fields

Basic journal report fields	Extended journal report fields
Sender	To
Subject	Cc
Message-ID	Bcc
Recipient	On-Behalf-Of

Whether extended journal report fields are populated depends on whether recipient addressing can be determined. This happens in the following circumstances:

- **MAPI submission to a Client Access server** Recipient addressing can be determined when a message is submitted to a Client Access server using a MAPI client such as Microsoft Outlook 2010.
- **Authenticated SMTP submission to a Hub Transport server** Recipient addressing can also be determined when a message is submitted to a Hub Transport server in an authenticated SMTP session. The authenticated sender must not have the `ms-Exch-Smtp-Accept-Any-Sender` permission because this generally indicates that the sender was an Exchange server.

If recipient addressing can be determined for a particular recipient, the recipient e-mail

address is inserted into the appropriate extended To, Cc, or Bcc fields described in the "Extended journal report fields" table later in this topic. The recipient e-mail address isn't inserted into the basic Recipient field described in the "Basic journal report fields" table later in this topic.

If a message is submitted to a Hub Transport server by using any other method, such as anonymous submission from an Edge Transport server or submission from a server running Exchange Server 2003, Exchange can't verify that the recipient addressing hasn't been tampered with. If recipient addressing can't be verified, the recipient e-mail address is inserted in the basic Recipient field and not into an extended To, Cc, or Bcc field.

For each recipient addressed on a message, one recipient journal report field is added. No recipient field contains more than one recipient e-mail address, except as follows:

- Recipient fields that contain recipients that have been expanded from a distribution group
- Recipient fields that contain recipients that have received a message forwarded from another mailbox

For expanded or forwarded messages, the e-mail address of the recipient that received final delivery of the message and the e-mail address of the distribution group or mailbox that was originally addressed are included.

Basic Journal Report Fields

Basic fields in Exchange 2010 journal reports include the sender, subject, and Message-ID of the original message. All journal reports include this information if it's present in the original message.

The fourth basic field is the Recipient field. Exchange 2010 only classifies information that it knows is correct. If Exchange can't determine whether a recipient was included in the To, Cc, or Bcc recipient fields, the recipient is added to the Recipient field in the journal report.

The following table lists the basic fields that are included in the body of journal reports.

Basic journal report fields

Field name	Description
Sender	The Sender field displays the SMTP address of the sender specified in the From header. If the message is sent on behalf of another sender, the field displays the address specified in the Sender header.
Subject	The Subject field displays the subject header value.
Message-ID	The Message-ID field displays the SMTP Message-ID.
Recipient	The Recipient field displays the SMTP address of a recipient included in an e-mail message when Exchange can't determine the recipient addressing of that message. This includes messages from the Internet or unauthenticated senders and messages that originated from legacy Exchange servers. Recipients added by transport rules or other transport agents are also listed in the Recipient field.

Extended Journal Report Fields

Extended fields in Exchange 2010 journal reports provide more recipient details, if available. The To, Cc, and Bcc fields in the journal report let you view how recipients are addressed in the original message.

The On-Behalf-Of field is populated if the SMTP headers of a message contain both the From and Sender header fields, regardless of whether the message was submitted directly to a Hub Transport server. The SMTP address contained in the From header field is populated in the On-Behalf-Of field.

The following table lists the extended fields that may be included in the body of journal reports.

Extended journal report fields

Field name	Description
On-Behalf-Of	The On-Behalf-Of field displays the SMTP address of the mailbox from which the message appears if the Send On Behalf Of feature is specified by the sender.
To	The To field displays the SMTP address of a recipient included in the message envelope and in the To header field of the message. The recipient address can be included either directly by the sender, or indirectly through distribution list expansion or if the message was forwarded to the recipient by another mailbox. To indicate whether the message went through distribution list expansion or was forwarded, the To field may also contain one Expanded field or one Forwarded field, separated with commas. For more information about these fields, see the "Expanded and Forwarded fields" table later in this topic.
Cc	The Cc field displays the SMTP address of a recipient included in the message envelope and in the Cc header field of the message. The recipient address can be included either directly by the sender, or indirectly through distribution list expansion or if the message was forwarded to the recipient by another mailbox. To indicate whether the message went through distribution list expansion or was forwarded, the Cc field may also contain one Expanded field or one Forwarded field, separated with commas. For more information about these fields, see the "Expanded and Forwarded fields" table later in this topic.
Bcc	The Bcc field displays the SMTP address of a recipient included in the message envelope and in the Bcc header field of the message. The recipient address can be included either

	directly by the sender, or indirectly through distribution list expansion or if the message was forwarded to the recipient by another mailbox. To indicate whether the message went through distribution list expansion or was forwarded, the Bcc field may also contain one Expanded field or one Forwarded field, separated with commas. For more information about these fields, see the "Expanded and Forwarded fields" table later in this topic.

Expanded and Forwarded Fields

The Expanded and Forwarded fields are included as fields on Recipient, To, Cc, or Bcc fields when that recipient has either been expanded from a distribution group or has had the message forwarded from another mailbox. The following table describes the Expanded and Forwarded fields.

Expanded and Forwarded fields

Field	Description
Expanded	The Expanded field is displayed as a field of the To, Cc, and Bcc fields that are described earlier in this topic. The Expanded field is preceded by a comma. The SMTP address displayed in the Expanded field is the address of the distribution group that contains either the recipient specified in the To, Cc, or Bcc field or the nested distribution lists that contain the specified recipient. The address displayed in this field is always the first distribution list to be expanded, regardless of how many nested distribution lists may be between the original parent distribution list and the expanded final recipient specified in the To, Cc, or Bcc field.
Forwarded	The Forwarded field is displayed as a field of the To, Cc, and Bcc fields that are described earlier in this topic. The Forwarded field is preceded by a comma. Usually, the Forwarded field displays the e-mail address of a mailbox configured to forward e-mail messages to the account specified in the To, Cc, or Bcc field. If a chain of forwarding mailboxes is configured, where each mailbox forwards messages to the next one, the first forwarding mailbox is displayed in this field and the SMTP address of the final, non-forwarding mailbox in the chain is displayed in the To, Cc, or Bcc field.

The Journaling agent generates a journal report if a journaling recipient (the recipient specified in a journal rule) is detected in one of the following scenarios:

- The journaling recipient is the sender or a recipient specified in the To, Cc, or

Bcc fields.
- The journaling recipient is a member of a distribution group that's specified in the To, Cc, or Bcc fields.
- A message is automatically forwarded to a journaling recipient.

In the following cases, information about some recipients who aren't journaling recipients may not be included in the journal report.

- **Message chipping occurs** When a Hub Transport server handles a message that's sent to more than 1,000 recipients, either through distribution group expansion or if more than 1,000 recipients are specified in the To, Cc or Bcc fields, the server generates a separate or copy of the message for every 1,000 recipients. This is performed to reduce system resources used during message expansion. By default, each copy contains a maximum of 1,000 recipients. This is known as *message chipping*. Each instance of the message is known as a *chipped message*.
  The Journaling agent processes each chipped message to determine if there are any journaling recipients included in the recipient list. For example, if a message is sent to a distribution group that contains 5,000 members, the Hub Transport server generates five chipped messages, each containing 1,000 recipients. The Journaling agent generates a single journal report for each chipped message that contains a journaling recipient. The journal report contains details of only the 1,000 recipients included in the recipient list of the chipped message. If the distribution group membership contains only one journaling recipient, the Journaling agent generates a single journal report. That report lists only the 1,000 members that were expanded as a result of message chipping.
- **Distribution group expansion servers are specified** When a Hub Transport server receives a message sent to an individual recipient or a distribution group marked for journaling, and a distribution group which has another Hub Transport server specified as the expansion server, the journal report lists the distribution groups as To, Cc, or Bcc recipients, but the Expanded field doesn't include members of the distribution group that wasn't expanded on that server.
  For example, consider a message sent to two distribution groups (DL-Journaled, DL-NotJournaled) and a mailbox user (UserA). The DL-Journaled distribution contains journal recipients. The DL-NotJournaled distribution group has the Hub Transport server HT2 specified as an expansion server. In this example, the following steps are taken:
  .1.The message is first processed by Hub Transport server HT1. HT1 expands DL-Journaled and detects journaling recipients. HT1 generates a journal report that contains the following noteworthy fields:
    To/Cc/Bcc This field includes DL-Journaled, DL-NotJournaled, and UserA.
    Expanded This field includes members of DL-Journaled. If DL-Journaled contains more than 1,000 members, message chipping may occur, which would generate more than one chipped message. It may also include membership of any other distribution groups expanded on HT1 for this particular chipped message (for example, a distribution group that's a member of DL-Journaled).
  .2.HT1 delivers the journal report to the journaling mailbox.
  .3.HT1 marks the message as journaled by inserting the x-header `X-MS-Exchange-Organization-Processed-By-Journaling`.
  .4.HT1 bifurcates the message and sends it to HT2, the expansion server specified for DL-NotJournaled.
  .5.HT1 delivers the message to the next hop for the recipients expanded from DL-Journaled (which could include further bifurcation) and UserA.
  .6.HT2 receives the message. It inspects the message headers and determines that the message has been journaled.
  .7.HT2 expands the DL-NotJournaled distribution group. None of the expanded

recipients are journaling recipients. Therefore, no additional journal reports are generated.

.8. HT2 delivers the message to the next hop for the recipients expanded from DL-NotJournaled (which could include further bifurcation).

Return to top

Journal Report Headers

In Exchange 2003, the journaling of messages and the identification of journal reports are controlled by using the X-EXCH50 binary large object (BLOB). In Exchange 2010, the X-EXCH50 BLOB is deprecated and replaced with SMTP headers. The organization SMTP headers can be accessed only by the Exchange 2010 transport components, and they're removed by the header firewall before a message is delivered to a mailbox or to an SMTP server outside the Exchange 2010 organization.

The following headers are used by the journaling agent:

- `X-MS-Exchange-Organization-Journal-Report` This SMTP header identifies an Exchange 2010 journal report. This allows the message to act as a system message, allowing it to bypass message size and mailbox recipient restrictions. The header is removed when the journal report is delivered to a journal mailbox.
- `X-MS-Journal-Report` This SMTP header is added to a journal report when it's delivered to a journal mailbox, to indicate the message is a journal report. This header lets you differentiate a journal report from a regular message, but it isn't used by any Exchange 2010 transport components.
- `X-MS-Exchange-Organization-Processed-By-Journaling` This SMTP header identifies messages that have been processed by the Exchange 2010 Journaling agent. If the header is included in a message, Exchange 2010 recognizes that the message has already been processed by the Journaling agent on a previous Hub Transport server, and it doesn't journal the message again. This header is removed before the message is delivered to recipients.

These SMTP headers don't contain values. As previously described, the existence of these headers in a message determines whether the message is a journal report or has been processed by the Journaling agent.

For more information, see the following topics:

- Understanding Header Firewall
- Understanding Journaling in a Mixed Exchange 2003 and Exchange 2010 Environment

Return to top

Examples of Journal Reports

The first figure in this section shows an example of a journal report that was generated when a message was sent from an Exchange 2010 mailbox to a Hub Transport server. The message was sent by mailbox user Jennifer Kim to the following recipients:

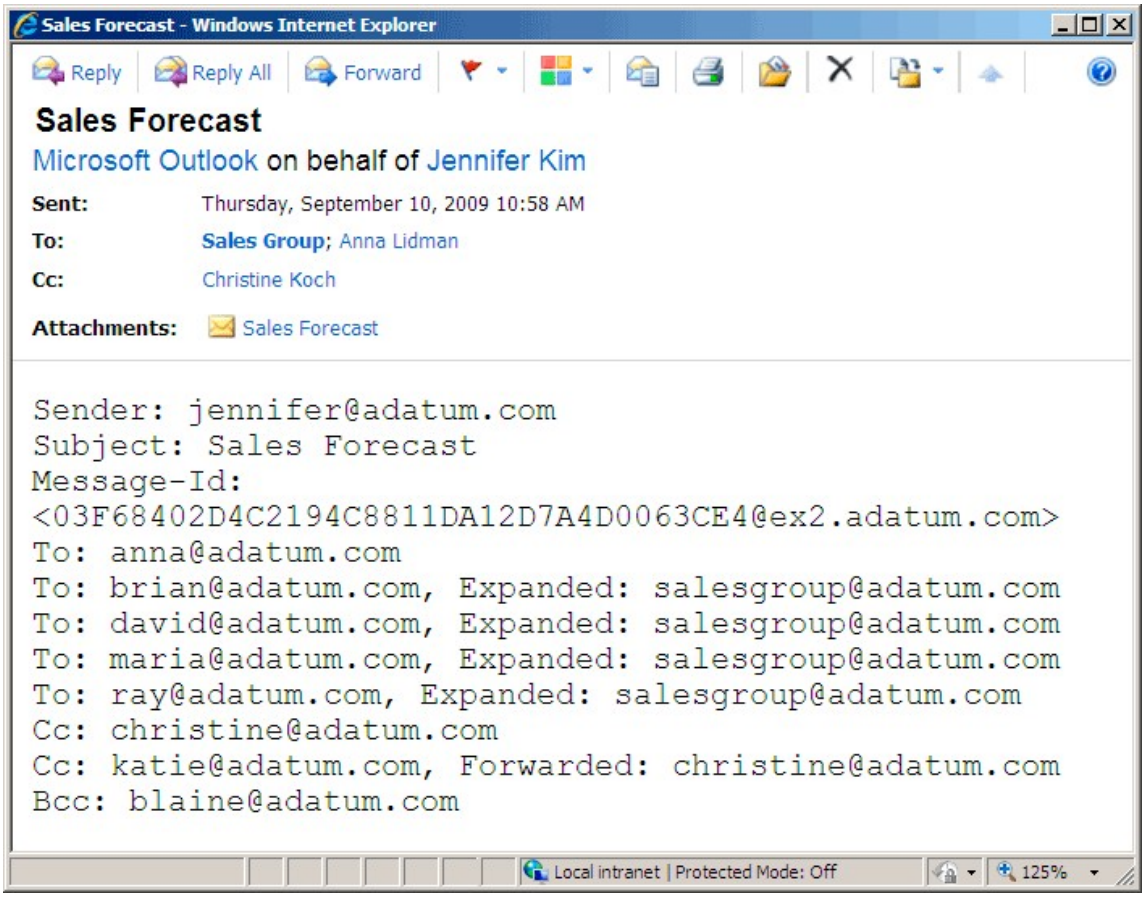
- To: SalesGroup distribution group, Anna Lidman
- Cc: Christine Hughes

  Note:

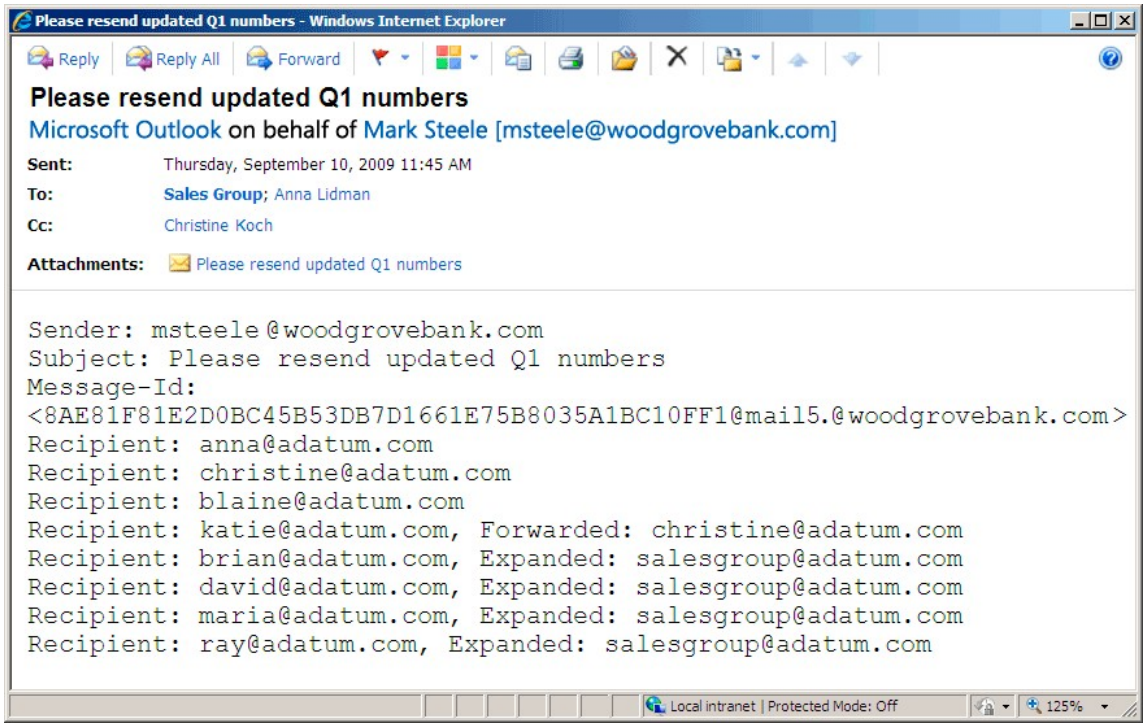
  Christine's mailbox is configured to automatically forward messages to the mailbox for Katie Jordan, and also keep a copy.

- Bcc: Blaine Dockter

A single journal report was created when the original message was sent. The journal report shown in the following figure lists all the recipients addressed in the To field, including recipients expanded from the SalesGroup distribution group, the Cc field, including recipients to whom the message was forwarded automatically, and the Bcc field recipient.



The following figure shows an example of a journal report that was generated when a message that originated from the Internet was processed by a Hub Transport server. The recipients addressed in this example are the same as the recipients in the previous example. However, in the journal report in this figure, all recipients are included in the Recipient field because the original message was sent from the Internet, and Exchange can't verify that the recipient addressing hasn't been tampered with. As with the first example, a single journal report is created.



Return to top

1.11.5.3 Understanding How to Manage Journal Reports

Understanding How to Manage Journal Reports

Exchange Server 2010 > Messaging Policy and Compliance > Journaling >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-13*

When you use Microsoft Exchange Server 2010 to deploy journaling, the following factors can affect the delivery and availability of journal reports generated when a recipient or sender receives or sends messages that are journaled:

- **Journaling mailbox size** You must determine how high to set the mailbox quota on journaling mailboxes.
- **Alternate journaling mailbox** You should consider how configuring an alternate journaling mailbox affects journal report delivery.

For more information, see Understanding Journaling.

Looking for management tasks related to journaling? See Managing Journaling.

Journaling Mailbox Size

When you configure a journaling mailbox to accept journal reports, you must determine the maximum size of the journaling mailbox. As with any other mailbox, the maximum size depends on the data to be stored in the mailbox, the hardware resources available, and the disaster recovery requirements for the server where the journaling mailbox is located. In addition to these considerations, you must also consider what will occur if a journaling

mailbox exceeds the configured mailbox quota.

When you configure the **Prohibit send and receive at (KB)** option for a storage quota on a journaling mailbox, the mailbox accepts journal reports until it reaches the configured storage quota. When the prohibit send and receive storage quota is exceeded, the journaling mailbox stops accepting journal reports.

Exchange doesn't return journal reports to the original sender as it does with regular messages. Instead, it holds undelivered journal reports in a mail queue and tries to redeliver them until delivery is successful. Although this enables Exchange to eventually deliver all the journal reports generated, it can be problematic in organizations with high messaging traffic because the mail queues on the affected Hub Transport servers can grow quickly.

To reduce the possibility that your journaling mailbox will reject journal reports because it has reached the configured storage quota, we recommend that you configure its prohibit send and receive storage quota to the maximum size that your hardware resources and disaster recovery capabilities allow for.

Important:

If you configure journaling mailboxes without storage quotas, monitor the Mailbox server to ensure that it doesn't exceed the available hardware resources or disaster recovery capabilities.

If you must configure a prohibit send and receive storage quota on a journaling mailbox and expect that the configured storage quota might be exceeded, you can configure an alternate journaling mailbox. For more information about alternate journaling mailboxes, see "Alternate Journaling Mailbox" later in this topic. When a journal report is rejected by a journaling mailbox, Event ID 8010 is logged in the Application event log. By monitoring the Application event log for this event, you can be alerted to a potential problem with the journaling mailbox and resolve the situation quickly.

For information about how to configure storage quotas on a journaling mailbox, see Configure Storage Quotas for a Mailbox.

Alternate Journaling Mailbox

When the journaling mailbox is unavailable, you may not want rejected journal reports to collect in an e-mail queue on Hub Transport servers. Instead, you can configure an alternate journaling mailbox to store those journal reports. The alternate journaling mailbox receives the journal reports as attachments in the non-delivery reports (NDRs) generated when the journaling mailbox or the server on which it's located refuses delivery of the journal report or becomes unavailable.

When the journaling mailbox becomes available again, you can use the **Send Again** feature of Microsoft Office Outlook to submit journal reports for delivery to the journaling mailbox.

Different mailbox databases and journal rules may be configured to deliver journal reports to different journaling mailboxes. However, when you configure an alternate journaling mailbox, all the journal reports that are rejected or can't be delivered across your entire Exchange 2010 organization are delivered to the alternate journaling mailbox. Therefore, it's important to make sure that the alternate journaling mailbox and the Mailbox server where it's located can support many journal reports.

Caution:

If you configure an alternate journaling mailbox, you must monitor the mailbox to make sure that it doesn't become unavailable. If the alternate journaling mailbox also becomes unavailable or rejects journal reports at the same time, the rejected journal reports are

lost and can't be retrieved. This is an important factor when considering whether to use an alternate journaling mailbox.

After an alternate journaling mailbox is configured, only journal reports submitted for delivery to any unavailable journaling mailbox are redirected to it. Journal reports that have already failed delivery before the alternate journaling mailbox is configured aren't redirected.

If you configure an alternate journaling mailbox, you can reduce the load on your Hub Transport servers and Mailbox servers. Exchange doesn't continually try to deliver the journal reports to an unavailable journaling mailbox. Instead, Exchange redirects them to the alternate journaling mailbox where they can remain until you're ready to resubmit them to the journaling mailbox.

However, because the alternate journaling mailbox collects all the rejected journal reports for the entire Exchange 2010 organization, you must make sure that this doesn't violate any laws or regulations that apply to your organization. If laws or regulations prohibit your organization from allowing journal reports sent to different journaling mailboxes from being stored in the same alternate journaling mailbox, you may be unable to configure an alternate journaling mailbox. Discuss this with your legal representatives to determine whether you can use an alternate journaling mailbox.

When you configure an alternate journaling mailbox, you should use the same criteria that you used when you configured the journaling mailbox. You must make sure that the following conditions are true:

- **Authorized submission** Only authorized accounts should be able to submit journal reports.
- **Authorized access** Only those individuals who are authorized to access the mailbox are given access to the mailbox.
- **Adequate storage quota** Configure a storage quota that meets the needs of your data, hardware, and disaster recovery needs.

Remember that because the alternate journaling mailbox accepts rejected journal reports for all journaling mailboxes in your Exchange 2010 organization, the hardware resource requirements and mailbox storage quotas may be significantly larger than those required for a journaling mailbox.

For more information about how to configure an alternate journaling mailbox, see Configure or Remove an Alternate Journaling Mailbox.

1.11.5.4 Understanding Journaling in a Mixed Exchange 2003 and Exchange 2010 Environment

Understanding Journaling in a Mixed Exchange 2003 and Exchange 2010 Environment

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-20*

When planning for journaling in a mixed Microsoft Exchange Server 2010 and Exchange Server 2003 environment, it's important to understand how they interoperate.

Note:

For journaling interoperability, Exchange 2003, Exchange 2010, and Exchange Server 2007 have similar characteristics.

To learn more about journaling, see Understanding Journaling.

Looking for management tasks related to managing journaling? See Managing Journaling.

Contents

Journaling in Exchange 2003

The journaling feature in Exchange 2003 allows you to journal all the mailboxes on a mailbox database. If you want to journal only some mailboxes in a mailbox database, you have to do either of the following:

- Journal all the mailboxes in that mailbox database.
- Create a new mailbox database, enable journaling on that mailbox database, and then move the mailboxes to be journaled to the new database.

Exchange 2003 doesn't let you centrally manage its journaling capabilities. You have to manage journaling on a per-mailbox store and per-Mailbox server basis.

By default, when a message is journaled in Exchange 2003, only the original message is delivered to the journaling mailbox. To journal the envelope information of the original message, you must manually enable *envelope journaling*. Even with envelope journaling enabled, only basic subject and recipient information is captured.

Return to top

Journaling in Exchange 2010

The journaling feature in Exchange 2010 has been significantly redesigned to enable more control over what recipients and senders you journal. In Exchange 2010, you can create journal rules to target specific recipients and senders, distribution groups, or a combination of both. It doesn't matter where the recipients or senders are located.

Using journal rules, the granularity of journaling is improved so that you can selectively journal one or more recipients. You can also locate mailboxes that you want to journal on a mailbox database that may also contain mailboxes you don't want to journal. Only the messages that are sent from or to senders and recipients for which you've created journal rules are journaled.

In addition, you manage journal rules centrally on Hub Transport servers. Journal rules are stored in Active Directory. Journal rules created on a Hub Transport server are automatically replicated throughout the Active Directory forest and become available to all Hub Transport servers. This means that all Hub Transport servers in your organization use the same journaling configuration.

In Exchange 2010, you can still journal messages on a per-mailbox database basis. This configuration is equivalent to the Exchange 2003 per-mailbox database configuration where all messages sent to or from mailboxes on a journaled mailbox database are

journaled.

Exchange 2010 uses envelope journaling and provides much more information in the journal envelopes to help you sift through the potentially large amount of data that can be collected when mailboxes are journaled. The journal envelopes are formatted to enable automated searching of journal report contents by third-party or custom applications.

For more information about journal reports in Exchange 2010, see Understanding Journal Reports.

Return to top

How Exchange 2003 and Exchange 2010 Identify Journal Reports and Journaled Messages

In Exchange 2003, the journaling of messages and the identification of journal reports are controlled by using the X-EXCH50 binary large object (BLOB). The X-EXCH50 BLOB contains extended information about the message that can't be stored elsewhere in the e-mail message. The information stored in the X-EXCH50 BLOB contains a variety of information, such as journaling, spam confidence level (SCL), and other MAPI properties that don't have MIME representation.

By examining the X-EXCH50 BLOB, Exchange 2003 can determine whether a message is a journal report and therefore bypasses various system limits, such as message size and mailbox recipient restrictions. Exchange 2003 also uses the X-EXCH50 BLOB to determine whether a message has already been journaled on a previous hop on another Exchange 2003 server. This prevents other Exchange 2003 servers that may handle the message from journaling it again. However, the limitation of the X-EXCH50 BLOB is that it's a proprietary Extended Simple Mail Transfer Protocol (ESMTP) verb. As such, it can't be propagated by computers that don't have Exchange installed.

In Exchange 2010, the X-EXCH50 BLOB is deprecated and replaced with SMTP headers to which the header firewall is applied. These SMTP headers can be accessed only by the Exchange 2010 transport components. They are removed from messages before delivery to mailboxes or delivery outside the Exchange 2010 organization. The following SMTP headers are used by the Exchange 2010 Journaling agent:

- **X-MS-Exchange-Organization-Processed-By-Journaling** This SMTP header identifies messages that have been processed by the Exchange 2010 Journaling agent. If this header is included in a message, Exchange 2010 recognizes that the message has already been processed by the Journaling agent on a previous hop by another Hub Transport server and doesn't journal the message again.
- **X-MS-Exchange-Organization-Journal-Report** This SMTP header identifies an Exchange 2010 journal report in the transport pipeline. If this header is included in a message, Exchange 2010 knows the message is a journal report. It allows the message to act as a system message and bypass message size and mailbox recipient restrictions.
- **X-MS-Journal-Report** Before delivering a journal report to the journaling mailbox or an external journaling recipient, the header firewall removes all Exchange Server Organization headers, including the `X-MS-Exchange-Organization-Journal-Report` header. Instead, the `X-MS-Journal-Report` header is added to identify it as an Exchange 2010 journal report after it has left the transport pipeline. This header isn't used by any Exchange

2010 transport components. It lets you differentiate a journal report from a regular message.

For more information about the SMTP header firewall, see Understanding Header Firewall.

Return to top

Exchange 2003 and Exchange 2010 Journaling Interoperability

This section describes how journaling functionality works in a mixed Exchange environment.

Supporting Exchange 2003 Journaling in an Exchange 2010 Organization

Exchange 2003 and Exchange 2010 identify journal reports and journaled messages differently. To support journaling in a mixed Exchange 2003 and Exchange 2010 organization, Exchange 2010 supports using the X-EXCH50 BLOB. However, Exchange 2003 doesn't support or recognize the new SMTP headers that are used by Exchange 2010.

When Exchange 2010 journals a message, it adds a property to the X-EXCH50 BLOB in addition to the `X-MS-Exchange-Organization-Processed-By-Journaling` SMTP header so that Exchange 2003 servers that encounter the message know that the message has already been journaled.

Exchange 2010 treats journal reports similarly. When a journal report is created in Exchange 2010, the X-EXCH50 BLOB is added to the message in addition to the `X-MS-Journal-Report` header. This enables the journal report to travel through the Exchange organization and to be treated as a journal report by all the Exchange servers that it encounters.

Exchange 2010 also reads the Exchange 2003 journaling configuration from Active Directory. This configuration tells the Exchange 2010 Hub Transport servers which Exchange 2003 mailbox databases have journaling enabled and also which journaling mailboxes they have sent the journal reports to. When a message is sent to a recipient on a journaled Exchange 2003 mailbox database from Exchange 2010, the Exchange 2010 Hub Transport server journals the message and sends a journal report to the journaling mailbox configured on the Exchange 2003 mailbox database.

For more information about journal reports in Exchange 2010, see Understanding Journal Reports.

Configuring Routing Group Connectors Between Exchange 2003 and Exchange 2007

When you install a Hub Transport server in an Exchange 2003 organization, Exchange 2010 automatically creates the routing group **Exchange Routing Group (DWBGZMFD01QNBJR)**. This routing group contains all the computers in the organization that are running Exchange 2010. All Exchange 2010 servers are members of this routing group. Exchange 2010 configures a routing group connector to connect the Exchange 2010 routing group to an existing Exchange 2003 routing group.

The routing group connector created by Exchange 2010 is configured to enable the X-EXCH50 BLOB to pass between Exchange 2010 servers and Exchange 2003 servers. If you create additional routing group connectors between the Exchange 2010 routing group and other Exchange 2003 routing groups, the connectors are also configured to enable the X-EXCH50 BLOB to pass between Exchange 2010 servers and Exchange 2003

servers.

Important:

You must use the **New-RoutingGroupConnector** cmdlet to create routing group connectors between Exchange 2010 servers and Exchange 2003 servers. The **New-RoutingGroupConnector** cmdlet configures the required permissions and defaults to enable communication between Exchange 2010 and Exchange 2003. For more information, see New-RoutingGroupConnector.

For more information about routing group connectors, see the following topics:

- Understanding Message Routing
- Create Additional Routing Group Connectors from Exchange 2010 to Exchange 2003

Reducing Multiple Journal Reports

In a native Exchange 2010 organization, when a message passes through Hub Transport servers, the message is evaluated by the Journaling agent. Unless the recipient list changes on that message before delivery, the Journaling agents on later Hub Transport servers don't reevaluate the message. Because the message is evaluated for journaling only on one Hub Transport server, only one journal report is typically created and sent to the journaling mailbox.

When messages are journaled in a mixed Exchange 2003 and Exchange 2010 organization, the possibility of creating multiple journal reports for a single message increases. This is because both an Exchange 2010 Hub Transport server and the Exchange 2003 server that receive or send the message from or to a Hub Transport server evaluate the message for journaling.

Exchange 2010 reduces multiple journal reports that are generated for a single message by supporting the X-EXCH50 BLOB. The Exchange 2010 Hub Transport server stamps the X-EXCH50 BLOB on the original message with the address of the journaling mailbox where the journal report was sent. When an Exchange 2003 server receives the message from the Exchange 2010 Hub Transport server, the Exchange 2003 server examines the X-EXCH50 BLOB to see whether the message has been journaled. If it has been journaled, and if the journal report was sent to the same journaling mailbox configured on the mailbox store where the mailbox resides, Exchange 2003 doesn't generate another journal report.

Note:

Although Exchange 2010 supports the X-EXCH50 BLOB, the Journaling agent doesn't read it when it evaluates a message that was received from an Exchange 2003 server. If a message matches an Exchange 2010 journal rule, a journal report is created, even if Exchange 2003 already journaled the message and sent a journal report to the same journaling mailbox.

Journaling Mailbox Location

If you want to journal mailboxes that reside on an Exchange 2003 mailbox database, the journaling mailbox must be located in an Exchange 2003 mailbox database that doesn't have journaling enabled. Configuring a mailbox database to journal messages to a mailbox located on a non-Exchange 2003 mailbox database isn't supported. If you locate a journaling mailbox in an Exchange 2003 mailbox database being journaled, excessive disk utilization can occur.

You can configure Exchange 2010 journal rules to deliver journal reports to either Exchange 2003 or Exchange 2010 mailboxes.

Distribution Group Expansion

Both Exchange 2003 and Exchange 2010 provide distribution groups. Distribution groups are mail-enabled groups that can contain any number of e-mail recipients. When a sender

sends a message to a distribution group, the server takes the original message, accesses the distribution group membership, and sends the message to each recipient in the membership list. This process is known as distribution group expansion.

In both Exchange 2003 and Exchange 2010, you can specify which servers perform distribution group expansion. This is typically done to optimize server and network traffic load. By default, Exchange 2010 distribution groups are configured to use any Hub Transport server as a distribution group expansion server. Any Exchange server can act as a distribution group expansion server in Exchange 2003.

When you install Exchange 2010 into an existing Exchange 2003 organization and perform journaling in this mixed organization, we recommend that you configure all distribution groups to use Exchange 2010 Hub Transport servers as distribution group expansion servers. This is recommended because messages wouldn't be journaled, even if the recipients are configured for journaling, if the following conditions are true:

- Exchange 2010 recipients are configured for journaling.
- Exchange 2010 recipients are included in the distribution group Sales, for example.
- The Sales distribution group is configured to use an Exchange 2003 distribution list expansion server.

In this scenario, the following chain of events occurs if an Exchange 2010 sender sends a message to the Sales distribution group:

1. The message is sent to a Hub Transport server.
2. Because the Sales distribution group isn't configured to use a Hub Transport server as the distribution group expansion server, the journal rules in the Exchange 2010 organization can't access the distribution group recipients. Therefore, no journal rules can be applied to the recipients in the distribution group.
3. The message is routed to the Exchange 2003 server for expansion.
4. The Exchange 2003 server expands the distribution group. Because the Exchange 2003 server can't access the Exchange 2010 journal rule configuration, no messages are journaled.
5. The Exchange 2003 server routes the expanded messages back to the Exchange 2010 Hub Transport server for delivery to the Exchange 2010 recipients.
6. The Hub Transport server receives the message. Because this isn't the first server to route these messages, the Hub Transport server assumes the messages have already been evaluated for journaling and the journal rules aren't applied.

Return to top

1.11.5.5 Protecting Journal Reports

Protecting Journal Reports

Exchange Server 2010 > Messaging Policy and Compliance > Journaling >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-26*

If journaling is configured in a Microsoft Exchange Server 2010 organization, the Journaling agent generates journal reports that contain message metadata, and the entire original message is attached to the journal report. It's important to protect the integrity of journal reports and the journaling mailbox, and to protect them from unauthorized access.

You can protect journal reports sent inside an Exchange 2010 organization and journal reports that are sent to third-party solution providers.

Looking for management tasks related to journaling? See Managing Journaling.

Protecting Journal Reports Sent Inside an Exchange 2010 Organization

Exchange 2010 protects journal reports in transit by performing the following tasks:

- It uses secure links between Hub Transport servers and Mailbox servers in the Exchange 2010 organization.
- It sends the journal report as Exchange and authenticates the session between the Hub Transport server and the Mailbox server.
- It accepts only secure, authenticated connections when journal reports are sent between Hub Transport servers and Mailbox servers in the same Exchange 2010 organization.

We recommend that you configure the journaling mailbox to accept messages sent only from the Exchange recipient object and that you configure the mailbox to require senders to be authenticated. This helps reduce the possibility of tampering with journal reports delivered to the journaling mailbox. For more information, see Create and Configure a Journaling Mailbox.

Additionally, you must implement adequate access controls to ensure the journaling mailbox is protected from unauthorized access. These controls should include measures such as recording and monitoring password changes to journaling mailbox user accounts, domain logons by such user accounts, and changes to mailbox permissions for journaling mailboxes.

Caution:

Improperly secured communication links, journaling mailboxes, or servers can expose sensitive data.

Protecting Journal Reports Sent to Third-Party Solution Providers

You can configure Exchange 2010 to send journal reports to a recipient that doesn't reside in the same Exchange 2010 organization as the Hub Transport server, including recipients residing on another e-mail system within the organization, or to an e-mail system outside the organization. You can use such a configuration to send journal reports to third-party providers of archival or other journaling solutions that aren't Exchange 2010-based.

In configurations where the source and destination servers aren't servers running Exchange 2010 or Exchange Server 2007 in the same Exchange organization, the connections between the two servers may not be automatically encrypted. However, even in these configurations, you can use Exchange 2010 to help protect the journal reports sent to the third-party solution providers.

You can use the following Exchange solutions to help protect communication between the Exchange server and the third-party solution providers:

- Configure Transport Layer Security (TLS) between the two systems.
- Require authentication on the receiving system.
- Accept only e-mail messages from the SMTP address of the Exchange contact.
- Configure a mail-enabled contact that sends e-mail messages to the SMTP address of the third-party solution and configure Exchange 2010 to send

journal reports to that contact. Then configure the contact to accept journal reports only from an Exchange recipient.

Caution:
Improperly secured communication links, journaling mailboxes, or servers can expose sensitive data.

TLS is a standard protocol used to provide secure communications over TCP/IP networks such as the Internet. It enables clients to authenticate servers or, optionally, servers to authenticate clients. It also provides a secure channel by encrypting communications. For more information, see TLS Functionality and Related Terminology in Exchange 2010.

Important:
TLS encrypts the SMTP session between two hosts. If you configure TLS to protect journal messages, and Exchange doesn't directly deliver mail to the destination server that stores the journal reports, you must configure TLS between each server through which the journal report travels to the destination server.

Important:
Journal message recipients in a distribution group cannot view decrypted message attachments in an Exchange 2010 environment
This issue occurs because Exchange 2010 does not decrypt the journal message if at least one SMTP address of a distribution group member is not present in any journal rules. This behavior is by design.

For More Information

Understanding Journal Reports

Understanding How to Manage Journal Reports

Understanding Journaling

1.11.5.6 Managing Journaling

Managing Journaling

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-09-24*

Create and Configure a Journaling Mailbox

Configure or Remove an Alternate Journaling Mailbox

Create a Journal Rule

Configure Journal Rule Properties

Enable or Disable a Journal Rule

Remove a Journal Rule

Disable or Enable Journaling of Voice Mail and Missed Call Notifications

Enable Per-Mailbox Database Journaling

Disable Per-Mailbox Database Journaling

1.11.5.6.1 Create and Configure a Journaling Mailbox

Create and Configure a Journaling Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If journaling is enabled in an Exchange organization, either by using journal rules or standard journaling (per-mailbox database journaling), you can create a mailbox that's used for collecting journal reports. This is known as a journaling mailbox.

This topic shows you how to create a journaling mailbox. Additionally, this topic provides the following recommended steps to configure the journaling mailbox.

- **Configure the journaling mailbox to accept messages only from the Microsoft Exchange recipient** Journaling mailboxes receive journal reports from the Journaling agent. To maintain the integrity of the journaling mailbox, and to prevent fake journal reports and other messages, you should configure the journaling mailbox to receive e-mail only from the Journaling agent. The Journaling agent delivers journal reports to the journaling mailbox by using the Microsoft Exchange recipient, a system mailbox that isn't visible in the global address list (GAL). For more information about the Microsoft Exchange recipient, see Understanding the Microsoft Exchange Recipient.
- **Disable storage quota limits for the journaling mailbox** A journaling mailbox is used by the Journaling agent to deliver a journal report for the following:
  - Every message that matches the parameters of a journal rule
  - Every message that is sent or received by mailboxes on a mailbox database (if you use per-mailbox database journaling)

  Depending on the messaging traffic in your organization, and the number of messages that have to be journaled, a journaling mailbox can potentially grow to a very large size. If you set a low storage quota, delivery of new journal reports to the mailbox will stop after the quota is reached. Therefore, we recommend that you disable mailbox quotas for the journaling mailbox or enable a **Prohibit send and receive quota**. For more information about mailbox storage quotas, see Understanding Quota Messages.

  Important:
  If you disable mailbox storage quota limits on a mailbox, we recommend that you monitor the mailbox size. We recommend that you configure the mailbox to accept messages only from the Microsoft Exchange recipient, and not accept messages sent by unauthenticated senders.
- **Grant Full Access permissions to users for the journaling mailbox** After you've created a journaling mailbox, if the mailbox is intended for programmatic access or if you want to grant access to authorized users such as records managers, you must grant full access permission to access the mailbox.

To learn more about journaling mailboxes and the Journaling agent, see Understanding Journaling.

Important:
Journaling mailboxes contain very sensitive information. You must secure journaling

mailboxes because they collect messages that are sent to and from recipients in your organization. These messages may be part of legal proceedings or may be subject to regulatory requirements. Various laws require that messages remain tamper-free before they're submitted to an investigatory authority. We recommend that you create policies that govern who can access the journaling mailboxes in your organization, limiting access to only those individuals who have a direct need to access them. Speak with your legal representatives to make sure that your journaling solution complies with all the laws and regulations that apply to your organization.

Looking for other management tasks related to journaling? Check out Managing Journaling.

Step 1: Use the EMC or the Shell to create a journaling mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "User mailboxes" entry in the Mailbox Permissions topic.

Use the EMC

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Mailbox**.
3. On the **Introduction** page, click **User Mailbox**.
4. On the **User Type** page, click **New User**.
5. On the **User Information** page, complete the following fields:
   - **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.
   - **First name**, **Initials**, and **Last name** Because this mailbox will be used to collect journal reports, it isn't necessary to complete these fields.
   - **Name** Use this box to type a display name for the journaling mailbox. This is the name that's listed in Active Directory. By default, this box is populated with the names you enter in the **First name**, **Initials**, and **Last name** boxes. If you didn't use those boxes, you must still type a name in this field. The name can't exceed 64 characters.
   - **User logon name (User Principal Name)** Use this box to type the name that the user will use to log on to the journaling mailbox. The user logon name consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides.
   - **User logon name (pre-Windows 2000)** Use this box to type the name for the user that's compatible with the legacy versions of Microsoft Windows (prior to the release of Windows 2000 Server). This field is automatically populated based on the **User logon name (User Principal Name)** field. This field is required.
   - **Password** Use this box to type the password that the user must use to log on to the journaling mailbox.

     Note:
     Journaling mailboxes can potentially contain sensitive information. We recommend using a complex password that exceeds the

password requirements your organization may have for normal user accounts.

- **Confirm password** Use this box to confirm the password that you typed in the **Password** box.
- **User must change password at next logon** Select this check box if you want the user to reset the password when they first log on to the journaling mailbox.

  If you select this check box, at first logon, the user will be prompted with a dialog box in which to change the password. The user won't be allowed to perform any tasks until the password is successfully changed.

  Requiring a password change at first logon is a good practice for accounts you create for your users. It forces the user to change the password, which prevents the use of any default passwords provided by the administrator during account creation. A forced password change on first logon also ensures that the administrator doesn't have knowledge of the user password after first logon. This may not be necessary for journaling mailboxes because the associated user accounts are created and used by the administrator or by administrator-controlled processes that may access the journaling mailbox.

6. On the **Mailbox Settings** page, complete the following fields:
   - **Alias** Use this box to type an alias for the journaling mailbox. The alias can't exceed 64 characters and must be unique in the forest.
   - **Specify the mailbox database rather than using a database automatically selected** Select this check box to specify a mailbox database instead of allowing Exchange to select a database for you. Click **Browse** to open the **Select Mailbox Database** dialog box. This dialog box lists all the mailbox databases in your Exchange organization. By default, the mailbox databases are sorted by name. You can also click the title of the corresponding column to sort the databases by storage group name or server name. Select the mailbox database you want to use, and then click **OK**. This is an optional field.

     Note:

     When you plan to use journaling, consider the storage requirements for journaling mailboxes. These will vary depending on the number and size of messages captured by the Journaling agent.

   - **Managed folder mailbox policy** Select this check box to specify a managed folder mailbox policy for the journaling mailbox. A managed folder mailbox policy is a logical grouping of managed folders. When a managed folder mailbox policy is applied to a user's mailbox, all the managed folders that are linked to the policy are deployed in a single operation, thereby making the deployment of messaging records management (MRM) easier. To learn more, see Understanding Managed Folders.

     Click **Browse** to open the **Select Managed Folder Mailbox Policy** dialog box. Use this dialog box to select the managed folder mailbox policy to be associated with this mailbox. This is an optional field.

     Some third-party archiving or retention solutions retrieve journal reports from the journaling mailbox and store them in an external database, or require you to automatically forward a copy of the journal report to the external database or e-mail address. If you use a similar solution, and if it doesn't automatically purge messages from the journaling mailbox after retrieving them, the journaling mailbox may continue to grow and consume storage space. You can create a managed folder mailbox policy and apply it to the journaling mailbox to

automatically purge messages after a certain period.

- **Exchange ActiveSync mailbox policy** Journaling mailboxes are not meant to be accessed by using Microsoft Exchange ActiveSync. You don't have to select this option when you create a journaling mailbox.

7. On the **Archive Settings** page, leave the **Create an archive mailbox for this account** check box cleared.
8. On the **New Mailbox** page, review your configuration settings. To make any configuration changes, click **Back**. To create the journaling mailbox, click **New**.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell

This example creates a journaling mailbox with the following parameters:

- **Name** Vault5
- **User Principal Name** vault@contoso.com
- **Mailbox Database** Database2

After you enter the first command, you are prompted for a password.

```
$password = Read-Host "Enter password" -AsSecureString
New-Mailbox -Name Vault5 -UserPrincipalName vault@contoso.com -Database "Database
```

For detailed syntax and parameter information, see New-Mailbox.

Step 2 (optional but recommended): Use the Shell to configure the journaling mailbox to accept messages only from the Microsoft Exchange recipient

Caution:

This procedure shouldn't be performed in organizations in which the journaling mailbox is required to receive e-mail from non-Exchange mail hosts, unauthenticated senders, or senders other than the Microsoft Exchange recipient.

Note:

You can't use the EMC to perform this procedure because the Microsoft Exchange recipient, a system mailbox, isn't visible in the GAL.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "User mailboxes" entry in the Mailbox Permissions topic.

This example configures delivery restrictions on a journaling mailbox with the display name Journaling Mailbox to accept messages only from the Microsoft Exchange recipient and to accept messages only from authenticated senders.

```
Set-Mailbox "Journaling Mailbox" -AcceptMessagesOnlyFromSendersOrMembers "Microso
```

For detailed syntax and parameter information, see Set-Mailbox.

Step 3 (optional but recommended): Use the EMC or the Shell to disable storage quota limits for the journaling mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "User mailboxes " entry in the Mailbox Permissions topic.

Use the EMC

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the journaling mailbox you created.
3. In the action pane, click **Properties**.
4. On the **Mailbox Settings** tab, select **Storage Quotas**, and then click **Properties**.
5. In **Storage Quotas**, clear the **Use mailbox database defaults** check box, and then click **OK**.
6. Click **Apply**, and then click **OK**.

Use the Shell

This example disables mailbox quotas for the journaling mailbox vault.

```
Set-Mailbox "vault" -UseDatabaseQuotaDefaults $false -IssueWarningQuota unlimited
```

For detailed syntax and parameter information, see Set-Mailbox.

Step 4 (optional but recommended): Grant Full Access permissions to selected users for accessing the journaling mailbox

For detailed instructions about how to grant Full Access permissions to a mailbox, see Manage Full Access Permissions.

Other Tasks

After you create and configure a journaling mailbox, you may also want to perform the following procedures.

- Configure or Remove an Alternate Journaling Mailbox
- Create a Journal Rule
- Enable Per-Mailbox Database Journaling

1.11.5.6.2 Configure or Remove an Alternate Journaling Mailbox

Configure or Remove an Alternate Journaling Mailbox

Messaging Policy and Compliance > Journaling > Managing Journaling >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If a journaling mailbox becomes unavailable, journal reports sent to it are rejected and resubmitted for delivery. Journal reports are never returned to the original sender. If you don't want the rejected journal reports to remain in the delivery queue, you can configure an alternate journal mailbox to receive the journal reports until the journaling mailbox becomes available.

Only journal reports submitted for delivery after an alternate journaling mailbox is configured are redirected. Journal reports that failed delivery before the alternate journaling mailbox was configured aren't redirected. Journal reports are delivered to the alternate journaling mailbox as attachments in a non-delivery report (NDR). When the journaling mailbox becomes available, you can use the **Send Again** feature in Outlook 2010 to resubmit the journal reports for delivery.

Important:

When you configure an alternate journaling mailbox, it applies to the whole Exchange organization. Journal reports rejected by any journaling mailbox are redirected to the same alternate journaling mailbox.

For more information about how to manage journal reports, see Understanding How to Manage Journal Reports.

Looking for other management tasks related to journaling? Check out Managing Journaling.

Caution:

If you configure an alternate journaling mailbox, you must monitor the mailbox to make sure that it doesn't become unavailable. If the alternate journaling mailbox also becomes unavailable and rejects journal reports, the rejected journal reports are lost and can't be retrieved.

Use the Shell to configure an alternate journaling mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the EMC to configure an alternate journaling mailbox.

To configure Exchange to redirect rejected journal reports to an alternate journaling mailbox, you must specify the SMTP address of an existing mailbox in your organization.

1. Create a mailbox to use as the alternate journaling mailbox. For information about how to create and configure a journaling mailbox, see Create and Configure a Journaling Mailbox.
2. Use the Shell to configure the mailbox as the alternate journaling mailbox. This example configures the alternate journaling mailbox alternatemailbox@contoso.com.

```
Set-TransportConfig -JournalingReportNdrTo alternatemailbox@contoso.co
```

For detailed syntax and parameter information, see Set-TransportConfig.

Use the Shell to remove an alternate journaling mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to remove an alternate journaling mailbox.

If you no longer want to redirect rejected journal reports to an alternate journaling mailbox, you must remove the SMTP address of that mailbox. When you remove the SMTP address of the mailbox, rejected journal reports stay in the delivery queue until they're successfully delivered.

This example removes an alternate journaling mailbox.

```
Set-TransportConfig -JournalingReportNdrTo "<>"
```

For detailed syntax and parameter information, see Set-TransportConfig.

1.11.5.6.3 Create a Journal Rule

Create a Journal Rule

Messaging Policy and Compliance > Journaling > Managing Journaling >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Journal rules are used to enable journaling of specific recipients. Journal rules are replicated across the Exchange organization to all the Hub Transport servers. Journal rules use premium journaling. To use premium journaling, you must have an Exchange Enterprise client access license (CAL). For more information, see Understanding Journaling.

Caution:
There are important security and resource considerations when you configure the journaling mailbox that receives journal reports. For more information, see "Journaling Mailbox" in Understanding Journaling and Protecting Journal Reports.

Looking for other management tasks related to journaling? Check out Managing Journaling.

Prerequisites

A journaling mailbox has been created, or an existing mailbox is available for use as the journaling mailbox.

What Do You Want to Do?

- Use the EMC to create a journal rule
- Use the Shell to create a journal rule

Use the EMC to create a journal rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance

Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **Journal Rules** tab, and then in the action pane, click **New Journal Rule**.
3. On the **New Journal Rule** page, complete the following fields:
   - 3.a. **Rule name** Type a name for the journal rule.
   - 3.b. **Send Journal reports to e-mail address** Click **Browse**. In the **Select Recipient** window, select the recipient that will receive the journal reports.
   - 3.c. **Scope** Select the scope to which the journal rule should be applied. The following scopes are available:
     - **Global** Global rules process all e-mail messages that pass through a Hub Transport server. These include messages that may have already been processed by internal rules and external rules.
     - **Internal** Internal rules process e-mail messages sent and received by recipients in the Exchange 2010 organization.
     - **External** External rules process e-mail messages sent to recipients or sent from senders outside the Exchange 2010 organization.
   - 3.d. **Journal messages for recipient** If you want to journal messages sent to or from a specific recipient, click **Browse** to select the recipient. In the **Select Recipient** window, select the mailbox, contact, or distribution group that you want to journal, and then click **OK**. All messages sent to or from this recipient are journaled.
   - 3.e. **Enable Rule** Journal rules are enabled by default. To create the rule in a disabled state, clear the check box.
4. Click **New** to create the journal rule.
5. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - 5.a. A status of **Completed** indicates that the wizard completed the task successfully.
   - 5.b. A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a journal rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

This example creates a journal rule to journal all messages sent to and received by the recipient user1@contoso.com.

```
New-JournalRule -Name "Discovery Journal Recipients" -Recipient user1@contoso.com
```

For detailed syntax and parameter information, see New-JournalRule.

Other Tasks

After you create a journal rule, you may also want to:

- Configure or Remove an Alternate Journaling Mailbox
- Enable or Disable a Journal Rule
- Configure Journal Rule Properties
- Remove a Journal Rule

1.11.5.6.4 Configure Journal Rule Properties

Configure Journal Rule Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

A journal rule defines the scope of messages to journal, the journaled recipient, and the journaling mailbox to which journal reports are delivered. You can use either the EMC or the Shell to view or configure a journal rule.

Important:

If you specify a distribution group as the journal recipient, messages sent to the distribution group, as well as messages sent and received by members of the distribution group, are journaled.

These procedures describe how to configure premium journaling. To use premium journaling, you must have the Exchange Enterprise Client Access License (CAL). For more information, see Understanding Journaling.

Looking for other management tasks related to journal rules? Check out Managing Journaling.

Cautions

- If you don't specify a journal recipient in the **Journal messages for recipient** field in the EMC or the *Recipient* parameter of the journal rule when modifying it from the Shell, journal reports are generated for all messages within the selected scope. If you decide to not specify a journal recipient, we recommend that you consider the increase in messaging traffic and the storage requirements for the mailbox database where the journaling mailbox is located.
- There are important security and resource considerations when you configure the journaling mailbox that receives journal reports. For more information, see Protecting Journal Reports.

What Do You Want to Do?

- Use the EMC to view or configure journal rule properties
- Use the Shell to configure journal rule properties
- Use the Shell to view journal rule properties

Use the EMC to view or configure journal rule properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, expand the appropriate forest and then navigate to **Organization Configuration > Hub Transport**.

2. In the result pane, click the **Journal Rules** tab and then select the journal rule you want to view or configure.

3. In the action pane, click **Properties**.

4. Use the **General** tab to view or configure the following journal rule properties.
   - **Rule name** This field shows the name of the journal rule. You can change the journal rule name. The length of the name can't exceed 64 characters.
   - **Status** This field displays rule status as enabled or disabled. You can't modify this field.
   - **Modified** This field displays the timestamp when the rule was last modified or the rule creation time if the rule has never been modified. You can't modify this field.
   - **Send Journal reports to e-mail address** This field shows the recipient that will receive the journal reports. To change the e-mail address that receives journal reports, click **Browse**. In the **Select Recipient** window, select the mailbox, contact, or distribution group to send journal reports to, and then click **OK**.
   - **Scope** This field specifies whether the journal rule is applied to internal recipients and senders only, to external recipients and senders only, or to both. Select one of the following:
     - **Global** Global rules apply to all messages that pass through a Hub Transport server.
     - **Internal** Internal rules apply to messages sent and received by recipients in the Exchange organization.
     - **External** External rules apply to messages sent or received by recipients outside the Exchange organization.
   - **Journal messages for recipient** This field specifies the mailbox, contact, or distribution group that you want to journal. To target a specific recipient or distribution group, select the **Journal messages for recipient** check box and then click **Browse**. In the **Select Recipient** window, select the mailbox, contact, or distribution group that you want to journal, and then click **OK**.

Use the Shell to configure journal rule properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

This example changes the name of the journal rule `JR-Sales` to `TraderVault`. The following rule settings are also changed:

- Recipient
- JournalEmailAddress
- Scope

```
Set-JournalRule -Identity TraderVault -Recipient traders@woodgrovebank.com -Journ
```

Use the Shell to view journal rule properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the 'Journaling' entry in the Messaging Policy and Compliance

Permissions topic.

This example retrieves the journal rule Brokerage Journal Rule, and pipes the output to the **Format-List** command to display rule properties in a list format:

```
Get-JournalRule "Brokerage Journal Rule" | Format-List
```

For more information about pipelining, see Pipelining.

This example displays a summary list of all journal rules in the Exchange 2010 organization:

```
Get-JournalRule
```

For more information about how to work with the information returned by a command, see Working with Command Output.

For detailed syntax and parameter information, see Get-JournalRule.

For More Information

Understanding Journaling

Managing Journaling

Set-JournalRule

1.11.5.6.5 Enable or Disable a Journal Rule

Enable or Disable a Journal Rule

Messaging Policy and Compliance > Journaling > Managing Journaling >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use journal rules to perform granular journaling of messages sent and received by specified recipients. When you enable or disable journal rules on a Hub Transport server, the modified journal rule is replicated across the Microsoft Exchange Server 2010 organization and is available to all the Exchange 2010 Hub Transport servers.

Looking for other tasks related to journaling? Check out Managing Journaling.

Use the EMC to enable or disable a journal rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **Journal Rules** tab and select the journal rule that you want to enable or disable.
3. In the action pane, if the journal rule isn't enabled, click **Enable Rule** to enable it. If the journal rule is enabled, click **Disable Rule** to disable it.

Use the Shell to enable or disable a journal rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the 'Journaling' entry in the Messaging Policy and Compliance Permissions topic.

This example enables the Contoso Journal Rule.

```
Enable-JournalRule "Contoso Journal Rule"
```

This example disables the Contoso Journal Rule.

```
Disable-JournalRule "Contoso Journal Rule"
```

Other Tasks

After you've enabled or disabled a journal rule, you may also want to:

- Create a Journal Rule
- Remove a Journal Rule
- Configure Journal Rule Properties

1.11.5.6.6 Remove a Journal Rule

Remove a Journal Rule

Messaging Policy and Compliance > Journaling > Managing Journaling >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Journal rules allow you to perform granular journaling of messages sent and received by specified recipients. You can remove a journal rule when it's no longer needed. You can also temporarily disable a journal rule without removing it.

Looking for other tasks related to journaling? Check out Managing Journaling.

Important:

If you remove a journal rule from a Hub Transport server, the journal rule will be removed from the entire Exchange 2010 organization.

Use the EMC to remove a journal rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Hub Transport**.
2. In the result pane, click the **Journal Rules** tab, and then select the journal rule that you want to remove.
3. In the action pane, click **Remove**.
4. Click **Yes** to confirm that you want to remove the journal rule.

Use the Shell to remove a journal rule

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

Use the *WhatIf* parameter to verify that the results of the operation are what you expect. For more information about the *WhatIf* parameter, see WhatIf, Confirm, and ValidateOnly Switches.

This example removes the journal rule Brokerage Journal Rule.

```
Remove-JournalRule "Brokerage Journal Rule"
```

For detailed syntax and parameter information, see Remove-JournalRule.

Other Tasks

After you remove a journal rule, you may also want to:

- Create a Journal Rule
- Configure Journal Rule Properties

1.11.5.6.7 Disable or Enable Journaling of Voice Mail and Missed Call Notifications

Disable or Enable Journaling of Voice Mail and Missed Call Notifications

Messaging Policy and Compliance > Journaling > Managing Journaling >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Microsoft Exchange Server 2010, when you create a journal rule to journal e-mail messages sent to or from recipients or senders in an Exchange organization, voice mail and missed call notifications generated by Unified Messaging (UM) servers are included. Use the procedures in this topic to modify this behavior for your entire organization to support your organization's compliance policies.

Caution:

Before disabling or enabling journaling of voice mail messages and missed called notifications, we recommend that you ensure that the action meets your organization's compliance requirements.

Important:

Using this procedure in an organization where journaling isn't enabled has no impact.

Looking for other management tasks related to journaling? Check out Managing Journaling.

What do you want to do?

Use the Shell to disable journaling of voice mail and missed call notifications

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You cannot use the EMC to disable journaling of voice mail and missed call notifications.

This example disables journaling of voice mail and missed call notifications by setting the *VoicemailJournalingEnabled* parameter to `$false`.

```
Set-TransportConfig -VoicemailJournalingEnabled $false
```

For detailed syntax and parameter information, see Set-TransportConfig.

Use the Shell to enable journaling of voice mail and missed call notifications

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You cannot use the EMC to enable journaling of voice mail and missed call notifications.

This example enables journaling of voice mail and missed call notifications by setting the *VoicemailJournalingEnabled* parameter to `$true`.

```
Set-TransportConfig -VoicemailJournalingEnabled $true
```

For detailed syntax and parameter information, see Set-TransportConfig.

For More Information

Understanding Journaling

1.11.5.6.8 Enable Per-Mailbox Database Journaling

Enable Per-Mailbox Database Journaling

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Per-mailbox database journaling (also known as standard journaling) delivers a copy of all messages sent to and received by mailboxes on the specified mailbox database to the specified journaling mailbox.

Important:
Journaling mailboxes contain very sensitive information. You must secure journaling mailboxes because they collect messages that are sent to and from recipients in your organization. These messages may be part of legal proceedings or may be subject to regulatory requirements. Various laws require that messages remain tamper-free before they're submitted to an investigatory authority. We recommend that you create policies that govern who can access the journaling mailboxes in your organization, limiting access to only those individuals who have a direct need to access them. Speak with your legal representatives to make sure that your journaling solution complies with all the laws and regulations that apply to your organization.

Looking for other tasks related to journaling? Check out Managing Journaling.

Prerequisites

A journaling mailbox has been created. For details, see Create and Configure a Journaling Mailbox.

Important:
There are important security and resource considerations when you configure the journaling mailbox that receives journal reports. For more information, see Understanding Journaling and Understanding Journal Reports.

Use the EMC to enable per-mailbox database journaling

Note:
Because a mailbox database may be part of a database availability group (DAG) and therefore reside on multiple Exchange 2010 servers, mailbox database properties are managed from the **Organization Configuration** node in the Exchange Management Console.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

1. Navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab, and then click the mailbox database on which you want to enable journaling.
3. In the action pane, under the mailbox database name, click **Properties**.
4. In **<Mailbox Database> Properties**, click the **Maintenance** tab.
5. Select the **Journal Recipient** check box, and then click **Browse**.
6. In **Select Recipient**, select the recipient that will receive the journal reports, and then click **OK**.

Use the Shell to enable per-mailbox database journaling

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

This example enables journaling for the mailbox database Sales Database and sets Sales Database Journal Mailbox as the journal recipient. The *JournalRecipient* parameter specifies the secured e-mail mailbox to which journal reports are sent.

```
Set-MailboxDatabase "Sales Database" -JournalRecipient "Sales Database Journal Ma
```

For detailed syntax and parameter information, see Set-MailboxDatabase.

Other Tasks

After you enable per-mailbox database journaling, you may also want to:

- Disable Per-Mailbox Database Journaling
- Create a Journal Rule

1.11.5.6.9 Disable Per-Mailbox Database Journaling

Disable Per-Mailbox Database Journaling

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Per-mailbox database journaling delivers a copy of all messages sent to and received by mailboxes on the specified mailbox database to the specified journaling mailbox. You can use the EMC or the Shell to disable per-mailbox database journaling for a mailbox database. However, to disable per-mailbox database journaling for all mailbox databases in your organization, you must use the Shell.

Looking for other management tasks related to journaling? Check out Managing Journaling.

Caution:

Disabling message journaling on a mailbox database may result in your organization being out of compliance with any applicable messaging retention policies. When you disable message journaling on a mailbox database, journal receipts are no longer sent for messages sent or received by mailboxes on that mailbox database.

Use the EMC to disable per-mailbox database journaling

Note Because a mailbox database may be part of a database availability group (DAG) and therefore reside on multiple Exchange 2010 servers, mailbox database properties are managed from the **Organization Configuration** node in the Exchange Management Console.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

1. Navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab, and then click the mailbox database for which you want to disable per-mailbox database journaling.
3. In the action pane, click **Properties**.
4. On the **Maintenance** tab, clear the **Journal Recipient** check box.

Use the Shell to disable per-mailbox database journaling

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

This example disables per-mailbox database journaling on the Sales Database mailbox database.

```
Set-MailboxDatabase "Sales Database" -JournalRecipient $Null
```

This example disables per-mailbox database journaling on all mailbox databases in the Exchange organization. The Get-MailboxDatabase cmdlet is used to retrieve all mailbox databases in the Exchange organization, and results from the cmdlet are piped to the Set-MailboxDatabase cmdlet.

```
Get-MailboxDatabase | Set-MailboxDatabase -JournalRecipient $Null
```

For detailed syntax and parameter information, see Set-MailboxDatabase.

1.11.5.6.10 Export and Import Exchange 2007 Journal Rules

Export and Import Exchange 2007 Journal Rules

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Journal rules allow you to granularly journal messages sent to and from specific recipients. Journal reports containing message metadata fields such as sender, recipients, message ID, and subject are delivered to the journaling mailbox specified in the rule, along with a copy of the original message as an attachment. To learn more about journaling, see Understanding Journaling.

Microsoft Exchange Server 2010 and Exchange Server 2007 use the same X-headers to specify that a message has already been journaled and also to identify journal reports. An Exchange 2010 Hub Transport server won't generate a duplicate journal report for a message that's already been journaled by another Exchange 2010 or Exchange 2007 Hub Transport server. Journaling considerations for organizations that contain Exchange Server 2003 and Exchange 2010 servers are covered in Understanding Journaling in a Mixed Exchange 2003 and Exchange 2010 Environment.

Although journaling in Exchange 2010 is similar to journaling in Exchange 2007, there are some differences in the journal rule object. When you install the first Exchange 2010 Hub Transport server in an Exchange 2007 environment, Setup creates a new container for Exchange 2010 journal rules, converts all Exchange 2007 journal rules to the Exchange 2010 format, and stores them in this new container in Active Directory. After Setup completes, the Exchange 2010 journal rule collection is identical to the Exchange 2007 journal rule collection. The same journal rules are applied to messages at the first Hub Transport server that handles the messages, regardless of whether it's running Exchange 2010 or Exchange 2007.

Managing Journal Rules in Coexistence

During the time your Exchange organization contains both Exchange 2010 and Exchange 2007 Hub Transport servers, you must manage Exchange 2010 journal rules from the EMC or the Shell on an Exchange 2010 server, and Exchange 2007 journal rules from the EMC or the Shell on an Exchange 2007 server.

To help you keep journal rules consistent in Exchange 2010 and Exchange 2007, when you create or modify journal rules by using the EMC or the Shell in Exchange 2010, these tools provide you helpful messages prompting you to make the same changes in the Exchange 2007 environment.

Prerequisites

Your organization contains both Exchange 2010 and Exchange 2007 Hub Transport servers.

Use the Shell to export the journal rule collection from Exchange 2007

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the EMC to export the journal rule collection from Exchange 2007.

This example exports the Exchange 2007 journal rule collection. In the first step, the **Export-JournalRuleCollection** cmdlet is used to export Exchange 2007 journal rules and store them in a variable. In the second step, the **Set-Content** cmdlet is used to save exported journal rules from the variable to the Ex2007-JournalRules.xml file in the C:\MyDocs folder. You must perform this procedure on an Exchange 2010 Hub Transport server because the Exchange 2010 **Export-JournalRuleCollection** cmdlet is aware of both journal rule formats, and it exports the Exchange 2007 journal rules when you use the *ExportLegacyRules* switch.

```
$file = Export-JournalRuleCollection -ExportLegacyRules
Set-Content -Path "C:\MyDocs\Ex2007-JournalRules.xml" -Value $file.FileData -Enco
```

For detailed syntax and parameter information, see the following topics:

- Export-JournalRuleCollection
- Set-Content

Use the Shell to import the journal rule collection to Exchange 2010

Caution:

When you import journal rules, all Exchange 2010 journal rules are replaced with the rules imported from the .xml file. We recommend that you test this procedure in a test environment before implementing it in a production environment. To make sure you can roll back to the previous state, we recommend that you export the existing Exchange 2010 journal rules to a file before importing the Exchange 2007 journal rules. If you plan to save the file in the same location where you've saved the exported Exchange 2007

journal rules, use distinct and descriptive file names for the journal rules exported from each version.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Journaling" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to import the journal rule collection to Exchange 2010.

This example imports the journal rule collection from the Ex2007-JournalRules.xml file to the Exchange 2010 journal rule collection. In the first step, the **Get-Content** cmdlet is used to retrieve data from the .xml file to the variable *$Data*. In the second step, the **Import-JournalRuleCollection** cmdlet is used to import the rules from the variable *$Data*.

```
[Byte[]]$Data = Get-Content -Path "C:\MyDocs\Ex2007-JournalRules.xml" -Encoding B
Import-JournalRuleCollection -FileData $Data
```

For detailed syntax and parameter information, see the following topics:

- Import-JournalRuleCollection
- Get-Content

Other Tasks

After you export or import the journal rule collection, you may also want to:

- Create a Journal Rule
- Remove a Journal Rule

1.11.6 Messaging Records Management

Messaging Records Management

Exchange Server 2010 > Messaging Policy and Compliance >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

Understanding Messaging Records Management

Learn more about Messaging Records Management (MRM).

Understanding Retention Tags and Retention Policies

Learn more about retention policies, the new MRM feature in Exchange 2010.

Understanding Managed Folders

Learn more about managed folders, the MRM feature introduced in Exchange 2007 and also available in Exchange 2010.

Planning for Messaging Records Management

Learn more about the factors you should consider when planning to deploy MRM in your organization.

How Retention Age is Calculated

Learn how the retention age is calculated for different types of mailbox items, such as

e-mail messages, calendar items, and tasks.

Deploying Messaging Records Management

Learn how to deploy MRM in your Exchange 2010 organization.

Monitoring Messaging Records Management

Learn about the tools available to monitor MRM, including MRM-related performance counters.

Messaging Records Management Terminology in Exchange 2010

Learn more about the terminology used for MRM in Exchange 2010.

1.11.6.1 Understanding Messaging Records Management

Understanding Messaging Records Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-22*

Organizations and users handle an increasing volume of e-mail every day. The growing volumes of e-mail contain messages that are important to the organization from a business, legal, or regulatory perspective, and may need to be retained for a certain period, depending on the organization's messaging policies. However, many e-mail messages may not have any retention value beyond a certain period, if at all. For example, a user's mailbox may contain critical messages that need to be retained, such as messages related to business strategy, transactions, product development, or customer interactions. However, messages such as newsletter subscriptions or personal e-mail may not have any retention value, and therefore don't need to be retained beyond a certain period. Retaining messages with little retention value results in mailbox growth that requires more resources on mailbox servers.

Messaging records management (MRM) is the records management technology in Microsoft Exchange Server 2010 that helps organizations reduce the legal risks associated with e-mail. MRM makes it easier to keep the messages needed to comply with company policy, government regulations, or legal needs, and to remove content that has no legal or business value. This is accomplished through the use of retention policies or managed folders:

- **Retention policies** Retention policies, the new MRM technology in Exchange 2010, use retention tags to apply retention settings. You create retention tags, and link them to a retention policy. Mailboxes that have a retention policy applied to them are processed by the Managed Folder Assistant, a mailbox assistant that runs on a schedule and provisions retention tags in mailboxes. To learn more about retention policies, see Understanding Retention Tags and Retention Policies.
- **Managed folders** Managed folders, the MRM technology introduced in Exchange Server 2007 and also available in Exchange 2010, have managed content settings applied to them. You create managed folders and link them to a managed folder mailbox policy. Mailboxes that have managed folder mailbox policies applied are processed by the Managed Folder Assistant, a mailbox assistant that runs on a schedule and provisions managed folders in mailboxes. To learn more about managed folders, see Understanding Managed Folders.

When a message reaches its retention age, the retention action specified in the retention tag (or the managed content settings for a managed folder) is taken. Messages can be

moved to the Deleted Items folder, deleted with the ability to recover them from the Recoverable Items folder, or permanently deleted. Retention tags also provide an additional action of moving a message to the user's archive mailbox, if an archive mailbox has been provisioned for the user. Managed content settings for managed folders also provide an additional action of moving a message to a managed custom folder.

Messaging Records Management Strategy

Retention policies and managed folders provide two different approaches to MRM. You can use either MRM technology to enforce basic MRM policies on default folders and on the entire mailbox. For MRM to be effective, users must participate in the process of classifying messages based on their nature and retention value.

With retention tags, you can apply default retention settings to default folders such as the Inbox folder, and apply a default policy tag (DPT) to the entire mailbox. The DPT retention settings are applied to untagged items that may reside in folders without a retention tag, such as custom folders created by the user. Retention tags help both types of users: Users who file e-mail into folders and keep few messages in the Inbox, and users who leave most of their e-mail in the Inbox. Retention tags have a lesser impact on the user's workflow because users aren't required to file messages in folders based on the folder's retention settings. They can apply any personal tag to custom folders, and also explicitly apply a different tag to individual messages.

With managed folders, users participate in the MRM process by classifying their own messages and sorting them into managed folders. This sorting process ensures that messages are classified according to the users' preferences and the organization's needs. It also helps eliminate the mishandling of messages that can occur with a completely automated messaging management solution.

The strategy to make Exchange 2010 messaging retention management and policy enforcement more reliable, effective, and easy to use is based on three principles:

- Users classify their own messages.
- Messages that have no retention value are removed.
- Messages that have some retention value are retained.

Users Classify Their Own Messages

With Exchange 2010, users participate in the MRM process by classifying their own messages. Users with a retention policy applied can either move a message to a folder that has a retention tag applied or can apply a personal tag to the message. If the user doesn't take any action, one of the following retention settings is applied:

- **Messages in default folders with a retention policy tag applied** If the message is located in a default folder that has a retention policy tag applied, the folder's retention settings are applied to the message.
- **Messages in custom folders with a personal tag applied** If the message is located in a custom folder to which the user has applied a personal tag, the folder's retention settings are applied to the message.
- **Messages in default or custom folders without a retention tag** If the message is located in a default or custom folder that doesn't have a retention tag applied to it, the DPT is applied to the message.

Regardless of the location of the message, any time a user explicitly applies a tag to a message, the user's action is honored.

Messages That Have No Retention Value Are Removed

Retention policies and managed folder mailbox policies are applied to the user's mailbox by the Managed Folder Assistant. This assistant processes mailboxes that have a retention policy or a managed folder mailbox policy applied. For mailboxes that have a retention policy applied, the Managed Folder Assistant applies the retention tags included

in the policy to default folders and the entire mailbox. Any personal tags included in the policy are provisioned and become available to users in Microsoft Outlook 2010 and Microsoft Office Outlook Web App.

Messages That Have Some Retention Value Are Retained

Messages that have some retention value are retained based on the retention settings applied to the message, folder, or mailbox. However, keep in mind that users can delete or remove messages from their mailbox; MRM isn't designed to prevent users from deleting their own messages. If your organization requires messages to be retained outside a user's mailbox for long-term storage, consider implementing journaling. To learn more about journaling, see Understanding Journaling.

If your organization wants to preserve messages for users to meet e-discovery and retention requirements, consider deploying large mailboxes and placing those users on legal hold. To learn more about legal hold, see Understanding Litigation Hold.

1.11.6.2 Understanding Retention Tags and Retention Policies

Understanding Retention Tags and Retention Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-12-11*

Messaging records management (MRM) is the records management technology in Microsoft Exchange Server 2010 that helps organizations reduce legal risks associated with e-mail and other communications. MRM makes it easier to keep messages needed to comply with company policy, government regulations, or legal needs, and to remove content that has no legal or business value.

Organizations formulate MRM policies that specify the retention period for different classes of e-mail messages. However, in the past, enforcing those policies has often been challenging. Attempts to automate the MRM process have met with limited success. The MRM functionality in Exchange 2010 addresses these challenges.

Looking for management tasks related to MRM? See Deploying Messaging Records Management.

Contents

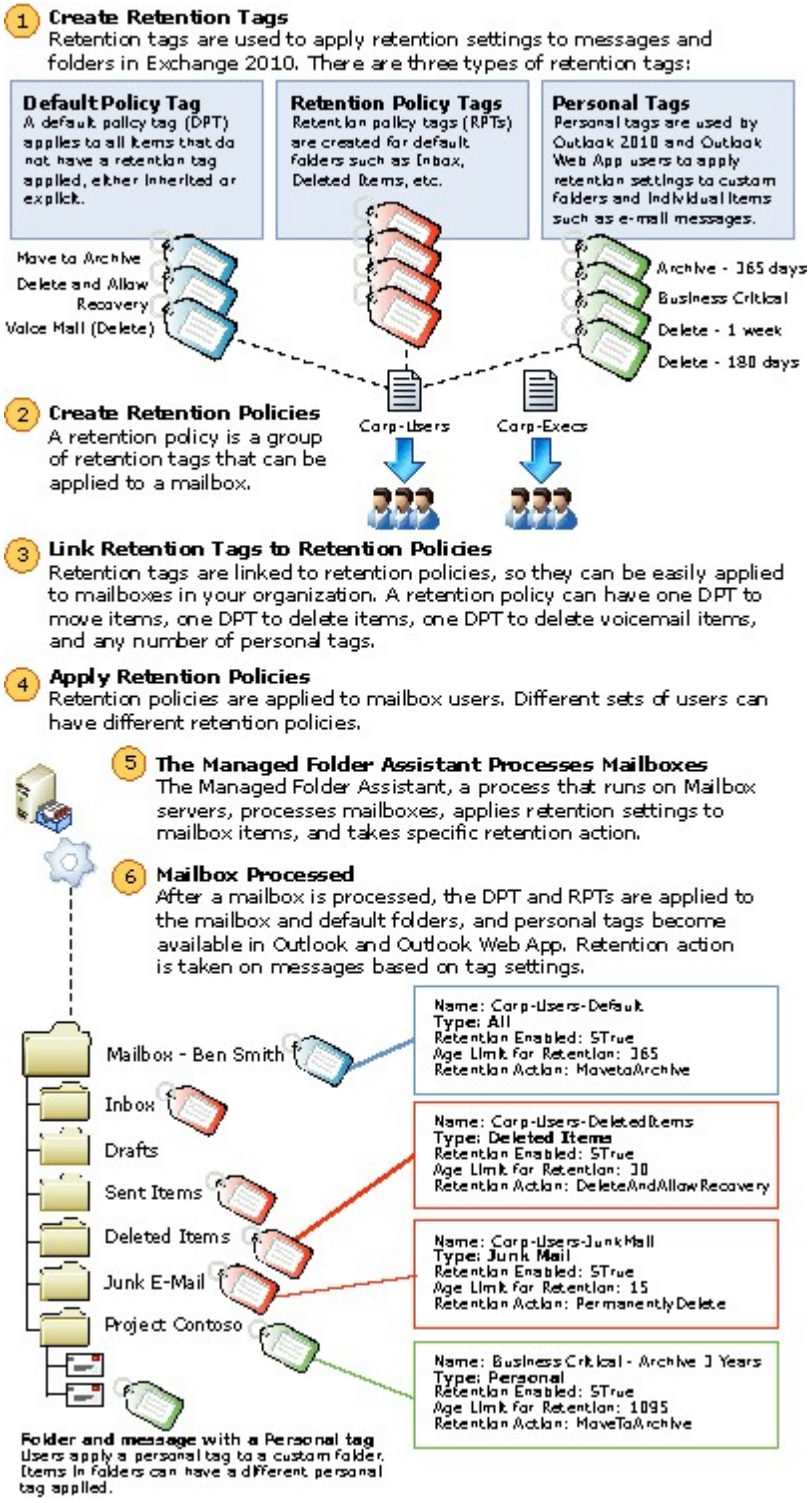
Messaging Records Management Strategy

MRM in Exchange 2010 is accomplished by using *retention tags* and *retention policies*.

Before discussing the details about each of these retention features, it's important to learn how the features are used in the overall Exchange 2010 MRM strategy. This strategy is based on:

- Assigning *retention policy tags* (RPTs) to default folders, such as the Inbox.
- Applying *default policy tags* (DPTs) to mailboxes to manage the retention of all untagged items.
- Allowing the user to assign *personal tags* to custom folders and individual items.
- Separating MRM functionality from users' Inbox management and filing habits. Users aren't required to file messages in managed folders based on retention requirements. Individual messages can have a different retention tag than the one applied to the folder in which they're located.

The following figure illustrates the tasks involved in implementing this strategy.



Return to top

Requirements

The following table shows requirements for the Mailbox server and client application.

Retention tag and retention policy requirements

Location	Requirement
Mailbox server	Exchange 2010 is required.
Client application (to view retention tags and apply personal tags)	Only Microsoft Outlook 2010 and Microsoft Office Outlook Web App users apply personal tags and view the retention tags applied to their mailbox folders or items. **Note:** Because retention policies are processed on Mailbox servers, they're independent of the Outlook version used by the users in your organization. You can still apply retention policies to user mailboxes running Microsoft Office Outlook 2007 and earlier. In these cases, RPTs in the policy apply to the default folders in their mailbox, and the DPT applies to untagged mailbox items.

Return to top

Retention Tags

As illustrated in the preceding figure, retention tags are used to apply retention settings to folders and individual items such as e-mail messages and voice mail. These settings specify how long a message remains in a mailbox and the action to be taken when the message reaches the specified retention age. When a message reaches its retention age, it's moved to the personal archive or deleted.

Unlike managed folders (the MRM feature introduced in Exchange Server 2007), retention tags allow users to tag their own mailbox folders and individual items for retention. Users no longer have to file items in managed folders provisioned by an administrator based on message retention requirements.

Note:

Managed folders are still available in Exchange 2010. To learn more, see Understanding Managed Folders.

Types of Retention Tags

There are three types of retention tags:

- **Default policy tags** DPTs apply to untagged mailbox items in the entire mailbox. Untagged items are mailbox items that don't already have a retention tag applied, either by inheritance from the folder in which they're located or by the user.
- **Retention policy tags** RPTs apply retention settings to default folders such as the Inbox, Deleted Items, and Sent Items. Mailbox items in a default folder that have an RPT applied inherit the folder's tag. Users can't apply or change an RPT applied to a default folder, but they can apply a different tag to the items in a default folder.
  You can create RPTs for the folders shown in the following table.

Folders in which you can create RPTs

Folder name	Details
Calendar	This default folder is used to store meetings and appointments. **Important:**

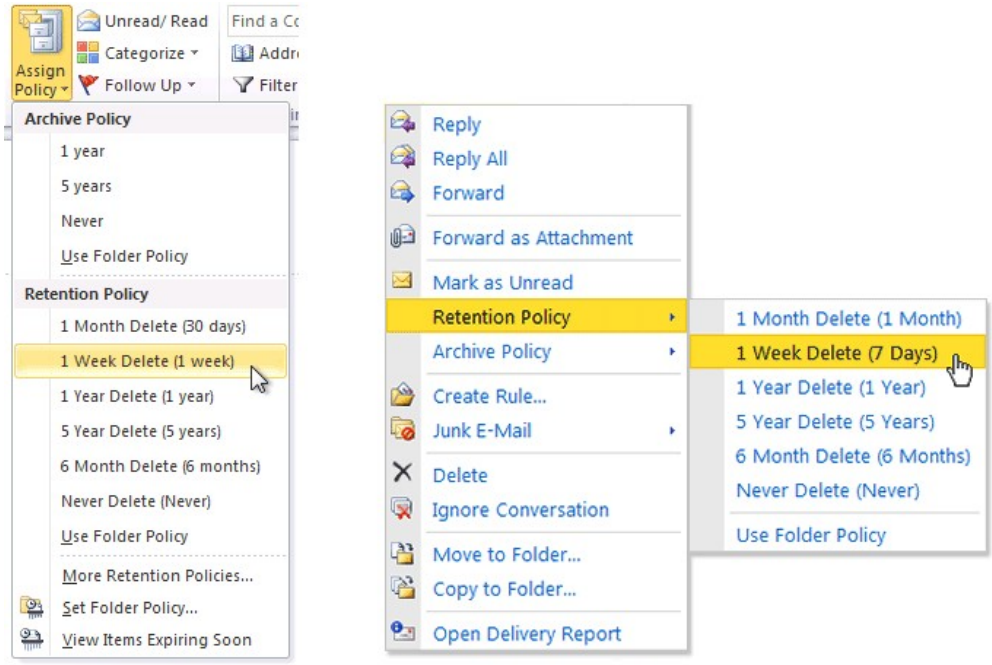
	RPTs for the Calendar and Tasks default folders are supported in Microsoft Exchange Server 2010 SP2 RU4. For details, see the Exchange Server Team Blog article Calendar and Tasks Retention Tag Support in Exchange 2010 SP2 RU4.
Conversation History	This folder is created by Microsoft Lync (previously Microsoft Office Communicator). Although it's not treated as a default folder by Outlook, it's treated as a special folder by Exchange and can have RPTs applied.
Deleted Items	This default folder is used to store items deleted from other folders in the mailbox. Outlook and Outlook Web App users can manually empty this folder. Users can also configure Outlook to empty the folder upon closing Outlook.
Drafts	This default folder is used to store draft messages that haven't been sent by the user. Outlook Web App also uses this folder to save messages that were sent by the user but not submitted to the Hub Transport server.
Inbox	This default folder is used to store messages delivered to a mailbox.
Journal	This default folder contains actions selected by the user. These actions are automatically recorded by Outlook and placed in a timeline view.
Junk E-mail	This default folder is used to save messages marked as junk e-mail by the content filter on an Exchange server or by the anti-spam filter in Outlook.
Notes	This folder contains notes created by users in Outlook. These notes are also visible in Outlook Web App. RPTs for the Notes folder are supported only in Exchange 2010 SP1.
Outbox	This default folder is used to temporarily store messages sent by the user until they're submitted to a Hub Transport server. A copy of sent messages is saved in the Sent Items default folder. Because messages usually remain in this folder for a brief period, it isn't necessary to create an RPT for this folder.
RSS Feeds	This default folder contains RSS feeds.
Recoverable Items	This is a hidden folder in the Non-IPM sub-tree. It contains the Deletions, Versions, Purges, and Audits sub-folders. Retention tags for this folder

	move items from the Recoverable Items folder in the user's primary mailbox to the Recoverable Items folder in the user's archive mailbox. You can assign only the **Move To Archive** retention action to tags for this folder. To learn more, see Understanding Recoverable Items.
Sent Items	This default folder is used to store messages that have been submitted to a Hub Transport server.
Sync Issues	This folder contains synchronization logs. To learn more, see Synchronization error folders.
Tasks	This default folder contains task items. Messages that are flagged by a user also appear in the To-Do List view. However, these messages are not task items, and do not reside in the Tasks folder. **Important:** RPTs for the Calendar and Tasks default folders are supported in Exchange Server 2010 SP2 RU4. For details, see the Exchange Server Team Blog article Calendar and Tasks Retention Tag Support in Exchange 2010 SP2 RU4.

Important:

You can't include more than one RPT for the same default folder type in one retention policy. For example, if a retention policy has an Inbox tag, you can't add another RPT of type Inbox to that retention policy.
You can't apply RPTs to the Contacts folder.

- **Personal tags** Personal tags are available to Outlook 2010 and Outlook Web App users as part of their retention policy. Users can apply personal tags to folders they create or to individual items, even if those items already have a different tag applied. In Outlook 2010 and Outlook Web App, personal tags with the **Move to Archive** action appear as **Archive Policy**, and personal tags with the **Delete and Allow Recovery** or **Permanently Delete** actions appear as **Retention Policy**, as shown in the following figure.



Outlook 2010 Outlook Web App

Messages that have a personal tag applied are always processed based on the personal tag's settings. Depending on the personal tags you create, users can apply a personal tag to a message so that it's moved or deleted sooner or later than the settings specified in the DPT or RPTs applied to that user's mailbox. You can also create personal tags with retention disabled. This allows users to tag items so they're never moved to an archive or never expire.

Note:

Users can apply archive policies to default folders, user-created folders or subfolders, and individual items. Users can apply a retention policy to user-created folders or subfolders and individual items (including subfolders and items in a default folder), but not to default folders.

In Exchange 2010 SP1, users can use the Exchange Control Panel (ECP) to select additional personal tags that aren't linked to their retention policy. The selected tags then become available in Outlook 2010 and Outlook Web App. To enable users to select additional tags from the ECP, you must add the MyRetentionPolicies Role to the user's role assignment policy. To learn more about role assignment policies for users, see Understanding Management Role Assignment Policies. If you allow users to select additional personal tags, all personal tags in your Exchange organization become available to them.

Note:

Personal tags are a premium feature. Mailboxes with policies that contain these tags (or as a result of users adding the tags to their mailbox) require an Exchange Enterprise client access license (CAL).

Retention Age Limit and Retention Actions

When you enable a retention tag, you must specify a retention age for the tag. This age indicates the number of days to retain a message after it arrives in the user's mailbox.

The retention age for non-recurring items (such as e-mail messages) is calculated differently than items that have an end date or recurring items (such as meetings and tasks). To learn how the retention age is calculated for different types of items, see How Retention Age is Calculated.

You can also create retention tags with retention disabled or disable tags after they're created. Because messages that have a disabled tag applied aren't processed by the Managed Folder Assistant, no retention action is taken. As a result, users can use a disabled personal tag as a **Never Move** tag or a **Never Delete** tag to override a DPT or RPT that would otherwise apply to the message.

When creating or configuring an RPT, you can select from one of the following actions to specify what retention action should be taken when a mailbox item reaches its retention age:

- **Move to Archive** This action moves a message to the user's archive mailbox. Tags that have this action applied are known as *archive tags*. Messages are moved to a folder in the archive mailbox that has the same name as the source folder in the user's primary mailbox. This allows users to easily locate messages in their archive mailbox. The **Move to Archive** action is available only for DPTs and personal tags. You can't create an RPT with the **Move to Archive** action. If the mailbox user doesn't have an archive mailbox, no action is taken. To learn more about archive mailboxes, see Understanding Personal Archives.
- **Delete and Allow Recovery** This action emulates the behavior when the Deleted Items folder is emptied. Tags that have this action applied are known as *deletion tags*. When this action occurs, and deleted item retention is configured for the mailbox database or the user, messages move to the Recoverable Items folder. The Recoverable Items folder (previously known as the dumpster) provides the user another chance to recover deleted messages. To do so, the user would access the **Recover Deleted Items** dialog box in Outlook 2010 or Outlook Web App. To learn more about recoverable items, see Understanding Recoverable Items.
- **Permanently Delete** This action permanently deletes a message. Like tags with the **Delete and Allow Recovery** action, tags that have this action applied are known as deletion tags. When this action is applied to a message, it's purged from the mailbox. This action is like a deleted message being removed from the Recoverable Items folder. After this happens, the user can no longer recover the message.
- **Mark as Past Retention Limit** This action isn't available in the Exchange Management Console (EMC); you must use the Shell. This action marks a message as expired after it reaches its retention age. In Outlook 2010 and Outlook Web App, expired items are displayed with the notification stating 'This item has expired' and 'This item will expire in 0 days'. In Outlook 2007, items marked as expired are displayed by using strikethrough text.

Important:

If litigation hold is enabled for a mailbox user, permanently deleted items are retained in the Recoverable Items folder until litigation hold is removed. Multi-Mailbox Search will still return permanently deleted messages in search results. To learn more, see Understanding Litigation Hold and Understanding Multi-Mailbox Search.

If single item recovery is enabled for the mailbox, permanently deleted items are retained in the Recoverable Items folder until the deleted item retention period for the mailbox database (or the deleted item retention period for the mailbox, if specified) is reached. To learn more, see Understanding Recoverable Items.

In Exchange 2010 SP1, the **Move to the Deleted Items Folder** and the **Move to a Managed Custom Folder** actions have been removed from retention tags.

For details about how to create retention tags, see Create a Retention Tag.

Return to top

Retention Policies

You can use retention policies to group one or more retention tags and apply them to mailboxes. A mailbox can't have more than one retention policy. Retention tags can be linked to or unlinked from a retention policy at any time, and the changes automatically take effect for all mailboxes that have the policy applied.

A retention policy can have the following retention tags:

- One or more RPTs for supported default folders

  Note:
  You can't link more than one RPT for a particular default folder (such as Deleted Items) to the same retention policy.

- One DPT with the **Move to Archive** action
- One DPT with the **Delete and Allow Recovery** or **Permanently Delete** actions
- One DPT for voice mail messages in Exchange 2010 SP1
- Any number of personal tags

Although you can add any number of personal tags to a retention policy, having many personal tags with different retention settings can confuse users. We recommend linking no more than 10 personal tags to a retention policy.

Note:
Although a retention policy doesn't need to have any retention tags linked to it, we don't recommend using this scenario. If mailboxes with retention policies don't have retention tags linked to them, this may cause mailbox items to never expire.

A retention policy can contain both archive tags (tags that move items to the personal archive mailbox) and deletion tags (tags that delete items). A mailbox item can also have both types of tags applied. Archive mailboxes don't have a separate retention policy. The same retention policy is applied to the primary and archive mailbox.

When planning to create retention policies, you must consider whether they'll include both archive and deletion tags. As mentioned earlier, a retention policy can have one DPT that uses the **Move to Archive** action and one DPT that uses either the **Delete and Allow Recovery** or **Permanently Delete** action. The DPT with the **Move to Archive** action must have a lower retention age than the DPT with a deletion action. For example, you can use a DPT with the **Move to Archive** action to move items to the archive mailbox in two years, and a DPT with a deletion action to remove items from the mailbox in seven years.

For details about how to create a retention policy, see Create a Retention Policy.

For details about how to add retention tags to a retention policy, see Add or Remove Retention Tags from a Retention Policy.

For details about how to apply a retention policy to mailboxes, see Apply a Retention Policy to Mailboxes.

Default Archive and Retention Policy

In Exchange 2010 SP1, Exchange Setup creates the retention policy Default Archive and Retention Policy. When you enable a personal archive for a mailbox, the Default Archive and Retention Policy is automatically applied to the mailbox if it doesn't already have a retention policy. If you later apply a retention policy to the mailbox, tags from the Default Archive and Retention Policy are no longer available to the mailbox. Existing items that have tags from the Default Archive and Retention Policy applied are still processed and moved to the archive or deleted based on the tag.

The following table lists the default retention tags linked to the Default Archive and Retention Policy.

Retention tags linked to the Default Archive and Retention Policy in Exchange 2010 SP1

Name	Type	Retention age (days)	Retention action
Default 2 years move to archive	DPT	730	Move to Archive
Personal 1 year move to archive	Personal tag	365	Move to Archive
Personal 5 year move to archive	Personal tag	1,825	Move to Archive
Personal never move to archive	Personal tag	Not applicable	Move to Archive
Recoverable Items 14 days move to archive	Recoverable Items folder	14	Move to Archive
1 Week Delete	Personal tag	7	Delete and Allow Recovery
1 Month Delete	Personal tag	30	Delete and Allow Recovery
6 Month Delete	Personal tag	180	Delete and Allow Recovery
1 Year Delete	Personal tag	365	Delete and Allow Recovery
5 Year Delete	Personal tag	1,825	Delete and Allow Recovery
Never Delete	Personal tag	Not applicable	Delete and Allow Recovery

In the release to manufacturing (RTM) version of Exchange 2010, Exchange Setup creates the retention policy called **Default Archive Policy**. This policy doesn't contain personal tags with the **Delete and Allow Recovery** action.

Return to top

Managed Folder Assistant

The Managed Folder Assistant, a mailbox assistant that runs on Mailbox servers, processes mailboxes that have a retention policy applied.

The Managed Folder Assistant applies the retention policy by inspecting items in the mailbox and determining whether they're subject to retention. It then stamps items subject to retention with the appropriate retention tags and takes the specified retention action on items past their retention age.

In Exchange 2010 SP1, the Managed Folder Assistant is a throttle-based assistant. Throttle-based assistants are always running and don't need to be scheduled. The system resources they can consume are throttled. You can configure the Managed Folder Assistant to process all mailboxes on a Mailbox server within a certain period (known as a *work cycle*). Additionally, at a specified interval (known as the *work cycle checkpoint*), the assistant refreshes the list of mailboxes to be processed. During the refresh, the

assistant adds newly created or moved mailboxes to the queue. It also reprioritizes existing mailboxes that haven't been processed successfully due to failures and moves them higher in the queue so they can be processed during the same work cycle.

You can also use the Start-ManagedFolderAssistant cmdlet to manually trigger the assistant to process a specified mailbox. For more details, see Configure the Managed Folder Assistant.

In Exchange 2010 RTM, the Managed Folder Assistant runs on a specified schedule. By default, it's scheduled to run daily from 01:00 through 09:00 (1:00 A.M. through 9:00 A.M.). You can schedule the assistant to run at a time when the Mailbox server is relatively idle or not under a heavy load. When determining a schedule for the assistant, consider other processes that compete for Mailbox server resources, such as offline defragmentation of the mailbox database and antivirus scans.

Note:

The Managed Folder Assistant doesn't take any action on messages that aren't subject to retention, specified by disabling the retention tag. You can also disable a retention tag to temporarily suspend items with that tag from being processed.

Moving Items Between Folders

A mailbox item moved from one folder to another inherits any tags applied to the folder to which it's moved. If an item is moved to a folder that doesn't have a tag assigned, the DPT is applied to it. If the item has a tag explicitly assigned to it, the tag always takes precedence over any folder-level tags or the default tag.

Removing or Deleting a Retention Tag from a Retention Policy

When a retention tag is removed from the retention policy applied to a mailbox, the tag is no longer available to the user and can't be applied to items in the mailbox.

Existing items that have been stamped with that tag continue to be processed by the Managed Folder Assistant based on those settings and any retention action specified in the tag is applied to those messages.

However, if you delete the tag, the tag definition stored in Active Directory is removed. This causes the Managed Folder Assistant to process all items in a mailbox and restamp the ones that have the removed tag applied. Depending on the number of mailboxes and messages, this process may significantly consume resources on all Mailbox servers that contain mailboxes with retention policies that include the removed tag.

Important:

If a retention tag is removed from a retention policy, any existing mailbox items with the tag applied will continue to expire based on the tag's settings. To prevent the tag's settings from being applied to any items, you should delete the tag. Deleting a tag removes it from any retention policies in which it's included.

Disabling a Retention Tag

If you disable a retention tag, the Managed Folder Assistant ignores items that have that tag applied. Items that have a retention tag for which retention is disabled are either never moved or never deleted, depending on the specified retention action. Because these items are still considered tagged items, the DPT doesn't apply to them. For example, if you want to troubleshoot retention tag settings, you can temporarily disable a retention tag to stop the Managed Folder Assistant from processing messages with that tag.

Note:

The retention period for a disabled retention tag is displayed to the user as **Never**. If a user tags an item believing it will never be deleted, enabling the tag later may result in unintentional deletion of items the user didn't want to delete. The same is true for tags with the **Move to Archive** action.

Return to top

Retention Hold

When users are temporarily away from work and don't have access to their e-mail, retention settings can be applied to new messages before they return to work or access their e-mail. Depending on the retention policy, messages may be deleted or moved to the user's personal archive. You can temporarily suspend retention policies from processing a mailbox for a specified period by placing the mailbox on retention hold. When you place a mailbox on retention hold, you can also specify a retention comment that informs the mailbox user (or another user authorized to access the mailbox) about the retention hold, including when the hold is scheduled to begin and end. Retention comments are displayed in supported Outlook clients. You can also localize the retention hold comment in the user's preferred language.

Note:

Placing a mailbox on retention hold doesn't affect how mailbox storage quotas are processed. Depending on the mailbox usage and applicable mailbox quotas, consider temporarily increasing the mailbox storage quota for users when they're on vacation or don't have access to e-mail for an extended period. For more information about mailbox storage quotas, see Configure Storage Quotas for a Mailbox.

During long absences from work, users may accrue a large amount of e-mail. Depending on the volume of e-mail and the length of absence, it may take these users several weeks to sort through their messages. In these cases, consider the additional time it may take the users to catch up on their mail before removing them from retention hold.

If your organization has never implemented MRM, and your users aren't familiar with its features, you can also use retention holds during the initial *warm-up and training* phase of your MRM deployment. You can create and deploy retention policies and educate users about the policies without the risk of having items moved or deleted before users can tag them. A few days before the warm-up and training period ends, you should remind users of the warm-up deadline. After the deadline, you can remove the retention hold from user mailboxes, allowing the Managed Folder Assistant to process mailbox items and take the specified retention action.

For details about how to place a mailbox on retention hold, see Place a Mailbox on Retention Hold.

Return to top

1.11.6.3 Understanding Managed Folders

Understanding Managed Folders

Exchange Server 2010 > Messaging Policy and Compliance > Messaging Records Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-14*

Managed folders are a messaging records management (MRM) feature introduced in Microsoft Exchange Server 2007 that's also available in Exchange Server 2010. Using managed folders, you can specify retention settings for default folders such as Inbox, Deleted Items, and Sent Items, and create custom managed folders with their own retention settings. Managed folders rely on users to classify messages for retention, and

move the messages to appropriate managed folders based on retention requirements.

Contents

Managed Folders

Managed folders are an Active Directory representation of folders in a mailbox. You can define two types of managed folders:

- **Managed default folders** Managed default folders are managed folder objects created for default folders such as Inbox, Deleted Items, Sent Items, and others. Exchange 2010 Setup creates a set of managed default folders. You can use these folders or create additional ones for different sets of users.
- **Managed custom folders** Managed custom folders are managed folder objects you can use to create custom folders in a user's mailbox. The folders are created under a top-level folder called Managed Folders.

Note:

Managed custom folders are a premium feature of MRM. Each mailbox that has managed custom folders requires an Exchange Server Enterprise client access license (CAL).

Return to top

Managed Content Settings

Managed content settings specify the retention and journaling settings for a managed folder. The settings can be for a specific message class (such as e-mail messages, calendar items, and tasks), or they can be for all message classes. You can specify multiple managed content settings for different message classes, allowing you to specify different retention settings for different types of items in the same folder.

These retention settings include a message class (whether retention is enabled for the specified message class), the retention age, and a retention action. The retention age specifies the period for which a message is retained in the mailbox. The retention action specifies the action to take after the item is past its retention age. For example, you can create a managed content setting for a managed default folder that moves all items to the Deleted Items folder after 120 days.

You can select from one of the following retention actions:

- **Move to the Deleted Items Folder** Use this action to move items to the Deleted Items folder upon expiration.
- **Move to a Managed Custom Folder** Use this action to move items to a managed custom folder. To use this action, you must first create the managed custom folder.
- **Delete and Allow Recovery** Use this action to move items to the Recoverable Items folder. Deleted items are available for recovery from the Recoverable Items folder until the deleted item retention time specified for the mailbox database or the user mailbox elapses.

- **Permanently Delete** Use this action to permanently delete items. Users can't recover items that have been permanently.
- **Mark as Past Retention Limit** Use this action to mark items as expired after they reach their retention age. Items marked as expired are displayed by using strikethrough text in Microsoft Outlook 2010 and Office Outlook 2007.

You can also specify whether the retention age is calculated from when a message is delivered to a mailbox or when it's moved to the folder it currently resides in. For calendar items and recurring tasks, the retention age is calculated from the end date of the item. For details about how the retention age is calculated, see How Retention Age is Calculated. For details about creating managed content settings for a managed folder, see Create Managed Content Settings.

Return to top

Journaling and Managed Folders

You can use managed folders to journal (automatically forward) copies of specific items to another location. Content can be journaled to any location that has an SMTP e-mail address, including another Exchange mailbox or a mail contact. You can assign a text label to messages to help preserve classification information and to enable automated sorting of journaled messages by the recipient. When an item is journaled, it's attached as an unaltered copy to a new e-mail message. Some properties of the item being journaled are assigned as properties of the new e-mail message, which facilitates review and automated sorting.

Important:

Journal reports generated by the Managed Folder Assistant on mailbox servers are different from journal reports generated by the Journaling agent on Hub Transport servers when you use standard (per-mailbox database) or premium journaling. To learn more about journaling, see Understanding Journaling.

Managed Folder Mailbox Polices

A managed folder mailbox policy is a logical grouping of managed folders that can be applied to mailboxes, allowing you to apply managed content settings for multiple managed folders to a user. A policy can contain a mix of managed default folders and managed custom folders. However, you can't add two managed default folders of the same type (such as the Inbox) to the same policy. Managed folders can be added or removed from a managed folder mailbox policy at any time. A mailbox user can have only one managed folder mailbox policy applied.

For details about how to create or apply a managed folder mailbox policy, see Create a Managed Folder Mailbox Policy and Apply a Managed Folder Mailbox Policy to Users.

Return to top

Managed Folder Assistant

The Managed Folder Assistant is a process that runs on Mailbox servers and applies managed folder mailbox policies to mailboxes located on that server. The assistant retrieves the list of managed folders associated with a policy, provisions managed folders in mailboxes, and processes items in those folders. Items for which retention is enabled are stamped with the retention age. The retention action specified in applicable managed content settings is taken on items that have reached their retention age.

In Exchange 2010 SP1, the Managed Folder Assistant is a throttle-based assistant. Throttle-based assistants don't run on a schedule. Instead, they're configured to process

all mailboxes on a Mailbox server within a certain period of time (known as a *work cycle*). Additionally, at a specified interval known as the *work cycle checkpoint*, the Managed Folder Assistant refreshes the list of mailboxes to be processed. During the refresh, the assistant adds newly created or moved mailboxes to the queue. It also reprioritizes existing mailboxes that haven't been processed successfully for awhile due to failures and moves them higher in the queue so they can be processed during the same work cycle.

In Exchange 2010, the Managed Folder Assistant is a schedule-based assistant that's scheduled to run from 01:00 through 09:00 (1:00 A.M. through 9:00 A.M.) every day. You can modify the assistant's schedule to make sure there's minimal user impact. You can also start and stop the assistant manually by using the Exchange Management Shell. To learn more about scheduling the assistant, see Configure the Managed Folder Assistant.

Note:
In Exchange 2010, the Managed Folder Assistant also applies retention policies for MRM. You can apply either a retention policy or a managed folder mailbox policy to a mailbox. If you modify the Managed Folder Assistant schedule, it impacts both MRM features.

Return to top

1.11.6.4 Planning for Messaging Records Management

Planning for Messaging Records Management

Exchange Server 2010 > Messaging Policy and Compliance > Messaging Records Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-06-02*

Although configuring and managing messaging records management (MRM) features in Microsoft Exchange Server 2010 is technically straightforward, planning for a successful MRM implementation can require time, thought, and input from a variety of business disciplines. In addition to Exchange administrators and the IT department, executives, records managers, human resources personnel, legal advisors, and even end users can play important roles in the planning process.

Where Do I Start?

Before implementing an MRM solution, there are many factors to consider, and not all of them are technical. The following sections describe some of these factors.

Sandbox

To learn about installing, configuring, and maintaining MRM, we recommend that you first set up a test environment (also known as a *sandbox* installation). Exchange administrators who are well versed in the details of setting up and configuring MRM in a test environment are in a better position to consult with and make recommendations to other members of the organization about the technical requirements for a successful MRM solution. You can set up a virtualized sandbox environment by using the Windows Server 2008 operating system and Hyper-V. For more information, see Virtualization with Hyper-V: Overview.

You can also use this virtualized environment to test other messaging policy and compliance features such as personal archive, Multi-Mailbox Search, journaling, and Information Rights Management (IRM).

Policies and Plans

The MRM features in Exchange 2010 help your organization implement its records retention and management policies. An effective MRM implementation begins with a records management policy. As you plan to implement an MRM solution, we recommend that you set up a team for the purposes of creating or updating the records management policy of your organization. Among the groups to consider including in the policy creation or review process are:

- Records management professionals
- Legal counsel
- Human resources
- Training
- Senior management
- Information technology (IT) management
- Consultants

The team's task is to create a records management policy that's sufficiently broad in scope to address the organization's current and future needs, but also sufficiently clear and detailed to enable the policy to be implemented by an Exchange administrator as an MRM solution. The process of developing this policy can be lengthy. This is because each team member considers, makes suggestions, and revises the work of the others, balancing legal requirements, budget, complexity, and administrative and human considerations to create a policy from which a manageable MRM implementation can be created.

Concerns for the team to consider, especially in organizations that have a well developed e-mail culture, include:

- User concerns and possible resistance to an MRM solution
- How to monitor and enforce the organization's messaging policies

Keeping Messages Where They Can Be Managed

To manage messages, the Managed Folder Assistant must have access to them. This means that messages must be stored on an Exchange server for effective MRM. This has two consequences:

- Users' mailboxes must often be increased in size so that they can hold more items.
- Access to personal folder (.pst) files on users' computers should be limited or eliminated.

Increasing Mailbox Size

Keeping all user messages in mailboxes on the server usually means increasing users' mailbox storage quotas, possibly to a gigabyte (GB) or more. The increased performance of Exchange 2010 helps to make these larger mailboxes manageable. A number of changes have been made to the Extensible Storage Engine (ESE) to increase performance and reduce storage requirements. These changes help you in planning for and deploying larger mailbox quotas at a lower cost. For more details about changes to ESE, see New Exchange Core Store Functionality.

Personal Archive

In Exchange 2010, you can provision personal archives for your users, allowing them to have an online archive mailbox that can be accessed using Microsoft Outlook 2010 and Microsoft Office Outlook Web App. Archive mailboxes provide functionality similar to .pst files used by Outlook, but eliminates the risks associated with using .pst files. For more details about some of the risks your organization is exposed to due to the use of .pst files, and how your users can benefit from a personal archive, see Understanding Personal Archives.

With a combination of larger mailboxes and archive mailboxes, you can plan to reduce the usage of .pst files in your organization, with the goal of eliminating it.

Limiting Access to .pst Files

You can start moving users away from using .pst files by creating a group policy that prevents new items from being added to existing .pst files. Making .pst files read-only gives users access to the .pst files they may already have while encouraging them to keep the messages that they want to keep in their Exchange mailboxes. If you plan to deploy archive mailboxes, data from pst files can be moved to the user's archive mailbox. Eventually, you may want to create a group policy to remove access to .pst files altogether.

Limiting access to .pst files can disrupt the work habits of some users, but it also has a number of advantages.

Keeping user messages on the server and limiting access to .pst files can:

- Significantly increase the effectiveness of MRM by keeping messages where they can be managed and monitored.
- Reduce the risk of losing important data that's stored on individual hard disks rather than on servers that are backed up regularly.
- Help to reduce the loss of the organization's intellectual property when vendors, interns, and employees leave the organization.
- Improve users' access to their data by keeping everything in their mailboxes.
- Make Outlook Web App more effective because all user messages are available anywhere with only a Web connection.
- Reduce the cost of legal discovery during a lawsuit. The process of capturing and discovering information that's stored in .pst files is labor-intensive and expensive because .pst files must first be located on user computers and then the contents must be processed by legal personnel.

Configuring User's Systems to Prevent Moving or Copying Exchange Mailbox Data to .pst Files

Outlook 2010 allows you to effectively control your organization's mailbox data so it can't be moved or copied to a .pst file. This allows users to open .pst files and copy the data into an Exchange mailbox, but not copy or move messages from the Exchange mailbox to .pst files. Using Outlook 2010, you can provide your users with a migration path to move messaging data from .pst files to their primary Exchange mailbox or their archive mailbox (if it's provisioned).

To disable the copying of Exchange mailbox data to a .pst file, set the following registry value for your Outlook 2010 users. You can set the registry value by configuring administrative templates in a group policy. You can add Outlook 2010 Group Policy settings to a Group Policy object by adding the Outlook14.adm policy file. For more information about adding or removing an administrative template, see Add or remove an Administrative Template (.adm file).

Caution:
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Registry path	**HKEY_CURRENT_USER/Software/Microsoft/Office/14/Outlook**
Registry value	**DisableCrossAccountCopy**
Value type	REG_MULTI_SZ
Value data	Domain names used for user's primary SMTP e-mail addresses. For example, use contoso.com to prevent copying or moving data from any mailbox that uses a contoso.com e-mail address as the primary SMTP e-mail address. Use * (asterisk) to

	prevent moving or copying data from any mailbox. **Note:** In Exchange 2010, domains used for generating e-mail addresses for recipients in your organization are configured as accepted domains. For more information, see Managing Accepted and Remote Domains.

Note:
Using the **DisableCrossAccountCopy** registry value on a computer running Outlook 2010 doesn't prevent the Outlook 2010 user from copying data to the primary or archive mailbox.

Configuring User's Systems to Operate Without .pst Files in Outlook 2010

Note:
The registry values in this section can also be set for Microsoft Office Outlook 2007. Change the Outlook version from 14 to 12.0 to apply these changes to Outlook 2007.

1. **Disable copying or moving messages to .pst files** Create a group policy that sets the following registry subkey to a value of 1. This setting prevents users from moving or copying messages to .pst files. Users can still create new .pst files but they can't add anything to them. This setting blocks only Microsoft Outlook .pst files. It allows Microsoft SharePoint .pst files to be connected and updated in a user's Outlook profile. A similar registry key can be used to disable writing to .pst files in Office Outlook 2003.

Caution:
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

Registry path	**HKEY_CURRENT_USER/Software/Microsoft/Office/14/Outlook/PST**
Registry value	**PstDisableGrow**
Value type	DWORD
Value data	1

2. **Disable AutoArchive** Create a group policy that sets the following registry subkeys to a value of 0. These settings disable the **AutoArchive** menu in Outlook and remove the **AutoArchive** option, which is shown when the user clicks **Tools** > **Options**, and then clicks the **Other** tab.

Registry path	**HKEY_CURRENT_USER/Software/Policies/Microsoft/Office/14/Outlook/Preferences**

Registry value	Value type	Value data
ArchiveDelete	DWORD	0
ArchiveMount	DWORD	0
ArchiveOld	DWORD	0
DeleteExpired	DWORD	0
DoAging	DWORD	0
PromptForAging	DWORD	0

3. **Disable creation of new .pst files** Create a group policy that sets the following registry subkey to a value of 5575. This setting removes the **Outlook Data File** option in Outlook, which is shown when the user clicks **File**, and then points to **New**.

Registry path	**HKEY_CURRENT_USER/Software/Policies/Microsoft/Office/14/Outlook/DisableCmdBarItemsList**
Registry value	**TCID1**
Value type	DWORD
Value data	5575

Pilot Program

Starting with a pilot implementation can help you to fine tune your MRM solution and learn about end-user satisfaction before an organization-wide implementation. For example, you may discover that users find a six-month retention period for the Inbox too short, and that they're more comfortable with a one-year limit. Or you may discover that additional journaling would result in a need to upgrade your archiving solution.

Members of an MRM planning team may also be good candidates for the first members of an MRM pilot program. Additional members can be recruited from IT personnel and from interested management personnel. When the pilot program is in stable operation, you can recruit additional members of the organization to join. Any user reluctance to adopt managed messaging can sometimes be lessened with the promise of a larger mailbox, automatic e-mail management (including automatic deletion of routine notices and messages that can be placed in a short-retention folder), and training to deal with any questions or concerns.

How Do I Implement MRM?

When it's time to implement your MRM solution in your organization, you may want to consider a phased implementation to allow the people in the organization and your Exchange system to adapt to the changes required.

Human Considerations During an MRM Implementation

Gradually introducing MRM to users gives them time to adapt to necessary changes in their work habits. A workable plan is to:

1. Start a pilot program to test and refine the solution.
2. Invite additional users to join the pilot program. Larger mailboxes and availability of an archive mailbox can be an incentive to join.
3. When you're ready to roll out MRM to the entire organization, start by offering training on MRM and relevant organization messaging policies.
4. Increase the size of users' mailboxes.
5. Apply retention policies to users' mailboxes, but with expiration turned off. Encourage users to familiarize themselves with MRM and to the appropriate retention tags according to their needs and the organization's message retention policy.
6. Three weeks after retention policies are applied to users, enable MRM and make .pst files read-only.
7. Be ready to provide a high level of support for users at the start of MRM implementation. (Training in advance of rollout reduces user questions and concern.)
8. Monitor system performance.
9. Monitor user compliance.

System Considerations During an MRM Implementation

Your Exchange system must adapt to MRM. The first time the Managed Folder Assistant runs, it typically processes a large number of items. This can be a resource-intensive process for both the Mailbox server and the network. It can also result in Outlook clients consuming large amounts of time and network resources while synchronizing mailbox contents with the server. You should plan carefully to avoid overloading resources. Running the Managed Folder Assistant when the load on the server is light and adding users gradually rather than all at once can help to ensure a smooth transition.

Training and the Human Element

People take their e-mail personally, even when it isn't their personal e-mail. If faced with abrupt changes to the organization's messaging policies, users may feel annoyed or confused, especially if the new policies involve automatically deleting messages. Changes to long-established methods (such as never emptying the Inbox or saving everything to .pst files) have the potential to cause significant disruption for some users. To assure that your MRM implementation proceeds with as little disruption as possible, consider the following recommendations.

Phased implementation

Introduce MRM gradually rather than all at once.

Training

Training users helps to address concerns in advance and makes for a smoother implementation. Some training topics to consider include:

- An introduction to the organization's messaging policies.
- The necessity for MRM in the modern workplace, including an overview of the potential legal liability that results from a lack of records management, and how that liability can cost the organization money and endanger jobs.
- How automatic e-mail deletion can be a timesaver by automatically deleting outdated content that routinely accumulates.
- How larger mailbox sizes provide more room for message storage.
- How server-based storage increases mobile access to data.
- How there may be unavoidable changes to the way users perform certain tasks (for example, not being able to add messages to .pst files), and the necessity of paying more attention to classifying and handling messages.
- How MRM helps to conserve the organization's IT resources.

Advance notice

Notify users in advance that changes are coming. Specifically, notify users of the exact dates that MRM will be implemented and remind them about the changes that will occur.

User support

Excellent user support in the early phases of the implementation can ease the transition to MRM. Issues that arise during the deployment phase are usually less technical than might be expected. Often, the concerns revolve around users asking questions of the "What do I do?" nature. Having a team of people who can answer this type of question will help to manage these concerns.

Compliance, Monitoring, and Enforcement

The following are some of methods by which users can evade MRM policies:

- Saving messages to .pst files (if .pst files aren't disabled by group policy)
- Forwarding messages to other locations (such as an external e-mail account)
- Saving messages as files on their computers
- Sending messages to Microsoft OneNote (by using Outlook 2010 or Outlook 2007)
- Printing messages
- If your organization has deployed managed folders, by placing all of their mailbox folders in the managed folder that has the longest retention setting.

Educating users about the messaging policies of your organization can help to ensure

compliance. However, monitoring may be necessary to ensure that your MRM solution is effective. Enforcement of messaging policies will likely require involvement and guidance from senior management.

Complying with Legal Discovery Orders

In Exchange 2010, Multi-Mailbox Search helps you to comply with legal discovery orders for electronically stored information. You can use Multi-Mailbox Search to search the contents of specified Exchange 2010 mailboxes. You can create powerful search queries using a number of search parameters. Messages returned by the search are copied to the specified Discovery mailbox. To learn more about Multi-Mailbox Search, see Understanding Multi-Mailbox Search.

1.11.6.5 How Retention Age is Calculated

How Retention Age is Calculated

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-12-11*

If you set a retention limit on items that have a retention tag or are within a managed folder, the Managed Folder Assistant tests the age of those items, and takes the specified action for items that have exceeded their retention limit.

Determining the Age of Different Types of Items

For mailboxes that use retention policies, the retention age of mailbox items is calculated from the date of delivery. When the Managed Folder Assistant processes items in a mailbox, it stamps a start date and an expiration date for all items that have retention tags with the **Delete and Allow Recovery** or **Permanently Delete** retention action. Items that have an archive tag are also stamped with a move date.

In Microsoft Exchange Server 2010 Service Pack 1 (SP1), the retention age for items in the **Deleted Items** default folder is calculated based on the date of delivery unless the item was moved or deleted from a folder that doesn't have an inherited or implicit retention tag. Consider the following examples:

- A user receives a message in the Inbox folder on 01/26/2011. The Inbox folder has a retention tag configured to delete items in 365 days.
  1. The Managed Folder Assistant processes the message. It stamps the message with a start date of 01/26/2011 and an expiration date of 01/26/2012.
  2. The user soft-deletes the item on 02/27/2011.The item is moved to the Deleted Items folder, which has a retention tag configured to delete the item in 30 days.
  3. The Managed Folder Assistant processes the message. It recalculates the expiration date based on the start date (01/26/2011).
  4. Because the item is older than 30 days, it is deleted immediately.
- A user receives an item in the Inbox folder on 01/26/2011. The Inbox folder doesn't have a retention tag applied, and the retention policy doesn't contain a default policy tag.
  1. The user soft-deletes the item on 02/27/2011. The item is moved to the Deleted Items folder, which has a retention tag configured to delete items in 30 days.

.2.The Managed Folder Assistant processes the mailbox on 03/27/2011, and determines that the item doesn't have a start date. It stamps the current date as the start date and 04/27/2011 as the expiration date.
.3.The item is deleted on 04/27/2011, which is 30 days after it was deleted or moved to the Deleted Items folder.

The same conditions are true for both *move tags* (tags that have the **Move to Archive** retention action) and *delete tags* (tags that have the **Delete and Allow Recovery** and **Permanently Delete** retention actions).

Important:
Retention tags include retention settings such as retention age and retention action. However, to configure retention settings for a managed folder, you must create managed content settings for it. A UNRESOLVED_TOKEN_VAL(xCoNameNoMk) Exchange Server 2010 mailbox can be configured to use either a retention policy or a managed folder mailbox policy.

When you create managed content settings for a managed folder, you can select one of the following options to specify how the Managed Folder Assistant determines when a retention period starts:

- When the item is delivered to the user's mailbox (or for calendar items and recurring tasks, when the item is older than its end date)
- When the user moves the item into the managed folder

After determining when a retention period starts, the Managed Folder Assistant uses rules to determine the age of items for the purpose of enforcing retention limits. The following tables describe the rules used for various items.

Calendar Items

Depending on whether a calendar item is in the Deleted Items folder, the Managed Folder Assistant uses the following rules to calculate the age of calendar items and enforce retention limits. The steps for each rule are listed in the order in which they are performed.

Location of calendar items	Rules
Calendar items in the Deleted Items folder	1.A calendar item expires according to its `message-received date`, if one exists. 2.If a calendar item doesn't have a `message-received date`, it expires according to its `message-creation date`. 3.If a calendar item has neither a `message-received date` nor a `message-creation date`, it doesn't expire.
Calendar items not in the Deleted Items folder	• Non-recurring calendar items expire according to their `end date`. • Recurring calendar items expire according to the `end date` of their last occurrence. Recurring calendar items with no `end date` don't expire.

Tasks

Depending on whether a task is in the Deleted Items folder, the Managed Folder Assistant uses the rules listed in the following table to calculate the age of tasks and enforce retention limits. The steps for each rule are listed in the order in which they are performed.

Location of tasks	Rules

Tasks in the Deleted Items folder	1. A task expires according to its `message-received date`, if one exists. 2. If a task doesn't have a `message-received date`, it expires according to its `message-creation date`. 3. If a task has neither a `message-received date` nor a `message-creation date`, it doesn't expire.
Tasks not in the Deleted Items folder	• Non-recurring tasks: .1. A non-recurring task expires according to its `message-received date`, if one exists. .2. If a non-recurring task doesn't have a `message-received date`, it expires according to its `message-creation date`. .3. If a non-recurring task has neither a `message-received date` nor a `message-creation date`, it doesn't expire. • A recurring task expires according to the `end date` of its last occurrence. If a recurring task doesn't have an `end date`, it doesn't expire. • A regenerating task (which is a recurring task that regenerates a specified time after the preceding instance of the task is completed) doesn't expire.

Note:

In Exchange 2010, retention tags aren't supported for the Calendar and Tasks default folders. The Managed Folder Assistant doesn't process items in these folders.

Other Items

For all other types of items, the Managed Folder Assistant uses the following rules to calculate the age and enforce retention limits. These items include:

- E-mail messages
- Contacts
- Documents
- Faxes
- Journal items
- Meeting requests, responses, and cancellations
- Missed calls

The steps for each rule are listed in the order in which they are performed.

Period at which retention starts	Rules
When an item is delivered to a user's mailbox	1. If the item has a `message-received date`, the `message-received date` is used. 2. If the item doesn't have a `message-received date`, the `message-creation date` is used. 3. If the item doesn't have a `message-creation date`, the message doesn't expire.

When a user moves the item to the managed folder	1. If the item has a `move date`, the move date is used. 2. If the item doesn't have a `move date`, the item doesn't expire.

Corrupted Items

Any corrupted items in a mailbox are skipped by the Managed Folder Assistant, and they don't expire.

1.11.6.6 Deploying Messaging Records Management

Deploying Messaging Records Management

Exchange Server 2010 > Messaging Policy and Compliance > Messaging Records Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-01*

1.11.6.6.1 Checklist: Deploying Retention Policies

Checklist: Deploying Retention Policies

Messaging Policy and Compliance > Messaging Records Management > Deploying Messaging Records Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-30*

Use this checklist to deploy retention policies in your Microsoft Exchange Server 2010 organization. Before you start working with this checklist, make sure you're familiar with the concepts in the following topics:

- Understanding Messaging Records Management
- Understanding Retention Tags and Retention Policies

Checklist for Deploying Retention Policies

Done?	Tasks	Topic
	Assess messaging records management (MRM) requirements for different sets of users.	Understanding Messaging Records Management
	Determine which Microsoft Outlook client versions are in use.	Get-LogonStatistics
	Create retention tags.	Create a Retention Tag
	Create retention policies.	Create a Retention Policy
	Add retention tags to retention policies.	Add or Remove Retention Tags from a Retention Policy
	Place mailboxes on retention hold.	Place a Mailbox on Retention Hold
	Apply a retention policy to a single mailbox for testing purposes.	Apply a Retention Policy to Mailboxes
	Optional: Implement client blocking to block legacy Outlook clients.	Configure Outlook Client Blocking
	Begin user communication and training activities. Include a deadline when retention policies will be processed, and items moved or deleted.	Not applicable
	Apply retention policy to additional mailboxes.	Apply a Retention Policy to Mailboxes
	A few days in advance, remind users about the deadline.	Not applicable
	At the deadline, remove the retention hold from mailboxes.	Place a Mailbox on Retention Hold

1.11.6.6.2 Create a Retention Tag

Create a Retention Tag

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Retention tags are used to apply retention settings to folders and individual items such as messages, notes, and contacts. These settings specify how long a message remains in the mailbox and the action to take when the message reaches the specified retention age. When a message reaches its retention age, it's moved to the archive mailbox, deleted, or flagged for user attention.

There are three types of retention tags:

- **Retention policy tags (RPTs)** These tags are created for default folders such as Inbox and Deleted Items.
- **Default policy tags (DPTs)** These tags apply to all items that don't have a retention tag applied, either inherited or explicit. You can have a maximum of three default policy tags in a retention policy: a DPT with the **Move to Archive** action, a DPT with the **Delete and Allow Recovery** or **Permanently Delete** action to delete messages from the primary and archive mailboxes, and a DPT for voice mail messages.
- **Personal tags** These tags are available to Microsoft Outlook 2010 and Microsoft Office Outlook Web App users as part of their retention policy. Users can apply personal tags to folders they create or to individual items, even if those items already have a different tag applied.

To learn more about retention tags, see Understanding Retention Tags and Retention Policies.

Note:

After you create retention tags, additional steps are required to deploy them to user mailboxes. You must add retention tags to a retention policy, and then apply the policy to a mailbox. For details, see Add or Remove Retention Tags from a Retention Policy and Apply a Retention Policy to Mailboxes.

Looking for other management tasks related to messaging records management (MRM)? Check out Deploying Messaging Records Management.

What Do You Want To Do?

- Use the EMC to create a retention tag
- Use the Shell to create a retention tag

Use the EMC to create a retention tag

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, expand the forest you want, and then navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Retention Policy Tag**.
3. On the **New Retention Policy Tag** page, complete the following fields:
   - **Tag Name** Use this box to type a name for the retention tag. This is the

name of the retention tag object in Active Directory. This name can contain up to 64 characters.

- **Tag Type** Use this list to select the type of retention tag that you want to create. To create a RPT for a default folder (for example, **Inbox**), select the default folder name. To create a DPT, select **All other folders in the mailbox**. To create a personal tag, select **Personal Folder**.
- **Age limit for retention (days)** Click this button to specify that items have a retention period. In the corresponding text box, type the number of days in the retention period. (The range of values is from 1 through 24,855 days.)
- **Action to take when the age limit is reached** After clicking **Age limit for retention (days)**, you can use this list to specify what should happen to an item when it's past the age limit for retention. The choices include:

  Delete and Allow Recovery If you select this option, messages are deleted but can be recovered by using the Recover Deleted Items feature in Outlook or Outlook Web App. To learn more about these features see the "Recover deleted items" topic for Outlook or Outlook Web App.

  Note:
  Users can only recover deleted items for the retention time you specify in the *RetainDeletedItemsFor* parameter of the Set-Mailbox cmdlet.

  Permanently Delete If you select this option, messages are permanently deleted and aren't recoverable by the user.
  Move to Archive If you select this option, messages are automatically moved to the user's archive mailbox. If you haven't created an archive mailbox for the user, no action is taken.

Note:
You can't use the EMC to create a retention tag with the Mark as Past Retention Limit retention action. You must use the New-RetentionPolicyTag cmdlet with the *MarkAsPastRetentionLimit* parameter.

- **Disable this tag** Click this button to disable the processing of this tag. The Managed Folder Assistant won't process messages that have a disabled tag applied.
- **Comments** Use this box to type a comment that will be displayed to the user in Outlook. For example, to alert users that MRM is enabled on the folder, you could type the following message: "Messages are removed from this folder after 120 days." The maximum length of this comment is 255 characters. To configure localized comments, use the Set-RetentionPolicyTag cmdlet.

4. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a retention tag

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Use the Shell to create a retention policy tag for the default

folder Deleted Items

This example creates a retention policy tag for the default folder Deleted Items. When the tag is applied to a mailbox, items in the Deleted Items folder are permanently deleted after 30 days.

```
New-RetentionPolicyTag "Corp-Exec-DeletedItems" -Type DeletedItems -Comment "Dele
```

For detailed syntax and parameter information, see New-RetentionPolicyTag.

Use the Shell to create a default policy tag to move messages

This example creates a default policy tag to move messages. When the tag is applied to a mailbox, items without an inherited or explicitly applied retention tag are moved to the archive mailbox after 365 days.

```
New-RetentionPolicyTag "Corp-Exec -Default" -Type All -Comment "Items without a r
```

For detailed syntax and parameter information, see New-RetentionPolicyTag.

Use the Shell to create a default policy tag to delete messages

This example creates a default policy tag to delete messages. When the tag is applied to a mailbox, items without an inherited or explicitly applied retention tag are deleted after 1,095 days (three years).

```
New-RetentionPolicyTag "Corp-Exec -Default" -Type All -Comment "Items without a r
```

For detailed syntax and parameter information, see New-RetentionPolicyTag.

Use the Shell to create a default policy tag for voice mail messages

This example creates a default policy tag for voice mail messages. When the tag is applied to a mailbox, voice mail messages without an inherited or explicitly applied retention tag are deleted after 14 days.

```
New-RetentionPolicyTag "Corp-Exec -Voice Mail" -Type All -MessageClass voicemail
```

Note:

By default, the *MessageClass* parameter defaults to *, which applies to all message types. A mailbox can have a maximum of three default tags: a DPT with the **Move to Archive** action, a DPT with the **Delete and Allow Recovery** or **Permanently Delete** actions to delete messages from the primary and archive mailboxes, and a DPT for voice mail messages. You can only specify the *MessageClass* parameter for voice mail DPTs.

For detailed syntax and parameter information, see New-RetentionPolicyTag.

Use the Shell to create a personal tag

This example creates the personal tag Corp-BusinessCritical. Items to which the tag is applied are moved to the user's archive mailbox after three years.

```
New-RetentionPolicyTag "Corp-BusinessCritical" -Type Personal -Comment "Business
```

For detailed syntax and parameter information, see New-RetentionPolicyTag.

Other Tasks

After you create a retention tag, you may also want to:

- Create a Retention Policy
- Apply a Retention Policy to Mailboxes
- Place a Mailbox on Retention Hold

1.11.6.6.3 Create a Retention Policy

Create a Retention Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Using retention policies, you can group one or more retention tags and apply them to mailboxes. A mailbox can't have more than one retention policy. Retention tags can be linked to or removed from a retention policy at any time.

A retention policy can contain the following retention tags:

- One or more retention policy tags (RPTs) for supported default folders
- One default policy tag (DPT) with the **Move to Archive** action.
- One DPT with the **Delete and Allow Recovery** or the **Permanently Delete** action.
- One DPT for voice mail.
- Any number of personal tags

To learn more about retention policies and retention tags, see Understanding Retention Tags and Retention Policies.

Looking for other management tasks related to messaging records management (MRM)? Check out Deploying Messaging Records Management.

Prerequisites

- A retention policy with the same name as the one being created doesn't already exist in your Exchange organization.
- One or more retention tags should exist so you can associate them to the new retention policy.

Note:

You can create a retention policy without linking any retention tags to it. Retention tags can be added or removed from a retention policy at any time. However, tags aren't applied to a mailbox until they're linked to a retention policy and the Managed Folder Assistant processes the mailbox.

What Do You Want To Do?

- Use the EMC to create a retention policy
- Use the Shell to create a retention policy

Use the EMC to create a retention policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, expand the forest you want, and then navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Retention Policy**.

3. On the **Introduction** page, complete the following fields:
   - **Name** Use this box to type a name for the retention policy.
   - **Add** Click this button to add retention tags to the policy. To remove a tag from the policy, click the tag name, and then click **Remove** ().

4. On the **Select Mailboxes** page, click **Add** to select the mailboxes to which you want to apply the retention policy.

   Note:
   You can create a retention policy without applying it to any mailboxes. You can also apply the policy to mailboxes at a later time by using the EMC or the Shell. For details, see Apply a Retention Policy to Mailboxes.

5. On the **New Retention Policy** page, review your configuration settings. To make any configuration changes, click **Back**. To create the retention policy, click **New**.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a retention policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example creates the retention policy Corp-Execs-RetPol and links the tags Corp-Exec-Default, Corp-Exec-Inbox, and Corp-Exec-DeletedItems to the policy.

```
New-RetentionPolicy "Corp-Execs-RetPol" -RetentionPolicyTagLinks "Corp-Exec-Defau
```

For detailed syntax and parameter information, see New-RetentionPolicy.

Other Tasks

After you create a retention policy, you may also want to:

- Apply a Retention Policy to Mailboxes
- Add or Remove Retention Tags from a Retention Policy
- Configure the Managed Folder Assistant
- Place a Mailbox on Retention Hold

1.11.6.6.4 Add or Remove Retention Tags from a Retention Policy

Add or Remove Retention Tags from a Retention Policy

Messaging Policy and Compliance > Messaging Records Management > Deploying Messaging Records Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can add retention tags to a retention policy when the policy is created or any time thereafter. For details about how to create a retention policy, including how to simultaneously add retention tags, see Create a Retention Policy.

A retention policy can contain the following retention tags:

- One or more retention policy tags (RPTs) for supported default folders
- One default policy tag (DPT) with the **Move to Archive** action.
- One DPT with the **Delete and Allow Recovery** or the **Permanently Delete** action
- One DPT for voice mail
- Any number of personal tags

Note:
Retention tags aren't applied to a mailbox until they're linked to a retention policy and the Managed Folder Assistant processes the mailbox. To learn more about the Managed Folder Assistant, see Configure the Managed Folder Assistant.

Looking for other management tasks related to messaging records management (MRM)? Check out Deploying Messaging Records Management.

Use the EMC to add retention tags to or remove retention tags from a retention policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Retention Policies** tab, select the retention policy to which you want to add retention tags.
3. In the action pane, click **Properties**.
4. In **<Retention policy name> Properties**, on the **General** tab, use the following settings:
   - **Add** Click this button to add a retention tag to the policy.
   - Select a tag from the list, and then click this button to remove the tag from the policy.

Use the Shell to add retention tags to or remove retention tags from a retention policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Mailbox Permissions topic.

This example adds the retention tags VPs-Default, VPs-Inbox, and VPs-DeletedItems to the retention policy RetPolicy-VPs, which doesn't already have retention tags linked to it.

Caution:
If the policy has retention tags linked to it, this command replaces the existing tags.

```
Set-RetentionPolicy -Identity "RetPolicy-VPs" -RetentionPolicyTagLinks "VPs-Defau
```

This example adds the retention tag VPs-DeletedItems to the retention policy RetPolicy-VPs, which already has other retention tags linked to it.

```
$TagList = (Get-RetentionPolicy "RetPolicy-VPs").RetentionPolicyTagLinks
$TagList.Add((Get-RetentionPolicyTag 'VPs-DeletedItems').DistinguishedName)
Set-RetentionPolicy "RetPolicy-VPs" -RetentionPolicyTagLinks $TagList
```

This example removes the retention tag VPs-Inbox from the retention policy RetPolicy-VPs.

```
$TagList = (Get-RetentionPolicy "RetPolicy-VPs").RetentionPolicyTagLinks
$TagList.Remove((Get-RetentionPolicyTag 'VPs-Inbox').DistinguishedName)
Set-RetentionPolicy "RetPolicy-VPs" -RetentionPolicyTagLinks $TagList
```

For detailed syntax and parameter information, see the following topics:

- Set-RetentionPolicy
- Get-RetentionPolicy
- Get-RetentionPolicyTag

Other Tasks

After you link retention tags to a retention policy, you may also want to:

- Apply a Retention Policy to Mailboxes
- Configure the Managed Folder Assistant
- Place a Mailbox on Retention Hold

1.11.6.6.5 Apply a Retention Policy to Mailboxes

Apply a Retention Policy to Mailboxes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can use retention policies to group one or more retention tags and apply them to mailboxes to enforce message retention settings. A mailbox can't have more than one retention policy.

Caution:

Messages are expired based on settings defined in the retention tags linked to the policy. These settings include actions such moving messages to the personal archive or permanently deleting them. Before applying a retention policy to one or more mailboxes, we recommended that you test the policy and inspect each retention tag associated with it.

Looking for other management tasks related to messaging records management (MRM)? Check out Deploying Messaging Records Management.

Use the EMC to apply a retention policy to a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Applying retention policies" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, expand the forest you want, and then navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox to which you want to apply the retention policy. You can select multiple mailboxes by using the Shift or Ctrl keys.
3. In the action pane, click **Properties**.
4. In **<Mailbox User> Properties**, on the **Mailbox Settings** tab, select **Messaging Records Management**, and then click **Properties**.
5. In **Messaging Records Management**, select the **Apply Retention Policy** check box, and then click **Browse** to select the retention policy you want to apply to the mailbox.
6. Click **OK**, and then in **<Mailbox User> Properties**, click **Apply**.

Use the Shell to apply a retention policy to a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Applying retention policies" entry in the Messaging Policy and Compliance Permissions topic.

This example applies the retention policy RP-Finance to Bharat's mailbox.

```
Set-Mailbox "Bharat" -RetentionPolicy "RP-Finance"
```

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to change a retention policy for mailboxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Applying retention policies" entry in the Messaging Policy and Compliance Permissions topic.

This example applies the new retention policy New-Retention-Policy to all mailboxes that have the old policy Old-Retention-Policy.

```
$OldPolicy={Get-RetentionPolicy "Old-Retention-Policy"}.distinguishedName
Get-Mailbox -Filter {RetentionPolicy -eq $OldPolicy} -Resultsize Unlimited | Set-
```

For detailed syntax and parameter information, see the following topics:

- Get-RetentionPolicy
- Get-Mailbox
- Set-Mailbox

1.11.6.6.6 Export and Import Retention Tags

Export and Import Retention Tags

Messaging Policy and Compliance > Messaging Records Management > Deploying Messaging Records Management >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2012-03-08*

There are several scenarios in which you may want to export or import retention tags, including:

- Applying the same retention policies across all servers in a multi-forest Exchange organization
- Applying the same retention policies in a hybrid deployment where some mailboxes reside in your on-premises Exchange organization and some reside in Exchange Online
- Applying retention policies in an Exchange Online Archiving scenario, where users with on-premises Exchange 2010 mailboxes have a cloud-based archive

In these scenarios, the Managed Folder Assistant can correctly process an item that has a retention tag applied after the item or the mailbox is moved to another organization.

Note:

To keep retention tags and retention policies synchronized between two organizations, every time you make changes to a retention tag or policy in the source organization, you must perform this procedure to export retention tags and policies from the source organization and import them in the destination organization.
You can't select specific retention tags or policies to export. The `Export-RetentionTags.ps1` script exports all retention tags and policies from an organization.

Looking for other management tasks related to messaging records management (MRM)? Check out Deploying Messaging Records Management.

Export retention tags from an on-premises Exchange organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. Run this Exchange Management Shell command to change directory to the **Scripts** subdirectory in your Exchange installation path.

```
Cd "<Exchange Server installation path>\Scripts"
```

Important:

If you're importing or exporting retention tags and retention policies to Exchange Online, you must connect your Windows PowerShell session to Exchange Online. For details, see Connect Windows PowerShell to the Service.

Run the `Export-RetentionTags.ps1` script to export retention tags to an .xml file.

```
Export-RetentionTags.ps1 "c:\docs\ExportedRetentionTags.xml"
```

Import retention tags to an Exchange organization

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. Run this Shell command to change the directory to the **Scripts** subdirectory in

your Exchange installation path.

```
Cd "<Exchange Server installation path>\Scripts"
```

2. Run the `Import-RetentionTags.ps1` script to import retention tags from a previously exported .xml file.

Important:
If you're importing or exporting retention tags and retention policies to Exchange Online, you must connect your Windows PowerShell session to Exchange Online. For details, see Connect Windows PowerShell to the Service.

Note:
When running this script against Exchange Online, you may be prompted to confirm that you want to run software from an untrusted publisher. Verify that the name of the publisher appears as `CN=Microsoft Corporation, OU=MOPR, O=Microsoft Corporation, L=Redmond, S=Washington, C=US`, and then click `R` to allow the script to be run once or `A` to always run.

```
Import-RetentionTags.ps1 "c:\docs\ExportedRetentionTags.xml"
```

3. If the destination organization contains any retention tags or retention policies that aren't found in the .xml file you're importing, you'll be prompted whether you want to delete them. If true synchronization of retention tags and retention policies between the source and destination organizations is desired, select the option to delete them. This makes sure both organizations contain the same retention tags and retention policies.

Warning:
If you delete a retention policy in the destination organization that's applied to mailbox users, you may receive additional prompts before deleting the policy. If you delete a retention policy that's applied to mailbox users, those users will no longer have a retention policy applied. Depending on your organization's compliance requirements, you should apply another retention policy to these users to avoid the risk of being out of compliance.

Other Tasks

After you export and import retention tags, you may also want to:

- Apply a Retention Policy to Mailboxes
- Add or Remove Retention Tags from a Retention Policy

1.11.6.6.7 Configure the Managed Folder Assistant

Configure the Managed Folder Assistant

Messaging Policy and Compliance > Messaging Records Management > Deploying Messaging Records Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

The *Managed Folder Assistant* is a Microsoft Exchange Mailbox Assistant that applies message retention settings configured in retention policies or managed folder mailbox policies. If a mailbox uses a managed folder mailbox policy, it also creates any managed folders and applies managed content settings to them.

Looking for other management tasks related to messaging records management (MRM)? Check out Deploying Messaging Records Management.

Differences Between Exchange 2010 SP1 and Exchange 2010 RTM

Before performing the procedures in this topic, it's important that you understand how the Managed Folder Assistant works in Microsoft Exchange Server 2010 Service Pack 1 (SP1) and in the release to manufacturing (RTM) version of Exchange 2010:

- **Exchange 2010 SP1** In Exchange 2010 SP1, the Managed Folder Assistant is a throttle-based assistant. Throttle-based assistants are always running and don't need to be scheduled. The system resources they can consume are throttled. You can configure the Managed Folder Assistant to process all mailboxes on a Mailbox server within a certain period (known as a *work cycle)*.
- **Exchange 2010 RTM** In Exchange 2010 RTM, the Managed Folder Assistant is a schedule-based assistant. Schedule-based assistants run based on the schedule specified for the assistant.

Important:

In Exchange 2010 RTM, the Managed Folder Assistant is scheduled to run from 01:00 (1:00 A.M.) to 09:00 (9:00 A.M.) daily. You can modify the schedule to suit your requirements.

Note:

The Managed Folder Assistant stops as soon as all mailboxes are processed. It doesn't run continuously until the end of the scheduled period.

When the Managed Folder Assistant is running, it processes all the mailboxes on a server. If the Managed Folder Assistant doesn't finish processing the mailboxes on the server during the time that you've scheduled, it automatically resumes processing where it left off the next time it runs. There is one Managed Folder Assistant for each server.

Running the Managed Folder Assistant is a resource-intensive process, especially when it's run for the first time. The first time the Managed Folder Assistant runs, it typically processes a large number of items. This can be a resource-intensive process for the Mailbox server and the network. It can also result in Microsoft Outlook clients consuming large amounts of time and network resources while synchronizing with the server. Be sure to plan carefully to avoid overloading resources.

You should run the Managed Folder Assistant only when your server can tolerate the extra load. This is usually during off-peak hours. You should also run the Managed Folder Assistant often enough to meet your organization's message retention requirements.

Use the Shell to configure the Managed Folder Assistant in Exchange 2010 SP1

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the EMC to configure the Managed Folder Assistant in Exchange 2010 SP1.

This example configures the Managed Folder Assistant to process all mailboxes within one day.

```
Set-MailboxServer MyMailboxServer -ManagedFolderWorkCycle 1
```

For detailed syntax and parameter information, see Set-MailboxServer.

Use the EMC to schedule the Managed Folder Assistant in Exchange 2010 RTM

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Server Configuration** > **Mailbox**.
2. In the result pane, right-click the Mailbox server for which you want to schedule the Managed Folder Assistant, and then click **Properties**.
3. Click the **Messaging Records Management** tab.
4. In the **Schedule the Managed Folder Assistant** box, select **Use Custom Schedule**, and then click **Customize**.
5. In **Schedule**, select the times and days during which you want the Managed Folder Assistant to run.
6. Click **OK**.

Use the Shell to schedule the Managed Folder Assistant in Exchange 2010 RTM

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

In Exchange 2010 RTM, the Managed Folder Assistant is a schedule-based assistant. This example sets the Managed Folder Assistant schedule to start running at 14:00 (2:00 P.M.) Sunday and continue running until all mailboxes are processed or until 13:00 (1:00 P.M.) the following Sunday, whichever comes first.

```
Set-MailboxServer -Identity MyMailboxServer -ManagedFolderAssistantSchedule "Sun.
```

For detailed syntax and parameter information, see Set-MailboxServer.

Use the Shell to start the Managed Folder Assistant in Exchange 2010 SP1

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to start the Managed Folder Assistant in Exchange 2010 SP1.

In Exchange 2010 SP1, you can use the **Start-ManagedFolderAssistant** cmdlet to have the Managed Folder Assistant process the specified mailbox.

This example triggers the Managed Folder Assistant to immediately process Bharat Suneja's mailbox.

```
Start-ManagedFolderAssistant -Identity bharat.suneja@contoso.com
```

Use the Shell to start the Managed Folder Assistant in Exchange 2010 RTM

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the EMC to start the Managed Folder Assistant in Exchange 2010 RTM.

In Exchange 2010 RTM, you can use the **Start-ManagedFolderAssistant** cmdlet to manually start the Managed Folder Assistant. You may need to manually start the assistant during testing, troubleshooting, or to process mailboxes immediately during a period when the assistant isn't scheduled to run. Every time the **Start-ManagedFolderAssistant** cmdlet is run, processing of mailboxes stops and then restarts, reprocessing all the mailboxes on the server from the beginning.

This example manually starts the Managed Folder Assistant. When you manually start the Managed Folder Assistant, it continues running until all mailboxes on the Mailbox server are processed or until the assistant is stopped manually.

```
Start-ManagedFolderAssistant
```

This example triggers the Managed Folder Assistant to immediately process Bharat Suneja's mailbox.

```
Start-ManagedFolderAssistant -Mailbox bharat.suneja@contoso.com
```

For detailed syntax and parameter information, see Start-ManagedFolderAssistant.

1.11.6.6.8 Configure Outlook Client Blocking

Configure Outlook Client Blocking

Messaging Policy and Compliance > Messaging Records Management > Deploying Messaging Records Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2010, you can use retention policies or managed folders for messaging records management (MRM). Only users running Microsoft Outlook 2010 have access to all client features for retention policies and managed folders. Users running Office Outlook 2007 have access only to managed folders. However, both retention policies and managed folder mailbox policies are applied on the Mailbox server by the Managed Folder Assistant, regardless of the Outlook client version used by the user. Older Outlook clients do not expose the MRM functionality of these features. For example, because Outlook 2007 does not support retention policies, users can't apply personal tags to items or folders.

You can block users who are running older versions of Outlook from accessing their Exchange mailboxes. You can also block access on a per-mailbox or on a per-Client Access server basis.

Looking for other management tasks related to MRM? Check out Deploying Messaging

Records Management.

MRM Feature Availability by Client Application and Version

The following table lists the MRM features available in various client applications and versions.

MRM features

Client application	Available MRM client features
Outlook 2010	All
Outlook 2007	Managed folders
Outlook 2003 Service Pack 2 (SP2) while connected to an Exchange server and working in online mode	The following applies: • Managed folder comments are displayed only when the user clicks the managed folder icon in the folder header or clicks **View**, and then clicks **Policy**. • Managed folder quotas are supported. Error messages appear when a folder exceeds the quota.

Outlook 2003 SP2 while disconnected from an Exchange server and working in Cached Exchange Mode	The following applies:
	• Managed custom folder icons are displayed.
	• Managed folder comments aren't displayed.
	• Managed folder quotas aren't supported. Specifically:
	  • No folder quota error messages are displayed.
	  • Folder quota information isn't synced with the Exchange server.

Outlook versions earlier than Outlook 2003 SP2	None
Other e-mail client software	None

The following table shows version numbers for Outlook.

Outlook versions

Outlook version	Version number
Outlook 2010	14
Outlook 2007	12
Outlook 2003	11
Outlook 2002	10
Outlook 2000	9
Outlook 98	8.5
Outlook 97	8

Note:
Before making any changes, note that hotfixes and service pack releases may affect the client version string. Be careful when you restrict client access because server-side Exchange components must also use MAPI to log on. Some components report their client version as the component name (such as SMTP or OLE DB), while others report the Exchange build number (such as 6.0.4712.0). For this reason, avoid restricting clients that have version numbers that start with 6.<*x.x.*>. For example, to prevent MAPI access completely, instead of specifying **0.0.0-6.5535.65535.65535**, specify the two ranges so that the server components can log on. For example, specify the following: **0.0.0-5.9.9; 7.0.0-**.

After you perform these procedures, be aware that when users are blocked from accessing their mailboxes, they will receive the following warning message.

Your Exchange Server administrator has blocked the version of Outlook that you are using. Contact your administrator for assistance.

To bypass the warning that MRM features aren't supported for e-mail clients running versions of Outlook earlier than Outlook 2010, you can use the *ManagedFolderMailboxPolicyAllowed* parameter of the **New-Mailbox**, **Enable-Mailbox**, and **Set-Mailbox** cmdlets in the Shell. When a managed folder mailbox policy is assigned to a mailbox by using the *ManagedFolderMailboxPolicy* parameter, the warning appears by default unless you use the *ManagedFolderMailboxPolicyAllowed* parameter.

Use the Shell to block versions of Outlook on a per-mailbox basis

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "User mailboxes" entry in the Mailbox Permissions topic.

Note:
You can't use the EMC to block versions of Outlook on a per-mailbox basis.

This example blocks all Outlook versions earlier than 11.8010.8036.

```
Set-CASMailbox -Identity adam@contoso.com -MAPIBlockOutlookVersions "-11.8010.803
```

This example restores access to a mailbox that's blocked by a version of Outlook.

```
Set-CASMailbox -Identity adam@contoso.com -MAPIBlockOutlookVersion $null
```

For detailed syntax and parameter information, see Set-CASMailbox.

Use the Shell to block Outlook versions on a Client Access server

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "RPC Client Access settings" entry in the Client Access Permissions topic.

This example blocks Outlook clients prior to version 12.0.0 from accessing the mailbox on an Exchange 2010 Client Access server.

Important:
The value used for the *Value* parameter in this command is an example. You must

determine the correct client version numbers. In Exchange 2010, you can use the Get-LogonStatistics cmdlet to retrieve the versions of MAPI clients that are connected to the mailbox database.

```
Set-RpcClientAccess -Server CAS01 -BlockedClientVersions "0.0.0-5.65535.65535;7.0
```

For detailed syntax and parameter definition, see Set-RpcClientAccess.

1.11.6.6.9 Migrate from Managed Folders

Migrate from Managed Folders

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2010, messaging records management (MRM) is performed by using retention tags and retention policies. A retention policy is a group of retention tags that can be applied to a mailbox. Managed folders, the MRM technology introduced in Exchange Server 2007, are supported for interoperability.

A mailbox that has a managed folder mailbox policy applied can be migrated to use a retention policy. To do so, you must create retention tags that are equivalent to the managed folders linked to the user's managed folder mailbox policy.

Important:

Before you migrate from managed folders to retention policies in your production environment, we recommend that you test the process in a test environment.

Looking for other management tasks related to MRM? Check out Deploying Messaging Records Management.

Comparing Retention Tags to Managed Folders

Unlike managed folders, which require users to move items to a managed folder based on retention settings, retention tags can be applied to a folder or an individual item in the mailbox. This process has minimal impact on the user's workflow and e-mail organization methods. When a folder has retention tags applied, all items in that folder inherit the retention settings. Users can further specify retention settings by applying different retention tags to individual items in that folder.

Managed folders support different managed content settings for a folder, each with a different message class (such as e-mail items or calendar items). Retention tags don't require a separate managed content settings object because the retention settings are specified in the tag's properties. It isn't supported to create retention tags for particular message classes. Retention tags also don't allow you to use journaling (which is performed by the Managed Folder Assistant).

The following table compares the MRM functionality available when using retention tags or managed folders.

Retention tags vs. managed folders

Functionality	Retention tags	Managed folders
Specify retention settings for default folders (such as Inbox)	Use retention policy tags (RPTs)	Use managed default folders
Specify retention settings for entire mailbox	Use a default policy tag (DPT)	Use managed default folders
Use retention settings for custom folders	Use personal tags	Using managed custom folders
Require managed content settings	No (retention settings included in a retention tag)	Yes
Use retention settings for different message classes (such as e-mail messages, voice mail, or calendar items)	No	Yes
Support the Move To Archive action, which moves items to the user's archive mailbox	Yes	No
Support the Move To Managed Folder action	No	Yes
Allow journaling using the Managed Folder Assistant	No	Yes
Policy applied to user	Retention policy	Managed folder mailbox policy
Maximum number of policies that can be applied to a mailbox user	1	1
Processed by the Managed Folder Assistant	Yes	Yes
Client support	Microsoft Outlook 2010 and Office Outlook Web App	Outlook 2010, Office Outlook 2007, and Outlook Web App

Use the Shell to migrate mailbox users from managed folders

Note:
You can't use the EMC to migrate mailbox users from managed folders.

For the following procedures, Contoso mailboxes have a managed folder mailbox policy applied containing the following managed folders.

Managed folders for Contoso

Managed folder	Managed content settings	Retention enabled	Retention age	Retention action
Corp-DeletedItems	CS-Corp-DeletedItems	Yes	30 days	Delete and Allow Recovery

Corp-SentItems	CS-Corp-SentItems	Yes	1,825 days	Move to Deleted Items
Corp-JunkMail	CS-Corp-JunkMail	Yes	30 days	Permanently Delete
Corp-EntireMailbox	CS-Corp-EntireMailbox	Yes	365 days	Move to Deleted Items
30 Days	CS-30Days	Yes	30 days	Move to Deleted Items
5 Years	CS-5Years	Yes	1,825 days	Move to Deleted Items
Never Expire	CS-NeverExpire	No	365 days	Not applicable

The following are general steps for migrating users from this managed folder mailbox policy to a retention policy. Each step is detailed later in this topic:

1. Create retention tags for the migration.
2. Create a retention policy and link the newly created retention tags to the policy.
3. Apply the retention policy to user mailboxes.

Important:
After you apply the retention policy to a user and the Managed Folder Assistant runs, the managed folders in the user's mailbox become unmanaged.

Step 1: Create retention tags for the migration

There are two methods you can use for this step:

- Create retention tags based on the managed folders and their corresponding managed content settings. With this method, you use the **New-RetentionPolicyTag** cmdlet with the *ManagedFolderToUpgrade* parameter. When you specify this parameter, the corresponding retention tag is automatically applied to the managed folder.
- Create retention tags by manually specifying the retention settings. With this method, you use the **New-RetentionPolicyTag** cmdlet without the *ManagedFolderToUpgrade* parameter. When you don't specify this parameter, any retention policy tags you add to the policy are applied to the default folders, and the default policy tag is applied to the entire mailbox. However, any personal tags you add to the policy aren't automatically applied to the managed folders.

Create retention tags based on managed folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example creates retention tags based on the corresponding managed content settings shown in the Contoso managed folder mailbox policy.

```
New-RetentionPolicyTag Corp-DeletedItems -ManagedFolderToUpgrade Corp-DeletedItem
New-RetentionPolicyTag Corp-SentItems -ManagedFolderToUpgrade Corp-SentItems
New-RetentionPolicyTag Corp-JunkMail -ManagedFolderToUpgrade Corp-JunkMail
New-RetentionPolicyTag Corp-EntireMailbox -ManagedFolderToUpgrade Corp-EntireMail
New-RetentionPolicyTag 30Days -ManagedFolderToUpgrade 30Days
New-RetentionPolicyTag 5Years -ManagedFolderToUpgrade 5Years
New-RetentionPolicyTag NeverExpire -ManagedFolderToUpgrade NeverExpire
```

For detailed syntax and parameter information, see New-RetentionPolicyTag.

Create retention tags manually

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example creates retention tags based on the managed folders and corresponding managed content settings shown in the Contoso managed folder mailbox policy. The retention settings are specified manually without using the *ManagedFolderToUpgrade* parameter.

```
New-RetentionPolicyTag Corp-DeletedItems -Type DeletedItems -RetentionEnabled $tr
New-RetentionPolicyTag Corp-SentItems -Type SentItems -RetentionEnabled $true -Ag
New-RetentionPolicyTag Corp-JunkMail -Type JunkMail -RetentionEnabled $true -AgeL
New-RetentionPolicyTag Corp-EntireMailbox -Type All -RetentionEnabled $true -AgeL
New-RetentionPolicyTag 30Days -Type Personal -RetentionEnabled $true -AgeLimitFor
New-RetentionPolicyTag 5Years -Type Personal -RetentionEnabled $true -AgeLimitFor
New-RetentionPolicyTag NeverExpire -Type Personal -RetentionEnabled $false
```

For detailed syntax and parameter information, see New-RetentionPolicyTag.

Step 2: Create a retention policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example creates the retention policy RP-Corp and links the newly created retention tags to the policy.

```
New-RetentionPolicy RP-Corp -RetentionPolicyTagLinks Corp-DeletedItems,Corp-SentI
```

For detailed syntax and parameter information, see New-RetentionPolicy.

Step 3: Apply the retention policy to user mailboxes

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Applying retention policies" entry in the Messaging Policy and Compliance Permissions topic.

This example applies the newly created retention policy RP-Corp to the mailbox user Ken Kwok.

```
Set-Mailbox -Identity Kwok -RetentionPolicy RP-Corp
```

For detailed syntax and parameter information, see Set-Mailbox.

1.11.6.6.10 Port Managed Folder

Port Managed Folder

Messaging Policy and Compliance > Messaging Records Management > Deploying Messaging Records Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

In Microsoft Exchange Server 2010, retention policies, the new Exchange 2010 messaging records management (MRM) feature, replace managed folders, the MRM feature

introduced in Exchange Server 2007. Using the Port Managed Folder wizard, you can port managed folders to retention tags, thereby maintaining the same retention settings as the managed folder.

Considerations

When porting a managed folder to a retention tag, consider the following:

- Managed folders have associated managed content settings. These settings control the lifespan of items in users' mailboxes, including the age limit for retention, the retention action, and the message type. In this case, message type refers to the type of message such as e-mail messages, appointments, meeting requests, and voice mail.
- A managed folder can have multiple managed content settings for the different message classes associated with it.
- The following retention tags don't support different message classes:
  - Retention policy tags (RPTs) which are applied to default folders such as Inbox and Deleted Items.
  - Personal tags, which are available to Microsoft Outlook 2010 and Microsoft Office Outlook Web App users to apply to custom folders and individual messages.
- Default policy tags (DPTs), which are applied to the entire mailbox, are the only retention tags that support the `Voicemail` message class (in addition to the `All` message class, denoted by the asterisk (*) symbol).
- If the managed folder you want to port has multiple managed content settings for different message classes, only one retention tag is created, and the highest retention age of all the managed content settings is used as the retention age for the ported tag, irrespective of the message class of the managed content settings.
  For example, review the following managed content settings for the managed folder Corp-DeletedItems.

Managed content settings	Message class	Retention age	Retention action
CS-DeletedItems	*	60	Permanently Delete
CS-DeletedItems-Voicemail	Voicemail	14	Permanently Delete
CS-DeletedItems-Fax	Fax	120	Delete and Allow Recovery

  When you port the managed folder Corp-DeletedItems to the retention tag Ported-DeletedItems, the tag will have the following settings.

Retention tag	Message class	Retention age	Retention action
Ported-DeletedItems	*	120 (the highest retention age of all managed content settings associated with the ported managed folder)	Delete and Allow Recovery

- By default, managed default folders of the type All are ported to DPTs.
- Managed default folders of folder types other than All are ported to RPTs.
- Managed custom folders are ported to personal tags.
- Retention tags created by porting managed folders contain the managed folder name in the **LegacyManagedFolder** property. After you port or create

retention tags, you must link the tags to a retention policy and apply the policy to a mailbox. When the Managed Folder Assistant processes the mailbox and finds a managed folder that matches a ported retention tag, the assistant applies the retention tag to the managed folder. The ported retention tag must be linked to the user's retention policy for this to occur.

Looking for other management tasks related to MRM? See Deploying Messaging Records Management.

What Do You Want To Do?

- Use the EMC to port a managed folder
- Use the Shell to port a managed folder

Use the EMC to port a managed folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. Navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **Port from Managed Folder to Tag**.
3. On the **Introduction** page, complete the following fields:
   - **Tag Name** Use this box to type a name for the new retention tag. This name can be up to 64 characters in length.
   - **Select the managed folder to upgrade** Click **Browse** to select a managed folder to port.
   - **Comments** Use this box to type a comment that will be displayed to the user in Outlook. For example, to alert users that MRM is enabled on the folder, you could type the following message: "Messages are removed from this folder after 120 days." The maximum length of this comment is 255 characters. To configure localized comments, use the Set-RetentionPolicyTag cmdlet.
4. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to port a managed folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example ports the managed folder MF-Corp-DeletedItems to the retention tag Tag-Corp-DeletedItems.

```
New-RetentionPolicyTag -Name 'Tag-Corp-DeletedItems' -ManagedFolderToUpgrade 'MF-
```

For detailed syntax and parameter information see New-RetentionPolicyTag.

Other Tasks

After you port a managed folder, you may also want to:

- Create a Retention Policy
- Apply a Retention Policy to Mailboxes
- Place a Mailbox on Retention Hold

1.11.6.6.11 Place a Mailbox on Retention Hold

Place a Mailbox on Retention Hold

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Placing a mailbox on retention hold suspends the processing of a retention policy or managed folder mailbox policy for that mailbox. Retention hold is designed for scenarios such as a user being on vacation or away temporarily.

During retention hold, users can log on to their mailbox and change or delete items. When you perform a mailbox search, deleted items that are past the deleted item retention period aren't returned in search results. To make sure items changed or deleted by users are preserved in legal hold scenarios, you must place a mailbox on legal hold. For more information, see Place a Mailbox on Litigation Hold.

You can also include retention comments for mailboxes you place on retention hold. The comments are displayed in supported versions of Microsoft Outlook.

Looking for other management tasks related to messaging records management (MRM)? Check out Deploying Messaging Records Management.

Use the EMC to place a mailbox on retention hold

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can use the EMC to place a mailbox on retention hold, regardless of whether the mailbox has a retention policy or a managed folder mailbox policy applied. Mailboxes that have a retention policy or a managed folder mailbox policy applied are processed by the Managed Folder Assistant.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox you want to place on retention hold.
3. In the action pane, click **Properties**.
4. In **<Mailbox> Properties**, on the **Mailbox Settings** tab, click **Messaging Records Management**, and then click **Properties**.
5. In **Messaging Records Management**, complete the following fields:
   - **Halt Retention Policy during this period** Select this check box to place the mailbox on retention hold.
   - **Start date** Select this check box and use the associated lists to specify when the retention hold should begin.

- **End date** Select this check box and use the associated lists to specify when the retention hold should end.

Use the Shell to place a mailbox on retention hold

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example places Michael Allen's mailbox on retention hold.

```
Set-Mailbox "Michael Allen" -RetentionHoldEnabled $true
```

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to remove retention hold for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example removes the retention hold from Michael Allen's mailbox.

```
Set-Mailbox "Michael Allen" -RetentionHoldEnabled $false
```

For detailed syntax and parameter information, see Set-Mailbox.

Other Tasks

After you place a mailbox on retention hold, you may also want to:

- Increase the mailbox quota. See Configure Storage Quotas for a Mailbox.
- Perform a discovery search on the mailbox. See Create a Discovery Search.

1.11.6.6.12 Configure Retention Tag Properties

Configure Retention Tag Properties

Messaging Policy and Compliance > Messaging Records Management > Deploying Messaging Records Management >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-10*

Retention tags are used to apply retention settings to folders and individual items such as messages and notes. These settings specify how long a message remains in the mailbox and the action to take when the message reaches the specified retention age. When a message reaches its retention age, it's moved to the archive mailbox, deleted, or flagged for user attention.

There are three types of retention tags:

- **Retention policy tags (RPTs)** These tags are created for default folders such as Inbox and Deleted Items.
- **Default policy tags (DPTs)** These tags apply to all items that don't have a retention tag applied, either inherited or explicit. You can have a maximum of three default policy tags in a retention policy: a DPT with the **Move to Archive** action, a DPT with the **Delete and Allow Recovery** or **Permanently Delete** action to delete messages from the primary and archive mailboxes, and a DPT for voice mail messages.
- **Personal tags** These tags are available to Outlook 2010 and Outlook Web App users as part of their retention policy. Users can apply personal tags to folders they create or to individual items, even if those items already have a different tag applied.

To learn more about retention tags, see Understanding Retention Tags and Retention Policies.

Looking for other management tasks related to messaging records management (MRM)? Check out Deploying Messaging Records Management.

What Do You Want to Do?

- Use the EMC to configure retention tag properties
- Use the Shell to configure retention tag properties

Use the EMC to configure retention tag properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Retention Policy Tags** tab, select the retention tag you want to configure.
3. In the action pane, click **Properties**.
4. Use the **General** tab to view or modify the following settings:
   - **Name** Use this unlabeled box at the top of the page to view or change the tag name.
   - **Modified** This read-only field displays the last date and time that the retention tag was modified.
   - **Tag Type** This read-only field displays the tag type.
   - **Age limit for retention (days)** Click this button to specify that items have a retention period. In the corresponding text box, type the number of days in the retention period. (The range of values is from 1 through 24,855 days.)
   - **Action to take when the age limit is reached** After clicking **Age limit for retention (days)**, you can use this list to specify what should happen to an item when it's past the age limit for retention. The choices include:

     Move to the Deleted Items Folder This option isn't available for retention tags. If you select this option for a retention tag, messages that have the tag applied won't be moved to the Deleted Items folder.

     Move to a Managed Custom Folder This option isn't available for retention tags. An error is generated if you select this option.

     Delete and Allow Recovery If you select this option,

messages are deleted but can be recovered by using the Recover Deleted Items feature in Outlook or Outlook Web App. To learn more about these features see the "Recover deleted items" topic for Outlook or Outlook Web App.

Note:
Users can only recover deleted items for the retention time you specify in the *RetainDeletedItemsFor* parameter of the Set-Mailbox cmdlet.

Permanently Delete If you select this option, messages are permanently deleted and aren't recoverable by the user.
Mark as Past Retention Limit This option isn't available for retention tags. If you select this option for a retention tag, messages that have the tag applied won't be marked as past the retention limit.
Move to Archive If you select this option, messages are automatically moved to the user's archive mailbox. If you haven't created an archive mailbox for the user, no action is taken.

- **Disable this tag** Click this button to disable the tag. If a DPT or a RPT is disabled, the tag is no longer applied to the mailbox. If a personal tag is disabled, the retention period is displayed to the user as **Never**. If the user applies the tag to an item, the item never expires. .

Important:
Items that have a disabled retention tag applied aren't processed by the Mailbox Assistant. If you want to prevent a tag from being applied to items, we recommend disabling the tag rather than deleting it. When you delete a tag, the tag configuration is deleted from Active Directory, and the Mailbox Assistant processes all messages to remove the deleted tag.

Note:
If a user applies a tag to an item believing the item will never be deleted, enabling the tag later may delete items the user wanted to retain. The same is true for tags with the **Move to Archive** action.

- **Comments** Use this box to type a comment that will be displayed to Outlook and Outlook Web App users. For example, to alert users that MRM is enabled on the folder, you could type the message: "Messages are removed from this folder after 120 days." The maximum length of this comment is 255 characters. To configure localized comments, use the Set-RetentionPolicyTag cmdlet.

Use the Shell to configure retention tag properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example disables the Corp-BusinessCritical tag.

```
Set-RetentionPolicyTag "Corp-BusinessCritical" -RetentionEnabled $false
```

This example retrieves all retention policy tags for the Inbox default folder and disables them.

```
Get-RetentionPolicyTag -Types Inbox | Set-RetentionPolicyTag -RetentionEnabled $f
```

This example retrieves all retention policy tags for the Inbox default folder and sets the retention age to 30 days.

```
Get-RetentionPolicyTag -Types DeletedItems | Set-RetentionPolicyTag -AgeLimitForR
```

For detailed syntax and parameter information, see Set-RetentionPolicyTag and Get-RetentionPolicyTag.

1.11.6.6.13 Configure Retention Policy Properties

Configure Retention Policy Properties

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

To apply retention tags to a mailbox, you must add them to a retention policy, and then apply the policy to the mailbox. A mailbox can't have more than one retention policy. Retention tags can be added to or removed from a retention policy at any time. To learn more about retention policies, see Understanding Retention Tags and Retention Policies.

A retention policy can contain the following retention tags:

- One or more retention policy tags (RPTs) for supported default folders
- One default policy tag (DPT) with the **Move to Archive** action
- One DPT with the **Delete and Allow Recovery** or the **Permanently Delete** action
- One DPT for voice mail
- Any number of personal tags

Note:

Retention tags aren't applied to a mailbox until they're linked to a retention policy and the Managed Folder Assistant processes the mailbox. To learn more about the Managed Folder Assistant, see Configure the Managed Folder Assistant.

Looking for other management tasks related to messaging records management (MRM)? See Deploying Messaging Records Management.

What Do You Want to Do?

- Use the EMC to configure a retention policy
- Use the Shell to configure a retention policy

Use the EMC to configure a retention policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Retention Policies** tab, select the retention policy you want to configure.
3. In the action pane, click **Properties**.

4. Use the **General** tab to view or modify the following settings:
   - **Name** Use this unlabeled box at the top of the page to view or change the policy name.
   - **Add** Click this button to add a retention tag to the policy.
   - Select a tag from the list, and then click this button to remove the tag from the policy.

5. Use the **Mailboxes** tab to view or modify the list of mailboxes to which the policy applies:
   - **Add** Click this button to add mailboxes to the policy.
   - Select a mailbox from the list, and then click this button to remove the mailbox from the policy.

Use the Shell to configure a retention policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example links the retention tags VPs-Default, VPs-Inbox, and VPs-DeletedItems to the retention policy RetPolicy-VPs, which doesn't already have retention tags linked to it.

Caution:
If the policy has retention tags linked to it, this command replaces the existing tags.

```
Set-RetentionPolicy -Identity RetPolicy-VPs -RetentionPolicyTagLinks "VPs-Default
```

This example adds the retention tag VPs-DeletedItems to the retention policy RetPolicy-VPs, which already has other retention tags linked to it.

```
$TagList = (Get-RetentionPolicy RetPolicy-VPs).RetentionPolicyTagLinks
$TagList.Add((Get-RetentionPolicyTag 'VPs-DeletedItems').DistinguishedName)
Set-RetentionPolicy RetPolicy-VPs -RetentionPolicyTagLinks $TagList
```

This example removes the retention tag VPs-Inbox from the retention policy RetPolicy-VPs.

```
$TagList = (Get-RetentionPolicy RetPolicy-VPs).RetentionPolicyTagLinks
$TagList.Remove((Get-RetentionPolicyTag 'VPs-Inbox').DistinguishedName)
Set-RetentionPolicy RetPolicy-VPs -RetentionPolicyTagLinks $TagList
```

This example applies the retention policy RetPolicy-VPs to Bharat Suneja's mailbox.

```
Set-Mailbox "Bharat Suneja" -RetentionPolicy "RetPolicy-VPs"
```

This example removes the retention policy from Tony Smith's mailbox.

```
Set-Mailbox "Tony Smith" -RetentionPolicy $null
```

For detailed syntax and parameter information, see the following topics:

- Set-RetentionPolicy
- Get-RetentionPolicy
- Get-RetentionPolicyTag
- Set-Mailbox

1.11.6.6.14 Deploying Managed Folders

Deploying Managed Folders

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-10-12*

1.11.6.6.14.1 Create a Managed Default Folder

Create a Managed Default Folder

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

A managed default folder is a mailbox folder (such as the Inbox folder) that appears in Office Outlook 2007 by default and to which MRM has been applied. The retention and journaling of messages in managed default folders are controlled by managed content settings that are applied to the folder

Note:

Additional steps are necessary to deploy new managed folders. You can perform these steps by using other wizards in the Exchange Management Console or cmdlets in the Exchange Management Shell. For example, you can use the New Managed Content Settings wizard or the **New-ManagedContentSettings** cmdlet to create managed content settings for managed default folders. These settings control how the messages in the folder are handled. For more information about the steps required to fully implement managed folders, see Deploying Managed Folders.

Looking for other management tasks related to managed folders? Check out Deploying Managed Folders.

Use the Shell to create a managed default folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:
In Exchange 2010 SP1, you can't use the Exchange Management Console (EMC) to create a managed default folder.

This example creates a managed default folder Corp-VPs-Inbox of type Inbox. The comment 'Messages are removed from the Inbox folder after 120 days ' will be displayed in supported clients, and users will be unable to minimize the comment in Outlook.

```
New-ManagedFolder -Name 'Corp-VPs-Inbox' -DefaultFolderType Inbox -Comment 'Messa
```

For detailed syntax and parameter information, see New-ManagedFolder.

1.11.6.6.14.2 Create a Managed Custom Folder

Create a Managed Custom Folder

Messaging Records Management > Deploying Messaging Records Management > Deploying Managed Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-09*

A *managed custom folder* is a managed folder that's created by an Exchange administrator and placed in a user's mailbox for messaging records management (MRM) purposes. The retention and journaling of messages in managed custom folders are controlled by managed content settings that are applied to the folder.

Note:
Managed custom folders are a premium feature of MRM. Each mailbox that has managed custom folders requires an Exchange Server Enterprise client access license (CAL). To learn more about the licensing requirements for MRM, see "Client Access Licenses and MRM" in Understanding Messaging Records Management.

Note:
Additional steps are required to deploy new managed folders. You can perform these steps by using other wizards in the Exchange Management Console or cmdlets in the Exchange Management Shell. For example, you can use the New Managed Content Settings wizard or the **New-ManagedContentSettings** cmdlet to create managed content settings for managed custom folders. These settings control how the messages in the folder are handled. For more information about the steps required to fully implement MRM, see Deploying Managed Folders.

Looking for other management tasks related to managed folders? Check out Deploying Managed Folders.

Use the Shell to create a managed custom

folder

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:
In Exchange 2010 SP1, you can't use the Exchange Management Console (EMC) to create a managed custom folder.

This example creates the Business Critical managed custom folder that has a folder quota of 1.99 gigabytes. A folder comment is also enabled.

```
New-ManagedFolder -Name 'Business Critical' -FolderName 'Business Critical' -Stor
```

Note:
You cannot specify a value larger than 1.99 GB for the *StorageQuota* parameter when you run this command. Instead, you can use the value "unlimited" if you want to specify a size that is larger than 1.99 GB.

For detailed syntax and parameter information, see New-ManagedFolder.

1.11.6.6.14.3 Create Managed Content Settings

Create Managed Content Settings

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Managed content settings are used to define message retention settings and retention action for managed folders. Message lifespan is controlled in two ways:

- By controlling content *retention* and removing content that is no longer needed.
- By automatically *journaling* (copying) important content to a separate storage location outside the mailbox. This can be any location that has a SMTP e-mail address, including another Exchange mailbox. When the item is journaled, a label is applied to it that indicates how the user classified the item.

Important:
The managed folder assistant generates journal reports based on managed content settings for a managed folder. This approach is different than that of the Journaling agent, which generates journal reports as a part of either standard or premium journaling. For more details about Journaling, see Understanding Journaling.

For example, the managed content settings that you apply to a user's Inbox folder could specify that its contents should be automatically deleted or moved to another folder after 60 days.

Note:
In addition to the well-known message types (such as **All mailbox content** and **Calendar items**) to which you can apply managed content settings, you can use the *MessageClass* parameter of the **New-ManagedContentSettings** cmdlet in the Exchange Management Shell to specify a custom message class or a specific message class such as

IPM.NOTE.SMIME. For more information, see New-ManagedContentSettings

Looking for other management tasks related to managed folders? Check out Deploying Managed Folders.

Caution

Be cautious when using the managed default folder named Entire Mailbox. Managed content settings that are applied to the Entire Mailbox folder control every folder in the mailbox except:

- Managed custom folders (and their subfolders)
- Managed default folders (and their subfolders)

A managed default folder is a default folder in the mailbox (such as Inbox, Calendar, or Contacts) that is linked to a managed folder mailbox policy. If a default folder in the mailbox is not linked to a managed folder mailbox policy, then the "entire mailbox" policy will apply to that default folder.

Prerequisite

You must have at least one managed default folder or one managed custom folder for which to create managed content settings. For detailed instructions, see the following topics:

- Create a Managed Default Folder
- Create a Managed Custom Folder

Use the Shell to create managed content settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:

In Exchange 2010 SP1, you can't use the EMC to create managed folder content settings.

This example creates managed content settings for the managed default folder Calendar with the following parameters:

- **Name** MyCalendarSettings
- **MessageClass** CalItems
- **AgeLimitForRetention** 30 days
- **RetentionAction** MoveToDeletedItems

```
New-ManagedContentSettings -FolderName Calendar -MessageClass CalItems -Name MyCa
```

For detailed syntax and parameter information, see New-ManagedContentSettings.

Other Tasks

After you create managed content settings for a managed folder, you may also want to:

- Create a Managed Folder Mailbox Policy
- Add a managed folder to a managed folder mailbox policy. For instructions, see Configure Managed Folder Mailbox Policy Properties.

1.11.6.6.14.4 Create a Managed Folder Mailbox Policy

Create a Managed Folder Mailbox Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Managed folder mailbox policies are used to create logical groupings of managed folders. When a managed folder mailbox policy is applied to users' mailboxes, all the managed folders that are linked to the policy are deployed in a single operation.

You can create as many managed folder mailbox policies as you want. You can also add as many managed folders to each policy as you want, but each user mailbox can have only one managed folder mailbox policy.

If your organization has existing managed folders (including their corresponding managed content settings), you can add them to the managed folder mailbox policy as you create it. You can also add or remove managed folders from a managed folder mailbox policy any time after the policy is created.

Note:

Managed custom folders are a premium feature of messaging records management (MRM). Mailboxes with policies that include managed custom folders require an Exchange Server Enterprise client access license (CAL). Managed default folders require only an Exchange Server Standard CAL.

Caution

Be cautious when using the managed default folder named Entire Mailbox. Managed content settings that are applied to the Entire Mailbox folder control every folder in the mailbox except:

- Managed custom folders (and their subfolders)
- Managed default folders (and their subfolders)

A managed default folder is a default folder in the mailbox (such as Inbox, Calendar, or Contacts) that is linked to a managed folder mailbox policy. If a default folder in the mailbox is not linked to a managed folder mailbox policy, then the "entire mailbox" policy will apply to that default folder.

Use the Shell to create a managed folder mailbox policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:

In Exchange 2010 SP1, you can't use the Exchange Management Console (EMC) to create a managed folder mailbox policy.

This example creates the managed folder mailbox policy MyManagedFolderMailboxPolicy and links the Inbox managed default folder and Business Critical managed customer folder to the policy.

```
New-ManagedFolderMailboxPolicy -Name "MyManagedFolderMailboxPolicy" -ManagedFolde
```

For detailed syntax and parameter information, see New-ManagedFolderMailboxPolicy.

Other Tasks

After you create a managed folder mailbox policy, you may also want to:

- Apply a Managed Folder Mailbox Policy to Users
- Configure the Managed Folder Assistant

1.11.6.6.14.5 Apply a Managed Folder Mailbox Policy to Users

Apply a Managed Folder Mailbox Policy to Users

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Managed folder mailbox policies are used to create logical groupings of managed folders. When a managed folder mailbox policy is applied to users' mailboxes, all the managed folders linked to the policy are deployed in a single operation. You can apply only one managed folder mailbox policy to a user mailbox.

Important:

Managed custom folders are a premium feature of messaging records management (MRM). Mailboxes with policies that include managed custom folders require an Exchange Server Enterprise client access license (CAL).

Use the Shell to apply a managed folder mailbox policy to a user's mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:

In Exchange 2010 SP1, you can't use the Exchange Management Console (EMC) to apply a managed folder mailbox policy to a mailbox.

This example applies the mailbox policy Corp-VPs Managed Folder Mailbox Policy to user Chris' mailbox.

```
Set-Mailbox -Identity Chris -ManagedFolderMailboxPolicy "Corp-VPs Managed Folder
```

For detailed syntax and parameter information, see Set-Mailbox.

Other Tasks

After you apply a managed folder mailbox policy to a mailbox, you may also want to Configure the Managed Folder Assistant.

1.11.6.6.14.6 Turn Off or Suspend Messaging Records Management

Turn Off or Suspend Messaging Records Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

To meet individual, IT, or business requirements, you may need to turn off or temporarily suspend messaging records management (MRM) for an individual user or for a Mailbox server. Reasons you may need to turn off or suspend MRM include:

- If a mailbox user is away from the office or is otherwise unable to access e-mail, you can temporarily disable MRM for the mailbox by placing it on retention hold. When a mailbox is on retention hold, it's no longer processed by the Managed Folder Assistant. When the mailbox user returns or is able to access the mailbox again, you can remove the retention hold from the mailbox.
- If you need to test or troubleshoot performance issues, you can temporarily turn off MRM on that server by clearing the schedule for the Managed Folder Assistant.
- If you need to remove a retention tag from mailboxes (which have a retention policy with that tag applied), you can remove the tag from the policy.
- If you want a retention policy or a managed folder mailbox policy to no longer apply to a mailbox, you can remove the policy from the mailbox.
- If your organization decides not to use MRM features, you can turn off MRM permanently for the entire organization. If you later decide to deploy MRM, you have the ability to do so.

Place mailboxes on retention hold

You can place mailboxes on retention hold to turn off MRM temporarily (for example when users are on vacation). This suspends the processing of managed folder mailbox policies for the mailbox until retention hold is disabled. This is different from placing mailboxes on legal hold.

For details about how to place a mailbox on retention hold, see Place a Mailbox on Retention Hold.

To learn more about legal hold, see Understanding Litigation Hold.

Turn off MRM temporarily for individual servers

There are two ways in which you can stop the Managed Folder Assistant from running on a server:

- Use the EMC to clear the managed folder assistant's schedule. For detail instructions, see Configure the Managed Folder Assistant.

- In the Shell, run the Set-MailboxServer cmdlet and set the *ManagedFolderAssistantSchedule* parameter to $null.

When you stop the Managed Folder Assistant, managed content settings are no longer applied to managed folders on that server. No new managed custom folders are created and retention and journaling policies aren't enforced. However, folder quotas continue to be enforced.

Remove retention tags from mailboxes

To remove a retention tag from a mailbox, you unlink the tag from the retention policy. When you unlink a retention policy tag (RPT) for a default folder, the default mailbox tag applies to all items in that folder. When you unlink a personal tag, it's no longer available to the user.

This Shell example unlinks the retention tag Delete - 3 Days from the retention policy Corp-Users.

```
$tags = (Get-RetentionPolicy "Corp-Users").RetentionPolicyTagLinks
$tags -= "Deleted Items - 3 Days"
Set-Retention Policy "Corp-Users" -RetentionPolicyTagLinks $tags
```

Remove retention policies from mailboxes

You can stop a retention policy from applying to a mailbox by removing the policy from the mailbox user's properties.

This Shell example removes the retention policy from the mailbox jpeoples.

```
Set-Mailbox jpeoples -retentionpolicy $null.
```

This Shell example removes the retention policy from all mailboxes in the Exchange organization.

```
Get-Mailbox -ResultSize unlimited -Filter {RetentionPolicy -ne $null} | Set-Mailb
```

This Shell example removes the retention policy Corp-Finance from all mailbox users who have the policy applied.

```
Get-Mailbox -ResultSize unlimited -Filter {RetentionPolicy -eq "Corp-Finance"} |
```

For detailed syntax and parameter information, see Set-Mailbox and Get-Mailbox.

Remove managed folder mailbox policies from mailboxes

This example removes managed folder mailbox policy from the mailbox jpeoples, without affecting the managed folders in the mailbox.

```
Set-Mailbox -Identity jpeoples -ManagedFolderMailboxPolicy:$null
```

Remove managed folders and MRM policies from mailboxes

In Exchange Server 2010, you can use the *ManagedFolderMailboxPolicy* parameter of the Set-Mailbox cmdlet to remove all MRM policies and attributes from a mailbox. When you run this cmdlet, the following tasks are performed:

- MRM policies and MRM properties for any managed folders that were created as part of any MRM policies are removed
- Managed folders that are empty are removed from the mailbox
- Managed folders that contain items are converted to standard folders

This Shell example removes the managed folder mailbox policy and all managed folders from the mailbox jpeoples.

```
Set-Mailbox -Identity jpeoples -RemoveManagedFolderAndPolicy
```

Turn off MRM permanently for an entire organization

To turn off MRM for an organization, delete all its managed custom folders and delete all managed folder mailbox policies. After this is complete, folder quotas, retention, and journaling policies aren't enforced, and the MRM root folder and all managed custom folders are converted into normal folders that can be moved, renamed, or deleted by the user.

For details about how to turn off MRM, see Permanently Turn Off Messaging Records Management for an Organization.

Note:

If the user deletes all the managed custom folders in the **Managed Folders** root folder, the **Managed Folders** root folder is converted into a normal folder—one that can be moved, renamed, or deleted like any other folder.
If the user doesn't delete all the managed custom folders in the **Managed Folders** root folder, users won't be able to move, rename, or delete it.

Permanently Turn Off Messaging Records Management for an Organization

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Deleting all the managed default folders and managed custom folders within your organization will eliminate all messaging records management (MRM) functionality. If you do this, mailbox retention settings will no longer be checked and message content won't be journaled (copied) to other locations.

Although deleting all the managed custom folders from Active Directory removes the managed content settings that apply to folders, it doesn't remove the folders from users' mailboxes. Instead, the root folder for managed custom folders (called Managed Folders) and any managed custom folders are converted into normal, unmanaged folders that can be moved, renamed, or deleted by the user like any other folder.

Looking for other management tasks related to MRM? Check out Deploying Managed Folders.

Use the EMC to permanently turn off messaging records management

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the Exchange Management Console (EMC) to remove retention tags and retention policies. You must use the Shell to remove them.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Managed Custom Folders** tab.
3. Right-click a managed folder, and then click **Remove**.
4. Repeat steps 3 and 4 until all of the managed folders have been deleted.
5. In the result pane, click the **Managed Folders Mailbox Policies** tab.
6. Right-click a managed folder mailbox policy, and then click **Remove**.
7. Repeat steps 6 and 7 until all the managed folder mailbox policies are deleted.
8. In the result pane, click the **Managed Default Folders** tab.
9. Repeat steps 4 through 8.

Use the Shell to permanently turn off messaging records management

To permanently turn off MRM, you must remove all retention tags, retention policies, managed folders, and managed folder mailbox policies.

Important:
When you remove a retention tag from Active Directory, all mailboxes to which the tag is applied as a part of retention policy are processed by the Managed Folder Assistant. All items in affected mailboxes are restamped. This may result in additional resource consumption on the Mailbox servers containing the affected mailboxes. We recommend that you consider the server load and usage profile and schedule the Managed Folder Assistant on those servers to run at a time when there will be minimal impact on users. For details about how to schedule the Managed Folder Assistant, see Configure the Managed Folder Assistant.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Remove retention tags

This example removes the retention tag Corp-Users-Default

```
Remove-RetentionPolicyTag "Corp-Users-Default"
```

This example removes all retention tags.

```
Get-RetentionPolicyTag | Remove-RetentionPolicyTag
```

For detailed syntax and parameter information, see Remove-RetentionPolicyTag and Get-RetentionPolicyTag.

Remove retention policies

This example removes the retention policy Corp-Users.

```
Remove-RetentionPolicy "Corp-Users"
```

This example removes all retention policies.

```
Get-RetentionPolicy | Remove-RetentionPolicy
```

For detailed syntax and parameter information, see Remove-RetentionPolicy and Get-RetentionPolicy.

Remove managed folders

This example removes the managed folder My Managed Folder.

```
Remove-ManagedFolder "My Managed Folder"
```

This example removes all managed folders.

```
Get-ManagedFolder | Remove-ManagedFolder
```

For detailed syntax and parameter information, see Remove-ManagedFolder and Get-ManagedFolder.

Remove managed folder mailbox policies

This example removes the managed folder mailbox policy My Managed Folder Policy.

```
Remove-ManagedFolderMailboxPolicy "My Managed Folder Policy"
```

This example removes all managed folder mailbox policies.

```
Get-ManagedFolderMailboxPolicy | Remove-ManagedFolderMailboxPolicy
```

For detailed syntax and parameter information, see Remove-ManagedFolderMailboxPolicy and Get-ManagedFolderMailboxPolicy.

1.11.6.6.14.7 Configure Managed Content Settings

Configure Managed Content Settings

Messaging Records Management > Deploying Messaging Records Management > Deploying Managed Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Managed content settings are applied to the managed folders in users' mailboxes to control the retention and journaling of messages for messaging records management (MRM). Managed content settings define when messages that are no longer needed are to be removed or journaled (copied) to a separate storage location outside the mailbox. For example, the managed content settings that you apply to a user's Inbox folder could specify that its contents should be automatically deleted or moved to another folder after 60 days.

Important:

The managed folder assistant generates journal reports based on managed content settings for a managed folder. This approach is different than that of the Journaling agent, which generates journal reports as a part of either standard or premium journaling. For more details about Journaling, see Understanding Journaling.

Looking for other management tasks related to managed folders? Check out Deploying Managed Folders.

Configure managed content settings

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:
In Exchange 2010 SP1, you can't use the EMC to configure managed content settings.

The following command configures the managed content setting MyManagedContentSettings to apply a retention age of 120 days, delete messages upon expiration, and allow recovery.

```
Set-ManagedContentSettings -Identity MyManagedContentSettings -RetentionEnabled $
```

For detailed parameter and syntax information, see Set-ManagedContentSettings.

For More Information

Understanding Messaging Records Management

Understanding Managed Folders

Create Managed Content Settings

Deploying Managed Folders

1.11.6.6.14.8 Configure Managed Folder Properties

Configure Managed Folder Properties

Messaging Records Management > Deploying Messaging Records Management > Deploying Managed Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

A *managed folder* is a folder in a user's mailbox to which messaging records management (MRM) has been applied. There are two types of managed folders:

- *Managed default folders* (such as the Inbox) appear, by default, in a user's Office Outlook 2007 or later mailbox.
- *Managed custom folders* are created by Exchange administrators specifically for MRM.

Note:
Managed custom folders are a premium feature of MRM. Each mailbox that has managed custom folders requires an Exchange Server Enterprise client access license (CAL). Managed default folders require only an Exchange Server Standard CAL.

The retention and journaling of messages in managed folders are controlled by managed content settings that are applied to the folder.

Note:
Managed custom folders are typically given names that reflect their intended role in users' mailboxes. For example, a managed custom folder for personal e-mail may be

given the name **Personal E-mail**.

Looking for other management tasks related to managed folders? Check out Deploying Managed Folders.

Use the Shell to configure managed folder properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:
In Exchange 2010 SP1, you can't use the EMC to configure managed folder properties.

This example applies to managed default folders

This example changes the name of the Inbox managed default folder to Corp-VPs-Inbox and sets a comment to be displayed in supporting clients.

```
Set-ManagedFolder -Identity Inbox -Name Corp-VPs-Inbox -Comment "Email messages w
```

For detailed parameter and syntax information, see Set-ManagedFolder.

Note:
Although the comment in this example mentions a specific retention period, actual retention time for messages in a managed folder depends on the folder's managed content settings. A managed folder can have multiple managed content settings for different message classes, such as e-mail messages, calendar items, and tasks, with different retention settings.

This example applies to managed custom folders

This example changes the name of the managed custom folder Business Critical to Corp-Business Critical. It also specifies a storage limit of 500 MB on the folder and sets a comment to be displayed in supporting clients.

```
Set-ManagedFolder -Identity "Business Critical" -FolderName "Corp-Business Critic
```

Note:
Although the comment in this example mentions a specific retention period, actual retention time for messages in a managed folder depends on the folder's managed content settings. A managed folder can have multiple managed content settings for different message classes, such as e-mail messages, calendar items, and tasks, with different retention settings.

For detailed parameter and syntax information, see Set-ManagedFolder.

1.11.6.6.14.9 Configure Managed Folder Mailbox Policy Properties

Configure Managed Folder Mailbox Policy Properties

Messaging Records Management > Deploying Messaging Records Management > Deploying Managed Folders >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-02*

A *managed folder mailbox policy* is a logical grouping of managed folders. When a managed folder mailbox policy is applied to a user's mailbox, all the managed folders that are linked to the policy are deployed in a single operation, thereby making the deployment of messaging records management (MRM) easier. This topic shows you how to view the properties of a managed folder mailbox policy and how to add or remove associated folders from that policy.

Note:
After you assign a managed folder mailbox policy to a mailbox user, the managed folders and settings are applied to the mailbox when the Managed Folder Assistant runs and processes the mailbox.

Looking for other management tasks related to managed folders? Check out Deploying Managed Folders.

Configure managed folder mailbox policies

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

Note:
In Exchange 2010 SP1, you can't use the EMC to configure managed folder mailbox policies.

The following command adds the Inbox managed default folder and Business Critical managed custom folder to the managed folder mailbox policy MyManagedFolderPolicy.

```
Set-ManagedFolderMailboxPolicy -Identity MyManagedFolderPolicy -ManagedFolderLink
```

For detailed parameter and syntax information, see Set-ManagedFolderMailboxPolicy.

For More Information

Messaging Records Management

Understanding Managed Folders

Deploying Managed Folders

1.11.6.6.14.10 Use Exchange Management Shell Scripts for Managed Folders

Use Exchange Management Shell Scripts for Managed Folders

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

You can use Shell cmdlets and scripts to manage messaging records management (MRM)

in Microsoft Exchange Server 2010. We recommend that you test MRM features in a non-production environment first. When you're ready to implement MRM in production, you can use the same scripts in your production environment to accurately and consistently replicate managed folders, managed content settings, and managed folder mailbox policies.

Note:

Managed custom folders are a premium feature of MRM. Each mailbox that has managed custom folders requires an Exchange Server Enterprise client access license (CAL). Mailboxes with policies that include managed custom folders require an Exchange Server Enterprise CAL.

Use the Shell to manage managed folders

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. Create a script by entering Shell commands in a text editor, as shown in the sample script that follows.
2. Save the text file for the script with the .ps1 file extension (for example, MRM_Sample_Script.ps1).
3. At the command prompt in the Shell, enter the path and file name of the script (for example, **C:\Scripts\MRM_Sample_Script.ps1**, or **.\MRM_Sample_Script.ps1** for a script in the working directory).

The following is a sample script for MRM. For an explanation of the actions performed, see the comments within the script.

```
# MRM_Sample_Script.ps1
# This script demonstrates the fundamentals of performing messaging records manag
# Create a new managed custom folder.
New-ManagedFolder -Name "Important E-mail" -FolderName "Business Folder A"
# Create a variable, "$age," to use in the next command.
$age = New-TimeSpan -Day 30
# Create managed content settings for the new managed custom folder that delete i
New-ManagedContentSettings -Name "Retention settings for Business Folder A" -Fold
# Create a managed folder mailbox policy.
New-ManagedFolderMailboxPolicy -Name "Business Folder A" -ManagedFolderLinks "Imp
# Apply the managed folder mailbox policy to a mailbox.
Set-Mailbox -Identity Administrator -ManagedFolderMailboxPolicy "Business Folder
# Schedule the Managed Folder Assistant to run the entire week.
$ServerName= cmd /c echo %computername%
Set-MailboxServer -ID $ServerName -ManagedFolderAssistantSchedule "Sun.12:00-Sun.
# Start the Managed Folder Assistant.
Start-ManagedFolderAssistant
```


1.11.6.7 Monitoring Messaging Records Management

Monitoring Messaging Records Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-03*

View Performance Counters for Messaging Records Management

Performance Counters for Messaging Records Management

Messaging Records Management Errors and Events

1.11.6.7.1 View Performance Counters for Messaging Records Management

View Performance Counters for Messaging Records Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-09*

You can use Windows Reliability and Performance Monitor (Perfmon.exe) to select and view performance counters for messaging records management (MRM). By using performance counters, you can monitor the Managed Folder Assistant while it runs resource-intensive MRM processes.

For a list of performance counters for MRM, see Performance Counters for Messaging Records Management.

Looking for other tasks related to monitoring MRM? Check out Monitoring Messaging Records Management.

Use Windows Reliability and Performance Monitor to view performance counters for MRM

To perform this procedure, the account you use must be delegated membership in the local Administrators group.

1. To start Windows Reliability and Performance Monitor, click **Start**, click **Run**, and then type **perfmon**.
2. In the console tree, navigate to **Monitoring Tools** > **Performance Monitor**.
3. Click the plus sign (+) button on the toolbar. The **Add Counters** dialog box appears.
4. From the **Select counter from computer** list, select one of the following options:
   - If you are performing this procedure on a local computer, select **<Local computer>**. This is the default selection.
   - If you are performing this procedure remotely, select the server you want to monitor.
5. In the list of performance counters, expand **MSExchange Assistants - Per Database** or the **MSExchange Managed Folder Assistant**.
6. Select the performance counters you want to monitor.
7. For performance counters under **MSExchange Assistants - Per Database**, to view the counters for all mailbox databases, in **Instances of selected object**, click **All instances**. Or, to specify one or more mailbox databases, select instances from the list.
8. To add the selected counters so that the counters appear in Windows Reliability and Performance Monitor, and to begin collecting performance data, click **Add**.

1.11.6.7.2 Performance Counters for Messaging Records Management

Performance Counters for Messaging Records Management

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-23*

The performance counters in this topic monitor the Managed Folder Assistant as it implements messaging records management (MRM) for Microsoft Exchange Server 2010. Because running the Managed Folder Assistant is a resource-intensive process, you should run it only when your server can tolerate the additional load. You should also monitor server performance when the Managed Folder Assistant is running. In addition to the performance counters listed in this topic, you may also want to monitor additional performance counters that monitor items such as disk performance and CPU usage.

For more information about monitoring computers running MRM, see Monitoring Messaging Records Management.

Performance Counters for MRM

The following table describes performance counters for MRM.

Performance counters, performance objects, and description

Performance counter	Performance object	Description
Average Mailbox Processing Time In Seconds	MSExchange Assistants	Counts the average processing time of mailboxes for time-based assistants.
Mailboxes Processed	MSExchange Assistants	Counts the number of mailboxes processed by time-based assistants since the service started.
Mailboxes processed/sec	MSExchange Assistants	Determines the rate of mailboxes processed by time-based assistants per second.
Items Deleted but Recoverable	MSExchange Managed Folder Assistant	Counts the number of items deleted by the Managed Folder Assistant since the start of the most recent schedule interval. (The items are still recoverable through the Recoverable Items folder.) The number includes items in the mailboxes scheduled for processing during the schedule interval and items in any mailboxes that you specified for processing. This counter is reset to zero at the start of each schedule interval.
Items Journaled	MSExchange Managed Folder Assistant	Counts the number of items journaled by the Managed Folder Assistant since the start of the most recent schedule

		interval. The number includes items in the mailboxes scheduled for processing during the current work cycle and items in any mailboxes you specified for processing. This counter is reset to zero at the start of each work cycle.
Items Marked as Past Retention Date	MSExchange Managed Folder Assistant	Counts the number of items marked as past their retention date by the Managed Folder Assistant since the start of the most recent schedule interval. The number includes items in mailboxes scheduled for processing during the schedule interval and items in any mailboxes you specified for processing. This counter is reset to zero at the start of each schedule interval.
Items Moved	MSExchange Managed Folder Assistant	Counts the number of items moved by the Managed Folder Assistant since the start of the most recent schedule interval. The number includes items in the mailboxes scheduled for processing during the schedule interval and items in any mailboxes you specified for processing. This counter is reset to zero at the start of each schedule interval.
Items Permanently Deleted	MSExchange Managed Folder Assistant	Counts the number of items permanently deleted by the Managed Folder Assistant since the beginning of the most recent schedule interval. The number includes items in the mailboxes scheduled for processing during the schedule interval and items in any mailboxes you specified for processing. This counter is reset to zero at the beginning of each schedule interval.
Items Subject to Retention Policy	MSExchange Managed Folder Assistant	Counts the number of items subject to retention policy by the Managed Folder Assistant since the start of the most recent schedule interval. The number includes items in the mailboxes scheduled for processing during the schedule interval and items in any mailboxes you specified for processing. This counter is reset to zero at the start of each schedule interval. This counter is the sum of the following four expiration-related counters: • Items Journaled • Items Marked as Past Retention Date • Items Moved

		• Items Permanently Deleted
TotalSizeItemsExpired - Size of Items subject to Retention Policy (In Bytes)	MSExchange Managed Folder Assistant	Indicates the total size of items expired by the Managed Folder Assistant (SoftDelete, HardDelete, MoveToArchive). The following items are included: • Messages subject to deletion or move to a managed custom folder by a managed folder mailbox policy • Messages subject to deletion or move to archive by the user's retention policy • Messages expired by dumpster policy • Messages cleaned up by system cleanup tags This counter is reset to zero at every work cycle checkpoint of the Managed Folder Assistant work cycle.
TotalSizeItemsSoftDeleted - Size of Items Deleted but Recoverable (In Bytes)	MSExchange Managed Folder Assistant	Indicates the total size of items soft deleted by the Managed Folder Assistant. The following items are included: • Messages soft deleted by a managed folder mailbox policy • Messages soft deleted by a retention policy This counter is reset to zero at every work cycle checkpoint of the Managed Folder Assistant work cycle.
TotalSizeItemsPermanentlyDeleted - Size of Items Permanently Deleted (In Bytes)	MSExchange Managed Folder Assistant	Indicates the total size of items soft deleted by the Managed Folder Assistant. The following items are included: • Messages hard deleted by a managed folder mailbox policy • Messages hard deleted by a retention policy • Messages hard deleted by the Recoverable Items policy This counter is reset to zero at every work cycle checkpoint of the Managed Folder Assistant work cycle.
TotalSizeItemsMoved -	MSExchange Managed	Indicates the total size of items

Size of Items Moved due to an Archive policy tag (In Bytes)	Folder Assistant	moved to a folder or moved to archive by the Managed Folder Assistant. The following items are included: • Messages moved to a managed custom folder by a managed folder mailbox policy • Messages moved to the personal archive by a retention policy This counter is reset to zero at every work cycle checkpoint of the Managed Folder Assistant work cycle.
TotalItemsWithPersonalTag - Items stamped with Personal Tag (Expiry or Archive)	MSExchange Managed Folder Assistant	Indicates the number of times a user tags items with a personal tag. This includes both Deletion and Archive tags. For example: • An item is tagged with a personal tag. • An item with a personal tag is retagged with another personal tag. If a folder is tagged with a personal tag, the counter is incremented by the total number of items in the folder.
TotalItemsWithDefaultTag - Items stamped with Default Tag (Expiry or Archive)	MSExchange Managed Folder Assistant	Indicates the number of items assigned a default policy tag (DPT) based on a user action, for example, when a user selects a message with a personal tag and selects **Use folder policy**. If a new user is assigned a retention policy with a DPT, the counter is incremented by the number of items that will be assigned the DPT due to the retention policy. **Note:** If a user has a retention policy with a DPT, new messages that arrive through transport get a default tag, and this isn't tracked by this counter.
TotalItemsWithSystemCleanupTag - Items stamped with System Cleanup Tag	MSExchange Managed Folder Assistant	Indicates the number of items tagged with the system cleanup tag. This includes mailbox metadata items that aren't visible to users.
TotalItemsExpiredByDefaultExpiryTag - Items expired due to a default	MSExchange Managed Folder Assistant	Indicates the number of items expired (soft or hard deleted) by the Managed Folder Assistant due to any non-personal (default or system) tag in a

Expiry Tag		retention policy. This doesn't include the items expired by Recoverable Items clean up or system clean up.
TotalItemsExpiredByPersonalExpiryTag - Items expired due to a personal Expiry Tag	MSExchange Managed Folder Assistant	Indicates the number of items expired (soft or hard deleted) by the Managed Folder Assistant due to a personal tag in the retention policy.
TotalItemsMovedByDefaultArchiveTag - Items moved due to a default Archive Tag	MSExchange Managed Folder Assistant	Indicates the number of items moved to the archive by the Managed Folder Assistant due to any non-personal (default or system) archive tag in a retention policy. This doesn't include the items moved to the Recoverable Items folder in archive by Recoverable Items cleanup.
TotalItemsMovedByPersonalArchiveTag - Items Moved due to an Archive Tag	MSExchange Managed Folder Assistant	Indicates the number of items moved to the archive by the Managed Folder Assistant due to a personal archive tag in a retention policy.
TotalMovedDumpsterItems - Mailbox Dumpsters Moved Items	MSExchange Managed Folder Assistant	Indicates the number of items moved to the Recoverable Items folder in the archive by Recoverable Items cleanup.

1.11.6.7.3 Messaging Records Management Errors and Events

Messaging Records Management Errors and Events

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-09*

Messaging records management (MRM) generates events that you can view in Event Viewer. This allows you to troubleshoot and verify the performance of the Managed Folder Assistant. Event Viewer tracks the following kinds of events in the following order, based on importance:

1. Error events
2. Warning events
3. Informational events

MRM Errors and Events

The following tables provide lists of events that you can use to troubleshoot MRM. The logging types include the following:

- Events labeled as **LogAlways** are always logged individually.
- Events labeled as **LogPeriodic** are logged only once in any five-minute period, not every time they occur. This helps to prevent excessive log entries.

MRM events in the Managed Folder Assistant category

Event ID	Category	Event type	Logging	Value or description
10001	Managed Folder Assistant	Error	LogAlways	The Managed Folder Assistant failed to provision mailbox *<display name, mailbox GUID, legacy DN>* because of damaged data in Active Directory. Exception details: *<details>*. To correct this, run the **Get-ManagedFolder** cmdlet and fix the errors reported.
10002	Managed Folder Assistant	Error	LogAlways	There was an invalid update to managed folder *<folder>* in Active Directory. You may resolve this by deleting and recreating the managed folder object.
10003	Managed Folder Assistant	Error	LogPeriodic	Could not get the server configuration object from Active Directory. *<Exception details>*. Check for domain controller network connectivity issues or incorrect DNS configuration.
10004	Managed Folder Assistant	Error	LogAlways	The retention policy for folder *<folder>* in mailbox *<mailbox>* will not be applied. The managed folder assistant is unable to process managed content setting *<content setting>*

				for the managed folder <*managed folder*>. The RetentionAction is MoveToFolder but a destination folder was not specified. Please specify a destination folder.
10005	Managed Folder Assistant	Error	LogAlways	Retention policy will not be applied to folder <*folder*> in mailbox <*mailbox*>. Unable to process Managed Content Setting <*content setting*> for the Managed Folder <*managed folder*>. The RetentionAction is MoveToFolder but the destination folder <*folder*> is the same as the source folder <*folder*>. Please specify a destination folder that is different from the source folder.
10006	Managed Folder Assistant	Error	LogAlways	Unable to apply the managed content setting on folder <*folder*> because the folder was not found in mailbox <*mailbox*>.
10007	Managed Folder Assistant	Error	LogAlways	The managed folder assistant will not process mailboxes on this server because one or more managed folders in Active Directory have invalid data. Please verify all the managed folders contained

				in the managed folders container in Active Directory. Exception details: *<details>*
10008	Managed Folder Assistant	Error	LogAlways	The retention policy for folder *<folder>* in mailbox *<mailbox>* will not be applied. The managed folder assistant is unable to process managed content setting *<setting>* for the managed folder *<folder>*. The RetentionAction is MoveToFolder but a destination folder was not specified. Please specify a destination folder.
10009	Managed Folder Assistant	Error	LogAlways	The managed folder assistant skipped processing all databases on the local server because it could not read the audit log parameters from Active Directory. It will try again later in the schedule window. Current database: *<database>*
10010	Managed Folder Assistant	Error	LogAlways	The managed folder assistant skipped processing all databases on the local server because the audit log is enabled but the path to the audit log is missing in Active Directory.

				It will try again later in the schedule window. Current database: *<database>*
10011	Managed Folder Assistant	Error	LogAlways	The managed folder assistant could not configure the audit log. It will stop processing the current database: '%1'. It will try again later in the schedule window. Exception details: *<details>*
10012	Managed Folder Assistant	Error	LogAlways	The managed folder assistant did not write to the audit log. It will stop processing the current database: *<database>*. It will try to write to the audit log again later in the schedule window. Exception details: *<details>*
10013	Managed Folder Assistant	Warning	LogAlways	The managed folder assistant was unable to provision the managed default folder *<folder>* in mailbox *<mailbox>* because it was not found in the mailbox.
10014	Managed Folder Assistant	Error	LogAlways	The managed folder assistant was unable to create the managed root folder *<folder>* in mailbox *<mailbox>* because the

				mailbox has several folders with the same name.
10015	Managed Folder Assistant	Error	LogAlways	The managed folder assistant detected a cycle among the policies in mailbox *<mailbox>* that will enforce retention by moving items to a destination folder and then back to the source folder. The policies involved are: *<policies>*
10016	Managed Folder Assistant	Error	LogPeriodic	Managed content setting *<setting>* will not be applied to mailbox *<mailbox>* because the AgeLimitForRetention is not greater than 0.
10017	Managed Folder Assistant	Error	LogAlways	An exception occurred in the Managed Folder Assistant while it was processing Mailbox: *<mailbox>* Folder: Name: *<folder name>* Id: *<folder ID>* Item: Ids: *<IDs>*. Exception: *<exception>*.

MRM events in the Assistants category

Event ID	Category	Event type	Logging	Value or description
9004	Assistants	Warning	LogAlways	Service *<service>*. *<service>* failed to process mailbox *<mailbox>*. The following exception caused the failure: *<exception>*

9014	Assistants	Warning	LogAlways	Service *<service>*. Unable to process schedule changes. The following exception caused the failure: *<exception>*
9017	Assistants	Information	LogAlways	Service *<service>*. *<service>* for database *<database>* is entering a scheduled time window. There are *<number>* mailboxes to process.
9018	Assistants	Information	LogAlways	Service *<service>*. *<service>* for database *<database>* is exiting a scheduled time window. *<number>* out of *<number>* mailboxes were successfully processed. *<number>* mailboxes were skipped due to errors. *<number>* mailboxes were processed separately. *<number>* mailboxes were not processed due to insufficient time. **Note:** The Managed Folder Assistant will resume where it left off the next time it runs.
9019	Assistants	Warning	LogPeriodic	Service *<service>*. Unable to save progress for *<service>* on database *<database>*. (The assistant was unable to save where it stopped

				so that it could resume there when it restarts.) The following exception caused the failure: *<exception>*
9020	Assistants	Warning	LogAlways	Service *<service>*. *<assistant name>* failed to start for database *<database>*. The following exception caused the failure: *<exception>*
9021	Assistants	Information	LogAlways	Service *<service>*. *<service>* for database *<database>* is processing an on-demand request. There are *<number>* mailboxes to process.
9022	Assistants	Information	LogAlways	Service *<service>*. *<service>* for database *<database>* has finished an on-demand request. *<number>* out of *<number>* mailboxes were successfully processed. *<number>* mailboxes were skipped due to errors.
9023	Assistants	Warning	LogAlways	Service *<service>*. *<service>* failed to start time window processing on database *<database>*. The following exception caused the failure: *<exception>*
9025	Assistants	Information	LogAlways	Service *<service>*. *<service>* skipped *<number>* mailboxes on

				database *<database>*. Mailboxes: *<mailboxes>*
9026	Assistants	Warning	LogAlways	Service *<service>*. *<service>* failed to start on-demand processing on database *<database>*. The following exception caused the failure: *<exception>*
9027	Assistants	Error	LogAlways	Service *<service>*. *<service>* caused the process to terminate *<number>* times while processing mailbox *<mailbox>* on database *<database>*. This mailbox will no longer be processed in the requested time window or on-demand request. The following exception caused the failure: *<exception>*
9028	Assistants	Warning	LogAlways	Service *<service>*. *<service>* caused the process to terminate *<number>* times while processing mailbox *<mailbox>* on database *<database>*. The following exception caused the failure: *<exception>*
9033	Assistants	Warning	LogAlways	Service *<service>*. *<service>* for database *<database>* received an on-demand request. However, there are no mailboxes to process.

9034	Assistants	Information	LogAlways	Service *<service>* halted time based operations for managed folder assistant on database *<database>*.
9035	Assistants	Warning	LogAlways	Service *<service>*. *<assistant name>* was unable to process *<number>* mailboxes because insufficient time.
9037	Assistants	Error	LogAlways	Service *<service>*. An exception was encountered while processing a RPC. Method: *<method>*, Exception: *<exception>*

1.11.6.8 Messaging Records Management Terminology in Exchange 2010

Messaging Records Management Terminology in Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-09*

The following table defines the core components associated with messaging records management (MRM) in Microsoft Exchange Server 2010. MRM is a records management technology in Exchange 2010 that helps organizations reduce the risks associated with e-mail and other communications. MRM makes it easier to keep messages needed to comply with company policy, government regulations, or legal needs, and to remove content that has no legal or business value.

default policy tag (DPT)

New with Exchange 2010, a DPT is a retention tag that applies to all items in a mailbox that don't already have a retention tag applied. You can have only one DPT in a retention policy.

filer user or filer

A user who regularly files mailbox items into folders.

Compare to piler user or piler.

journaling

The ability to record communications, including e-mail communications, in an organization for use in the organization's e-mail retention or archival strategy. In MRM, journaling commonly refers to the process of sending a journal report about messages in a managed folder to the specified SMTP address. This process is performed by the Managed Folder Assistant.

managed content settings

The retention information created for managed folders. A managed folder can have multiple content settings for different message types such as e-mail messages, voice mail, and calendar items. Message retention settings defined in content settings for a managed folder apply to messages in that managed folder.

managed folder

In the Exchange management interfaces (Exchange Management Console and Exchange Management Shell), a managed folder is an Active Directory object. In a mailbox, a managed folder is a folder to which managed content settings have been applied.

Managed Folder Assistant

One of the Microsoft Exchange Mailbox Assistants in Exchange 2010. The Managed Folder Assistant is responsible for message expiration and compliance. It processes mailboxes and applies retention policies and managed folder mailbox policies.

managed folder mailbox policy

A logical grouping of managed folders. When a managed folder mailbox policy is applied to a user's mailbox, all managed folders linked to the policy are deployed in a single operation.

personal tag

New with Exchange 2010, a personal tag is a retention tag available to Microsoft Office Outlook Web App and Microsoft Outlook 2010 users for applying retention settings to custom folders and individual items, such as e-mail messages.

piler user or piler

A user who doesn't file mailbox items regularly. Piler users tend to have a large Inbox and rely on search to find messages.

Compare to filer user or filer.

policy

See retention policy or managed folder mailbox policy.

retention policy tag (RPT)

New with Exchange 2010, an RPT is a retention tag that's applied to default folders such as Inbox and Deleted Items.

retention policy

New with Exchange 2010, a retention policy is logical grouping of retention tags. When a retention policy is applied to a user’s mailbox, all retention tags linked to the policy are deployed in a single operation.

retention tag

New with Exchange 2010, retention tags are used to apply retention settings to messages and folders to user mailboxes. There are three types of retention tags:

- Default policy tags (DPTs)
- Retention policy tags (RPTs)
- Personal tags

1.11.7 Discovery

Discovery

Exchange Server 2010 > Messaging Policy and Compliance >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-26*

Understanding Multi-Mailbox Search

Learn about the Multi-Mailbox Search feature that enables authorized users to search mailboxes across your Exchange 2010 organization.

Managing Discovery

Learn how to manage Multi-Mailbox Search.

1.11.7.1 Understanding Multi-Mailbox Search

Understanding Multi-Mailbox Search

Exchange Server 2010 > Messaging Policy and Compliance > Discovery >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-10*

If your organization adheres to legal discovery requirements (related to organizational policy, compliance, or lawsuits), Microsoft Exchange Server 2010 Multi-Mailbox Search can help you perform discovery searches for relevant content within Exchange mailboxes.

Multi-Mailbox Search uses the content indexes created by Exchange Search. The Exchange Control Panel (ECP) provides an easy-to-use search interface for non-technical personnel such as legal and compliance officers, records managers, and human resources (HR) professionals. Role Based Access Control (RBAC) provides the Discovery Management management role group to delegate discovery tasks to non-technical personnel, without the need to provide elevated privileges that may allow a user to make any operational changes to Exchange configuration.

Contents

Looking for management tasks related to Multi-Mailbox Search? See Managing Discovery.

Uses for Multi-Mailbox Search

The following are common uses of Multi-Mailbox Search:

- **Legal discovery** Complying with legal discovery requests for messaging records is one of the most important tasks for organizations involved in lawsuits. Without a dedicated tool, searching messaging records within several mailboxes that may reside in different mailbox databases can be a time-consuming and resource-intensive task. Using Multi-Mailbox Search, you can search a large volume of e-mail messages stored in mailboxes across one or more Exchange 2010 servers, and possibly in different locations.
- **Internal investigations** Multi-Mailbox Search can help you facilitate requests from managers or legal departments as part of internal investigations.
- **Human Resources monitoring** Multi-Mailbox Search can help you facilitate HR requests, such as standard e-mail monitoring requirements or a specific search.

Return to top

Exchange Search and Advanced Query Syntax

Multi-Mailbox Search uses the content indexes created by Exchange Search. To provide the extensive search functionality required by Multi-Mailbox Search, new capabilities have been added to Exchange Search. With a single content indexing engine, no additional resources are used to crawl and index mailbox databases for Multi-Mailbox Search when discovery requests are received by IT departments.

To learn more about Exchange Search, see Understanding Exchange Search.

Multi-Mailbox Search also uses Advanced Query Syntax (AQS), the familiar query syntax used by Windows Search and Instant Search in Microsoft Office Outlook 2007 and Outlook 2010. Users proficient with AQS can easily construct powerful search queries to search content indexes.

For more information about AQS, see Using Advanced Query Syntax Programmatically.

Return to top

Discovery Management Role Group and Management Roles

For users to perform discovery searches, you must add them to the Discovery Management RBAC role group. This role group consists of two management roles: the Mailbox Search role, which allows a user to perform a discovery search, and the Legal Hold role, which allows a user to place a mailbox on litigation hold. To learn more about the Discovery Management RBAC role group, see Discovery Management. To learn more about RBAC, see Understanding Role Based Access Control.

By default, the Discovery Management role group doesn't have any members. The permissions to perform discovery-related tasks aren't assigned to any user. Also, by default, Exchange administrators don't have the permissions to perform a discovery search. Exchange administrators who are members of the Organization Management management role group can add users to the Discovery Management role group and

create custom role groups to narrow the scope of a discovery manager to a subset of users. Auditing of RBAC role changes makes sure that adequate records are kept to track assignment of the Discovery Management role group. For details, see Overview of Administrator Audit Logging.

Important:
If a user hasn't been added to the Discovery Management role group or isn't assigned the Mailbox Search role, the Multi-Mailbox Search user interface isn't displayed to the user in the ECP, and the Multi-Mailbox Search cmdlets aren't available in the Exchange Management Shell.

For more information about adding users to the Discovery Management role group, see Add a User to the Discovery Management Role Group.

Caution:
Multi-Mailbox Search is a powerful feature that allows a user with the appropriate permissions to potentially have access to all messaging records stored throughout the Exchange 2010 organization. It's important to control and monitor discovery activities, including addition of members to the Discovery Management role group or any other role group with the Mailbox Search management role, assignment of the Mailbox Search management role, and assignment of mailbox access permission to discovery mailboxes.

Return to top

Discovery Mailboxes

When performing a discovery search, you must specify a target mailbox in which to store the search results. A discovery mailbox is a special type of Exchange 2010 mailbox that provides the following functionality:

- **Easier and secure target mailbox selection** When you use the ECP to create a discovery search, only discovery mailboxes are made available as a repository in which to store search results. You don't need to sort through a potentially long list of mailboxes available in the organization. This also eliminates the possibility of a discovery manager accidentally selecting another user's mailbox or an unsecured mailbox in which to store potentially sensitive message content.
- **Large mailbox storage quota** The target mailbox should be able to store a large amount of message data that may be returned by a discovery search. By default, discovery mailboxes have a mailbox storage quota of 50 gigabytes (GB). You can modify the quota to suit your requirements.

  Note:
  In Exchange 2010 Service Pack 1 (SP1), a discovery manager can get an estimate of search results to determine the total number and size of items returned by a discovery search.

- **Secure by default** Like all mailbox types, a discovery mailbox has an associated Active Directory user account. However, this account is disabled by default. Only users explicitly authorized to access a discovery mailbox have access to it. Members of the Discovery Management role group are assigned Full Access permissions to the default discovery mailbox. Any additional discovery mailboxes you create don't have mailbox access permissions assigned to any user.

  Important:
  In Exchange 2010 SP1, you can enable mailbox audit logging to audit access to mailboxes and actions such as folder or message access and deletions by mailbox owners, delegates, and administrators. For more details, see Understanding Mailbox Audit Logging.

- **E-mail delivery disabled** Although visible in Exchange address lists, users can't send e-mail to a discovery mailbox. E-mail delivery to discovery mailboxes is prohibited by using delivery restrictions. This preserves the integrity of search results.

Exchange 2010 Setup creates one discovery mailbox with the display name **Discovery Search Mailbox**. You can use the Shell to create additional discovery mailboxes. By default, the additional discovery mailboxes you create won't have any mailbox access permissions assigned. For details about how to create a discovery mailbox, see Create a Discovery Mailbox.

Multi-Mailbox Search also uses a system mailbox with the display name **SystemMailbox {e0dc1c29-89c3-4034-b678-e6c29d823ed9}** to hold Multi-Mailbox Search metadata. System mailboxes aren't visible in the Exchange Management Console (EMC) or in Exchange address lists. Before removing a mailbox database where the Multi-Mailbox Search system mailbox is located, you must move the mailbox to another mailbox database.

Return to top

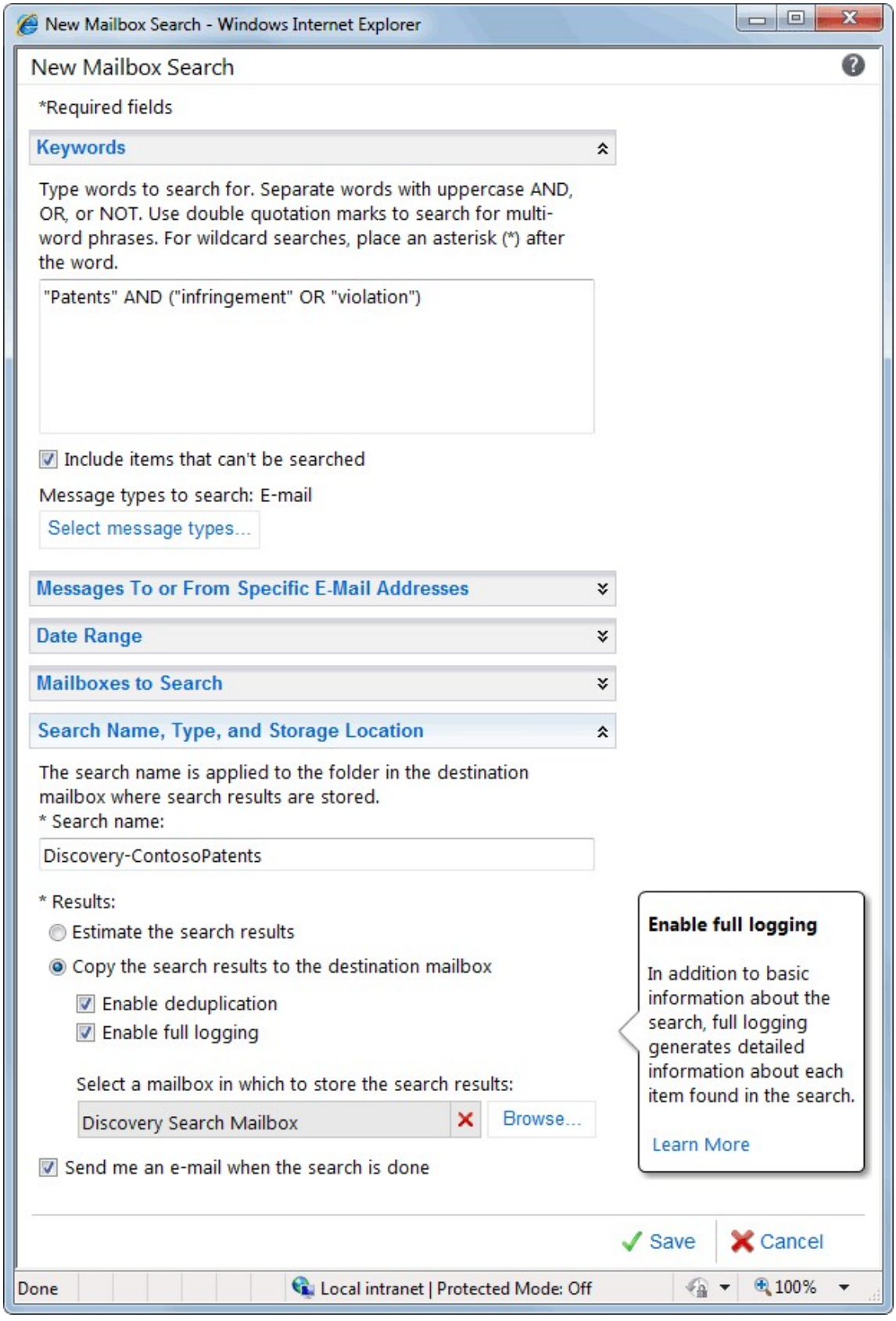
Performing a Discovery Search

Users who have been added to the Discovery Management role group can perform discovery searches. To learn more about the Discovery Management role group, see Discovery Management Role Group and Management Roles earlier in this topic.

You can perform a discovery search using the Web-based interface in the ECP, as shown in the following figure. This makes it easier for non-technical users such as records managers, compliance officers, or legal and HR professionals to use Multi-Mailbox Search. You can also use the Shell to perform discovery searches.

Note:

In a hybrid deployment, which is an environment where some mailboxes exist on your on-premises Mailbox servers and some mailboxes exist in a cloud-based organization, you can perform discovery searches of your cloud-based mailboxes using the ECP in your on-premises organization. If you intend to copy messages to a discovery mailbox, you must select an on-premises discovery mailbox. Messages from cloud-based mailboxes that are returned in search results are copied to the specified on-premises discovery mailbox. For more details about hybrid deployments, see Understanding Hybrid Deployment.


New Mailbox Search - Windows Internet Explorer
New Mailbox Search
*Required fields
Keywords
Type words to search for. Separate words with uppercase AND, OR, or NOT. Use double quotation marks to search for multi-word phrases. For wildcard searches, place an asterisk (*) after the word.
"Patents" AND ("infringement" OR "violation")
Include items that can't be searched
Message types to search: E-mail
Select message types...
Messages To or From Specific E-Mail Addresses
Date Range
Mailboxes to Search
Search Name, Type, and Storage Location
The search name is applied to the folder in the destination mailbox where search results are stored.
* Search name:
Discovery-ContosoPatents
* Results:
Estimate the search results
Copy the search results to the destination mailbox
Enable deduplication
Enable full logging
Select a mailbox in which to store the search results:
Discovery Search Mailbox
Browse...
Send me an e-mail when the search is done
Enable full logging
In addition to basic information about the search, full logging generates detailed information about each item found in the search.
Learn More
Save
Cancel
Done
Local intranet | Protected Mode: Off
100%

When performing a search, a search object is created in Exchange 2010. This object can be manipulated to start, stop, modify, and remove the search. Items returned by a discovery search are copied to the discovery mailbox selected as the target mailbox for the search. Multiple searches can run concurrently.

Note:

Multi-Mailbox Search is an Exchange 2010 feature. Only mailboxes located on Exchange 2010 servers can be searched using Multi-Mailbox Search. You can search a maximum of 25,000 mailboxes in a single search. To search more than 25,000 mailboxes, you can split the search into multiple searches. For example you can search mailboxes of users in a distribution group or a dynamic distribution group.
Multi-Mailbox Search doesn't search messages in .pst files. To decrease management and legal discovery costs, we recommend provisioning archive mailboxes for users. To learn more about archive mailboxes, see Understanding Personal Archives.

The following applies to performing a discovery search:

- **Keywords** You can specify keywords and phrases to search message content. You can also use the logical operators **AND**, **OR**, and **NOT**. To search for an exact match of a multiple word phrase, you must enclose the phrase in quotation marks. For example, searching for the phrase **"plan and competition"** returns messages that contain an exact match of the phrase, whereas specifying **plan AND competition** returns messages that contain the words **plan** and **competition** anywhere in the message. You can also use AQS. For details, see Using Advanced Query Syntax Programmatically. For more information about advanced keyword searches, see Advanced Keyword Searches.

  Note:

  Multi-Mailbox Search doesn't support regular expressions.

  You must capitalize logical operators such as **AND** and **OR** for them to be treated as operators instead of keywords. We recommend that you use explicit parenthesis for any query that mixes multiple logical operators (AND, OR, NOT, etc.) to avoid mistakes or misinterpretations. For example, if you want to search for messages that contain either WordA or WordB AND either WordC or WordD, you must use **(WordA OR WordB) AND (WordC OR WordD)**.
- **Senders or recipients** To narrow a search, you can specify the senders or recipients of messages. You can use e-mail addresses, display names, or the name of a domain to search for items sent to or from everyone in the domain. For example, to find e-mail sent by anyone to Contoso, Ltd, specify **@contoso.com** in the **From** field in the ECP. You can also specify **@contoso.com** in the *Senders* parameter in the Shell.
- **Date range** By default, Multi-Mailbox Search doesn't limit searches by a date range. To search for messages sent during a specific date range, you can narrow the search by specifying the start and end dates. If you don't specify an end date, the search will return the latest results every time you restart it.
- **Mailboxes** Multi-Mailbox Search can search all mailboxes located on Exchange 2010 Mailbox servers in the Exchange organization, or you can specify the mailboxes to be searched. You can also specify a distribution group to include mailbox users who are members of the group.
- **Personal archive** By default, if the personal archive is enabled for a mailbox user, Multi-Mailbox Search also searches the archive mailbox. There's no option in the ECP to override this. To exclude archive mailboxes, you must use the Shell to create or modify the search.
- **Message types** By default, only e-mail messages are searched. However, you can also include the following message types to search: contacts, documents, instant messaging conversations, journal, meetings, and notes.
- **Attachments** Multi-Mailbox Search searches attachments supported by Exchange Search. Support for additional file types can be added by installing

search filters (also known as an iFilter) for the file type on Mailbox servers.

- **Unsearchable items** Unsearchable items are mailbox items that can't be indexed by Exchange Search. Reasons include lack of an installed search filter for an attached file, a filter error, and encrypted messages. When creating a discovery search, you can include unsearchable items in search results.
- **Safe list** Certain file types don't contain content that can be indexed and, as a result, aren't indexed by Exchange Search. These file types aren't considered unsearchable items. Mailbox items containing these file types aren't returned in the list of unsearchable items. For more details, see Default Filters for Exchange Search.
- **Encrypted items** Because messages encrypted using S/MIME aren't indexed by Exchange Search, Multi-Mailbox Search doesn't search these messages. If you select the option to include failed items in search results, these S/MIME-encrypted messages are returned as failed items.
- **IRM-protected items** Messages protected using Information Rights Management (IRM) are indexed by Exchange Search and therefore included in discovery search results. Messages must be protected by using an Active Directory Rights Management Services (AD RMS) server in the same Active Directory forest as the Exchange 2010 Mailbox server. For more information about IRM, see Information Rights Management.

  Important:

  When Exchange Search fails to index an IRM-protected message, either due to a decryption failure or because IRM is disabled, the protected message isn't added to the list of failed items. If you select the option to include failed items in search results, the results may not include protected messages that couldn't be decrypted.
  To include IRM-protected messages in a search, you can create another discovery search to return messages with .rpmsg attachments. You can use the query string `attachment:rpmsg` to search all protected messages. This will return all IRM-protected messages from the mailboxes searched, whether indexed or not. This may result in some duplication of search results in scenarios where one search returns messages that match the search criteria, including protected messages that have been indexed successfully. The search doesn't return protected messages that couldn't be indexed. Performing a second search for all protected messages also includes protected messages that were successfully indexed and returned by the first search. Additionally, the protected messages returned by the second search may not match the search criteria such as keywords used for the first search.

- **Deduplication** In Exchange 2010 SP1, you can enable *deduplication* of discovery search results to copy only one instance of a unique message to the discovery mailbox. Deduplication has the following benefits:
  - Lower storage requirement and smaller discovery mailbox size due to reduced number of messages copied.
  - Reduced workload for discovery managers, legal counsel, or others involved in reviewing discovery search results.
  - Reduced cost of discovery, depending on the number of duplicate items in search results.

  If you select a discovery mailbox located on an Exchange 2010 server that hasn't been upgraded to Exchange 2010 SP1, deduplication of search results isn't performed. To use deduplication, you must select a discovery mailbox located on an Exchange 2010 SP1 Mailbox server.
- **Search result estimates** When creating a discovery search in Exchange 2010 SP1, the discovery manager can select the option to estimate the search results before deciding whether to copy messages returned by the search to the discovery mailbox. The search result estimate includes the total number of items returned by the search, their total size, and a breakdown of items returned for each keyword specified. A search estimate provides the following benefits:
  - The discovery manager can determine the effectiveness of the search query.

Using search estimates, a discovery manager can perform a **what-if** analysis of search queries and keywords, and then create more effective queries.

- The discovery manager can avoid copying a large number of items that may not meet the requirements or the purpose of the search, but still need to be reviewed.
- In scenarios where a search query results in a large number of items that need to be copied, the discovery manager can work with the Exchange administrator to determine if adequate storage is available to store the results in the discovery mailbox.

Note:

Deduplication isn't considered when calculating search result estimates. When you run the search again with the option to copy messages to a discovery mailbox, the actual number of messages copied may be less than the estimate provided when you use the estimate-only option.

For details about how to perform a discovery search, see Create a Discovery Search.

Return to top

Viewing Search Results

Search results are copied to the discovery mailbox selected as the target mailbox for the search. If you use a target mailbox other than the default Discovery Search Mailbox, you must assign mailbox access permissions to authorized users so they can access that discovery mailbox. Authorized users can access the mailbox using Microsoft Office Outlook Web App or Outlook.

For information about how to assign Full Access mailbox permissions for a mailbox, see Manage Full Access Permissions.

If a discovery manager selects the option to copy search results to a discovery mailbox, a folder with the same name as the search is created in the target mailbox. To store messages returned from that mailbox, a subfolder is created for each mailbox searched. The folder name consists of the mailbox user's display name along with the date and time when the search was created. Messages are copied to a folder that has the same name as their location in the searched mailbox. For example, if the search name is Discovery-ProjectContoso, and a message located in the Inbox folder in Paul Shen's primary mailbox is returned, the folder hierarchy created in the discovery mailbox would be **Discovery-ProjectContoso -> Paul Shen-9/4/2009 3:57:10 PM -> Primary Mailbox > Inbox**. Any message flags, including read/unread status and follow-up flags, are maintained.

Note:

If the discovery manager selects the deduplication option, a single instance of messages found in multiple locations across all mailboxes searched is copied to the **Results - <timestamp>** folder. If the discovery manager selects the full logging option for the search, the search log contains an entry for each instance of the message.

Annotations

In Exchange 2010 SP1, when a discovery manager reviews messages copied to a discovery mailbox, he or she can add annotations to the message. The discovery manager can then search the discovery mailbox for messages with annotations containing specific words or phrases.

Discovery managers can use annotations to associate a case number or another unique identifier with a message, making it easy to search for all items with that number.

Note:

Annotations are stored with the message in the discovery mailbox. If you deliver messages to a third party, consider that the information in annotations may be accessible

to the third party. We recommend that you not store any confidential information in annotations.

Return to top

Logging of Discovery Searches

There are two types of logging available for discovery searches:

- **Basic logging** Basic logging is enabled by default for all mailbox searches. It includes information about the search and who performed it. Information captured about basic logging appears in the body of the e-mail message sent to the mailbox where the search results are stored. This message is located in the folder created to store search results.
- **Full logging** Full logging includes information about all messages returned by the search. This information is provided in a comma-separated value (.csv) file attached to the e-mail message that contains basic logging information. The name of the search is used for the .csv file name. This information may be required for compliance or record-keeping purposes. To enable full logging, you must select **Enable full logging** in the ECP or specify the logging level using the *LogLevel* parameter in the Shell. In Exchange 2010 SP1, the .csv log file is included in a compressed (.zip) file.

Note:

When using the Shell to create or modify a search, you can also disable logging.

For details, see Multi-Mailbox Search Logging.

Return to top

Litigation Hold and Discovery

As part of discovery requests, you may be required to preserve mailbox content until a lawsuit is disposed. To preserve mailbox content, messages deleted or altered by the mailbox user must also be preserved. In Exchange 2010, this is accomplished by using litigation hold.

When a mailbox is placed on litigation hold, messages and other mailbox items deleted by the user, and all instances of changes made to certain properties of mailbox items, are preserved in the Recoverable Items folder. To learn more about litigation hold, see Understanding Litigation Hold. For details about how to place a mailbox on litigation hold, see Place a Mailbox on Litigation Hold.

Return to top

Preserving Mailboxes for Discovery

When an employee leaves an organization, it's a common practice to disable or remove the mailbox. After you disable a mailbox, it is disconnected from the user account but remains in the mailbox database for a certain period, 30 days be default. The Managed Folder Assistant does not process disconnected mailboxes and any retention policies or managed folder mailbox policies are not applied during this period. You can't search content of a disconnected mailbox. Upon reaching the deleted mailbox retention period, the mailbox is purged from the mailbox database.

If your organization requires that retention settings be applied to messages of employees who are no longer in the organization or if you may need to retain an ex-employee's

mailbox for an ongoing or future discovery search, you must not disable or remove the mailbox. You can take the following steps to ensure the mailbox can't be accessed and no new messages are delivered to it.

1. Disable the Active Directory user account using **Active Directory Users & Computers** or other Active Directory or account provisioning tools or scripts. This prevents mailbox logon using the associated user account.

   Important:

   Users with full access mailbox permission will still be able to access the mailbox. To prevent access by others, you must remove their full access permission from the mailbox. For more information about how to remove Full Access permissions on a mailbox, see Manage Full Access Permissions.

2. Set the message size limit for messages that can be sent from or received by the mailbox user to a very low value, 1 KB for example. This prevents delivery of new mail to and from the mailbox. For more information about how to configure message size limits for a mailbox, see Configure Message Size Limits for a Mailbox or a Mail-Enabled Public Folder.
3. Configure delivery restrictions for the mailbox so nobody can send messages to it. For details, see Configure Message Delivery Restrictions

Important:

You must take the above steps along with any other account management processes required by your organization, but without disabling or removing the mailbox or the associated user account.

When planning to implement mailbox retention for messaging retention management or discovery, you must take employee turnover into consideration. Long-term retention of ex-employee mailboxes will require additional storage on Mailbox servers and also result in an increase in Active Directory database because it requires that the associated user account be retained for the same duration. Additionally, it may also require changes to your organization's account provisioning and management processes.

1.11.7.2 Managing Discovery

Managing Discovery

Exchange Server 2010 > Messaging Policy and Compliance > Discovery >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-01-28*

Add a User to the Discovery Management Role Group

Create a Discovery Search

Start or Stop a Discovery Search

Modify a Discovery Search

Remove a Discovery Search

Create a Discovery Mailbox

Use Mailbox Search to Delete Messages

Re-create Discovery and Other System Mailboxes in Exchange 2010

1.11.7.2.1 Add a User to the Discovery Management Role Group

Add a User to the Discovery Management Role Group

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

If you want users to be able to use Microsoft Exchange Server 2010 Multi-Mailbox Search, you need to add them to the Discovery Management role group. Members of the Discovery Management role group have Full Access mailbox permission for the Discovery Search Mailbox that's created by Exchange Setup.

Note:

Be default, the Discovery Management role group doesn't have any members. Administrators with the Organization Management role are also unable to create or manage discovery searches without being added to the Discovery Management role group.

For more information about the Discovery Management role group, see Discovery Management.

For more information about Role Based Access Control (RBAC), see Understanding Role Based Access Control.

Looking for other management tasks related to Multi-Mailbox Search? Check out Managing Discovery.

Use the Shell to add a user to the Discovery Management role group

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Role groups" entry in the Role Management Permissions topic.

Note:

You can't use the EMC to add a user to the Discovery Management role group.

This example adds the user EAdams to the Discovery Management role group.

```
Add-RoleGroupMember -Identity "Discovery Management" -Member Eadams
```

Other Tasks

After you add a user to the Discovery Management role group, you may also want to:

- Create a Discovery Search
- Start or Stop a Discovery Search
- Remove a Discovery Search

Create a Discovery Search

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use Exchange Management Shell cmdlets or the Exchange Control Panel (ECP) to create a discovery search. Search results are copied to the discovery mailbox selected as the target mailbox for the search.

Looking for other management tasks related to search? Check out Managing Discovery.

Caution:

Not specifying any source mailboxes to search will result in searching all mailboxes on all Exchange 2010 servers in the entire Exchange organization.
Not specifying a search query will result in the entire content of the specified mailboxes being copied to the target mailbox.
Depending on the scope of the search and the number and size of items returned, the discovery mailbox you select to store search results can potentially grow to a large size. Make sure the disk volumes where the mailbox database and transaction logs are located have adequate free space.
If you use mailbox quotas to limit mailbox sizes, be sure to configure the target mailbox with an adequate quota limit to allow sufficient storage for items returned by the search.

What Do You Want to Do?

- Create a New Multi-Mailbox Search
- Use the Shell to create a discovery search

Use the Shell to create a discovery search

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Multi-Mailbox Search" entry in Messaging Policy and Compliance Permissions topic.

This example creates the discovery search Contoso-Case1. The search will return e-mail messages that meet the following conditions:

- Contain the words Contoso and Project A
- Sent or received from January 1, 2009, through December 31, 2009

The search is run against all mailboxes within all Exchange 2010 Mailbox servers in the organization. Search results will be saved in the mailbox Discovery Search Mailbox, in a folder with the same name as the search. Full logging is enabled for the search.

```
New-MailboxSearch -Name "Contoso-Case1" -StartDate "1/1/2009" -EndDate "12/31/200
```

For detailed parameter and syntax information, see New-MailboxSearch.

Note:

By default, a discovery search doesn't include items that can't be indexed by Exchange Search. To include such items in the search results, the *IncludeUnsearchableItems* switch is included in the preceding command.

Other Tasks

After you create a discovery search, you may also want to:

- Start or Stop a Discovery Search
- Modify a Discovery Search
- Remove a Discovery Search

1.11.7.2.3 Start or Stop a Discovery Search

Start or Stop a Discovery Search

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can stop or restart a discovery search at any time. For example, if you want to modify search properties such as keywords or mailboxes searched, you must first stop a search. You can then restart the search after making the required changes.

Looking for other management tasks related to search? Check out Managing Discovery.

Use the Shell to start or stop a discovery search

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the 'Multi-Mailbox Search' entry in Messaging Policy and Compliance Permissions topic.

This example stops the search Discovery-ProjectContoso

```
Stop-MailboxSearch -Name "Discovery-ProjectContoso"
```

This example starts the stopped search Discovery-ProjectContoso.

```
Start-MailboxSearch -Name "Discovery-ProjectContoso"
```

For detailed parameter and syntax information, see Start-MailboxSearch and Stop-MailboxSearch.

Use the ECP to start or stop a discovery search

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the 'Multi-Mailbox Search' entry in Messaging Policy and Compliance Permissions topic.

1. Navigate to **My Organization** > **Reporting** > **Mailbox Searches**.
2. To stop a search that's in progress, select the search, and then click the **Stop Search** icon.
3. To start a search that was stopped, select the search, and then click the **Restart Search** icon. A warning appears, stating that the existing search will be removed from the target mailbox. Click **Yes**.

Other Tasks

After you start a discovery search, you may also want to:

- Modify a Discovery Search
- Remove a Discovery Search

1.11.7.2.4 Modify a Discovery Search

Modify a Discovery Search

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After you create a discovery search, you can modify it to change the search parameters. For example, you can change the mailboxes to be searched, date ranges, key words, logging options, or you can specify a different discovery mailbox to store search results. Any changes you make to the search properties will be used when you restart the search.

You can use the Shell to modify a discovery search. However, you can also use the Exchange Control Panel for the same task. For instructions about using the Exchange Control Panel to modify a discovery search, see Edit a Mailbox Search.

Looking for other management tasks related to managing Multi-Mailbox Search? Check out Managing Discovery.

Caution:

If a discovery search is running, you must stop it before modifying it. When you restart the search, the results from the last time the search was run are removed from the discovery mailbox. However, the logs from previous searches are saved.

Prerequisites

A discovery search has been created and isn't running.

Use the Shell to modify a discovery search

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Multi-Mailbox Search" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the EMC to modify a discovery search.

This example modifies the discovery search Search-Project Contoso to search mailboxes belonging to members of the DG-ProjectManagers distribution group.

```
Set-MailboxSearch -Identity "Search-Project Contoso" -SourceMailboxes "DG-Project
```

For detailed syntax and parameter information, see Set-MailboxSearch.

Other Tasks

After you modify a discovery search, you may also want to:

- Remove a Discovery Search
- Start or Stop a Discovery Search

1.11.7.2.5 Remove a Discovery Search

Remove a Discovery Search

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Microsoft Exchange Server 2010, you can use Multi-Mailbox Search to create a discovery search. You can remove a discovery search at any time. When you remove a discovery search, search results are removed from the discovery mailbox.

Looking for other management tasks related to Multi-Mailbox Search? Check out Managing Discovery.

Use the Shell to remove a discovery search

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Multi-Mailbox Search" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to remove a discovery search.

This example removes the discovery search Discovery-ProjectContoso.

```
Remove-MailboxSearch "Discovery-ProjectContoso"
```

For detailed syntax and parameter information, see Remove-MailboxSearch.

Use the Exchange Control Panel to remove a discovery search

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Multi-Mailbox Search" entry in the Messaging Policy and Compliance Permissions topic.

1. Navigate to **My Organization** > **Reporting** > **Mailbox Searches**.
2. Select the search you want to remove, and then click  .

Other Tasks

After you remove a discovery search, you may also want to create a discovery search. For detailed steps, see Create a Discovery Search.

1.11.7.2.6 Create a Discovery Mailbox

Create a Discovery Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Microsoft Exchange Server 2010 Setup creates a Discovery mailbox by default. Discovery mailboxes are available as target mailboxes for discovery searches in the Exchange Control Panel. You can create additional Discovery mailboxes as required. A Discovery mailbox can't be repurposed or converted to another type of mailbox. You can remove a Discovery mailbox using the same procedure used to remove other types of mailboxes.

Caution:
After a discovery search is completed, the Discovery mailbox used as a target mailbox for the search can potentially contain sensitive information. You should control access to Discovery mailboxes and ensure only authorized persons have access to them.

Looking for other management tasks related to Multi-Mailbox Search? Check out Managing Discovery.

Use the Shell to create a Discovery mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Creating discovery mailboxes" entry in Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to create a Discovery mailbox.

This example creates the Discovery mailbox SearchResults using the **New-Mailbox** cmdlet with the `Discovery` switch.

```
New-Mailbox SearchResults -Discovery -UserPrincipalName SearchResults@contoso.com
```

For detailed syntax and parameter information, see New-Mailbox.

This example lists Discovery mailboxes in an Exchange organization.

```
Get-Mailbox -Resultsize unlimited -Filter {RecipientTypeDetails -eq "DiscoveryMai
```

Other Tasks

After you create a Discovery mailbox, you may also want to:

- Add a User to the Discovery Management Role Group
- Create a Discovery Search

1.11.7.2.7 Use Mailbox Search to Delete Messages

Use Mailbox Search to Delete Messages

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Exchange 2010 Service Pack 1 (SP1), you can use the **Search-Mailbox** cmdlet to search for and delete messages from a mailbox.

To search for and delete messages in one step, run the **Search-Mailbox** cmdlet with the *DeleteContent* switch. However, when you do this, you can't preview search results or generate a log of messages that will be returned by the search. To preview a log of the messages found in the search before they're deleted, you can run the **Search-Mailbox** cmdlet with the *LogOnly* switch.

As an additional safeguard, you can first copy the messages to another mailbox by using the *TargetMailbox* and *TargetFolder* parameters. By doing this, you retain a copy of the deleted messages in case you need to access them again.

Looking for other management tasks related to discovery? Check out Managing Discovery.

Prerequisites

- If the mailbox from which you want to delete messages has single item recovery enabled, you must first disable the feature. For details, see Enable Single Item Recovery for a Mailbox.
- If the mailbox from which you want to delete messages is placed on litigation hold, we recommend that you check with your records management or legal department before removing the hold and deleting the mailbox content. After you obtain approval, follow the steps listed in the topic Clean Up the Recoverable Items Folder.

Use the Shell to search for messages and log the search results

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Delete mailbox content" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the Exchange Management Console (EMC) to search for messages and log search results.

This example searches April Stewart's mailbox for messages that contain the phrase "Your bank statement" in the Subject field and logs the search results in the SearchAndDeleteLog folder of the administrator's mailbox. Messages aren't copied to or deleted from the target mailbox.

Note:
The *LogOnly* parameter is available only in Exchange 2010 SP1.

```
Search-Mailbox -Identity "April Stewart" -SearchQuery "Subject:'Your bank stateme
```

For detailed syntax and parameter information, see Search-Mailbox.

Use the Shell to search for and delete messages

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Delete mailbox content" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the Exchange Management Console (EMC) to search for and delete messages.

This example searches April Stewart's mailbox for messages that contain the phrase "Your bank statement" in the Subject field and deletes the messages from the source mailbox without copying the search results to another folder.

Important:
When you use the **Search-Mailbox** cmdlet with the *DeleteContent* switch, messages are permanently deleted from the source mailbox. Before you permanently delete messages, we recommend that you either use the *LogOnly* switch to generate a log of the messages found in the search before they're deleted or copy the messages to another mailbox before deleting them from the source mailbox.

```
Search-Mailbox -Identity "April Stewart" -SearchQuery "Subject:'Your bank stateme
```

This example searches April Stewart's mailbox for messages that contain the phrase "Your bank statement" in the Subject field, copies the search results to the folder AprilStewart-DeletedMessages in the mailbox BackupMailbox, and deletes the messages from April's mailbox.

```
Search-Mailbox -Identity "April Stewart" -SearchQuery "Subject:'Your bank stateme
```

For detailed syntax and parameter information, see Search-Mailbox.

1.11.7.2.8 Re-create Discovery and Other System Mailboxes in Exchange 2010

Re-create Discovery and Other System Mailboxes in Exchange 2010

See Also

Messaging Policy and Compliance > Discovery > Managing Discovery >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-14*

This article describes how to re-create and enable missing Discovery and other system mailboxes in Microsoft Exchange Server 2010.

Arbitration user accounts and mailboxes are created when you run the Setup.com /PrepareAD command to prepare Active Directory as part of the Exchange 2010 installation. Arbitration mailboxes are used for managing approval workflow. For example, an arbitration mailbox is used for handling moderated recipients and distribution group membership approval.You can find the Arbitration user accounts in the Users Organizational Unit (OU) in Active Directory. The accounts resemble the following:

- SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9} – This account is used by the Multi-Mailbox Search process to store discovery search metadata.
- FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042 – This account is used for federated mail.
- SystemMailbox{1f05a927-af78-475a-aba4-fc281398eb54} – This account is used for moderated transport.
- DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852} – This account is used as the target mailbox for discovery searches in the exchange control panel. Discovery search is used when you search for emails across all the mailboxes.

Because system mailboxes are not visible in the Exchange Management Console (EMC) or in Exchange address lists, they are rarely deleted accidentally.

If a system mailbox is deleted accidentally, features that rely on that mailbox no longer work. For example, if the Discovery system mailbox is deleted accidentally, the search process does not function correctly, and discovery managers can no longer perform searches or manage existing searches. To enable the discoverability functionality in this case, you must re-create the Discovery system mailbox.

For more information about the Discovery process, see Managing Discovery.

For more information about Arbitration mailboxes, see Understanding Moderated Transport.

Use the Exchange Management Shell to re-create the system mailboxes and user accounts

1. You must first delete the user accounts for the accidentally deleted mailboxes from Active Directory. By default, Exchange 2010 Setup creates system mailboxes in the Users container in Active Directory. For example, the account that was deleted may resemble one of the following:
   - SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}
   - SystemMailbox{1f05a927-af78-475a-aba4-fc281398eb54}
   - FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042
   - DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}

   For more information about how to delete a user account from Active Directory, see Delete a User Account.
2. Prepare Active Directory. To do this, run Microsoft Exchange 2010 Setup by using the **/PrepareAD** switch in the root domain of your Active Directory forest. For more information, see Prepare Active Directory and Domains.
3. Make sure that you enable the mailbox only for the accounts that were re-created. You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

The following example describes how to enable the Arbitration and Discovery system mailboxes:

```
Enable-Mailbox -Arbitration -Identity "FederatedEmail.4c1f4d8b-8179-4148-93bf-00a
Enable-Mailbox -Arbitration -Identity "SystemMailbox{1f05a927-8668-4003-adad-9b80
Enable-Mailbox -Arbitration -Identity "SystemMailbox{e0dc1c29-89c3-4034-b678-e6c2
Enable-Mailbox -Discovery "DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E0933
```

To set the correct display for the **SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}** mailbox, you can use the Set-Mailbox command. For example, run the following command:

```
Set-Mailbox -Arbitration -Identity "SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d8
```

If you have re-created the FederatedEmail system mailbox, you can reset the default quota for the **FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042** mailbox by using the Set-Mailbox command. For example, run the following command:

```
Set-Mailbox -Arbitration -Identity "FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95f
```

To determine whether the Enable-Mailbox and Set-Mailbox commands were applied correctly, you can use the Get-Mailbox command. Run the following command to verify the status of the Arbitration mailboxes:

```
Get-Mailbox -Arbitration
```

If the Enable-Mailbox and Set-Mailbox commands were applied correctly, the following results are returned.

Name	Alias	ServerName	ProhibitSendQuota
SystemMailbox {e0dc1c29-89c3-4034-b678-e6c29d823ed9}	SystemMailbox {e0dc1c29-89c3-4034-b678-e6c29d823ed9}	*EXch1*	Unlimited
FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	*EXch1*	Unlimited
SystemMailbox {1f05a927-af78-475a-aba4-fc281398eb54}	SystemMailbox {1f05a927-af78-475a-aba4-fc281398eb54}	*EXch1*	1 MB (1,048,576 bytes)

Run the following command to verify the status of the DiscoverySearchMailbox mailbox:

```
Get-Mailbox -Identity DiscoverySearchMaibox*
```

If the Enable-Mailbox and Set-Mailbox commands were applied correctly, the following result is returned.

Name	Alias	ServerName	ProhibitSendQuota
DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}	DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}	*EXch1*	50 GB (53,687,091,200 bytes)

See Also

Concepts

Managing Discovery

1.11.8 Litigation Hold

Litigation Hold

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-23*

Understanding Litigation Hold

Learn about the litigation hold feature, which allows you to preserve items in user mailboxes and protect the items from deletion by users or automated processes.

Place a Mailbox on Litigation Hold

Learn how to use the Exchange Management Console, the Exchange Control Panel, or the Exchange Management Shell to place a mailbox on litigation hold.

1.11.8.1 Understanding Litigation Hold

Understanding Litigation Hold

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-23*

When a reasonable expectation of litigation exists, organizations are required to preserve electronically stored information (including e-mail) that's relevant to the case. This expectation can occur before the specifics of the case are known, and preservation is often broad. Organizations may preserve all e-mail related to a specific topic, or all e-mail for certain individuals. Depending on the organization's electronic discovery (eDiscovery) practices, some of the measures adopted by organizations to preserve e-mail include the following:

- End users may be asked to preserve e-mail by not deleting any messages. However, users may still delete e-mail knowingly or inadvertently.
- Automated deletion mechanisms such as messaging records management (MRM) may be suspended. This could result in large volumes of e-mail cluttering the user mailbox, and thus impacting user productivity. Suspending automated deletion also doesn't prevent users from manually deleting e-mail.
- Some organizations copy or move e-mail to an archive to make sure it isn't deleted, altered, or tampered with. This increases costs due to manual efforts required to copy or move messages to an archive, or third-party products used to collect and store e-mail outside Microsoft Exchange.

Failure to preserve e-mail may expose an organization to legal and financial risks such as scrutiny of the organization's records retention and discovery processes, adverse legal judgments, sanctions, or fines.

In Exchange Server 2010, you can use litigation hold to accomplish the following goals:

- Enable users to be placed on hold and keep mailbox items in an unaltered state
- Preserve mailbox items that may have been deleted or edited by users
- Preserve mailbox items automatically deleted by MRM
- Keep the litigation hold transparent from the user by not having to suspend

MRM
- Enable discovery searches of items placed on hold

Placing a Mailbox on Litigation Hold

Authorized users that have been added to the Discovery Management role-based access control (RBAC) role group or assigned the legal hold management role can place mailbox users on litigation hold. You can delegate the task to records managers, compliance officers, or attorneys in your organization's legal department, while assigning the least privileges. To learn more about assigning the Discovery Management role group, see Add a User to the Discovery Management Role Group.

In Exchange 2010 SP1, you can use the Exchange Management Console (EMC), the Exchange Control Panel (ECP) or the Exchange 2010 Management Shell to place a mailbox on litigation hold. In Exchange 2010 RTM, you must use the Set-Mailbox cmdlet to place a mailbox on litigation hold. To learn more about placing a mailbox on litigation hold, see Place a Mailbox on Litigation Hold.

Many organizations require that users be informed when they're placed on litigation hold. Additionally, when a mailbox is on litigation hold, any retention policies applicable to the mailbox user don't need to be suspended. Because messages continue to be deleted as expected, users may not notice they're on litigation hold. If your organization requires that users on litigation hold be informed, you can add a notification message to the mailbox user's **Retention Comment** property. Outlook 2010 displays the notification in the backstage area. The **Retention Comment** property can be added using the Exchange Management Console (EMC) or the Exchange Management Shell.

Note:

In Exchange 2010, the **Retention Comment** property is used to display a notification for both retention hold and litigation hold.

Litigation Hold and Mailbox Quotas

Items in the Recoverable Items folder aren't calculated toward the user's mailbox quota. In Exchange 2010, the Recoverable Items folder has its own quota. When a user's Recoverable Items folder exceeds the warning quota for recoverable items (as specified by the *RecoverableItemsWarningQuota* parameter), an event is logged in the Application event log of the Mailbox server. When the folder exceeds the quota for recoverable items (as specified by the *RecoverableItemsQuota* parameter), users won't be able to empty the Deleted Items folder or permanently delete mailbox items. Also copy-on-write won't be able to create copies of modified items. Therefore, it's critical that you monitor the Recoverable Items quotas for mailbox users placed on litigation hold.

For mailbox databases, the default *RecoverableItemsWarningQuota* and *RecoverableItemsQuota* values are set to 20 Gb and 30 Gb respectively. These settings are usually sufficient for storing several years of mailbox data when on litigation hold. To modify these values for a mailbox database, use the Set-MailboxDatabase cmdlet. To modify them for individual mailboxes, use the Set-Mailbox cmdlet.

Litigation Hold and the Recoverable Items Folder

Litigation hold uses a new Exchange 2010 feature called the Recoverable Items folder. This folder replaces the feature informally known as the *dumpster* in previous versions of Exchange. The Recoverable Items folder is hidden from the default view of Microsoft Outlook, Microsoft Office Outlook Web App, and other e-mail clients. To learn more about the Recoverable Items folder, see Understanding Recoverable Items.

By default, when a user deletes a message from a folder other than the Deleted Items folder, the message is moved to the Deleted Items folder. This is known as a *move*. When a user *soft deletes* an item (accomplished by pressing the SHIFT and DELETE keys) or deletes an item from the Deleted Items folder, or empties the Deleted Items folder, the message is moved to the Recoverable Items folder, thereby disappearing from the user's view.

Items in the Recoverable Items folder are retained for the deleted item retention period configured on the user's mailbox database. By default, the deleted item retention period is set to 14 days for mailbox databases. In Exchange 2010, you can also configure a storage quota for the Recoverable Items folder. This protects the organization from a potential denial of service (DoS) attack due to rapid growth of the Recoverable Items folder and therefore the mailbox database. If a mailbox is not placed on litigation hold, items are purged permanently from the Recoverable Items folder on a first in, first out (FIFO) basis when the Recoverable Items warning quota is exceeded, or if the item has resided in the folder for a longer time than the deleted item retention period.

The Recoverable Items folder has the following three subfolders used to store deleted items in various states and facilitate litigation hold:

1. **Deletions** Items removed from the Deleted Items folder or soft deleted from other folders are moved to the Deletions subfolder and are visible to the user when using the Recover Deleted Items feature in Outlook. By default, items reside in this folder until the deleted item retention period configured for the mailbox expires.
2. **Purges** When a user deletes an item from the Recoverable Items folder (by using the Recover Deleted Items tool in Outlook or Outlook Web App), the item is moved to the Purges folder. Items that exceed the deleted item retention period configured on the mailbox database or the mailbox are also moved to the Purges folder. Items in this folder aren't visible to users if they use the Recover Deleted Items tool. When the mailbox assistant processes the mailbox, items in the Purges folder are purged from the mailbox database. When you place the mailbox user on litigation hold, the mailbox assistant doesn't purge items in this folder.
3. **Versions** In Exchange 2010, when a user who is placed on litigation hold changes specific properties of a mailbox item, the original item is preserved to meet discovery obligations. A copy of the original mailbox item is created before the changed item is written. The original copy is saved in the Versions folder. This process is known as *copy on write*. Copy on write applies to items residing in any mailbox folder. The Versions folder isn't visible to users. The following table lists the message properties that trigger copy on write.

Properties that trigger copy on write

Item type	Properties that trigger copy on write
Messages (IPM.Note*) Posts (IPM.Post*)	• Subject • Body • Attachments • Senders/Recipients • Sent/Received Dates
Items other than messages and posts	Any change to a visible property, except the following: • Item location (when an item is moved between folders) • Item status change (read or unread) • Changes to retention tag applied to an item
Items in the default folder Drafts	None (items in the Drafts folder exempt from copy on write)

Important:
In Exchange 2010 SP1, copy-on-write is disabled for calendar items in the organizer's mailbox when meeting responses are received from attendees and the tracking information for the meeting is updated. Changes to RSS feeds are not captured by copy-on-write.

Note:
Although the Purges and Versions folders aren't visible to the user, all items in the Recoverable Items folder are indexed by Exchange Search, and are discoverable using Multi-Mailbox Search.

After a mailbox user is removed from litigation hold, items in the Purges and Versions folders are purged by the mailbox assistant.

1.11.8.2 Place a Mailbox on Litigation Hold

Place a Mailbox on Litigation Hold

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

A litigation hold preserves deleted mailbox items and records changes made to mailbox items. Deleted and changed items are returned in a discovery search.

Use the EMC to place a mailbox on litigation hold

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Litigation hold" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox you want to place on litigation hold.
3. In the action pane, click **Properties**.
4. In **<Mailbox> Properties**, on the **Mailbox Settings** tab, click **Messaging Records Management**, and then click **Properties**.
5. In **Messaging Records Management**, complete the following fields:
   - **Enable Litigation Hold** Select this check box to place the mailbox on litigation hold.
   - **Messaging Records Management Description URL** Use this box to enter the location of a Web page or document that contains more information about the litigation hold or retention hold policies in your organization. The URL is displayed in the Backstage area of Microsoft Outlook 2010. This makes it easier for users to access linked Help documents, and may reduce calls to your Help desk or Legal department by answering common questions.
   - **Comments** Use this box to enter the text that you want to be displayed to the mailbox user in the Backstage area of Outlook 2010.

Use the ECP to place a mailbox on litigation hold

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Litigation hold" entry in the Messaging Policy and Compliance Permissions topic.

For details about using the Exchange Control Panel (ECP) to place a mailbox on litigation hold, see Put a Mailbox on Litigation Hold.

Use the Shell to place a mailbox on litigation hold

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Litigation hold" entry in the Messaging Policy and Compliance Permissions topic.

This example places the mailbox joe@contoso.com on litigation hold.

Note:
It may take up to an hour for the litigation hold to take effect.

```
Set-Mailbox joe@contoso.com -LitigationHoldEnabled $true
```

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to remove a mailbox from litigation hold

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Litigation hold" entry in the Messaging Policy and Compliance Permissions topic.

This example removes the mailbox joe@contoso.com from litigation hold.

```
Set-Mailbox joe@contoso.com -LitigationHoldEnabled $false
```

For detailed syntax and parameter information, see Set-Mailbox.

Other Tasks

After you place a mailbox on litigation hold, you may also want to create a discovery search. For detailed steps, see Create a Discovery Search.

1.11.9 Archiving

Archiving

Exchange Server 2010 > Messaging Policy and Compliance >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-01*

Understanding Personal Archives

Learn about the new personal archive feature, which allows you to provision an on-

premises archive mailbox for your users.

Understanding Exchange Online Archiving

Learn about the new cloud-based archiving solution for your Exchange 2010 on-premises organization.

Configure Exchange Online Archiving

Learn how to setup your on-premises Exchange 2010 organization to use cloud-based archives with Exchange Online Archiving.

Archiving Terminology in Exchange 2010

Learn about the terminology used for archiving in Exchange 2010.

Managing Archives

Learn how to create and manage personal (on-premises) and cloud-based archives for your users.

1.11.9.1 Understanding Personal Archives

Understanding Personal Archives

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-13*

Personal archives (also called *on-premises archives*) help you regain control of your organization's messaging data by eliminating the need for personal store (.pst) files and allowing users to store messages in an *archive mailbox* accessible in Microsoft Outlook 2010 and Microsoft Office Outlook Web App.

Looking for management tasks related to personal archives? See Managing Archives.

Looking for information about cloud-based archives? See Understanding Exchange Online Archiving.

Contents

Messaging Data and .pst Files

Outlook uses .pst files to store data locally on users' computers or network shares. Unlike offline store (.ost) files (which are used by Outlook in Cached Exchange Mode to store a

copy of the mailbox for offline access), .pst files aren't synchronized with the user's Exchange mailbox. If a user moves messages to a .pst file, those messages are removed from the mailbox.

Using .pst files to manage messaging data can result in the following issues:

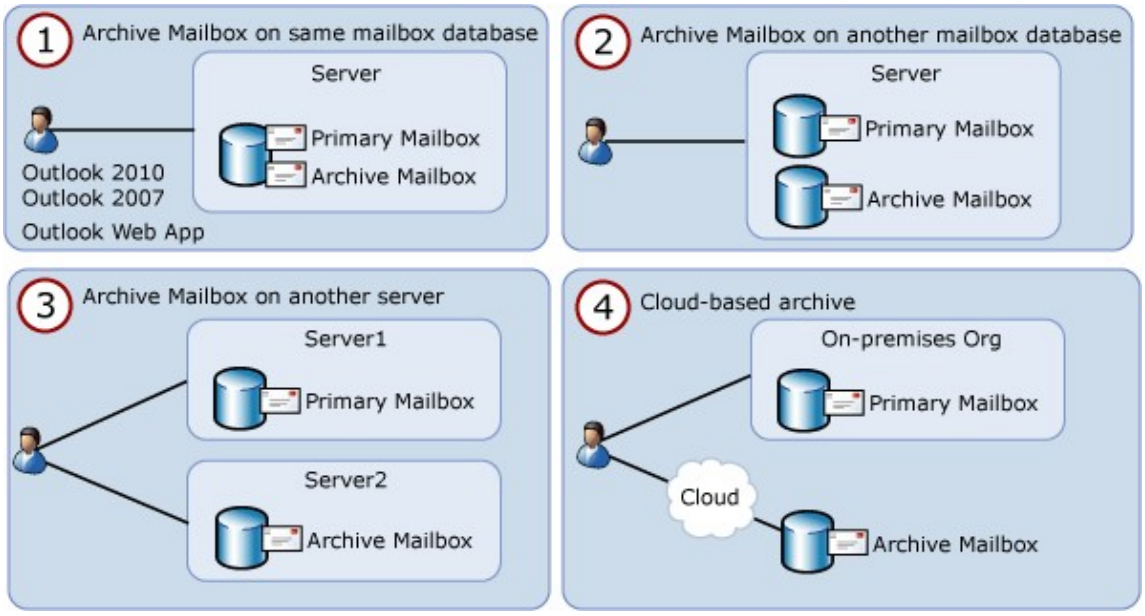
- **Unmanaged files** Generally, .pst files are created by users and reside on their computers or network shares. They aren't managed by your organization. As a result, users can create several .pst files containing the same or different messages and store them in different locations, with no organizational control.
- **Increased discovery costs** Lawsuits and some business or regulatory requirements sometimes result in discovery requests. Locating messaging data that resides in .pst files on users' computers can be a costly manual effort. Because tracking unmanaged .pst files can be difficult, .pst data may be undiscoverable in many cases. This could possibly expose your organization to legal and financial risks.
- **Inability to apply messaging retention policies** Messaging retention policies can't be applied to messages located in .pst files. As a result, depending on business or applicable regulations, your organization may not be in compliance.
- **Risk of data theft** Messaging data stored in .pst files is vulnerable to data theft. For example, .pst files are often stored in portable devices such as laptops, removable hard drives, and portable media such as USB drives, CDs, and DVDs.
- **Fragmented view of messaging data** Users who store information in .pst files don't get a uniform view of their data. Messages stored in .pst files are generally available only on the computer where the .pst file resides. As a result, if users access their mailboxes using Outlook Web App or Outlook on another computer, the messages stored in their .pst files are inaccessible.

Return to top

Personal Archives

In Microsoft Exchange Server 2010, personal archives provide users an alternative storage location in which to store historical messaging data. A personal archive is an additional mailbox (called an archive mailbox) enabled for a mailbox user. Outlook 2010, Outlook 2007, and Outlook Web App users have seamless access to their archive mailbox. Using either of these client applications, users can view an archive mailbox and move or copy messages between their primary mailbox and the archive. Personal archives present a consistent view of messaging data to users and eliminate the user overhead required to manage .pst files. Eliminating the use of .pst files significantly reduces your organization's exposure to the risks outlined in the previous section.

In Exchange 2010 Service Pack 1 (SP1), you can provision a user's personal archive on the same mailbox database as the user's primary mailbox, another mailbox database on the same Mailbox server, or a mailbox database on another Mailbox server in the same Active Directory site. This provides flexibility to use tiered storage architecture and to store archive mailboxes on a different storage subsystem, such as near-line storage. In cross-premises Exchange 2010 deployments, you can also provision a cloud-based archive for mailboxes located on your on-premises Mailbox servers.



Return to top

Client Access to Archive Mailboxes

The following table lists the client applications that can be used to access archive mailboxes.

Client access to archive mailboxes

Client	Access to archive mailbox
Outlook 2010, Outlook 2007, and Outlook Web App	Yes. Outlook 2010, Outlook 2007 and Outlook Web App users can copy or move items from their primary mailbox to their archive mailbox, and can also use retention policies to move items to the archive. **Note:** Outlook 2010 and Outlook 2007 users can also copy or move items from .pst files to their archive mailbox. Outlook 2007 users require the Office 2007 Cumulative Update for February 2011. Some differences in archive support exist between Outlook 2010 and Outlook 2007. For more information, see Exchange Team Blog article, see Yes Virginia, there is Exchange 2010 archive support in Outlook 2007.
Outlook 2003 and older clients	No.
Microsoft Exchange ActiveSync	No.

Note:
Personal archives are a premium feature and require an Exchange Enterprise client access license (CAL). For details about how to license Exchange, see Exchange Server Licensing. For details about the versions of Microsoft Outlook required to access an archive mailbox, see License requirements for Personal Archive and retention policies.

Outlook doesn't create a local copy of the archive mailbox on a user's computer, even if it's configured to use Cached Exchange Mode. Users can access an archive mailbox in online mode only.

Delegate Access

Delegate access is when a user or set of users is provided access to another user's mailbox. There are several scenarios for providing delegate access, including:

- Providing one or more users with access to the mailbox of a user who is no longer employed by the organization. In this case, users who may be given delegate access include the departed user's manager or supervisor or another user who will assume the departed user's responsibilities.
- Providing one or more users with access to a shared mailbox.
- Providing executive assistants with access to the mailboxes of the executives they're assisting.

In Exchange 2010 SP1, when you assign Full Access permissions to a mailbox, the delegate to which you assign the permissions can also access the user's personal archive. Delegates must use Outlook to access the mailbox, and they must connect to an Exchange 2010 SP1 Client Access server for Autodiscover purposes. Autodiscover is an Exchange 2010 service that provides configuration settings to automatically configure Outlook clients. When delegates use Outlook to access an Exchange 2010 SP1 mailbox, both the primary mailbox and the personal archive to which they have access are visible from Outlook. For details about assigning Full Access permissions, see Manage Full Access Permissions.

Return to top

Moving Messages to the Archive Mailbox

There are several ways to move messages to archive mailboxes:

- **Move or copy messages manually** Mailbox users can manually move or copy messages from their primary mailbox or a .pst file to their archive mailbox. The archive mailbox appears as another mailbox or .pst file in Outlook and Outlook Web App.
- **Move or copy messages using Inbox rules** Mailbox users can create Inbox rules in Outlook or Outlook Web App to automatically move messages to a folder in their archive mailbox. To learn more, see Learn About Inbox Rules.
- **Move messages using retention policies** You can use retention policies to automatically move messages to the archive. Users can also apply a personal tag to move messages to the archive. For details about archive and retention policies, see Archive and Retention Policies later in this topic.

  Note:
  Personal tags are available only in Outlook 2010 and Outlook Web App.

- **Import messages from .pst files** In Exchange 2010 SP1, you can use a mailbox import request to import messages from a .pst file to a user's archive or primary mailbox. For details, see Understanding Mailbox Import and Export Requests. Tools used to locate .pst files within an organization are available from Microsoft partners. For a list of Microsoft partners for archiving, see "Archive and Compliance Partners" in Independent Software Vendors.

Archive and Retention Policies

In Exchange 2010, you can apply archive policies to a mailbox to automatically move messages from a user's primary mailbox to the archive mailbox after a specified period. Archive policies are implemented by creating retention tags that use the **Move to Archive** retention action.

Messages are moved to a folder in the archive mailbox that has the same name as the

source folder in the primary mailbox. If a folder with the same name doesn't exist in the archive mailbox, it is created when the Managed Folder Assistant moves a message. Re-creating the same folder hierarchy in the archive mailbox allows users to find messages easily.

To learn more about retention policies, retention tags, and the **Move to Archive** retention action, see Understanding Retention Tags and Retention Policies.

Important:
You can't apply a managed folder mailbox policy to mailboxes that have a personal archive. Managed content settings created for managed folders can't use the **Move to archive** action. To learn more about managed folders, see Understanding Managed Folders.

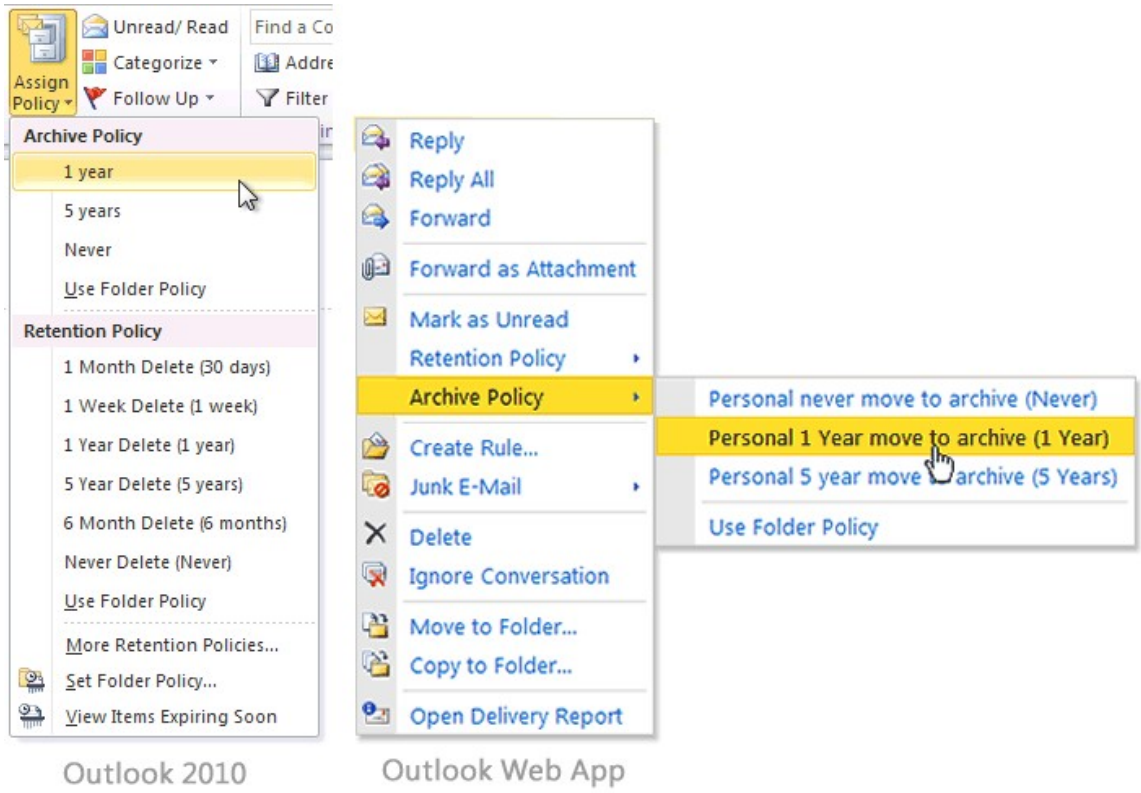
Default Archive and Retention Policy

Exchange Setup creates the default archive and retention policy **Default Archive and Retention Policy**. This policy contains retention tags that have the **Move to Archive** action, as shown in the following table.

Default archive and retention policy

Retention tag name	Tag type	Description
Default 2 year move to archive	Default	Messages are automatically moved to the archive mailbox after two years. Applies to items in the entire mailbox that don't have a retention tag applied explicitly or inherited from the folder.
Personal 1 year move to archive	Personal	Messages are automatically moved to the archive mailbox after one year.
Personal 5 year move to archive	Personal	Messages are automatically moved to the archive mailbox after five years.
Personal never move to archive	Personal	Messages are never moved to the archive mailbox.
Recoverable Items 14 days move to archive	Personal	Messages are moved from the Recoverable Items folder of the user's primary mailbox to the Recoverable Items folder of the archive mailbox. Users attempting to recover deleted items in the archive must use the Recover Deleted Items feature on the archive mailbox.

If you enable a personal archive for a mailbox user and the mailbox doesn't already have a retention policy assigned, the default archive and retention policy is automatically assigned. After the Managed Folder Assistant processes the mailbox, these tags become available to the user, who can then tag folders or messages to be moved to the archive mailbox. By default, e-mail messages from the entire mailbox are moved after two years.



Before provisioning archive mailboxes for your users, we recommend that you inform them about the archive policies that will be applied to their mailbox and provide subsequent training or documentation to meet their needs. This should include details about the following:

- Functionality available within the archive, the default archive and retention policies.
- Information about when messages may be moved automatically to the archive.
- Information about the folder hierarchy created in the archive mailbox.
- How to apply personal tags (displayed in the **Archive policy** menu in Outlook and Outlook Web App).

Note:
If you apply a retention policy to users who have an archive mailbox, the retention policy replaces the default archive and retention policy. You can create one or more retention tags with the **Move to Archive** action, and then link the tags to the retention policy. You can also add the default **Move to Archive** tags (which are created by Setup and linked to the Default Archive and Retention Policy) to any retention policies you create.

In Exchange 2010 SP1, the default archive and retention policy contains additional retention tags with the **Delete and Allow Recovery** action. To learn more, see Understanding Retention Tags and Retention Policies.

For information about compliance and archiving in Outlook 2010, see Plan for compliance and archiving in Outlook 2010.

Return to top

Archive Quotas

Archive mailboxes are designed so that users can store historical messaging data outside their primary mailbox. Often, users use .pst files due to low mailbox storage quotas and the restrictions imposed when these quotas are exceeded. For example, users can be prevented from sending messages when their mailbox size exceeds the Prohibit send quota. Similarly, users can be prevented from sending and receiving messages when their mailbox size exceeds the Prohibit send and receive quota.

To eliminate the need for .pst files, you can provide an archive mailbox with storage limits that meet the user's requirements. However, you may still want to retain some control of the storage quotas and growth of archive mailboxes to help monitor costs and expansion.

To help with this control, you can configure archive mailboxes with an *archive warning quota* and an *archive quota*. When an archive mailbox exceeds the specified archive warning quota, a warning event is logged in the Application event log. When an archive mailbox exceeds the specified archive quota, messages are no longer moved to the archive, a warning event is logged in the Application event log, and a quota message is sent to the mailbox user. By default, in Exchange 2010 SP1, the archive warning quota is set to 45 gigabytes (GB) and the archive quota is set to 50 GB. In Exchange 2010 release to manufacturing (RTM), both quotas are set to **Unlimited**.

The following table lists the events logged and warning messages sent when the archive warning quota and archive quota are met.

Archive quota alerts

Quota	Event ID	Type	Source	Category	Message
Archive warning quota	10022	Warning	MSExchangeMailboxAssistants	Managed Folder Assistant	The archive mailbox '*<Display Name>*:*<GUID>*:*<Mailbox Database>*:*<Server FQDN>*' exceeded the archive warning quota '*<Archive warning quota>*'. Archive mailbox size is '*<Size>*' bytes.
Archive quota	8538	Warning	MSExchangeIS	General	The archive mailbox for *<Legacy DN>* has exceeded the maximum archive mailbox size. You can't copy or move items into the archive mailbox. All message retention actions that move items to the archive

					mailbox will fail, and the primary mailbox may contain items with expired retention tags until the archive mailbox is within the maximum size limit. The mailbox owner should be notified about the condition of the archive mailbox.

For details about how to configure archive quotas, see Configure Archive Quotas for a Personal (On-Premises) Archive.

Return to top

Personal Archives and Other Exchange Features

This section explains the functionality between personal archives and various Exchange features:

- **Exchange Search** The ability to quickly search messages becomes even more critical with archive mailboxes. For Exchange Search, there's no difference between the primary and archive mailbox. Content in both mailboxes is indexed. Because the archive mailbox isn't cached on a user's computer (even when using Outlook in Cached Exchange Mode), search results for the archive are always provided by Exchange Search. When searching the entire mailbox in Outlook 2010, search results include the users' primary and archive mailbox. To learn more about Exchange Search, see Understanding Exchange Search.
- **Multi-Mailbox Search** When a discovery manager uses Multi-Mailbox Search to perform a discovery search, users' archive mailboxes are also searched. There's no option to exclude archive mailboxes when creating a discovery search from the Exchange Control Panel (ECP). When using the Exchange Management Shell to create a discovery search, you can exclude the archive by using the *DoNotIncludeArchive* switch. For details, see New-MailboxSearch.

  Note:
  You can't use Multi-Mailbox Search to search a disconnected mailbox.

  To learn more about Multi-Mailbox Search, see Understanding Multi-Mailbox Search.
- **Litigation hold** When you put a mailbox on litigation hold, the hold is placed on both the primary and the archive mailbox. To learn more about litigation hold, see Understanding Litigation Hold.
- **Recoverable Items folder** The archive mailbox contains its own Recoverable Items folder, and is subject to the same Recoverable Items folder quotas as the primary mailbox. To learn more about recoverable items, see Understanding Recoverable Items.

Return to top

Managing Archive Mailboxes

In Exchange 2010, creating and managing archive mailboxes is integrated with common mailbox management tasks, such as the following:

- **Creating an archive mailbox** You can create an archive mailbox when creating a mailbox, or you can enable an archive mailbox for an existing mailbox. For details, see Create a Personal (On-Premises) or Cloud-Based Archive for a New Mailbox and Enable a Personal (On-Premises) or Cloud-Based Archive for an Existing Mailbox.
- **Moving an archive mailbox** You can move a user's archive mailbox to another mailbox database on the same Mailbox server or to another server. In Exchange 2010 SP1, you can move a user's archive mailbox independent of the primary mailbox. In Exchange 2010 RTM, a user's archive mailbox resides on the same Mailbox server as the primary mailbox. To move a user's archive mailbox, you must create a mailbox move request. For details, see Create a Local Move Request.
- **Disabling an archive mailbox** You may want to disable a user's archive mailbox for troubleshooting purposes or if you're moving the primary mailbox to a version of Exchange that doesn't support personal archives. Disabling an archive is similar to disabling a primary mailbox. For details, see Disable a Personal (On-Premises) or Cloud-Based Archive for a Mailbox. A disabled archive mailbox is retained in the mailbox database until the deleted mailbox retention period for that database is reached. During this period, you can reconnect the archive to a mailbox user. When the deleted mailbox retention period is reached, the disconnected archive mailbox is purged from the mailbox database.
- **Retrieving mailbox statistics and folder statistics** You can retrieve mailbox statistics and mailbox folder statistics for a user's archive mailbox by using the *Archive* switch with the Get-MailboxStatistics and Get-MailboxFolderStatistics cmdlets.

Return to top

1.11.9.2 Understanding Exchange Online Archiving

Understanding Exchange Online Archiving

Exchange Server 2010 > Messaging Policy and Compliance > Archiving >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-04*

Microsoft Exchange Online Archiving is a cloud-based, enterprise-class archiving solution for your Exchange Server 2010 Service Pack 1 (SP1) or later on-premises organization. With Exchange Online Archiving, your organization can host your users' primary mailboxes on your on-premises servers and store their historical e-mail data in cloud-based archive mailboxes. This solution can assist your organization with archiving, compliance, regulatory, and e-discovery challenges, while simplifying your on-premises infrastructure. EOA provides you the following advantages:

- **Help meet long-term retention requirements** Cloud-based archives allow you to store large quantities of messaging data off-site in secure and controlled datacenters. Exchange Online Archiving helps your organization meet regulatory compliance or business requirements for long-term retention of e-

mail. Using archive policies, messages are moved from on-premises mailboxes to the cloud-based archives. The same retention policies applied to on-premises mailboxes can be enforced on cloud-based archives.

- **Help meet eDiscovery and litigation hold requirements** With cloud-based archives for your on-premises mailbox users, you can perform seamless discovery searches across both the on-premises primary mailbox and the cloud-based archive. When users are placed on litigation hold in your on-premises organization, their cloud-based archive is also placed on hold.
- **Lower storage costs** Moving historical e-mail data to a cloud-based archive allows you to reduce your organization's storage requirements. You can provision users' primary mailboxes with appropriate mailbox quotas, which keeps mailbox sizes in control and your storage costs low.
- **Provide Anywhere Access** Cloud-based archive mailboxes are similar to an on-premises archive mailbox. Using Outlook 2010, Outlook 2007 or Outlook Web App, users are able to access older messages and content in the archive transparently, without requiring any additional configuration on their computers.

Note:
Outlook users can access an archive mailbox in online mode. Archive mailboxes aren't cached to the user's computer when using Outlook in Cached Exchange Mode.

To learn about the various archiving terms used in Exchange 2010, see Archiving Terminology in Exchange 2010.

Exchange Online Archiving Requirements and Setup

The following are general requirements required to configure Exchange Online Archiving.

- You must purchase an Exchange Online Archiving subscription for the Exchange Online service included with Office 365. For more information, see Exchange Online Archiving subscription.
- User's primary mailboxes must be hosted on on-premises Exchange 2010 SP1 or later Mailbox servers.
- You must configure a subset of steps required for a hybrid deployment between your on-premises organization and Office 365. Details are described in Configure Exchange Online Archiving.
- Users must use Outlook 2010, Outlook 2007 SP2, or Outlook Web App to access the cloud-based archive mailbox.
- To use Office 2010 or Office 2007 with Exchange Online Archiving, you must configure your users' computers to support Office 365. For more information, see Manually update and configure desktops for Office 365.

To set up Exchange Online Archiving, you must perform a subset of steps required for a hybrid deployment for Exchange Online. If your on-premises organization has been upgraded to Exchange 2010 SP2, you can use the Hybrid Configuration Wizard to perform this setup. Additionally, you can configure single sign-on, which is based on Active Directory Federation Services (AD FS). This allows your users to access on-premises mailboxes and cloud-based archives with a single username and password..

Note:
Although you can configure Exchange Online Archiving without setting up single sign-on using AD FS, we highly recommend that you configure single sign-on. Doing so helps to avoid additional authentication prompts when users try to access their cloud-based archive.
If you deploy a configuration without AD FS, access to the cloud-based archive using Microsoft Outlook is supported only when the user's UPN in your on-premises and cloud-

based organizations matches and both use the same password. In this case, Microsoft Outlook users will be prompted for credentials when accessing the cloud-based archive for the first time. When entering credentials, users can select the **Save password** option to avoid subsequent authentication prompts.

For complete instructions about how to set up Exchange Online Archiving for you organization, see Configure Exchange Online Archiving

Managing Exchange Online Archiving

Managing cloud-based archives is similar to managing personal (on-premises) archives. You can use the Exchange Management Console (EMC) or the Exchange Management Shell to perform the following tasks:

- Create a cloud-based archive. For details, see Create a Personal (On-Premises) or Cloud-Based Archive for a New Mailbox.
- Enable a cloud-based archive. For details, see Enable a Personal (On-Premises) or Cloud-Based Archive for an Existing Mailbox.
- Disable a cloud-based archive. For details, see Disable a Personal (On-Premises) or Cloud-Based Archive for a Mailbox.

  Warning:

  When you disable a cloud-based archive, it is disconnected from the user account. Disconnected archives are retained in Exchange Online for a period of 30 days. During this period, it's possible to reconnect the archive to the same user account. After this period, the disconnected archive is purged from Exchange Online and can't be recovered.

- Connect a disconnected cloud-based archive to a user mailbox. For details, see Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive.

Moving Data to a Cloud-Based Archive

You can use retention policies to move messages to a user's cloud-based archive. When you enable an archive, the default retention policy called **Default Archive and Retention Policy** is automatically applied to the user. This policy has a default policy tag (DPT) assigned that moves items to the archive mailbox after two years. You can also create your own archive and retention policies and apply them to mailbox users. To learn more about archive policies, see Understanding Personal Archives. To learn more about retention tags and retention policies, see Understanding Retention Tags and Retention Policies.

Users can also move messages to their archive by using the following methods:

1. Apply archive policies to individual messages or folders. Archive policies are implemented by creating personal tags that use the **Move to Archive** action. For details about how to create retention tags, see Create a Retention Tag.
2. Use Inbox rules to either move messages to a folder that has an archive policy assigned or have the rule apply an archive policy to the message itself. To learn more about Inbox rules, see Manage email messages by using rules.
3. Move messages manually in Outlook or Outlook Web App.

For all these operations, the cloud-based archive behavior is similar to a personal archive.

Exporting Data From a Cloud-Based Archive

Users can move messages from their cloud-based archive to their primary mailbox by

using Outlook or Outlook Web App. Users can also move or export messages to a .pst file by using Outlook. For details, see Export Multi-Mailbox Search Results to an Outlook Data File (.pst).

Note:
To protect your organization's messaging data, you can disable users' ability to move messages from their primary mailbox or cloud-based archive to a .pst file or another mailbox. To do this, use Registry entries or the group policy settings included in the Office 2010 Administrative Templates. For details, see Plan for compliance and archiving in Outlook 2010.

You can also export a cloud-based archive to a .pst file by first moving it to an on-premises Mailbox server and then creating a mailbox export request. To learn more about export requests, see Understanding Mailbox Import and Export Requests.

Cloud-Based Archives and Retention

Archive policies, which you create on an on-premises Mailbox server, move messages to the user's personal or cloud-based archive. Once in the archive, messages must continue to be processed and removed based on the user's retention policy.

To accomplish this, you must export retention policies and retention tags from your on-premises organization and import them to your cloud-based organization in Exchange Online. After you complete the import process, the imported policies are applied to cloud-based archive mailboxes, and messages expire based on users' retention policies.

Important:
If you make changes to retention tags or retention policies in your on-premises organization (for example, if you create a new retention tag, modify the retention age property of an existing tag, or remove a tag), you must perform the export and import procedure again to make sure that the retention tags and policies from your on-premises organization are also updated in Exchange Online.

Cloud-Based Archives, Discovery, and Litigation Hold

In Exchange 2010, you can use Multi-Mailbox Search to perform discovery searches in mailboxes across your organization. When performing a discovery search, users' cloud-based archives are also searched. No additional action is required to include a cloud-based archive in the search. Messages returned in a search are copied to the on-premises discovery mailbox specified in the search. To learn more about discovery searches, see Understanding Multi-Mailbox Search.

Similarly, when a mailbox user is placed on litigation hold, the user's cloud-based archive is also placed on hold. Messages aren't purged from the cloud-based archive until the hold is removed. To learn more about litigation hold, see Understanding Litigation Hold.

Cloud-Based Archives and Auditing

The following auditing features in Exchange 2010 also work with Exchange Online Archiving:

Mailbox audit logging In Exchange 2010 SP1 and later, you can enable mailbox audit logging to log access by delegate users or administrators and the mailbox owner. When mailbox audit logging is enabled for a mailbox, the configured settings are also applied to the user's cloud-based archive. The same on-premises tools used to retrieve audit log entries for the on-premises mailbox also return mailbox audit entries for the cloud-based

archive. To learn more, see Understanding Mailbox Audit Logging.

Administrator audit logging In Exchange 2010 SP1 and later, administrator audit logging allows you to audit actions taken administrators when they use the EMC, Exchange Control Panel (ECP), or the Shell to make a change in your organization. If admin audit logging is enabled on your on-premises server, all administrative operations performed against Exchange Online Archiving are also logged. You must search the administrator audit logs in your on-premises Exchange organization separately from the Exchange Online Archiving audit logs. To learn more, see Overview of Administrator Audit Logging.

1.11.9.3 Configure Exchange Online Archiving

Configure Exchange Online Archiving

Exchange Server 2010 > Messaging Policy and Compliance > Archiving >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-02-20*

Microsoft Exchange Online Archiving is a cloud-based, enterprise-class archiving solution for your Exchange Server 2010 on-premises organization. With Exchange Online Archiving, your organization can host your users' primary mailboxes on your on-premises servers and store their historical e-mail data in Exchange Online archive mailboxes. This solution can help your organization with archiving, compliance, regulatory, and e-discovery challenges, while simplifying your on-premises infrastructure.

To learn more about the advantages of Exchange Online Archiving, download *Microsoft Exchange Online Archiving: Service Description*, available on the Microsoft Download Center as part of the Office 365 for Enterprise Service Descriptions.

Requirements for Configuring Exchange Online Archiving

The following are general requirements for configuring Exchange Online Archiving.

- You must purchase an Exchange Online Archiving subscription for the Exchange Online service included with Microsoft Office 365. For more information, see Exchange Online Archiving subscription.
- Your users' primary mailboxes must be hosted on on-premises Exchange 2010 Mailbox servers.
- You will configure a full hybrid deployment using the Hybrid Configuration wizard. For more information, see Configure Exchange Online Archiving with Exchange Server 2010 later in this topic.
- Users must use Outlook 2010, Outlook 2007 SP2, or Outlook Web App to access the cloud-based archive mailbox.

Note:

To use Office 2010 or Office 2007 with Exchange Online Archiving, you must configure your users' computers to support Office 365. For more information, see Manually update and configure desktops for Office 365.

Configure Exchange Online Archiving with

Exchange 2010

A hybrid deployment connects an Office 365 organization to your on-premises Exchange 2010 organization by configuring the hybrid features of one or more on-premises Exchange 2010 servers. These Exchange 2010 services must be updated to Service Pack 3 (SP3) for Exchange 2010 Server (SP3) or greater to enable hybrid functionality with the latest release of Office 365. After you configure a hybrid deployment using the Hybrid Configuration wizard, users in the on-premises organization can connect to Exchange Online archives that are located in the Office 365 organization and have other hybrid deployment features enabled. To learn more about hybrid deployments, see Understanding Hybrid Deployments with Exchange 2010 SP3.

To configure a hybrid deployment to support Exchange Online Archiving in your Exchange 2010 organization, a comprehensive deployment checklist with step-by-step procedures is available on the Microsoft Download Center. To select the appropriate checklist, you must first decide if your organization wants to use single sign-on. Single sign-on is optional for hybrid deployments, but strongly recommended. If you want to configure a full hybrid deployment and select different deployment options, you should see the Exchange Server Deployment Assistant for more information.

With single sign-on, which is based on Active Directory Federation Services (AD FS) 2.0, users can access both their personal (on-premises) archive and Exchange Online archive with a single user name and password. Single sign-on also benefits administrators. For example, you can control account policies through the on-premises Active Directory, which gives you the ability to manage password policies, workstation restrictions, lock-out controls, and more, without having to perform additional tasks in Office 365.

To deploy single sign-on, you must also deploy additional servers to support it. If you don't configure single sign-on, users with an Exchange Online archive will need to use separate user names and passwords for their on-premises and archive mailboxes.

For complete instructions about setting up single-sign on, including how to prepare for it, see Prepare for Single Sign-on.

If you want to configure a limited hybrid deployment to support Exchange Online Archiving in your Exchange 2010 organization, select the deployment checklist that is appropriate based on your decision regarding the use of single sign-on:

- To configure a limited hybrid deployment **with** single sign-on, download the following document: http://go.microsoft.com/fwlink/p/?linkid=248654
- To configure a limited hybrid deployment **without** single sign-on, download the following document: http://go.microsoft.com/fwlink/p/?linkid=248653

If you've already configured a full hybrid deployment in your Exchange 2010 organization and want to enable your deployment to support Exchange Online Archiving, you must purchase an Exchange Online Archiving subscription with Office 365. On-premises support for Exchange Online archiving is automatically configured and enabled by the Hybrid Configuration wizard. For more information about subscriptions, see Exchange Online Archiving subscription.

Managing Exchange Online Archiving

After Exchange Online Archiving is deployed in your organization, there are several management tasks you can perform. Managing Exchange Online archives is very similar to managing personal archives (also called *on-premises archives*).

For a list of management procedures, see Managing Archives. To learn more about personal archives, see Understanding Personal Archives.

1.11.9.4 Archiving Terminology in Exchange 2010

Archiving Terminology in Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-01*

archive mailbox

Generic term for a user's archive mailbox, whether hosted on-premises on an Exchange 2010 Mailbox server or in the cloud on Exchange Online. Archive mailboxes don't receive inbound mail. You can't create an archive mailbox for a user without a primary mailbox.

cloud-based archive

An archive mailbox in Exchange Online. For Exchange Online Archiving, a cloud-based archive is associated with an on-premises primary mailbox. Exchange Online and Office 365 customers can also have a cloud-based archive for a cloud-based primary mailbox.

cloud-based archive mailbox

See *cloud-based archive*

Exchange Online Archiving

Exchange Online Archiving is a cloud-based archiving solution for on-premises organizations running Exchange 2010 Service Pack 1 (SP1) or later. With Exchange Online Archiving, organizations can host their users' primary mailboxes on on-premises servers while storing the historical e-mail data in cloud-based archives. To learn more about Exchange Online Archiving, see Understanding Exchange Online Archiving.

online archive

The default Outlook and Outlook Web App display name for a personal or cloud-based archive mailbox. You can change the display name of an archive mailbox by using the **Set-Mailbox** cmdlet.

on-premises archive

See *personal archive*.

personal archive

Also known as an *on-premises archive*, a personal archive is an additional mailbox (called an *archive mailbox*) that's enabled for a mailbox user to provide an alternate storage location in which to store historical messaging data. To learn more about personal archives, see Understanding Personal Archives.

primary mailbox

An Exchange mailbox that receives inbound mail and can be cached to a user's computer when using Microsoft Outlook in Exchange Cached Mode. The primary mailbox also contains a set of default folders such as **Inbox**, **Deleted Items** and **Sent Items**.

1.11.9.5 Managing Archives

Managing Archives

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-08*

Create a Personal (On-Premises) or Cloud-Based Archive for a New Mailbox

Enable a Personal (On-Premises) or Cloud-Based Archive for an Existing Mailbox

Configure Archive Quotas for a Personal (On-Premises) Archive

Disable a Personal (On-Premises) or Cloud-Based Archive for a Mailbox

Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive

Modify Archive Policies

1.11.9.5.1 Create a Personal (On-Premises) or Cloud-Based Archive for a New Mailbox

Create a Personal (On-Premises) or Cloud-Based Archive for a New Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP1*

Topic Last Modified: *2012-07-23*

Creating a personal archive (also called an *on-premises archive*) or cloud-based archive for a mailbox helps you regain control of your organization's messaging data by eliminating the need for personal store (.pst) files and allowing you to meet your organization's message retention and eDiscovery requirements. With archiving enabled, users can store messages in an archive mailbox, which is accessible by using Microsoft Outlook 2010 and Outlook Web App.

In Exchange 2010 Service Pack 1 (SP1) and later, the archive and the mailbox can be located on different Mailbox servers in your on-premises Exchange organization. To learn more, see Understanding Personal Archives.

Looking for other management tasks related to archiving? Check out Managing Archives.

Prerequisites

The procedures in this topic show you how to create personal and cloud based archives. However, to create cloud-based archives, you must first configure Exchange Online Archiving. For details, see Configure Exchange Online Archiving.

Use the EMC to create a mailbox and enable a personal or cloud-based archive

You need to be assigned permissions before you can perform this procedure. To see what

permissions you need, see the "Mailbox users" entry in the Mailbox Permissions topic.

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Mailbox**.
3. On the **Introduction** page, select one of the following options:
   - **User Mailbox** Click this button to create a mailbox that is owned by a user to send and receive e-mail messages.
     The Active Directory account that is associated with user mailboxes must reside in the same forest as the Exchange server. To use an account in a trusted forest, select **Linked Mailbox**.
   - **Linked Mailbox** Click this button to create a user mailbox that is accessed by a user in a separate, trusted forest. You must still create a user account in the forest in which Exchange Server resides. This is required to create the necessary Active Directory object for storing the mailbox information.
     Linked mailboxes might be necessary for organizations that choose to deploy Exchange in a resource forest. The resource forest scenario allows an organization to centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests.
4. On the **User Type** page, click **New User**.
5. On the **User Information** page, complete the following fields:
   - **Specify the organizational unit rather than using a default one** Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. To learn more about recipient scopes, see Understanding Recipient Scope.
   - **First name** Use this box to type the first name of the user. This field is optional.
   - **Initials** Use this box to type the initials of the user. This field is optional.
   - **Last name** Use this box to type the last name of the user. This field is optional.
   - **Name** Use this box to type a name for the user. This is the name that's listed in Active Directory. By default, this box is populated with the names you enter in the **First name**, **Initials**, and **Last name** boxes. If you didn't use those boxes, you must still type a name in this field. The name can't exceed 64 characters.
   - **User logon name (User Principal Name)** Use this box to type the name that the user will use to log on to the mailbox. The user logon name consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides.
   - **User logon name (pre-Windows 2000)** Use this box to type the name for the user that is compatible with the legacy versions of Microsoft Windows (prior to the release of Windows 2000 Server). This field is automatically populated based on the **User logon name (User Principal Name)** field. This field is required.
   - **Password** Use this box to type the password that the user must use to log on to his or her mailbox.

     Note:
     Make sure that the password you supply complies with the password length, complexity, and history requirements of the domain in which you are creating the user account.
   - **Confirm password** Use this box to confirm the password that you typed

in the **Password** box.

- **User must change password at next logon** Select this check box if you want the user to reset the password when they first logon to the mailbox.

  If you select this check box, at first logon, the new user will be prompted with a dialog box in which to change the password. The user won't be allowed to perform any tasks until the password is successfully changed.

6. On the **Mailbox Settings** page, complete the following fields:
   - **Alias** Use this box to type an alias for the mailbox. The alias can't exceed 64 characters and must be unique in the forest.
   - **Specify the mailbox database rather than using a database automatically selected** Select this check box to specify an Exchange 2010 mailbox database instead of allowing Exchange to select a database for you. Click **Browse** to open the **Select Mailbox Database** dialog box. This dialog box lists all the Exchange 2010 mailbox databases in your Exchange organization. By default, the mailbox databases are sorted by name. You can also click the title of the corresponding column to sort the databases by database name or server name. Select the mailbox database you want to use, and then click **OK**. This is an optional field.
   - **Managed folder mailbox policy** Leave this check box cleared. Managed folders aren't compatible with archives because archives use retention policies. To learn more, see Understanding Retention Tags and Retention Policies.
   - **Exchange ActiveSync mailbox policy** Select this check box to specify an Exchange ActiveSync mailbox policy for the mailbox. Exchange ActiveSync enables access to an Exchange mailbox from a mobile device. To learn more, see Understanding Exchange ActiveSync Mailbox Policies.

     Click **Browse** to open the **Select ActiveSync Mailbox Policy** dialog box. Use this dialog box to select the policy that you want associated with this mailbox. This is an optional field.
7. On the **Archive Settings** page, select one of the following options:
   - **Create a local archive** Click this button to create a personal archive on an on-premises Exchange 2010 Mailbox server.

     If you want to specify a mailbox database on which to host the archive, select the associated check box and then click **Browse**.
   - **Create a remote hosted archive** Click this button to create a cloud-based archive in Exchange Online. Click **Browse** and then select the target delivery domain for your cloud-based organization. The target delivery domain is a remote domain that's created when you configure a hybrid deployment for Exchange Online Archiving. To learn more, see Configure Exchange Online Archiving.

     Note:

     When you enable a cloud-based archive for an on-premises mailbox, the user's archive status is displayed as **Cloud-based Archive Pending**. It may take up to two hours for the cloud-based archive to be created and the status updated in your on-premises organization. During this time, the user will still be able to access their primary mailbox.
8. On the **New Mailbox** page, review your configuration settings. To make any configuration changes, click **Back**. To create the new mailbox, click **New**.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Note:

If you selected the **Managed folder mailbox policy** check box on the **Mailbox Settings** page, you'll receive an error because archive mailboxes and managed folders are incompatible. Archive mailboxes use retention policies. To learn more, see Understanding Retention Tags and Retention Policies.

Use the Shell to create a mailbox and enable a personal archive

This example creates the user Chris Ashton in Active Directory, creates the mailbox on mailbox database DB01, and enables a personal archive. The password must be reset at the next logon. To set the initial value of the password, this example creates a variable (`$password`), prompts you to enter a password, and assigns that password to the variable as a **SecureString** object.

```
$password = Read-Host "Enter password" -AsSecureString
New-Mailbox -UserPrincipalName chris@contoso.com -Alias chris -Archive -Database
```

For detailed syntax and parameter information, see New-Mailbox.

Use the Shell to create a mailbox and enable a cloud-based archive

In this example, `service.contoso.com` is the target delivery domain. The domain must exist as a remote domain in your on-premises organization that's created when you configure a hybrid deployment for Exchange Online Archiving. Run this command to retrieve the target delivery domain:

```
Get-RemoteDomain | Where {$_.TargetDeliveryDomain -eq $true}
```

This example creates the user Chris Ashton in Active Directory, creates the mailbox on mailbox database DB01, and enables a cloud-based archive. The password must be reset at the next logon. To set the initial value of the password, this example creates a variable (`$password`), prompts you to enter a password, and assigns that password to the variable as a **SecureString** object. The *ArchiveDomain* parameter specifies the target delivery domain you retrieved in the previous command.

```
$password = Read-Host "Enter password" -AsSecureString
New-Mailbox -UserPrincipalName chris@contoso.com -Alias chris -Database "DB01" -N
```

Other Tasks

After you create the mailbox and a personal archive, you may also want to configure archive quotas to limit the size of the personal archive. For details, see Configure Archive Quotas for a Personal (On-Premises) Archive.

1.11.9.5.2 Enable a Personal (On-Premises) or Cloud-Based Archive for an Existing Mailbox

Enable a Personal (On-Premises) or Cloud-Based Archive for an Existing Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP1*

Topic Last Modified: *2012-07-23*

Enabling a personal archive (also called an *on-premises archive*) or cloud-based archive for an existing mailbox helps you regain control of your organization's messaging data by eliminating the need for personal store (.pst) files and allowing you to meet your organization's message retention and eDiscovery requirements. With archiving enabled, users can store messages in an archive mailbox, which is accessible by using Microsoft Outlook 2010 and Outlook Web App.

In Exchange 2010 Service Pack 1 (SP1) and later, the archive and the mailbox can be located on different Mailbox servers in your on-premises Exchange organization. To learn more, see Understanding Personal Archives.

Looking for other management tasks related to archiving? Check out Managing Archives.

Prerequisites

- The procedures in this topic show you how to enable personal and cloud based archives. However, to enable cloud-based archives, you must first configure Exchange Online Archiving. For details, see Configure Exchange Online Archiving.
- We recommend that mailbox users move all current archive data stored in their .pst files into their Inbox so they don't lose any messages. Alternatively, administrators can move the mailbox data by using the **Import-Mailbox** cmdlet. For more information, see Understanding Mailbox Import and Export Requests.

Use the EMC to enable a personal or cloud-based archive for an existing mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

Properties specific to a user mailbox are controlled by the **Set-Mailbox** cmdlet. In the EMC, you can set additional properties, and the permissions may vary depending upon the feature that you're configuring. With the permissions listed for this procedure, you can edit all of the settings available in the **<User Mailbox> Properties** dialog box.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox for which you want to enable a personal or cloud-based archive.
3. In the action pane, click **Enable Archive**.
4. In **Enable Archive Mailbox**, select one of the following options:
   - **Create a local archive** Click this button to enable a personal archive on an on-premises Exchange 2010 Mailbox server.
     If you want to specify a mailbox database on which to host the archive, select the associated check box, and then click **Browse**.
   - **Create a remote hosted archive** Click this button to enable a cloud-based archive in Exchange Online. Click **Browse** and then select the target delivery domain for your cloud-based organization. The target delivery domain is a remote domain that's created when you configure a hybrid deployment for Exchange Online Archiving. To learn more, see Configure Exchange Online Archiving.

Note:
When you enable a cloud-based archive for an on-premises mailbox, the user's archive status is displayed as **Cloud-based Archive Pending**. It may take up to two hours for the cloud-based archive to be created and the status updated in your on-premises organization. During this time, the user will still be able to access their primary mailbox.

Use the Shell to enable a personal archive for an existing mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

This example enables the personal archive for Tony Smith's mailbox.

```
Enable-Mailbox "Tony Smith" -Archive
```

This example enables the personal archive for all mailboxes on mailbox database DB01.

```
Get-Mailbox -Database DB01 | Enable-Mailbox -Archive
```

For detailed syntax and parameter information, see Enable-Mailbox and Get-Mailbox.

Use the Shell to enable a cloud-based archive for an existing mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Before you can enable a cloud-based archive, you need to obtain the target delivery domain. The domain must exist as a remote domain that's created in your on-premises organization when you configure a hybrid deployment for Exchange Online Archiving. Run this command to retrieve the target delivery domain.

```
Get-RemoteDomain | Where {$_.TargetDeliveryDomain -eq $true}
```

This example enables a cloud-based archive for the existing user Ayla Kol. The *ArchiveDomain* parameter specifies the target delivery domain that was retrieved in the previous command. In this example, service.contoso.com is the target delivery domain.

```
Enable-Mailbox ayla@contoso.com -RemoteArchive -ArchiveDomain "service.contoso.co
```

For detailed syntax and parameter information, see Enable-Mailbox.

Other Tasks

After you enable the personal archive, you may want to configure archive storage quotas. For details, see Configure Archive Quotas for a Personal (On-Premises) Archive.

1.11.9.5.3 Configure Archive Quotas for a Personal (On-Premises) Archive

Configure Archive Quotas for a Personal (On-Premises) Archive

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP1*

Topic Last Modified: *2012-07-23*

Because personal (on-premises) archives are created with unlimited storage quotas by default, you'll need to use the mailbox's property page to configure storage quotas for the personal archive. The following is a list of the quotas that you can configure with a description of each.

- **Archive warning quota** When a personal archive exceeds the specified archive warning quota, an event is logged for the Exchange administrator and a warning message is sent to the mailbox user.
- **Archive quota** When a personal archive exceeds the specified archive quota, messages are no longer moved to the archive and a warning message is sent to the mailbox user.

In the EMC, you can configure only the archive warning quota. In the Shell, you can configure the archive quota and the archive warning quota.

Looking for additional management tasks related to personal archive? Check out Managing Archives.

Use the EMC to configure the archive warning quota for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the user mailbox you want to configure.
3. In the action pane, click **Properties**.
4. In **<Mailbox Name> Properties**, click the **Mailbox Settings** tab.
5. Select **Archive Quota**, and then click **Properties**.
6. Select the **Issue warning at (MB)** check box, and then use the corresponding box to type the personal archive size in megabytes (MB), at which a warning will be sent to the user.
7. Click **OK**.

Use the Shell to configure the archive quota and archive warning quota for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Recipient Provisioning Permissions" section in the Mailbox Permissions topic.

Note:

You can't use the EMC to configure the archive quota for a mailbox.

This example sets the Chris Ashton mailbox archive quota to 1 gigabyte (GB), at which time the user will receive a warning message that the personal archive is full and will no

longer be able to move items to the personal archive. This example also sets the archive warning quota to 950 MB, at which time the user will receive a warning message that the personal archive is almost full.

```
Set-Mailbox -Identity "Chris Ashton" -ArchiveQuota 1GB -ArchiveWarningQuota 950MB
```

For detailed syntax and parameter reference, see Set-Mailbox.

1.11.9.5.4 Disable a Personal (On-Premises) or Cloud-Based Archive for a Mailbox

Disable a Personal (On-Premises) or Cloud-Based Archive for a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP1*

Topic Last Modified: *2012-07-23*

You may want to disable a user's personal (on-premises) or cloud-based archive for troubleshooting purposes or if you're moving the mailbox to a version of Exchange that doesn't support personal archives.

If you disable a personal archive, all information in the archive will be kept in the mailbox database until the mailbox retention time passes and the personal archive is permanently deleted. (By default, Exchange keeps disconnected mailboxes, including archive mailboxes, for thirty days. To modify the mailbox retention period, see Configure Deleted Mailbox and Disabled Personal Archive Retention.)

If you want to reconnect the personal archive to that mailbox, you can use the **Connect-Mailbox** cmdlet with the *Archive* parameter. If you want to reconnect a cloud-based archive to a mailbox, you can use the **Enable-Mailbox** cmdlet with the *RemoteArchive* parameter. For more information, see Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive.

Important:

The retention period for disconnected cloud-based archives is covered by the service level agreement (SLA) for Exchange Online Archiving. During this period, you can reconnect the cloud-based archive to the on-premises mailbox from which it was disconnected. After this period, the disconnected cloud-based archive is permanently deleted.

Looking for other management tasks related to personal archives? Check out Managing Archives.

Use the EMC to disable a personal archive

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Personal archives" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the mailbox for which you want to disable the personal archive.

   Note:

   You can create a filter to find all of the personal archives in your organization. In the result pane, click **Add Filter**. In the filter's list boxes, specify the following values: **Has Archive** > **Equals** > **Yes**. Click **Apply Filter**.
3. In the action pane, click **Disable Archive**.

4. A warning box appears confirming that you want to disable the archive. Click **Yes**.

Use the Shell to disable a personal archive

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Personal archives" entry in the Mailbox Permissions topic.

Disabling the personal archive will remove the archive from the mailbox and mark it in the mailbox database for deletion. This example disables the archive for Chris Ashton's mailbox. It doesn't disable the mailbox.

```
Disable-Mailbox -Identity "Chris Ashton" -Archive
```

A warning appears confirming that you want to disable the archive. Type **Y** to continue.

For detailed syntax and parameter information, see Disable-Mailbox.

Use the Shell to disable a cloud-based archive

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Personal archives" entry in the Mailbox Permissions topic.

Note:
You can’t use the EMC to disable a cloud-based archive.

Disabling the cloud-based archive removes the archive from the mailbox and marks it in Exchange Online for deletion. This example disables the cloud-based archive for Chris Ashton's mailbox. It doesn't disable the primary mailbox.

```
Disable-Mailbox -Identity "Chris Ashton" -RemoteArchive
```

A warning appears confirming that you want to disable the cloud-based archive. Type **Y** to continue.

For detailed syntax and parameter information, see Disable-Mailbox.

Other Tasks

After you disable the on-premises or cloud-based archive, you may want to reconnect the disconnected archive. For details, see Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive.

1.11.9.5.5 Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive

Connect a Disconnected Personal (On-Premises) or Cloud-Based Archive

Messaging Policy and Compliance > Archiving > Managing Archives >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP1*

Topic Last Modified: *2012-07-23*

When you disable a personal (on-premises) or cloud-based archive, it becomes disconnected. A disconnected personal archive is retained in the mailbox database for a specified amount of time. By default, Exchange retains disconnected personal archives for 30 days. During this time, you can recover the personal archive by associating it with an existing mailbox. You can modify the deleted mailbox retention period to retain a deleted mailbox or personal archive for a longer or shorter period. For more information, see Configure Deleted Mailbox and Disabled Personal Archive Retention.

Note:
If you disable a personal archive for a user mailbox and then enable a personal archive for that same mailbox, the mailbox will get a new personal archive.

The retention period for disconnected cloud-based archives is covered by the service level agreement (SLA) for Exchange Online Archiving. During this period, you can reconnect the cloud-based archive to the on-premises mailbox from which it was disconnected. After this period, the disconnected cloud-based archive is permanently deleted.

Looking for other management tasks related to personal archives? Check out Managing Archives.

Use the EMC to connect a disconnected personal archive

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Personal archives" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Disconnected Mailbox**.

   Note:
   If the personal archive that you want to connect to a mailbox isn't displayed in the result pane, restart the Microsoft Exchange Information Store service, and then run the **Clean-MailboxDatabase** cmdlet against the mailbox database that contains the personal archive.

2. In the result pane, select the personal archive that you want to connect to a primary mailbox.
3. In the action pane, click **Connect to Primary Mailbox**.
4. A warning appears confirming that you want to connect the personal archive to a specific user. This is the user to whom the archive belongs. Click **Yes**.

Use the Shell to connect a disconnected personal archive

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Personal archives" entry in the Mailbox Permissions topic.

1. If you don't know the name of the personal archive, you can view it in the Shell by running the following command. This example finds all disconnected personal archives on mailbox database DB01 and displays additional information about the personal archives such as the GUID and item count.

   ```
   Get-MailboxDatabase "DB01" | Get-MailboxStatistics | Where {($_.Discon
   ```

2. Connect the personal archive to the primary mailbox. This example connects Chris Ashton's archive to Chris Ashton's primary mailbox and uses the GUID as the personal archive's identity.

   ```
   Connect-Mailbox -Identity "8734c04e-981e-4ccf-a547-1c1ac7ebf3e2" -Arch
   ```

3. A warning appears stating that you'll have to wait for Active Directory replication to complete before the user can access the personal archive.

For detailed syntax and parameter information, see the following topics:

- Get-MailboxDatabase
- Get-MailboxStatistics
- Connect-Mailbox

Connect a disabled cloud-based archive

You can connect a disabled cloud-based archive to the user account from which it was disconnected by enabling a cloud-based archive for the mailbox. If a disconnected cloud-based archive exists for the mailbox, it will be connected. For details, see Enable a Personal (On-Premises) or Cloud-Based Archive for an Existing Mailbox.

Important:

When you attempt to connect a disconnected cloud-based archive to a mailbox, if the cloud-based archive has been permanently deleted, a new cloud-based archive is created.

1.11.9.5.6 Modify Archive Policies

Modify Archive Policies

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

In Exchange 2010 SP1 and later, you can use archive policies to automatically move mailbox items to personal (on-premises) or cloud-based archives. Archive policies are retention tags that use the **Move to Archive** retention action.

Exchange Setup creates a retention policy called **Default Archive and Retention Policy**. This policy has a default policy tag (DPT) assigned that moves items to the archive mailbox after two years. The policy also includes a number of personal tags that users can apply to folders or mailbox items to automatically move or delete messages. If a mailbox doesn't have a retention policy assigned when it's archive-enabled, the **Default Archive and Retention Policy** is automatically applied to it by Exchange. You can also create your own archive and retention policies and apply them to mailbox users. To learn more, see Understanding Retention Tags and Retention Policies.

You can modify retention tags included in the default policy to meet your business requirements. For example, you can modify the archive DPT to move items to the archive after three years instead of two. You can also create additional personal tags and either add them to a retention policy, including the **Default Archive and Retention Policy**, or allow users to add personal tags to their mailboxes from the Exchange Control Panel (ECP).

Looking for other management tasks related to archives? Check out Managing Archives.

Use the EMC to modify the default archive policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, on the **Retention Policy Tags** tab, select the **Default 2 year move to archive** retention tag.
3. In the action pane, click **Properties**.

4. Use the **General** tab to view or modify the following settings:
   - **Name** Use this unlabeled box at the top of the page to view or change the tag name.
   - **Modified** This read-only field displays the last date and time that the retention tag was modified.
   - **Tag Type** This read-only field displays the tag type.
   - **Age limit for retention (days)** Click this button to specify that items be moved to archive after a certain period. By default, this setting is configured to move items to the archive after two years (730 days). To modify this setting, in the corresponding text box, type the number of days in the retention period. The range of values is from 1 through 24,855 days.
   - **Action to take when the age limit is reached** Don't modify this field for archive policies.
   - **Disable this tag** Click this button to disable the tag. If a DPT or a RPT is disabled, the tag is no longer applied to the mailbox. If a personal tag is disabled, the retention period is displayed to the user as **Never**. If the user applies the tag to an item, the item is never moved to the user's archive mailbox.

     Important:
     Items that have a disabled retention tag applied aren't processed by the Mailbox Assistant. If you want to prevent a tag from being applied to items, we recommend disabling the tag rather than deleting it. When you delete a tag, the tag configuration is deleted from Active Directory, and the Mailbox Assistant processes all messages to remove the deleted tag.

     Note:
     If a user applies a tag to an item believing the item will never be moved, enabling the tag later may move items the user wanted to retain in the primary mailbox.
   - **Comments** Use this box to type a comment that will be displayed to Outlook and Outlook Web App users. For example, to alert users that MRM is enabled on the folder, you could type the message: "Messages are removed from this folder after 120 days." The maximum length of this comment is 255 characters. To configure localized comments, use the Set-RetentionPolicyTag cmdlet.

Use the Shell to modify archive policies

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Messaging records management" entry in the Messaging Policy and Compliance Permissions topic.

This example modifies the `Default 2 year move to archive` tag to move items after 1,095 days (3 years).

```
Set-RetentionPolicyTag "Default 2 year move to archive" -Name "Default 3 year mov
```

This example disables the `Default 2 year move to archive` tag.

```
Set-RetentionPolicyTag "Default 2 year move to archive" -RetentionEnabled $false
```

This example retrieves all archive DPTs and personal tags and disables them.

```
Get-RetentionPolicyTag | ? {$_.RetentionAction -eq "MoveToArchive"} | Set-Retenti
```

For detailed syntax and parameter information, see Set-RetentionPolicyTag and Get-RetentionPolicyTag.

1.11.10 Mailbox Audit Logging

Mailbox Audit Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-22*

Understanding Mailbox Audit Logging

Learn about the new Mailbox Audit Logging feature that allows you to track mailbox owner, delegate, and administrator logons to a mailbox, as well as what actions are taken while the user is logged on.

Managing Mailbox Audit Logging

Learn how to manage Mailbox Audit Logging.

1.11.10.1 Understanding Mailbox Audit Logging

Understanding Mailbox Audit Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-08-30*

Because mailboxes can potentially contain sensitive, high business impact (HBI) information and personally identifiable information (PII), it's important that you track who logs on to the mailboxes in your organization and what actions are taken. It's especially important to track access to mailboxes by users other than the mailbox owner. These users are referred to as *delegate users*.

By using *mailbox audit logging*, you can log mailbox access by mailbox owners, administrators, and delegates (including administrators who have full mailbox access permissions). Mailboxes are considered to be accessed by an administrator only in the following scenarios:

- Discovery search is used to search a mailbox
- The New-MailboxExportRequest cmdlet is used to export a mailbox
- Microsoft Exchange Server MAPI Editor is used to access the mailbox

When you enable audit logging for a mailbox, you can specify which user actions (for example, accessing, moving, or deleting a message) should be logged for a logon type (administrator, delegate user, or owner). The audit log entries also include important information, such as the client IP address, host name, and the process or client that is used to access the mailbox. For items that are moved, the entry includes the name of the destination folder.

Note:

For mailboxes such as the Discovery Search Mailbox, which may contain more sensitive information, consider enabling mailbox audit logging for mailbox owner actions such as message deletion.

Contents

Mailbox Audit Logs

Mailbox audit logs are generated for each mailbox that has mailbox audit logging enabled. Log entries are stored in the Audits subfolder of the audited mailbox Recoverable Items folder. This ensures that all audit logs are available from a single location, regardless of which client access method was used to access the mailbox or which server or workstation an administrator used to access the mailbox audit log. If you move a mailbox to another Mailbox server, the mailbox audit logs for that mailbox are also moved because they're located in the mailbox.

By default, mailbox audit log entries are retained in the mailbox for 90 days. You can modify this retention period by using the *AuditLogAgeLimit* parameter together with the **Set-Mailbox** cmdlet. If a mailbox is on litigation hold, audit logs are retained until the hold is removed.

Return to top

Enabling Mailbox Audit Logging

Mailbox audit logging is enabled per mailbox. Use the **Set-Mailbox** cmdlet to enable or disable mailbox audit logging. For details, see Enable or Disable Mailbox Audit Logging for a Mailbox.

When you enable mailbox audit logging for a mailbox, access to the mailbox and certain administrator and delegate actions are logged by default. To log actions taken by the mailbox owner, you must specify which owner actions should be audited. The following table lists the actions logged by mailbox audit logging, including the logon types for which the action is logged.

Mailbox actions logged by mailbox audit logging

Action	Description	Administrator	Delegate	Owner
Copy	An item is copied to another folder.	Yes	Not applicable	Not applicable
Create	An item is created in the mailbox. (For example, a message is sent or received.) **Note:** Folder creation isn't audited.	Yes*	Yes*	Yes

FolderBind	A mailbox folder is accessed.***	Yes*	Yes**	Yes
HardDelete	An item is deleted permanently from the Recoverable Items folder.	Yes*	Yes*	Yes
MessageBind	An item is accessed in the reading pane or opened.***	Yes	Not applicable	Not applicable
Move	An item is moved to another folder.	Yes*	Yes	Yes
MoveToDeletedItems	An item is moved to the Deleted Items folder.	Yes*	Yes	Yes
SendAs	A message is sent using Send As permissions.	Yes*	Yes*	Not applicable
SendOnBehalf	A message is sent using Send on Behalf permissions.	Yes*	Yes	Not applicable
SoftDelete	An item is deleted from the Deleted Items folder.	Yes*	Yes*	Yes
Update	An item's properties are updated.	Yes*	Yes*	Yes

* Audited by default if auditing is enabled for a mailbox.

** Entries for folder bind actions that are performed by delegates are consolidated. One log entry is generated for individual folder access within a time span of three hours.

*** FolderBind and MessageBind are not logged for the default calendar.

Mailbox access by authorized automated processes, such as accounts used by third-party tools or accounts used for lawful monitoring, can create a large number of mailbox audit log entries. This may not be of interest to your organization. You can configure such accounts to bypass mailbox audit logging. For details, see Bypass a User Account From Mailbox Audit Logging.

If you no longer require certain types of mailbox actions to be audited, you should modify the mailbox's audit logging configuration to disable those actions. Existing log entries aren't purged until the configured audit log age for the mailbox is reached.

Return to top

Searching Mailbox Audit Log Entries

You can use the following methods to search mailbox audit log entries:

- **Synchronously search a single mailbox** You can use the **Search-MailboxAuditLog** cmdlet to synchronously search mailbox audit log entries for a single mailbox. The cmdlet displays search results in the Exchange Management Shell window. For more information, see Search-MailboxAuditLog and Search the Mailbox Audit Log for a Mailbox.
- **Asynchronously search one or more mailboxes** You can create a mailbox audit log search to asynchronously search mailbox audit logs for one or more mailboxes, and then have the search results sent to a specified e-mail address. The search results are sent as an XML attachment. To create the search, use the New-MailboxAuditLogSearch cmdlet. For details, see Create a Mailbox Audit Log Search.
- **Use auditing reports in Exchange Control Panel** You can use the **Auditing** tab in Exchange Control Panel (ECP) to run auditing reports or export entries from the mailbox audit log and the administrator audit log. For details, see Auditing Tab.

Mailbox Audit Log Entries

The following table describes the fields logged in a mailbox audit logging entry.

Mailbox audit log fields

Field	Populated with
Operation	One of the following actions: • Copy • Create • FolderBind • HardDelete • MessageBind • Move • MoveToDeletedItems • SendAs • SendOnBehalf • SoftDelete • Update
OperationResult	One of the following results: • Failed • PartiallySucceeded • Succeeded
LogonType	Logon type of the user who performed the operation. Logon types include: • Owner • Delegate • Admin
DestFolderId	Destination folder GUID for move operations.
DestFolderPathName	Destination folder path for move operations.
FolderId	Folder GUID.
FolderPathName	Folder path.
ClientInfoString	Details that identify which client or Exchange component performed the operation.
ClientIPAddress	Client computer IP address.
ClientMachineName	Client computer name.

ClientProcessName	Name of the client application process.
ClientVersion	Client application version.
InternalLogonType	Logon type of the user who performed the operation. Logon types include: • Owner • Delegate • Admin
MailboxOwnerUPN	Mailbox owner user principal name (UPN).
MailboxOwnerSid	Mailbox owner security identifier (SID).
DestMailboxOwnerUPN	Destination mailbox owner UPN, logged for cross-mailbox operations.
DestMailboxOwnerSid	Destination mailbox owner SID, logged for cross-mailbox operations.
DestMailboxOwnerGuid	Destination mailbox owner GUID.
CrossMailboxOperation	Information about whether the operation logged is a cross-mailbox operation (for example, copying or moving messages among mailboxes).
LogonUserDisplayName	Display name of user who is logged on.
DelegateUserDisplayName	Delegate user display name.
LogonUserSid	SID of user who is logged on.
SourceItems	ItemID of mailbox items on which the logged action is performed (for example, move or delete). For operations performed on a number of items, this field is returned as a collection of items.
SourceFolders	Source folder GUID.
ItemId	Item ID.
ItemSubject	Item subject.
MailboxGuid	Mailbox GUID.
MailboxResolvedOwnerName	Mailbox user resolved name in the format *DOMAIN\SamAccountName*.
LastAccessed	Time when the operation was performed.
Identity	Audit log entry ID.

Return to top

1.11.10.2 Managing Mailbox Audit Logging

Managing Mailbox Audit Logging

Exchange Server 2010 > Messaging Policy and Compliance > Mailbox Audit Logging >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-16*

Enable or Disable Mailbox Audit Logging for a Mailbox

Bypass a User Account From Mailbox Audit Logging

Search the Mailbox Audit Log for a Mailbox

Create a Mailbox Audit Log Search

1.11.10.2.1 Enable or Disable Mailbox Audit Logging for a Mailbox

Enable or Disable Mailbox Audit Logging for a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-03*

By using mailbox audit logging, you can track logons to a mailbox, and also track what actions are taken while the user is logged on. When you enable mailbox audit logging for a mailbox, some actions performed by administrators and delegates are logged by default. None of the actions performed by the mailbox owner are logged. To learn more about mailbox audit logging, see Understanding Mailbox Audit Logging.

Caution:
Auditing of mailbox owner actions can generate a large number of mailbox audit log entries. Therefore, this feature is disabled by default. We recommend that you enable auditing only of specific owner actions that are needed to meet business or security requirements.

Note:
You can't use the Exchange Management Console (EMC) or the Exchange Control Panel (ECP) to enable or disable mailbox audit logging.

Looking for other management tasks related to mailbox audit logging? Check out Managing Mailbox Audit Logging.

Use the Shell to enable or disable mailbox audit logging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox audit logging" entry in the Messaging Policy and Compliance Permissions topic.

This example enables mailbox audit logging for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditEnabled $true
```

This example disables mailbox audit logging for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditEnabled $false
```

For detailed syntax and parameter information, see Set-Mailbox.

Use the Shell to specify logging settings for administrator, delegate, and owner access

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox audit logging" entry in the Messaging Policy and Compliance Permissions topic.

This example specifies that the `SendAs` or `SendOnBehalf` actions performed by delegate users will be logged for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditDelegate SendAs,SendOnBehalf -AuditEnable
```

This example specifies that the `MessageBind` and `FolderBind` actions performed by administrators will be logged for Ben Smith's mailbox.

Note:
MessageBind and FolderBind actions are not logged for the default Calendar.

```
Set-Mailbox -Identity "Ben Smith" -AuditAdmin MessageBind,FolderBind -AuditEnable
```

This example specifies that the `HardDelete` action performed by the mailbox owner will be logged for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditOwner HardDelete -AuditEnabled $true
```

For detailed syntax and parameter information, see Set-Mailbox.

Other Tasks

After you enable mailbox audit logging, you may also want to:

- Search the Mailbox Audit Log for a Mailbox
- Create a Mailbox Audit Log Search

1.11.10.2.2 Bypass a User Account From Mailbox Audit Logging

Bypass a User Account From Mailbox Audit Logging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you enable mailbox audit logging for a mailbox, specified mailbox access events (for example, accessing a folder or a message, or permanently deleting a message) are logged. However, access by some authorized accounts, such as accounts used by third-party tools or accounts used for lawful monitoring, can create a large number of mailbox audit log entries and may not be of interest to your organization.

You can configure a user or computer account to bypass mailbox audit logging, so actions taken by that user or account for any mailbox aren't logged. By bypassing trusted user or

computer accounts that need frequent access to mailboxes, you can reduce the noise in mailbox audit logs.

Note:
When an account is configured to bypass mailbox audit logging, access to any mailbox by that account won't be logged. You can't configure an account to bypass the logging of access to a specific mailbox.

Caution:
If you use mailbox audit logging to audit mailbox access and actions, you must monitor mailbox audit bypass associations at regular intervals. If a mailbox audit bypass association is added for an account, the account can access any mailbox in the organization to which it has been assigned permissions, without any mailbox audit logging entries being generated for such access or any actions taken (such as message deletions).

Looking for other management tasks related to mailbox audit logging? Check out Managing Mailbox Audit Logging.

Use the Shell to enable mailbox audit logging bypass for an account

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox audit logging" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to enable mailbox audit logging bypass for an account.

This example enables mailbox audit logging bypass for the ServiceAccess account.

```
Set-MailboxAuditBypassAssociation -Identity "ServiceAccess" -AuditBypassEnabled $
```

For detailed syntax and parameter information, see Set-MailboxAuditBypassAssociation.

Use the Shell to disable mailbox audit logging bypass for an account

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox audit logging" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to disable mailbox audit logging bypass for an account.

This example disables mailbox audit logging bypass for the ServiceAccess account.

```
Set-MailboxAuditBypassAssociation -Identity "ServiceAccess" -AuditBypassEnabled $
```

For detailed syntax and parameter information, see Set-MailboxAuditBypassAssociation.

Other Tasks

After you enable or disable mailbox audit logging bypass for a user or computer account, you may also want to:

- Enable or Disable Mailbox Audit Logging for a Mailbox
- Search the Mailbox Audit Log for a Mailbox
- Create a Mailbox Audit Log Search

1.11.10.2.3 Search the Mailbox Audit Log for a Mailbox

Search the Mailbox Audit Log for a Mailbox

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can synchronously search mailbox audit log entries for a mailbox and have the search results displayed in the Shell.

Note:
By default, mailbox audit logging is disabled for all mailboxes. For each mailbox you want to audit, you must enable audit logging and specify the mailbox owner, delegate, or administrator actions you want to audit. For more details, see Enable or Disable Mailbox Audit Logging for a Mailbox.

If you want to search mailbox audit logs for multiple mailboxes and have the results sent by e-mail to a specified address, you must create a mailbox audit log search instead. For more information, see Create a Mailbox Audit Log Search.

Looking for other management tasks related to mailbox audit logging? Check out Managing Mailbox Audit Logging.

Use the Shell to search the mailbox audit log for a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox audit logging" entry in the Messaging Policy and Compliance Permissions topic.

Note:
You can't use the EMC to search the mailbox audit log for a mailbox.

This example retrieves mailbox audit log entries for Ken Kwok's mailbox for actions performed by administrators and user delegates between 1/1/2010 and 12/31/2010. A maximum of 2,000 log entries are returned.

```
Search-MailboxAuditLog -Identity kwok -LogonTypes Admin,Delegate -StartDate 1/1/2
```

For detailed syntax and parameter information, see Search-MailboxAuditLog.

Other Tasks

After you search the mailbox audit log for a mailbox, you may also want to enable or disable mailbox audit logging. For detailed steps, see Enable or Disable Mailbox Audit Logging for a Mailbox.

1.11.10.2.4 Create a Mailbox Audit Log Search

Create a Mailbox Audit Log Search

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can create a mailbox audit log search to asynchronously search one or more mailboxes and have the search results sent by e-mail as an XML file to specified addresses.

Note:

By default, mailbox audit logging is disabled for all mailboxes. For each mailbox you want to audit, you must enable audit logging and specify the mailbox owner, delegate, or administrator actions you want to audit. For more details, see Enable or Disable Mailbox Audit Logging for a Mailbox.

To search mailbox audit logs for a single mailbox and have the results displayed in the Shell, see Search the Mailbox Audit Log for a Mailbox.

Looking for other management tasks related to mailbox audit logging? Check out Managing Mailbox Audit Logging.

Use the Shell to create a mailbox audit log search

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Mailbox audit logging" entry in the Messaging Policy and Compliance Permissions topic.

Note:

You can't use the Exchange Management Console (EMC) to create a mailbox audit log search.

This example creates the mailbox audit log search Admin and Delegate Access to search Ken Kwok's and April Stewart's mailboxes for administrator and delegate logons from 1/1/2010 to 12/31/2010. The search results are sent by e-mail to auditors@contoso.com.

```
New-MailboxAuditLogSearch "Admin and Delegate Access" -Mailboxes "Ken Kwok","Apri
```

For detailed syntax and parameter information, see New-MailboxAuditLogSearch.

Other Tasks

After you create a mailbox audit log search, you may also want to enable or disable mailbox audit logging. For detailed steps, see Enable or Disable Mailbox Audit Logging for a Mailbox.

1.12 Security

Security

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-14*

By default, Exchange Server 2010 is designed to help your organization be more secure. The server role-based Exchange Setup installs only the code required for a selected server role, thereby minimizing attack surface. Setup enables only the services required for a given server role and creates the necessary firewall exceptions (rules) in Windows Firewall with Advanced Security to allow communication with those services.

The following topics are gateways to information about security in Exchange 2010.

Exchange 2010 Security Guide

The Exchange 2010 Security Guide provides a comprehensive overview of the security features included in Exchange 2010.

Certificates

View a list of links to topics that provide information about managing digital certificates in Exchange 2010.

Securing Client Access Servers

View a list of links to topics that provide information about managing the security of your Client Access servers.

Securing Transport Servers

View a list of links to topics that provide information about managing the security of your transport infrastructure.

Securing Unified Messaging Servers

View a list of links to topics that provide information about managing the security of your Unified Messaging servers.

Permissions

View a list of links to topics that provide information about the permissions models used by Exchange 2010, including the permissions required to perform operations in each area of Exchange 2010.

Administrator Audit Logging

View a list of links to topics that provide information about administrator audit logging and how to use it to log the cmdlets run in the Exchange Management Shell, the Exchange Management Console, and the Exchange Control Panel.

Mailbox Audit Logging

View a list of links to topics that provide information about mailbox audit logging, a feature that allows you to track mailbox owner, delegate, and administrator logons to a mailbox, as well as what actions are taken while the user is logged on.

1.12.1 Exchange 2010 Security Guide

Exchange 2010 Security Guide

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-08*

This guide is written for the IT administrator responsible for securing the Microsoft Exchange Server 2010 deployment and is designed to help the IT administrator understand and manage the overall security environment where Exchange is installed.

In the past, for each version of Microsoft Exchange, the Exchange team has published stand-alone security hardening guides with permission and security information. This approach made sense for locking down services and directories after Exchange 2010 Setup ran. However, starting with Microsoft Exchange Server 2007, Exchange Setup enables only those services that are required by the server role that's being installed. Microsoft Exchange is no longer installed and then hardened for security. It's designed to help you be more secure by default.

Therefore, unlike earlier versions of Microsoft Exchange where IT administrators had to perform multiple procedures to lock down their servers that were running Microsoft Exchange, Exchange 2010 requires no lock-down or hardening.

Scope

Exchange 2010 was developed using Microsoft Security Development Lifecycle (SDL) principles. A security review was performed for each feature and component. Carefully chosen default settings ensure a more secure deployment. The scope of this guide is to inform administrators about security-related features and the features that may affect security considerations. This guide links to security-related topics in Exchange 2010 documentation. These topics are listed in Appendix 1: Additional Security-Related Documentation. This guide doesn't cover any steps to harden the Windows Server operating system.

Contents

What's New

Exchange 2010 includes the following new security features:

- **Role-Based Access Control** Exchange 2010 includes a new role-based access control model that lets your organization granularly manage permissions assigned to different stakeholders such as recipient administrators, server administrators, records and discovery managers, and organization administrators.
- **Throttling Policies** Exchange 2010 introduces throttling mechanisms on Mailbox, Client Access, and Transport servers to protect your organization from denial of service attacks and reduce the impact of such attacks.
- **Federated Delegation** Exchange 2010 introduces new federated delegation features that enable you to allow your users to securely collaborate with users in external organizations. Using federated delegation, users can share their calendar and contacts with users in external federated organizations. Cross-forest collaboration is also made possible, without the need to set up and manage Active Directory trust relationships.
- **Information Rights Management** Exchange 2010 includes new information protection and control features that enable you to protect sensitive message content at multiple levels while maintaining your organization's ability to decrypt, search, and apply messaging policies to protected content.
- **No Security Configuration Wizard** In Exchange 2010, Setup makes the configuration changes necessary to install and enable only those services required for a particular Exchange server role and to limit communication to only those ports required for the services and processes running on each server role. This removes the need for tools such as the Security Configuration Wizard (SCW) to configure these settings.

The Exchange 2010 Security Development Lifecycle

In early 2002, Microsoft introduced the Trustworthy Computing initiative. Since Trustworthy computing was introduced, the development process at Microsoft and in the Microsoft Exchange team has focused on developing software that helps you become more secure. For more information, see Trustworthy Computing.

In Exchange 2010, Trustworthy Computing was implemented in the following core areas:

- **Secure by design** Exchange 2010 was designed and developed in compliance with The Trustworthy Computing Security Development Lifecycle. The first step in creating a more secure messaging system was to design threat models and test each feature as it was designed. Multiple security-related improvements were built into the coding process and practices. Build-

time tools detect buffer overruns and other potential security threats. No system can guarantee complete security. However, by including secure design principles into the whole design process, Exchange 2010 is more secure than earlier versions have been.

- **Secure by default** One goal of Exchange 2010 was to develop a system in which most network communications are encrypted by default. Except for Server Message Block (SMB) communications and some Unified Messaging (UM) communications, the goal was met. By using self-signed certificates, the Kerberos protocol, Secure Sockets Layer (SSL), and other industry standard encryption techniques, almost all Exchange 2010 data is protected on the network. In addition, role-based setup makes it possible to install Exchange 2010 so that only the services, and the permissions related to those services, are installed with a specific and appropriate server role. In earlier versions of Microsoft Exchange, all services for all functionality had to be installed.
- **Anti-spam and antivirus functionality** Exchange 2010 includes a suite of anti-spam agents that run at the perimeter network on the Edge Transport server role, and can also be installed on the Hub Transport server role residing on the internal network. Antivirus functionality is further improved by the addition of Microsoft Forefront Protection 2010 for Exchange Server as a Microsoft solution.
- **Secure in deployment** As Exchange 2010 was developed, the pre-release version was deployed in the Microsoft IT production environment. Based on the data from that deployment, the Microsoft Exchange Server Best Practices Analyzer has been updated to scan for real-world security configurations, and pre-deployment and post-deployment best practices have been documented in the Exchange 2010 Help.
  In the past, permission management was documented and delivered after the core documentation was finished. However, we know that permissions management isn't an add-in process. It should be built into the overall planning and deployment of your Exchange 2010 deployment. Therefore, we've streamlined our permission documentation and integrated it into the core documentation to provide seamless context for administrators as they plan for and deploy their administrative model. Exchange 2010 includes a new role-based permissions model that allows you to grant granular permissions to administrators and users to enable them to perform tasks with the minimum permissions required.
- **Communications** Now that Exchange 2010 is released, the Exchange team is committed to keeping software up-to-date and you informed. By keeping your system up-to-date with Microsoft Update, you can make sure that the latest security updates are installed in your organization. Exchange 2010 also includes anti-spam updates. In addition, by subscribing to the Microsoft Technical Security Notifications, you can keep up with the latest security issues in Exchange 2010.

Getting Secure—Best Practices

Some basic best practices will help you create and maintain a more secure environment. Generally, running analyzer tools periodically and keeping software and antivirus signatures files up to date are the most effective ways to optimize your Exchange 2010 environment for security.

Setup and Installation Recommendations

These best practices will help you create a more secure Exchange 2010 environment:

- **Delegate Setup** The first Exchange 2010 server you install in your organization requires that the account you use to run Setup must be a member of the Enterprise Administrators group. The account you use is added to the Organization Management role group created by Exchange 2010 Setup. You can use delegated setup to allow administrators who aren't members of the Organization Management role group to set up subsequent servers. For more details, see Provision Exchange 2010 Server and Delegate Setup.

- **File system permissions** Exchange 2010 Setup assigns the minimum required permissions on the file system where Exchange binaries and data are stored. You must not make any changes to the Access Control Lists (ACLs) on the root folders and the Program Files folder on the file system.
- **Install paths** We recommend that you install Exchange 2010 binaries on a non-system drive (a volume other than where the operating system is installed). Exchange databases and transaction logs can grow rapidly, and must be located on non-system volumes sized for capacity and performance. Many other logs generated by different Exchange components, such as transport logs, are also stored in the same install path as Exchange binaries and can grow significantly, depending on the configuration and your messaging environment. In Exchange 2010, the maximum size of many log files and the maximum storage space a log file folder can occupy is configurable, and is set to a default of 250 Megabytes. To prevent a potential system outage because of low disk space, we recommend that you assess the logging requirements for each server role and configure the logging options and log file storage locations to meet your requirements.
- **Blocking legacy Outlook clients** Based on your requirements, you can configure Outlook client blocking to block legacy Outlook client versions. Certain Exchange 2010 features, such as Outlook Protection Rules and Personal Archives, don't support legacy Outlook clients. For more information about Outlook client blocking, see Configure Outlook Client Blocking.
- **Decoupling SMTP addresses from usernames** By default, Exchange generates e-mail addresses and aliases based on the mailbox user's username. Many organizations create an additional e-mail address policy to decouple user e-mail addresses from usernames for added security. For example, if the user Ben Smith's username is bsmith and the domain is contoso.com, the primary e-mail address generated by the default e-mail address policy is bsmith@contoso.com. You can create an additional e-mail address policy to generate e-mail addresses that don't use the user's alias or username. For example, creating an e-mail address policy to use the template `%g.%s@domain` generates e-mail addresses in the format Firstname.Lastname@domain. For the user Ben Smith, the policy will generate the address Ben.Smith@contoso.com. Or, you can decouple e-mail addresses from usernames by specifying an alias that's different from the username when you create or enable a mailbox.

Note:

If a user's primary SMTP address doesn't match the UPN on the account, the user can't use their e-mail address to sign in to Microsoft Office Outlook Web App and must provide a username using the DOMAIN\username format. When using Microsoft Outlook, the user must provide the username in DOMAIN \username format if prompted for credentials when Outlook connects to the Autodiscover service.

Microsoft Update

Microsoft Update is a service that offers the same downloads as Microsoft Windows Update—plus the latest updates for other Microsoft programs. It can help you keep your server more secure and performing at its best.

A key feature of Microsoft Update is Windows Automatic Update. This feature automatically installs high-priority updates that are critical to the security and reliability of your computer. Without these security updates, your computer is more vulnerable to attack from cyber-crooks and malicious software (malware).

The most reliable way to receive Microsoft Update is to have the updates delivered automatically to your computer by using Windows Automatic Updates. You can turn on Automatic Updates when you sign up for Microsoft Update.

Windows will then analyze the Microsoft software that's installed on your computer for

any current and past high-priority updates it requires and then download and install them automatically. After that, when you connect to the Internet, Windows repeats the update process for any new high-priority updates.

To enable Microsoft Update, see Microsoft Update.

The default mode of Microsoft Update requires that each Exchange server is connected to the Internet to receive automatic updates. If you are running servers that aren't connected to the Internet, you can install Windows Server Update Services (WSUS) to manage the distribution of updates to computers in your organization. You can then configure Microsoft Update on the internal Microsoft Exchange computers to contact your internal WSUS server for updates. For more information, see Microsoft Windows Server Update Services 3.0.

WSUS isn't the only Microsoft Update management solution available. For more information about Microsoft security releases, processes, communications and tools, see the Microsoft Security Update Guide.

Tasks No Longer Required in Exchange 2010

It's no longer necessary to install or run the following tools:

- The URLScan security tool isn't required for IIS 7. In earlier versions of Microsoft Exchange, it was a common practice to install IIS tools such as URLScan to secure an IIS installation. Exchange 2010 requires Windows Server 2008, which includes IIS 7. Many of the security features that were originally available in UrlScan are now available in the IIS 7 Request Filtering features.
- You no longer need to install the Exchange Best Practices Analyzer. In earlier versions of Microsoft Exchange, it was a common practice to install and run the Exchange Best Practices Analyzer before installation and regularly after that. Exchange 2010 Setup includes the Exchange Best Practices Analyzer components and runs them during setup. It isn't required to run the Exchange Best Practices Analyzer before setup.
- You no longer need to use the Security Configuration Wizard (SCW) or the Exchange templates for SCW. Exchange 2010 Setup installs only those services required for a given Exchange server role, and creates Windows Firewall with Advanced Security rules to open only the ports required for the services and processes for that server role. It's no longer required to run the Security Configuration Wizard (SCW) to do this. Unlike Exchange Server 2007, Exchange 2010 isn't included with SCW templates.

Staying Secure—Best Practices

These best practice recommendations will help you keep your Exchange 2010 environment secure.

Keeping Software up to Date

As mentioned in an earlier section, running Microsoft Update is a best practice. In addition to running Microsoft Update on all servers, it's also very important to keep all client computers up to date and to maintain antivirus updates on all computers in your organization.

In addition to Microsoft software, make sure that you run the latest updates for all software that's running in your organization.

Anti-Spam Updates

Exchange 2010 also uses the Microsoft Update infrastructure to keep the anti-spam filters up-to-date. By default, with manual updates, the administrator must visit Microsoft Update to download and install the content filter updates. The content filter update data is updated and available every two weeks.

Manual updates from Microsoft Update include the Microsoft IP Reputation Service or spam signature data. The Microsoft IP Reputation Service and spam signature data is only available with Forefront Security for Exchange Server anti-spam automatic updates.

For more information about how to enable Forefront anti-spam automatic updates, see Understanding Anti-Spam Updates.

Running Antivirus Software

Viruses, worms, and other malicious content transmitted by e-mail systems are a destructive reality faced by most Microsoft Exchange administrators. Therefore, you must develop a defensive antivirus deployment for all messaging systems. This section provides best practices recommendations for the deployment of antivirus software for Exchange 2010.

You should pay additional attention to two important changes in Exchange 2010 when you select an antivirus software vendor:

- Starting with Exchange Server 2007, Microsoft Exchange is based on a 64-bit architecture.
- Exchange 2010 includes transport agent functionality.

These two changes mean that antivirus vendors must provide Exchange 2010-specific software. Antivirus software that's written for earlier versions of Exchange is unlikely to operate correctly with Exchange 2010.

To use a defense-in-depth approach, we recommend that you deploy antivirus software that's designed for messaging systems at either the SMTP gateway or at the Exchange servers that host mailboxes, in addition to antivirus software on the user desktop.

You decide what types of antivirus software to use and where the software is deployed by determining the appropriate balance between the cost and risk you are willing to assume. For example, some organizations run antivirus messaging software at the SMTP gateway, file-level antivirus scanning at the Exchange server, and antivirus client software on the user desktop. This approach provides messaging-specific protection at the client. Other organizations may tolerate higher costs and therefore improve security by running antivirus messaging software at the SMTP gateway, file-level antivirus scanning at the Exchange server, and antivirus client software on the user desktop, together with antivirus software that's compatible with Exchange Virus Scanning Application Programming Interface (VSAPI) 2.5 on the Exchange Mailbox server.

Running Antivirus Software on Edge Transport Servers and Hub Transport Servers

Transport-based antivirus software is implemented as or includes transport agents. Transport agents act on transport events, much like event sinks in earlier versions of Microsoft Exchange. For more details, see Understanding Transport Agents.

Note:

Messages that aren't routed through transport, such as items in public folders, Sent Items, and calendar items, which can only be scanned on a Mailbox server, aren't protected by transport-only virus scanning.

Third-party developers can write customized transport agents to take advantage of the underlying MIME-parsing engine for robust transport-level antivirus scanning. For a list of Exchange antivirus and anti-spam partners, see Independent Software Vendors.

In addition, Forefront Protection for Exchange Server is an antivirus software package that's tightly integrated with Exchange 2010 and offers additional antivirus protection for your Exchange environment. For more information, see Microsoft Forefront Protection 2010 for Exchange Server.

The most important position for messaging antivirus software is at the first line of defense in your organization. This is the SMTP gateway through which external messages enter your messaging environment. In Exchange 2010, the first line of defense is the Edge Transport server.

If you use a non–Exchange SMTP server or gateway to receive inbound e-mail before Exchange, you should implement sufficient anti-spam and antivirus functionality on the non–Exchange SMTP hosts.

In Exchange 2010, all messages are routed through a Hub Transport server. This includes messages sent or received from outside the Exchange organization and messages sent within the Exchange organization. Messages sent to a mailbox located on the same Mailbox server as the sender. To better guard against virus outbreaks from inside the organization and to provide a second line of defense, we also recommend that you run transport-based antivirus software on Hub Transport servers.

Running Antivirus Software on Mailbox Servers

In addition to virus scanning on transport servers, a Microsoft Exchange Virus Scanning API (VSAPI) scanning solution running on Mailbox servers may be an important layer of defense in many organizations. You should consider running a VSAPI antivirus solution if any of the following conditions is true:

- Your organization doesn't have complete and reliable desktop antivirus scanning products deployed.
- Your organization wants the additional protection that scanning mailbox databases can provide.
- Your organization has developed custom applications that have programmatic access to an Exchange database.
- Your user community regularly posts messages in public folders.

Antivirus solutions that use Exchange VSAPI run directly within the Exchange information store process. VSAPI solutions are likely the only solutions that can protect against attack vectors that put infected content inside the Exchange information store while bypassing the standard client and transport scanning. For example, VSAPI is the only solution that scans data that's submitted to a database by CDO (Collaboration Data Objects), WebDAV, and Exchange Web Services (EWS). In addition, when a virus outbreak does occur, frequently a VSAPI solution provides the quickest way to remove and eliminate viruses from an infected mail database.

Exchange Server and File System Antivirus

If you deploy file-system antivirus software to protect your Exchange servers, consider the following:

- You must exclude Exchange server directories where the Exchange mailbox and public folder databases are stored, from file system antivirus scanners. For details, see File-Level Antivirus Scanning on Exchange 2010.
- File system antivirus scanners only protect files. To protect e-mail messages, you should also consider implementing Exchange-aware antivirus or messaging security products such as including Microsoft Forefront, or suitable partner or third-party products. For details about anti-spam and antivirus protection, see Understanding Anti-Spam and Antivirus Functionality. For details, see Forefront Protection 2010 for Exchange Server: Overview.
- You must keep antivirus and anti-spam signatures up-to-date for effective protection.
- Reports from antivirus and anti-spam software or services should be reviewed regularly to ensure protection is enabled and performing as required, detect incidents quickly, and take any required action.

Using Exchange Hosted Services

Spam and virus filtering is improved by or is also available as a service from Microsoft Exchange Hosted Services. Exchange Hosted Services is a set of four distinct hosted

services:

- Hosted Filtering, which helps organizations protect themselves from e-mail-borne malware
- Hosted Archive, which helps organizations satisfy compliance and retention requirements
- Hosted Encryption, which helps organizations encrypt data to preserve confidentiality
- Hosted Continuity, which helps organizations preserve access to e-mail during and after outages

These services integrate with any on-premises Exchange servers that are managed in house. For more information, see Forefront Online Protection for Exchange.

Using Attachment Filtering

In Exchange 2010, attachment filtering lets you apply filters on Edge Transport servers to control the attachments that users receive. Attachment filtering is increasingly important in today's environment where many attachment types contain harmful viruses or unsuitable material that may cause significant damage to the user's computer or to the organization by damaging important documentation or releasing sensitive information to the public.

You can use the following types of attachment filtering to control attachments that enter or leave your organization through an Edge Transport server:

Filtering based on file name or file name extension You can filter attachments by specifying the exact file name or file name extension to be filtered. An example of an exact file name filter is BadFilename.exe. An example of a file name extension filter is *.exe.

Filtering based on file MIME content type You can also filter attachments by specifying the MIME content type to be filtered. MIME content types indicate what the attachment is, whether it's a JPEG image, an executable file, a Microsoft Office Excel 2010 file, or some other file type. Content types are express as type/subtype. For example, the JPEG image content type is express as image/jpeg.

If an attachment matches one of these filtering criteria, you can configure the following actions to be performed on the attachment:

- Block whole message and attachment
- Strip attachment but allow message through
- Silently delete message and attachment

For more details, see Understanding Attachment Filtering.

Note:

You can't use the Attachment Filter agent to filter attachments based on their content. You can use transport rules to inspect the message and attachment content, and take actions such as deleting or rejecting the message, or IRM-protecting the message and attachments. For details, see Understanding Transport Rules.

File Filtering Using Forefront Protection for Exchange Server

The file filtering functionality that's provided by Forefront Protection for Exchange Server includes advanced features aren't available in the Attachment Filter agent included with Exchange 2010.

For example, container files, which are files that contain other files, can be scanned for offending file types. Forefront Protection for Exchange Server filtering can scan the following container files and act upon embedded files:

- PKZip (.zip)
- GNU Zip (.gzip)
- Self-extracting compressed file archives (.zip)
- Compressed files (.zip)

- Java archive (.jar)
- TNEF (winmail.dat)
- Structured storage (.doc, .xls, .ppt, and more)
- MIME (.eml0
- SMIME (.eml)
- UUEncode (.uue)
- Unix tape archive (.tar)
- RAR archive (.rar)
- MACBinary (.bin)

Note:
The Attachment Filter agent included with Exchange 2010 detects file types even if they've been renamed. Attachment filtering also makes sure that compressed Zip and LZH files don't contain blocked attachments by performing a file name extension match against the files in the compressed Zip or LZH file. Forefront Protection for Exchange Server file filtering has the additional capability of determining whether a blocked attachment has been renamed within a container file.

You can also filter files by file size. Also, you can configure Forefront Protection for Exchange Server to quarantine filtered files or to send e-mail notifications based Exchange on file filter matches.

For more information, see Protecting Your Microsoft Exchange Organization with Microsoft Forefront Security for Exchange Server.

Running the Exchange Best Practices Analyzer

The Exchange Best Practices Analyzer is one of the most effective tools that you can run regularly to help verify that your Exchange environment is secure. The Exchange Best Practices Analyzer automatically examines your Microsoft Exchange deployment and determines whether it's configured according to Microsoft best practices. In Exchange 2010, the Exchange Best Practices Analyzer is installed as part of Exchange Setup and can be run from the Tools section of the Exchange Management Console (EMC). With the appropriate network access, the Exchange Best Practices Analyzer examines all your Active Directory Domain Services (AD DS) servers and Exchange servers. The Exchange Best Practices Analyzer includes permissions inheritance checks. Also, it tests for validation of RBAC permissions. This include tests to ensure all users can access the Exchange Control Panel (ECP), all default RBAC roles created by Exchange Setup are configured properly, and there's at least one administrative account present within the Exchange organization.

Network Port Usage and Firewall Hardening

Windows Server 2008 includes Windows Firewall with Advanced Security, a stateful packet inspection firewall that's enabled by default. Windows Firewall with Advanced Security provides the following functionality:

- Filtering of all IP version 4 (IPv4) and IP version 6 (IPv6) traffic entering or leaving the computer. By default, all incoming traffic is blocked unless it's a response to a previous outgoing request from the computer (solicited traffic), or it's specifically allowed by a rule created to allow that traffic. By default, all outgoing traffic is allowed, except for service hardening rules that prevent standard services from communicating in unexpected ways. You can choose to allow traffic based on port numbers, IPv4 or IPv6 addresses, the path and name of an application, or the name of a service that's running on the computer, or other criteria.
- Protecting network traffic entering or exiting the computer by using the IPsec protocol to verify the integrity of the network traffic, to authenticate the

identity of the sending and receiving computers or users, and to optionally encrypt traffic to provide confidentiality.

Exchange 2010 is designed to run with the Windows Server Firewall with Advanced Security enabled. Exchange Setup creates the required firewall rules to allow Exchange services and processes to communicate. It creates only the rules required for the services and processes installed on a given server role. For more details about network port usage and firewall rules created for each Exchange 2010 server role, see Exchange Network Port Reference.

On Windows Server 2008 and Windows Server 2008 R2, Windows Firewall with Advanced Security allows you to specify the process or service for which a port is opened. This is more secure because it restricts usage of the port to the process or service specified in the rule. Exchange 2010 Setup creates firewall rules with the process name specified. In some cases, an additional rule that isn't restricted to the process is also created for compatibility purposes. You can disable or remove the rules that aren't restricted to the processes and keep the corresponding rules which are also created by Exchange 2010 Setup and are restricted to processes, if your deployment supports them. Rules that aren't restricted to processes are distinguished by the word (GFW) in the rule name. We recommend that you perform sufficient testing of the rules in your environment before you disable the rules that aren't restricted to a process.

The following table lists the Windows Firewall rules created by Exchange Setup, including the ports opened on each server role.

Windows Firewall rules

Rule name	Server roles	Port
MSExchangeRPCEPMap (GFW) (TCP-In)	All roles	RPC-EPMap
MSExchangeRPC (GFW) (TCP-In)	Client Access, Hub Transport, Mailbox, Unified Messaging	Dynamic RPC
MSExchange - IMAP4 (GFW) (TCP-In)	Client Access	143, 993 (TCP)
MSExchange - POP3 (GFW) (TCP-In)	Client Access	110, 995 (TCP)
MSExchange - OWA (GFW) (TCP-In)	Client Access	5075, 5076, 5077 (TCP)
MSExchangeMailboxReplication (GFW) (TCP-In)	Client Access	808 (TCP)
MSExchangeIS (GFW) (TCP-In)	Mailbox	6001, 6002, 6003, 6004 (TCP)
MSExchangeTransportWorker (GFW) (TCP-In)	Hub Transport	25, 587 (TCP)
SESWorker (GFW) (TCP-In)	Unified Messaging	Any
UMService (GFW) (TCP-In)	Unified Messaging	5060, 5061 (TCP)
UMWorkerProcess (GFW) (TCP-In)	Unified Messaging	5065, 5066, 5067, 5068

Important:

When modifying the default port used by an Exchange 2010 service, you must also

modify the corresponding Windows Firewall with Advanced Security firewall rule to allow communication over the nondefault port you decide to use. Exchange 2010 doesn't change firewall rules when you change default ports used for a service.

Throttling Parameters and Client Throttling Policies

Exchange 2010 includes throttling parameters on Transport, Client Access Server and Mailbox server roles to control different parameters of connections related to each protocol. Exchange 2010 also includes client throttling policies to control the load on Client Access servers. These throttling parameters and policies help you to control the load and protect Exchange 2010 servers from denial of service attacks targeted at different protocols.

Throttling Parameters on Transport Servers

On Exchange 2010 Transport servers, message throttling parameters are implemented on the server and on Send and Receive connectors to control message processing rates, SMTP connection rates, and SMTP session time-out values. Together, these throttling parameters protect transport servers from being overwhelmed by accepting and delivering lots of messages, providing protection from rogue SMTP clients and denial of service attacks.

You can configure the following throttling policies on Exchange 2010 Transport servers using the **Set-TransportServer** cmdlet.

Transport server throttling parameters

Parameter	Description
MaxConcurrentMailboxDeliveries	The *MaxConcurrentMailboxDeliveries* parameter specifies the maximum number of delivery threads that the Hub Transport server can have open at the same time to deliver messages to mailboxes. The store driver on the Hub Transport server is responsible for delivering messages to and from Mailbox servers. This limit applies to the delivery of messages to any mailboxes in the Exchange organization. **Default** 20 deliveries
MaxConcurrentMailboxSubmissions	The *MaxConcurrentMailboxSubmissions* parameter specifies the maximum number of delivery threads that the Hub Transport server can have open at the same time to accept messages from mailboxes. The store driver on the Hub Transport server is responsible for delivering messages to and from Mailbox servers. This limit applies to the acceptance of new messages from any mailboxes in the Exchange organization. **Default** 20 submissions
MaxConnectionRatePerMinute	The *MaxConnectionRatePerMinute* parameter specifies the maximum rate at which new inbound connections can be opened to the Hub Transport server or the Edge Transport server. These connections are opened to

	any Receive connectors that exist on the server. **Default** 1,200 connections per minute.
MaxOutboundConnections	The *MaxOutboundConnections* parameter specifies the maximum number of concurrent outbound connections that the Hub Transport server or Edge Transport server can have open at the same time. The outbound connections occur by using the Send connectors that exist on the server. The value that's specified by the *MaxOutboundConnections* parameter applies to all Send connectors that exist on the transport server. **Default** 1,000 connections. If you enter a value of unlimited, no limit is imposed on the number of outbound connections. This value can also be configured using the EMC.
MaxPerDomainOutboundConnections	The *MaxPerDomainOutboundConnections* parameter specifies the maximum number of connections that an Internet-facing Hub Transport server or Edge Transport server can have open to any single remote domain. The outbound connections to remote domains occur by using Send connectors that exist on the server. **Default** 20 connections per domain If you enter a value of unlimited, no limit is imposed on the number of outbound connections per domain. This value can also be configured using the EMC.
PickupDirectoryMaxMessagesPerMinute	The *MaxPerDomainOutboundConnections* parameter specifies the rate of message processing for both the **Pickup** directory and **Replay** directory. Each directory can independently process message files at the rate that's specified by the *PickupDirectoryMaxMessagesPerMinute* parameter. **Defaults** By default, the Pickup directory can process 100 messages per minute, and the Replay directory can process 100 messages per minute at the same time. The Pickup directory and the Replay directory scan for new message files once

	every 5 seconds, or 12 times per minute. This 5-second polling interval isn't configurable. This means the maximum number of messages that can be processed during each polling interval is the value that you assign to the *PickupDirectoryMaxMessagesPerMinute* parameter divided by 12 (PickupDirectoryMaxMessagesPerMinute/12). By default, a maximum of just over eight messages can be processed during each 5-second polling interval.

Throttling Parameters on Send Connectors

The following throttling parameters are available on Send connectors. Use the **Send-Connector** cmdlet to configure these parameters.

Send connector throttling parameters

Parameter	Description
ConnectionInactivityTimeOut	The *ConnectionInactivityTimeOut* parameter specifies the maximum time that an open SMTP connection with a destination messaging server can remain idle before the connection is closed. **Default** 10 minutes.
SmtpMaxMessagesPerConnection	The *SmtpMaxMessagesPerConnection* parameter specifies the maximum number of messages this Send connector server can send per connection. **Default** 20 messages

Throttling Parameters on Receive Connectors

You can configure the following throttling parameters on Receive connectors on Exchange 2010 Transport servers to control connection parameters such as inactivity timeouts, maximum number of connections and the number of SMTP protocol errors allowed during a connection. Use the **Set-ReceiveConnector** cmdlet to configure these parameters.

Receive connector throttling parameters

Parameter	Description
ConnectionInactivityTimeOut	The *ConnectionInactivityTimeOut* parameter specifies the maximum time that an open SMTP connection with a source messaging server can remain idle before the connection is closed. **Default on Hub Transport servers** 5 minutes. **Default on Edge Transport servers** 1 minute.
ConnectionTimeOut	The *ConnectionTimeOut* parameter specifies the maximum time that an SMTP connection with a source messaging server can remain

	open, even if the source messaging server is transmitting data. **Default on Hub Transport servers** 10 minutes **Default on Edge Transport servers** 5 minutes. The value specified by the ConnectionTimeout parameter must be larger than the value specified by the ConnectionInactivityTimeout parameter.
MaxInboundConnection	The *MaxInboundConnection* parameter specifies the maximum number of inbound SMTP connections that this Receive connector allows at the same time. **Default** 5,000
MaxInboundConnectionPercentagePerSource	The *MaxInboundConnectionPercentagePerSource* parameter specifies the maximum number of SMTP connections that a Receive connector allows at the same time from a single source messaging server. The value is expressed as the percentage of available remaining connections on a Receive connector. The maximum number of connections that are permitted by the Receive connector is defined by the *MaxInboundConnection* parameter. **Default** 2 percent
MaxInboundConnectionPerSource	The *MaxInboundConnectionPerSource* parameter specifies the maximum number of SMTP connections that a Receive connector allows at the same time from a single source messaging server. **Default** 100 connections
MaxProtocolErrors	The *MaxProtocolErrors* parameter specifies the maximum number of SMTP protocol errors that a Receive connector allows before the Receive connector closes the connection with the source messaging server. **Default** 5 errors

Throttling Parameters for the POP3 Service

The following throttling parameters are available for the Microsoft Exchange POP3 service on Client Access servers. Use the **Set-POPSettings** cmdlet to configure these parameters. For details, see Set Connection Limits for POP3.

POP3 service throttling parameters

Parameter	Description

MaxCommandSize	The *MaxCommandSize* parameter specifies the maximum size of a single command. The possible values are from 40 through 1024 bytes. **Default** 40 bytes.
MaxConnectonFromSingleIP	The *MaxConnectionFromSingleIP* parameter specifies the number of connections that the specified server accepts from a single IP address. The possible values are from 1 through 25,000. **Default** 2,000 connections
MaxConnections	The *MaxConnections* parameter specifies the total number of connections that the specified server accepts. This includes authenticated and unauthenticated connections. The possible values are from 1 through 25,000. **Default** 2,000 connections.
MaxConnectionsPerUser	The *MaxConnectionsPerUser* parameter specifies the maximum number of connections that the Client Access server accepts from a particular user. The possible values are from 1 through 25,000. **Default** 16 connections.
PreAuthenticationConnectionTimeOut	The *PreAuthenticatedConnectionTimeout* parameter specifies the time to wait before closing an idle connection that isn't authenticated. The possible values are from 10 through 3,600 seconds. **Default** 60 seconds.

Throttling Parameters for the IMAP4 Service

The following throttling parameters are available for the Microsoft Exchange IMAP4 service on Client Access servers. Use the **Set-IMAPSettings** cmdlet to configure these parameters. For details, see Set Connection Limits for IMAP4.

IMAP4 service throttling parameters

Parameter	Description
AuthenticationConnectionTimeOut	The *AuthenticatedConnectionTimeout* parameter specifies the period of time to wait before closing an idle authenticated connection. The possible values are from 30 through 86400 seconds. **Default** 1,800 seconds
MaxCommandSize	The *MaxCommandSize* parameter specifies the maximum size of a single command. The default size is 40 bytes. The possible values are from 40 through 1024 bytes.

	Default 40 bytes.
MaxConnectionFromSingleIP	The *MaxConnectionFromSingleIP* parameter specifies the number of connections that the specified server accepts from a single IP address. The possible values are from 1 through 25,000. **Default** 2,000 connections
MaxConnections	The MaxConnections parameter specifies the total number of connections that the specified server accepts. This includes authenticated and unauthenticated connections. The possible values are from 1 through 25,000. **Default** 2,000 connections
MaxConnectionsPerUser	The *MaxConnectionsPerUser* parameter specifies the maximum number of connections that the Client Access server accepts from a particular user. The possible values are from 1 through 25,000. **Default** 16 connections.
PreAuthenticatedConnectionTimeOut	The *PreAuthenticatedConnectionTimeout* parameter specifies the time to wait before closing an idle connection that isn't authenticated. The possible values are from 10 through 3600 seconds. **Default** 60 seconds

Client Throttling Policies

In Exchange 2010, you can use client throttling policies to manage Client Access server performance by controlling parameters such as the number of concurrent connections for each client access protocol, the percentage of time that a client session can use to run LDAP operations, RPC operations, and client access operations. There's a default client throttling policy that's generally sufficient to manage the load placed on Client Access servers. You can modify the default policy parameters or create custom policies that meet the requirements for your deployment.

Throttling policies are available for the following user groups and access methods:

- Anonymous access
- Cross-premises access (CPA)
- Exchange ActiveSync (EAS)
- Exchange Web Services (EWS)
- IMAP
- POP
- Outlook Web App (OWA)
- RPC Client Access (RCA)

The following throttling settings are available in client throttling policies for each of these user groups (Anonymous access and CPA) and access methods (EAS, EWS, IMAP, OWA, POP, and RCA).

Client throttling policy settings

Throttling setting	Anonymous Access	CPA	EAS	EWS	IMAP	OWA	POP	RCA
Max Concurrency	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Percent Time in AD	Yes	N. A.	Yes	Yes	Yes	Yes	Yes	Yes
Percent Time in CAS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Percent Time in Mailbox RPC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

CPA Cross-Premises Access

EAS Exchange ActiveSync

EWS Exchange Web Services

OWA Outlook Web App

In addition to these throttling settings based on user groups and access methods, the following throttling settings are available in a client throttling policy.

Client throttling policy parameters

Parameter	Description
CPUStartPercent	The *CPUStartPercent* parameter specifies the per-process CPU percentage at which users governed by this policy begin to be backed off. Valid values are from 0 through 100. Use $null to turn off CPU percentage-based throttling for this policy.
EASMaxDeviceDeletesPerMonth	The *EASMaxDeviceDeletesPerMonth* parameter specifies a limit to the number of Exchange ActiveSync partnerships that a user can delete per month. By default, each user can delete a maximum of 20 partnerships per calendar month. When the limit is reached, the partnership deletion attempt fails and an error message is displayed to the user.
EASMaxDevices	The *EASMaxDevices* parameter specifies a limit to the number of Exchange ActiveSync partnerships that a user can have at one time. By default, each user can create 10 Exchange ActiveSync partnerships with their Exchange account. After users exceed the limit, they must delete one of their existing partnerships before they can create any more new partnerships. An e-mail error

	message describing the limitation is sent to the user when the limit is exceeded. Also, an event is logged in the Application log when a user exceeds the limit.
EWSFastSearchTimeOutInSeconds	The *EWSFastSearchTimeoutInSeconds* parameter specifies the amount of time that searches made using Exchange Web Services continue before they time out. If the search takes more than the time indicated by the policy value, the search stops and an error is returned. The default value of this setting is 60 seconds.
EWSFindCountLimit	The *EWSFindCountLimit* parameter specifies the maximum result size of FindItem or FindFolder calls that can exist in memory on the Client Access server at the same time for this user in this current process. If an attempt is made to find more items or folders than your policy limit allows, an error is returned. However, the limit isn't strictly enforced if the call is made within the context of an indexed page view. Specifically, in this scenario, the search results are truncated to include the number of items and folders that fit within the policy limit. You can then continue paging into your results set via further FindItem or FindFolder calls.
EWSMaxSubscriptions	The *EWSMaxSubscriptions* parameter specifies the maximum number of active push and pull subscriptions that a user can have on a specific Client Access server at the same time. If a user tries to create more subscriptions than the configured maximum, the subscription fails, and an event is logged in Event Viewer.
ExchangeMaxCmdlets	The *ExchangeMaxCmdlets* parameter specifies the number of cmdlets that can be run within a specific time period before their execution is slowed down. The value specified by this parameter should be less than the value specified by the *PowerShellMaxCmdlets parameter*. The time period used for this limit is specified by the *PowerShellMaxCmdletsTimePeriod* parameter. We recommend that you set values for both parameters at the same time.
ForwardeeLimit	The *ForwardeeLimit* parameter specifies the limits for the number of recipients that can be configured in Inbox Rules when using the forward or redirect action. This parameter doesn't limit the number of messages that can be forwarded or redirected to the

	recipients that are configured.
MessageRateLimit	The *MessageRateLimit* parameter specifies the number of messages per minute that can be submitted to transport. For messages submitted through the Mailbox server role (Outlook Web App, Exchange ActiveSync, or Exchange Web Services), this results in the deferral of messages until the quota for the user is available. Specifically, messages appear in the Outbox or Drafts folder for longer periods of time when users submit messages at a rate greater than the MessageRateLimit parameter. For POP or IMAP clients submitting messages directly to transport using SMTP, clients receive a transient error if they submit at a rate that exceeds the MessageRateLimit parameter. Exchange tries to connect and send the messages at a later time.
PowerShellMaxCmdletQueueDepth	The *PowerShellMaxCmdletQueueDepth* parameter specifies the number of operations allowed to be run by the user. This value directly affects the behavior of the *PowerShellMaxCmdlets* and *PowerShellMaxConcurrency* parameters. For example, the *PowerShellMaxConcurrency* parameter consumes at least two operations defined by the *PowerShellMaxCmdletQueueDepth* parameter but additional operations are also consumed by per cmdlet execution. The number of operations depends on the cmdlets that are run. We recommend that the value for the *PowerShellMaxCmdletQueueDepth* parameter be at least three times larger than the value of the *PowerShellMaxConcurrency parameter*. This parameter won't affect Exchange Control Panel operations or Exchange Web Services operations.
PowerShellMaxCmdlets	The *PowerShellMaxCmdlets* parameter specifies the number of cmdlets that can be run within a specific time period before their execution is stopped. The value specified by this parameter should be more than the value specified by the *ExchangeMaxCmdlets* parameter. The time period used for this limit is specified by the *PowerShellMaxCmdletsTimePeriod* parameter. Both values should be set at the same time.
PowerShellMaxCmdletsTimePeriod	The *PowerShellMaxCmdletsTimePeriod* parameter specifies the time period, in seconds, that the throttling policy uses to determine whether the number of cmdlets being run exceeds the limits specified by

	the *PowerShellMaxCmdlets* and *ExchangeMaxCmdlets* parameters.
PowerShellMaxConcurrency	The *PowerShellMaxConcurrency* parameter specifies different information depending on context: In the context of Remote PowerShell, the *PowerShellMaxConcurrency* parameter specifies the maximum number of Remote PowerShell sessions that a Remote PowerShell user can have open at the same time. In the context of Exchange Web Services, the *PowerShellMaxConcurrency* parameter specifies the number of concurrent cmdlet executions that a user can have at the same time. This parameter value doesn't necessarily correlate to the number of browsers opened by the user
RecipientRateLimit	The *RecipientRateLimit* parameter specifies the limits on the number of recipients that a user can address in a 24-hour period.

For more details about Exchange 2010 throttling policies, see Understanding Client Throttling Policies.

Role-Based Access Control

Role-Based Access Control (RBAC) is the new permissions model in Exchange 2010 that allows you to control, at both broad and granular levels, what administrators and users can do. With RBAC, it's no longer required to modify Access Control Lists (ACLs) on Active Directory objects such as Organizational Units and containers to allow granular delegation of permissions to groups such as helpdesk operators or for functions such as recipient management. Active Directory

For more details, see Understanding Role Based Access Control. For a list of default RBAC management roles included in Exchange 2010, see Built-in Management Roles. For a list of default role groups, see Built-in Role Groups.

Role groups created by Exchange 2010 Setup or by you are created in Active Directory as universal security groups in the Microsoft Exchange Security Groups OU. You can add members to a role group by using the **New-RoleGroupMember** cmdlet or by using the Exchange Control Panel (ECP). When you add a member to a role group, the user or group is added to the corresponding Active Directory security group. You can use a Restricted Group policy to restrict membership for critical RBAC role groups such as Discovery Management. When you implement a Restricted Group policy, the group membership is monitored by Active Directory domain controllers and any users not included in the policy are automatically removed.

Important:
If you use Restricted Groups to restrict group membership for RBAC role groups, any changes you make to a role group using Exchange 2010 tools must also be made in the Restricted Group policy in Active Directory. For details, see Group Policy Security Settings.

Active Directory

Exchange Server stores configuration data in the Configuration partition and recipient data in the Domain partition of Active Directory Domain Services (AD DS). For details about permissions required to set up an Exchange 2010 organization, see Exchange 2010 Deployment Permissions Reference. Communication with Active Directory domain controllers is secured by using Kerberos authentication and encryption.

Exchange 2010 provides a new authorization layer inside Exchange, known as Role Based Access Control (RBAC), instead of relying on applying access control entries (ACEs) for every account that requires the appropriate permissions. In earlier versions of Microsoft Exchange, Exchange Setup relied on ACEs within Active Directory for Exchange administrators to be able to manage objects within the domain partition. Exchange administrators are granted the ability to perform certain operations within a specific scope through RBAC. The Exchange server runs the authorized actions on behalf of the administrator or users by using the permissions granted within Active Directory through the Exchange Windows Permissions and Exchange Trusted Subsystem security groups. For more information on RBAC, see Understanding Role Based Access Control.

In Exchange 2010, /PrepapareDomain doesn't apply any ACEs for the Exchange Windows Permissions universal security group to the **AdminSDHolder** container in Active Directory. If /PrepareDomain detects any ACEs granted to the Exchange Windows Permissions universal security group, the ACEs are removed. This has the following implications:

- Members of the Exchange Windows Permissions universal security group can't modify membership of protected security groups such as Enterprise Admins and Domain Admins. This has the following implications.
- Members of the Exchange Windows Permissions universal security group can't force password reset of an account protected by the **AdminSDHolder**.
- Members of the Exchange Windows Permissions universal security group can't alter the permissions of any group or account protected by the AdminSDHolder.

As a best practice, we recommend that you don't mailbox-enable accounts protected by the **AdminSDHolder** and do maintain separate accounts for Active Directory administrators: one account for Active Directory administration, and one account for regular day-to-day use, including e-mail. For details, see the following topics:

- Description and Update of the Active Directory AdminSDHolder Object
- Exchange 2010 and Resolution of the AdminSDHolder Elevation Issue

Exchange Server Accounts

Exchange 2010 Setup creates a new organizational unit (OU) in the root domain called Microsoft Exchange Security Groups. The following table shows the new universal security groups.

Microsoft Exchange security groups

Security group	Description
Exchange All Hosted Organizations	This group contains all the Exchange Hosted Organization Mailboxes groups. It's used for applying Password Setting Objects to all hosted mailboxes. This group shouldn't be deleted.
Exchange Servers	This group contains all the Exchange servers. This group should not be deleted. We strongly discourage making any membership changes to this group.

Exchange Trusted Subsystem	This group contains Exchange servers Exchange run Exchange cmdlets on behalf of users via Management service. Its members will have permission to read and modify all Exchange configuration, and also user accounts and groups. This group shouldn't be deleted.
Exchange Windows Permissions	This group contains Exchange servers that run Exchange cmdlets on behalf of users via Management service. Its members will have permission to read and modify all Windows accounts and groups. This group should not be deleted. We strongly discourage making any membership changes to this group, and suggest monitoring group membership.
ExchangeLegacyInterop	This group is for interoperability with Exchange 2003 servers within the same forest. This group should not be deleted.

In addition to these security groups, setup also creates the following security groups that correspond to RBAC role groups with the same name.

Security groups that correspond to RBAC role groups

Security group	RBAC role group
Delegated Setup	Delegated Setup
Discovery Management	Discovery Management
Help Desk	Help Desk
Hygiene Management	Hygiene Management
Organization Management	Organization Management
Public Folder Management	Public Folder Management
Recipient Management	Recipient Management
Records Management	Records Management
Server Management	Server Management
UM Management	UM Management
View-Only Organization Management	View-Only Organization Management

Also, when you create a new role group, Exchange 2010 creates a security group with the same name as the role group. For details, see the following topics:

- Built-in Role Groups
- Create a Role Group

Users are added or removed from these security groups when you add or remove users from role groups using the **Add-RoleGroupMember** or **Remove-RoleGroupMember** cmdlets, or by using the **Role Based Access Control (RBAC) User Editor** in the ECP.

File system

Exchange 2010 Setup creates directories with minimum permissions required for Exchange 2010 to function. We don't recommend any additional hardening of permissions to the default access control lists (ACLs) on directories created by setup.

Services

Exchange 2010 Setup doesn't disable any Windows services by default. The following table lists services enabled by default on each server role. Only the services required for operation of a particular Exchange 2010 server role are enabled by default.

Services installed by Exchange Setup

Service name	Service short name	Security context	Description and dependencies	Default startup type	Server roles	Required (R) or optional (O)
Microsoft Exchange Active Directory Topology	MSExchangeADTopology	Local System	Provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services cannot start. This service has no dependencies.	Automatic	Mailbox, Hub Transport, Client Access, Unified Messaging	R
Microsoft Exchange ADAM	ADAM_MSExchange	Network Service	Stores configuration data and recipient data on the Edge Transport server. This service represents the named instance of Active Directory Lightweight Directory Service (AD LDS) that's automatically created by	Automatic	Edge Transport	R

			Setup during Edge Transport server installation. This service depends on the COM+ Event System service.			
Microsoft Exchange Address Book	MSExchangeAB	Local System	Manages client address book connections. This service depends on the Microsoft Exchange Active Directory Topology service.	Automatic	Client Access	R
Microsoft Exchange Anti-spam Update	MSExchangeAntispamUpdate	Local System	Provides the Microsoft Forefront Protection 2010 for Exchange Server anti-spam update service. On Hub Transport servers, this service depends on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service depends on the Microsoft Exchange ADAM service.	Automatic	Hub Transport, Edge Transport	O

Microsoft Exchange Credential Service	MSExchangeEdgeCredential	Local System	Monitors credential changes in AD LDS and installs the changes on the Edge Transport server. This service depends on the Microsoft Exchange ADAM service.	Automatic	Edge Transport	R
Microsoft Exchange EdgeSync	MSExchangeEdgeSync	Local System	Connects to an AD LDS instance on subscribed Edge Transport servers over a secure LDAP channel to synchronize data between a Hub Transport server and an Edge Transport server. This service depends on the Microsoft Exchange Active Directory Topology service. If Edge Subscription isn't configured, this service can be disabled.	Automatic	Hub Transport	O
Microsoft Exchange File Distribution	MSExchangeFDS	Local System	Distributes offline address book (OAB) and custom Unified	Automatic	Client Access, Unified Messaging	R

			Messaging prompts. This service depends on the Microsoft Exchange Active Directory Topology and Workstation services.			
Microsoft Exchange Forms-Based Authentication	MSExchangeFBA	Local System	Provides forms-based authentication to Outlook Web App and the Exchange Control Panel. If this service is stopped, Outlook Web App and the Exchange Control Panel won't authenticate users. This service has no dependencies.	Automatic	Client Access	R
Microsoft Exchange IMAP4	MSExchangeIMAP4	Network Service	Provides IMAP4 service to clients. If this service is stopped, clients won't be able to connect to this computer using the IMAP4 protocol. This service depends on the Microsoft Exchange Active	Manual	Client Access	O

			Directory Topology service.			
Microsoft Exchange Information Store	MSExchangeIS	Local System	Manages the Exchange Information Store. This includes mailbox databases and public folder databases. If this service is stopped, mailbox databases and public folder databases on this computer are unavailable. If this service is disabled, any services that explicitly depend on it will fail to start. This service is dependent on the RPC, Server, Windows Event Log, and Workstation services.	Automatic	Mailbox	R
Microsoft Exchange Mail Submission Service	MSExchangeMailSubmission	Local System	Submits messages from the Mailbox server to Exchange 2010 Hub Transport servers. This service depends on the Microsoft	Automatic	Mailbox	R

			Exchange Active Directory Topology service.			
Microsoft Exchange Mailbox Assistants	MSExchange MailboxAssistants	Local System	Performs background processing of mailboxes in the Exchange store. This service depends on the Microsoft Exchange Active Directory Topology service.	Automatic	Mailbox	R
Microsoft Exchange Mailbox Replication Service	MSExchange MailboxReplication	Local System	Processes mailbox moves and move requests. This service depends on the Microsoft Exchange Active Directory Topology and Net.Tcp Port Sharing service.	Automatic	Client Access	O
Microsoft Exchange Monitoring	MSExchange Monitoring	Local System	Allows applications to call the Exchange diagnostic cmdlets. This service has no dependencies.	Manual	All	O
Microsoft Exchange POP3	MSExchange POP3	Network Service	Provides POP3 service to clients. If this service is stopped, clients can't connect to this	Manual	Client Access	O

			computer using the POP3 protocol. This service depends on the Microsoft Exchange Active Directory Topology service.			
Microsoft Exchange Protected Service Host	MSExchangeProtectedServiceHost	Local System	Provides a host for several Exchange services that must be protected from other services. This service depends on the Microsoft Exchange Active Directory Topology service.	Automatic	Hub Transport, Client Access	R
Microsoft Exchange Replication Service	MSExchangeRepl	Local System	Provides replication functionality for mailbox databases on Mailbox servers in a database availability group (DAG). This service depends on the Microsoft Exchange Active Directory Topology service.	Automatic	Mailbox	O
Microsoft Exchange RPC Client Access	MSExchangeRPC	Network Service	Manages client RPC connections for	Automatic	Mailbox, Client Access	O (Mailbox), R (Client Access)

			Exchange. This service depends on the Microsoft Exchange Active Directory Topology service.			
Microsoft Exchange Search Indexer	MSExchange Search	Local System	Drives indexing of mailbox content, which improves the performance of content search. This service depends on the Microsoft Exchange Active Directory Topology and Microsoft Search (Exchange Server) services.	Automatic	Mailbox	O
Microsoft Exchange Server Extension for Windows Server Backup	WSBExchange	Local System	Enables Windows Server Backup users to back up and recover application data for Microsoft Exchange. This service has no dependencies.	Manual	Mailbox	O
Microsoft Exchange Service Host	MSExchange ServiceHost	Local System	Provides a host for several Exchange services. On internal server roles,	Automatic	All	R

			this service depends on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service depends on the Microsoft Exchange ADAM service.			
Microsoft Exchange Speech Engine	MSSpeechService	Network Service	Provides speech processing services for Unified Messaging. This service depends on the Windows Management Instrumentation (WMI) service.	Automatic	Unified Messaging	R
Microsoft Exchange System Attendant	MSExchangeSA	Local System	Forwards directory lookups to a global catalog server for legacy Outlook clients, generates e-mail addresses and OABs, updates free/busy information for legacy clients, and maintains permissions and group memberships for the	Automatic	Mailbox	R

			server. If this service is disabled, any services that explicitly depend on it will fail to start. This service is dependent on the RPC, Server, Windows Event Log, and Workstation services.			
Microsoft Exchange Throttling	MSExchange Throttling	Network Service	Limits the rate of user operations. This service depends on the Microsoft Exchange Active Directory Topology service.	Automatic	Mailbox	R
Microsoft Exchange Transport	MSExchange Transport	Network Service	Provides SMTP server and transport stack. On Hub Transport servers, this service depends on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service depends on the Microsoft Exchange ADAM service.	Automatic	Hub Transport, Edge Transport	R

Microsoft Exchange Transport Log Search	MSExchangeTransportLogSearch	Local System	Provides remote search capability for Microsoft Exchange Transport log files. On Hub Transport servers, this service depends on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service depends on the Microsoft Exchange ADAM service.	Automatic	Hub Transport, Mailbox, Edge Transport	O
Microsoft Exchange Unified Messaging	MSExchangeUM	Local System	Enables Microsoft Exchange Unified Messaging features. This allows voice and fax messages to be stored in Exchange and gives users telephone access to e-mail, voice mail, calendar, contacts, or an auto attendant. If this service is stopped, Unified Messaging isn't	Automatic	Unified Messaging	R

			available. This service depends on the Microsoft Exchange Active Directory Topology and the Microsoft Exchange Speech Engine service.			
Microsoft Search (Exchange Server)	msftesql-Exchange	Local System	This is a Microsoft Exchange-customized version of Microsoft Search. This service is dependent on the RPC service.	Manual	Hub Transport, Mailbox	O

Certificates

Exchange 2010 Setup creates self-signed certificates to secure communication over different protocols such as HTTP, SMTP, POP3 and IMAP4. The self-signed certificates created by Setup are valid for five years. This ensures that the self-signed certificates don't have to be renewed for a significant part of an Exchange 2010 deployment and messaging services aren't affected by the expiration of self-signed certificates.

For external client access mechanisms and protocols, such as Outlook Web App, POP3, IMAP4, Outlook Anywhere, and AutoDiscover, we recommend that you:

- Use certificates signed by a commercial certification authority (CA) that's trusted by clients accessing those services.
- Use the New Exchange Certificate wizard or the New-ExchangeCertificate cmdlet to create certificate signing requests for commercial CAs. Certificate requests generated using these tools ensure that all Exchange certificate requirements are met.
- Consider the certificate requirements for each protocol or service for which you want to allow external client access.
  - On Client Access servers, certificates are used to protect HTTP traffic (Outlook Anywhere, Outlook Web App, AutoDiscover, Exchange ActiveSync, and Exchange Web Services) by using Secure Sockets Layer, and POP3 and IMAP4 traffic by using SSL or Transport Layer Security (TLS). For details, see Managing SSL for a Client Access Server.
  - On transport servers, certificates are used to protect SMTP traffic by using TLS. For details, see Understanding TLS Certificates.
  - On Unified Messaging servers, certificates are used to protect Voice over Internet Protocol (VoIP) traffic. For details, see Understanding Unified Messaging VoIP Security.
  - For Federation, certificates are used to encrypt SAML tokens exchanged with the Microsoft Federation Gateway (MFG) and with federated partner

organizations. For details, see Understanding Federation.

- Monitor certificate validity dates and renew certificates from CAs in a timely manner to avoid service disruption.
- When storing certificates exported with the associated private key, protect the exported file by using appropriate access controls on the folder/file where it's stored. Depending on your organization's security requirements, consider enabling auditing of file access for folders where certificate files with private keys are stored.

NTLM Considerations

The NTLM protocol is significantly less secure than the Kerberos protocol. In Exchange 2010, the POP3 and IMAP4 protocols don't support NTLM authentication when `SecureLogin` is specified as the *LoginType*. For details, see Configuring Authentication for POP3 and IMAP4. Exchange 2010 services that use Windows Integrated Authentication can use either NTLM or Kerberos protocols. Kerberos is used for Client Access server communication to an Exchange 2010 Mailbox server, and between Client Access servers for Outlook Web App, Exchange ActiveSync, and Exchange Web Services. For details about services that use NTLM to authenticate, see Exchange Network Port Reference.

Dual Factor Authentication

Dual factor authentication mechanisms use another authenticator in addition to the user's logon credentials (username and password), such as randomly generated tokens, or a digital certificate on a smartcard along with a PIN. Many organizations deploy dual factor authentication to allow secure access to the organization's network.

Exchange 2010 doesn't include native support for dual factor authentication. Exchange 2010 uses Internet Information Server (IIS) 7 for client access through HTTP (AutoDiscover, Outlook Web App, Outlook Anywhere, Exchange ActiveSync, and Exchange Web Services). Many dual factor authentication products that integrate with IIS are available from partners and third parties, and work with Exchange client access services such as Outlook Web App. Before deploying dual factor authentication products for Exchange services, we recommend that you test them adequately to ensure they meet your organization's security requirements and provide the functionality you require.

Federation

Exchange 2010 introduces new federation features to enable secure collaboration between federated Exchange organizations. Exchange 2010 organizations can create a federation trust with the Microsoft Federation Gateway, and then establish organization relationships with other federated organizations to share availability information and Calendars. Organizations can also allow users to share their availability information, Calendar and Contacts with users in external federated organizations by using Sharing Policies. For more details about Federation Trusts and Federated Sharing, see Understanding Federation and Understanding Federated Delegation.

After you establish a Federation Trust with MFG, sharing between two federated organizations doesn't occur unless you create an Organization Relationship. By default, however, sharing between your users and users in external federated organizations is enabled by using the Default Sharing Policy assigned to users. The policy allows Calendar sharing with free/busy information only to users in all external federated organizations. If you don't want to allow users to share their calendar and free/busy information with users in all external federated domains, you must disable the Default Sharing Policy or change the domain name specified in the policy to only those domains you want to allow sharing with. You must make this change before you create a Federation Trust with MFG. For more details, see Disable a Sharing Policy and Configure Sharing Policy Properties.

You can disable all Federation features for an organization, including Federated Delegation, by removing the organization's Federation Trust with MFG. For more details, see Remove a Federation Trust.

Secure/Multipurpose Internet Mail Extensions (S/MIME)

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of MIME data which provides authentication, message integrity, nonrepudiation, and data privacy for messaging data. Users can sign or encrypt messages, or both, using S/MIME certificates. For more information about S/MIME, see Understanding S/MIME.

S/MIME is a client-side technology without any interoperability requirements for e-mail servers. From a message transfer perspective, S/MIME signed or encrypted messages are transferred no differently than clear text (not encrypted) messages. Actual rendering of message is done on the client-side after certificate and message validation checks. For Outlook Web App, S/MIME support is provided by using an ActiveX control. Although Outlook Web App supports most popular browsers such as Microsoft Internet Explorer, Mozilla FireFox and Safari, ActiveX controls are an Internet Explorer feature. Outlook Web App users using other browsers can't access S/MIME features and may have to use another e-mail client which supports S/MIME. For more details about S/MIME support in Outlook Web App, see Outlook Web App and S/MIME.

For more details about S/MIME support in Outlook, see Overview of certificates and cryptographic e-mail messaging in Outlook.

Whereas S/MIME offers security benefits to an organization, when you evaluate the technology, you should consider the following:

- S/MIME encrypted messages are opaque to your organization. Messaging security software such as antivirus and anti-spam can't inspect message content, including message body and any attachments.
- Because message content and attachments are encrypted, your organization's messaging policies, including transport rules, can't be applied to S/MIME-encrypted messages.
- Modifying S/MIME-signed messages to comply with your organization's messaging policies, for example to apply a disclaimer or personalized signature, invalidates the message.
- Encrypted messaging content can't be inspected for any content violations, and your organization can't protect sensitive information. This includes any personally identifiable information (PII), from leaving the organization.
- S/MIME-encrypted messages can't be indexed by Exchange Search and are therefore not searchable by discovery.
- To meet local regulations or discovery requirements during litigation, your organization may be required to produce copies of all encrypted messages that are not encrypted.

Exchange 2010 offers Information Rights Management (IRM) features that allow your organization to apply persistent protection to sensitive messaging content so only specified recipients can access IRM-protected messages. Your organization can also implement controls on how such content is used after it's delivered to recipients. For example, you can prevent messages from being printed, replied to, or forwarded inside or outside the organization. Also, your organization can still decrypt the IRM-protected content for scanning by antivirus and anti-spam software and other transport agents, applying messaging policies using transport rules, and enable archiving and discovery of IRM-protected messages. IRM features are also available in all web browsers supported

by Outlook Web App and in Windows Mobile devices. For more details about IRM, see Understanding Information Rights Management.

Server Role Considerations

This section lists security-related considerations for the Exchange 2010 server role.

Mailbox Server Considerations

In Exchange 2010, architectural changes have been made to the Exchange store and connectivity from MAPI clients such as Outlook. MAPI clients connect to the Client Access Server, isolating the Mailbox server from client traffic. Mailbox servers communicate only with Client Access servers that use RPCSec, and with Active Directory Domain Services (AD DS) servers in your organization. Mailbox servers don't require Internet connectivity.

Storage

Storage is a critical component of Mailbox servers. You must plan your Mailbox server storage sub-system to ensure satisfactory performance and adequate storage space is available for your deployment. For more details about planning for Mailbox server storage, see Mailbox Server Storage Design.

After Mailbox server deployment, you should monitor the following the following:

- Availability of storage sub-system.
- Availability of sufficient free disk space on volumes that contain the mailbox database and transaction logs. A mailbox or Public Folder database is unmounted when the volume storing the database or transaction logs for it run out of free disk space.

You can use Microsoft Federation Gateway Systems Center Operations Manager to monitor storage availability and disk free space. For more details, see Systems Center Operations Manager 2007.

When planning for and monitoring storage, if you plan to use the following features, you must consider their storage requirements:

- **Journaling** When you use journaling to keep messages for long-term archival, depending on whether you use standard (per-mailbox database) or premium journaling (journal rules), messages sent to and from all recipients in a mailbox database or the recipients specified in a journal rule are delivered in a journal report to the journaling mailbox or recipient specified. The result can be a large number of journal reports delivered to a journaling mailbox. When planning storage for Mailbox servers, you must consider journaling mailbox sizes. You can control journaling mailbox sizes by configuring sufficient mailbox quotas for a journaling mailbox. For more details about journaling and mailbox quotas, see the following topics:
  - Understanding Journaling
  - Configure Storage Quotas for a Mailbox
- **Litigation Hold** When you place a mailbox on litigation hold, items deleted by the user by using the Recover Deleted Items functionality in Outlook and Outlook Web App and messages deleted by automated processes such as MRM are retained till litigation hold is removed. In Exchange 2010, the Recoverable Items warning quota and Recoverable Items quota are set to 20 GB and 30 GB. For more details, see the following topics:
  - Understanding Litigation Hold
  - Understanding Recoverable Items

High Availability

High Availability of Mailbox servers is critical in ensuring messaging service availability. Exchange 2010 includes Database Availability Groups (DAGs) for high availability of Mailbox servers. DAGs can provide availability when your Exchange deployment

experiences a failure of the storage sub-system, the server, or network connectivity, or an outage of a whole datacenter. For more details about planning and implementing a highly available Exchange 2010 deployment, see High Availability and Site Resilience.

By default, in Exchange 2010, replication (log shipping) traffic between DAG members located in different Active Directory sites is encrypted. You can encrypt replication traffic between servers in the same Active Directory site by setting the NetworkEncryption property of the DAG to Enabled. Use the **Set-DatabaseAvailabilityGroup** cmdlet to modify this property for a DAG.

Replication occurs over a single TCP port, by default TCP port 64327. You can modify the port used for replication. For details, see Configure Database Availability Group Properties.

Parameters for high availability

Parameter	Description
NetworkEncryption	The *NetworkEncryption* parameter specifies whether network encryption is enabled. Valid values include: • `Disabled` disabled on all networks • `Enabled` enabled on all networks • `InterSubnetOnly` Enabled for inter-subnet communication only • `SeedOnly` enabled only for seeding **Default** `InterSubnetOnly`
ReplicationPort	The *ReplicationPort* parameter specifies a Transmission Control Protocol (TCP) port for replication (log shipping and seeding) activity. **Default** If this parameter isn't specified, the default port for replication is TCP 64327.

Mailbox Permissions and Access

By default, Exchange 2010 doesn't allow administrators to access mailboxes. If your organization uses applications or services that require access to a mailbox, you must assign appropriate mailbox permissions to accounts used by such applications or services. We recommend that you don't configure such applications or services to use administrator credentials.

Although all mailboxes can potentially contain sensitive information valuable to an organization, the following mailboxes deserve special attention from a security perspective, and permissions to access these mailboxes must be controlled and monitored to meet your organization's security requirements.

- **Discovery mailboxes** Discovery mailboxes are used by the Exchange 2010 Multi-Mailbox Search feature. This allows discovery managers who are members of the Discovery Management role group to search messages in all mailboxes in an Exchange 2010 organization. Messages returned by a discovery search are copied to the specified Discovery mailbox. Exchange 2010 Setup creates a default Discovery Search Mailbox. For more details, see Understanding Multi-Mailbox Search.
- **Journaling mailboxes** When you configure journaling for a mailbox database or create Journal Rules to journal messages to and from specified recipients, journal reports are delivered to the specified journaling mailbox. For more details, see the following topics:
  - Understanding Journaling
  - Create and Configure a Journaling Mailbox

In addition to protecting these mailboxes, notice that an administrator can use transport rules to inspect message content and also deliver a copy of the message to another recipient, even as a Bcc recipient. The permissions required to manage transport rules are listed in the Transport rules entry in the Messaging Policy and Compliance Permissions topic. We recommend that you use adequate controls to monitor and control the creation and modification of transport rules and that you also regularly audit transport rule actions for all rules.

Client Access Server Considerations

In Exchange 2010, the following clients connect to Client Access servers to access mailboxes:

- Outlook clients using MAPI
- Outlook clients using Outlook Anywhere
- Web browsers using Outlook Web App,
- Mobile devices using Exchange ActiveSync
- POP3 & IMAP4 clients
- Applications that use Exchange Web Services (EWS)

By default, these client access methods are secured by using encrypted data paths. Also by default, Outlook clients connecting to a Client Access server using MAPI use RPC encryption. Outlook Web App, Outlook Anywhere and Exchange ActiveSync access is secured by using Secure Sockets Layer (SSL).

For external client access, you must obtain and install certificates signed by a certification authority (CA) trusted by the client. For more details, see Managing SSL for a Client Access Server.

By default, POP3 and IMAP4 services are disabled on Exchange 2010 Client Access servers. If you enable them, we recommend that you use Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to help secure communication by using these protocols. For more details, see the following topics:

- Understanding POP3 and IMAP4
- Configuring TLS and SSL for POP3 and IMAP4 Access

we recommend that you use appropriate firewalls and access controls when you publish Client Access servers for external access. Microsoft Forefront Threat Management Gateway (TMG) 2010 includes publishing wizards to easily and securely publish Exchange 2010 Client Access servers for external access. For more details, see Forefront Threat Management Gateway (TMG) 2010.

Important:
Locating Client Access servers on perimeter networks isn't supported.

On Client Access servers, Internet Information Server (IIS) is used to provide HTTP protocol access to services such as Outlook Web App, Exchange ActiveSync, Outlook Anywhere, AutoDiscover, Exchange Control Panel (ECP), Exchange Web Services and Offline Address Book (OAB). Remote PowerShell also uses IIS, And all RPS requests, including requests by the Exchange Management Console (EMC), are logged in IIS logs. IIS logs can grow to consume a large amount of disk space. IIS, a Windows Server component, doesn't include a mechanism to clear older logs based on the size of the directory in which the log files reside. As a best practice, IIS logs should be moved to a non-system volume, so growth of log files doesn't result in the system volume running out of disk space, which can cause a service outage. You should monitor log file growth and implement a mechanism to manually archive or delete logs as required. For details, see Configuring Logging in IIS 7.

Transport Server Considerations

Exchange 2010 offers two transport server roles that are designed for different purposes.

- **Edge Transport** The Edge Transport server role is a non-domain joined

transport server, usually located in perimeter networks, that transfers messages between your Exchange organization and external SMTP hosts. Although designed for perimeter networks, you can also locate Edge Transport servers on the internal network and join the server to an Active Directory domain as a member server.

- **Hub Transport** The Hub Transport server role transfers messages within the organization, including messages between Exchange servers, messages from SMTP clients such as users using POP3 and IMAP4, and application servers and devices.

By default, in Exchange 2010, SMTP communication is secured using TLS.

SMTP communication between Hub Transport servers Hub Transport servers in an Exchange organization use TLS to help secure SMTP communication within the organization. We recommend that you keep TLS enabled on Hub Transport servers. In Exchange 2010, organizations using non-Exchange devices or appliances to perform TLS encryption can offload TLS from Hub Transport servers to such appliances. For more details, see Disabling TLS Between Active Directory Sites to Support WAN Optimization.

SMTP communication between Hub Transport and Edge Transport servers All traffic between Hub Transport servers and Edge Transport servers is authenticated and encrypted. The underlying mechanism for authentication and encryption is mutual TLS. Instead of using X.509 validation to validate certificates, Exchange 2010 uses direct trust to authenticate certificates. Direct trust means the presence of the certificate in Active Directory or Active Directory Lightweight Directory Services (AD LDS) validates the certificate. Active Directory is considered a trusted storage mechanism. When direct trust is used, it doesn't matter whether the certificate is self-signed or signed by a certification authority (CA).When you subscribe an Edge Transport server to an Active Directory site, the Edge Subscription publishes the Edge Transport server's certificate in Active Directory. Hub Transport servers consider the published certificate valid. The Microsoft EdgeSync service updates AD LDS on Edge Transport servers that have Hub Transport server certificates, which are considered valid by the Edge Transport server.

SMTP communication between Edge Transport servers and external hosts In Exchange 2010, SMTP communication between Edge Transport servers and anonymous external hosts is secured by default using opportunistic TLS. You don't require a certificate issued by a trusted CA and no configuration steps are necessary. Receive Connectors offer TLS negotiation for inbound SMTP connections. Send Connectors also tries TLS negotiation for all outbound SMTP connections. Opportunistic TLS doesn't perform certificate validation, allowing the use of self-signed certificates. For details, see TLS Functionality and Related Terminology in Exchange 2010.

Note:

By default, Hub Transport servers can't communicate with external SMTP hosts as no Receive Connectors exist on Hub Transport servers that allow anonymous hosts to communicate. You can configure Hub Transport servers to communicate with anonymous hosts. For details, see Configure Internet Mail Flow Directly Through a Hub Transport Server. We don't recommend this topology because it increases security risks by exposing to the Internet the Exchange 2010 server and all roles installed on that server. We recommend that you implement a perimeter network-based SMTP gateway, such as the Edge Transport server, instead.

SMTP communication between Hub or Edge Transport servers and smart hosts In Exchange 2010, you can configure a Send Connector to route mail for remote domains, including Internet mail, to a SMTP gateway generally residing on the perimeter network. Although it's possible to create a Send Connector to route e-mail to a smart host without using any authentication, we recommend that you use appropriate authentication for such connectors. If you use Basic authentication, we recommend using Basic authentication over TLS. If you select the externally secured option, it's assumed that authentication is performed using a non-Exchange mechanism such as IPsec. When you

configure the connector with the address of a smart host, you can use either the smart host's IP address or its fqdn. We recommend using the smarthost's IP address because it offers protection against DNS poisoning, versus the convenience of using the FQDN.

Using Domain Security for SMTP communication with partners In Exchange 2010, you can use Domain Security to help secure message communication paths with partner domains. Domain Security uses mutual TLS to provide session-based encryption and authentication. For mutual TLS authentication, the source and destination hosts verify the connection by performing X.509 certificate validation. Transport servers communicating with partner domains configured for Domain Security require a certificate signed by a trusted third party or an internal certification authority. If using an internal CA, the certificate revocation list (CRL) must be published and reachable by the partner host. For details, see the following topics:

- Understanding Domain Security
- White Paper: Domain Security in Exchange 2007

Exchange 2010 uses the default SMTP port (TCP port 25) for SMTP communication. Exchange Setup creates the required firewall rules in Windows Firewall with Advanced Security to allow communication over default ports. If you specify a different port for a connector, Exchange doesn't modify firewall rules or automatically create a new rule to allow communication over the nondefault port. You must manually modify firewall configuration to allow communication over nondefault ports. When you configure a receive connector for a nondefault port, the SMTP clients submitting messages to the connector must also be configured to use the nondefault port.

In Exchange 2010, you can locate the Hub Transport server role on an Exchange 2010 Mailbox server. This includes a Mailbox server that's a member of a Database Availability Group (DAG). We recommend that you don't locate the Hub Transport server role on a Mailbox server, especially in topologies where no Edge Transport servers are deployed, in order to isolate Mailbox servers from the Internet. You can locate Hub Transport server role on Client Access servers. You must follow the sizing guidelines for each server role when collocating server roles on the same server.

When specifying a smart host for a Send Connector on a Hub Transport or an Edge Transport server, we recommend that you use IP addresses instead of the fully qualified domain name (FQDN) of a smart host, to protect from DNS poisoning and spoofing. This also minimizes the effect of any DNS outages on the transport infrastructure. DNS servers used in perimeter networks must be used only for outbound resolution. The perimeter DNS servers may contain records for Hub Transport servers. You can also use Hosts files on Edge Transport servers to avoid creating records for Hub Transport servers on DNS servers located in perimeter networks.

In addition to the steps discussed in this section, you should consider using sufficient message size restrictions on connectors, and message throttling settings on transport servers. For more details, see the following topics:

- Understanding Message Size Limits
- Understanding Message Throttling

Unified Messaging Considerations

When planning to deploy Unified Messaging (UM) server role, you must consider the different communication channels used by UM to communicate with IP gateways or IP PBX.

By default, when you create a UM dial plan, it will communicate in an unsecured mode. Also, the Unified Messaging servers associated with the UM dial plan will send and receive data from IP gateways, IP PBXs, and other Exchange 2010 computers by using no encryption. In unsecured mode, both the Real-Time Transport Protocol (RTP) media channel and SIP signaling information won't be encrypted.

You can configure a Unified Messaging server to use mutual TLS to encrypt the SIP and

RTP traffic sent and received from other devices and servers. When you add a Unified Messaging server to a UM dial plan and configure the dial plan to use SIP secured mode, only the SIP signaling traffic will be encrypted, and the RTP media channels will still use TCP. TCP isn't encrypted. However, if you add a Unified Messaging server to a UM dial plan and configure the dial plan to use secured mode, both the SIP signaling traffic and the RTP media channels are encrypted. A secure signaling media channel that uses Secure Real-Time Transport Protocol (SRTP) also uses mutual TLS to encrypt the VoIP data.

If the IP gateway or IP PBX you use supports IPsec, you can also use IPsec to help secure the communication between a UM server and the IP gateway or IP PBX.

For more details, see Understanding Unified Messaging VoIP Security.

UM also submits messages such as missed call notifications and voice mail messages to Hub Transport servers. By default, this communication occurs over SMTP using TLS encryption.

You can configure a UM mailbox policy for PIN-less access. This allows a caller to access voice mail without having to enter a PIN, based on the CallerID of the call. Spoofing of CallerID is insignificant. We recommend that you not enable PIN-less access to voice mail. Also, we recommend that you review the default PIN settings and configure them to meet your organization's security requirements. The following settings can be configured for a UM mailbox policy using the **Set-UMMailboxPolicy** cmdlet.

Parameters to control user PIN for voice mail access

Parameter	Description
AllowCommonPatterns	The *AllowCommonPatterns* parameter specifies whether to allow obvious PINs. Examples of obvious PINs include subsets of the telephone number, sequential numbers, or repeated numbers. If set to $false, sequential and repeated numbers and the suffix of the mailbox extension are rejected. If set to $true, only the suffix of the mailbox extension is rejected.
AllowPinlessVoiceMailAccess	The *AllowPinlessVoiceMailAccess* parameter specifies whether users associated with the UM mailbox policy are required to use a PIN to access their voice mail. A PIN is still required to access their e-mail and calendar. **Default** disabled (`$false`).
LogonFailusresBeforePINReset	The *LogonFailuresBeforePINReset* parameter specifies the number of sequential unsuccessful logon attempts before the mailbox PIN is automatically reset. To disable this feature, set this parameter to Unlimited. If this parameter isn't set to Unlimited, it must be set to less than the value of the *MaxLogonAttempts* parameter. The range is from 0 through 999. **Default** 5 failures.
MaxLogonAttempts	The *MaxLogonAttempts* parameter specifies the number of times users can try unsuccessfully to log on, in sequence,

	before the UM mailboxes are locked. The range is from 1 through 999. **Default** 15 attempts.
MinPINLength	The *MinPINLength* parameter specifies the minimum number of digits required in a PIN for UM-enabled users. The range is from 4 through 24. **Default** 6 digits
PINHistoryCount	The *PINHistoryCount* parameter specifies the number of previous PINs that are remembered and aren't allowed during a PIN reset. This number includes the first time that the PIN was set. The range is from 1 through 20. **Default** 5 PINs
PINLifetime	The *PINLifetime* parameter specifies the number of days until a new password is required. The range is from 1 through 999. If you specify Unlimited, the users' PINs won't expire. **Default** 60 days

In Exchange 2010, voice mail messages can be marked as protected. Voice mail messages are protected using Information Rights Management (IRM). You can configure voice mail protection settings by configuring the following parameter in a UM mailbox policy. For more details, see the following topics:

- Understanding Protected Voice Mail
- Understanding Information Rights Management

Protected voice mail parameters

Parameter	Description
ProtectAuthenticatedVoicemail	The *ProtectAuthenticatedVoiceMail* parameter specifies whether Unified Messaging servers that answer Outlook Voice Access calls for UM-enabled users associated with the UM mailbox policy create protected voice mail messages. If the value is set to Private, only messages marked as private are protected. If the value is set to All, every voice mail message is protected. **Default** None (No protection is applied to voice mail messages)
ProtectUnauthenticatedVoiceMail	The *ProtectUnauthenticatedVoiceMail* parameter specifies whether the Unified Messaging servers that answer calls for UM-enabled users associated with the UM mailbox policy create protected voice mail messages. This also applies when a message is sent from a UM auto attendant to a UM-enabled user associated with the

	UM mailbox policy. If the value is set to Private, only messages marked as private are protected. If the value is set to All, every voice mail message is protected. **Default** None (No protection is applied to voice mail messages)
RequireProtectedPlayOnPhone	The *RequireProtectedPlayOnPhone* parameter specifies whether users associated with the UM mailbox policy can only use Play on Phone for protected voice mail messages or whether users can use multimedia software to play the protected message. **Default** `$false`. Users are able to use both methods to listen to protected voice mail messages.

Important:

For UM servers to continue to answer calls, it's critical that they have access to Active Directory. We recommend that you monitor Active Directory availability

Appendix 1: Additional Security-Related Documentation

This section contains links to additional security-related Exchange documentation.

Anti-Spam and Antivirus Functionality

- Understanding Anti-Spam and Antivirus Functionality
- Managing Anti-Spam and Antivirus Features
- Anti-Spam Cmdlets

Certificates

- Understanding TLS Certificates
- Managing SSL for a Client Access Server
- Configure SSL for Exchange ActiveSync
- Configure SSL for Outlook Anywhere
- Configuring TLS and SSL for POP3 and IMAP4 Access
- Configure Outlook Web App Virtual Directories to Use SSL
- Create a New Exchange Certificate
- Import an Exchange Certificate
- View Exchange Certificate Properties
- Assign Services to a Certificate

Client Authentication and Security

- Configuring Authentication for Exchange ActiveSync
- Configuring Authentication for POP3 and IMAP4
- Setting Up Forms-Based Authentication for Outlook Web App
- Setting Up Standard Authentication Methods for Outlook Web App

Outlook Web App

- Managing Outlook Web App Security
- Configure Outlook Web App Virtual Directories to Use SSL
- Setting Up Forms-Based Authentication for Outlook Web App

- Setting Up Standard Authentication Methods for Outlook Web App
- **Configure Outlook Web App to Work with Active Directory Federation Services**
- Outlook Web App and S/MIME

Outlook Anywhere

- Managing Outlook Anywhere Security

POP3 and IMAP

- Managing POP3 and IMAP4 Security
- Configure Authentication for POP3
- Configure Authentication for IMAP4
- Configuring TLS and SSL for POP3 and IMAP4 Access

Permissions

- Exchange 2010 Deployment Permissions Reference
- Understanding Role Based Access Control
- Understanding Split Permissions
- Understanding Permissions Coexistence with Exchange 2003
- Understanding Permissions Coexistence with Exchange 2007
- Understanding Multiple-Forest Permissions
- Feature Permissions
- Managing Administrator and Specialist Users
- Managing End Users
- Management Roles and Role Entries
- Management Role Scopes
- Management Role Assignments
- Managing Split Permissions
- Permissions to Manage Mailbox Servers
- Securing Unified Messaging Servers

Protecting Mail Flow

- Understanding Domain Security
- Using PKI on the Edge Transport Server for Domain Security
- Using Domain Security: Configuring Mutual TLS
- Test PKI and Proxy Configuration

Messaging Policy and Compliance

- Understanding Information Rights Management
- Understanding Journaling
- Protecting Journal Reports
- Understanding Messaging Records Management
- Understanding Retention Tags and Retention Policies
- Understanding Multi-Mailbox Search
- Understanding Mailbox Audit Logging
- Managing Mailbox Audit Logging

Federation

- Understanding Federation
- Trusted Root Certification Authorities for Federation Trusts

1.12.2 Exchange Network Port Reference

Exchange Network Port Reference

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-09-25*

This topic provides information about ports, authentication, and encryption for all data paths that are used by Microsoft Exchange Server 2010. The "Notes" sections that follow each table clarify or define non-standard authentication or encryption methods.

Transport Servers

Exchange 2010 includes two server roles that perform message transport functionality: Hub Transport server and Edge Transport server.

The following table provides information about ports, authentication, and encryption for data paths between these transport servers and other Exchange 2010 servers and services.

Transport server data paths

Data path	Required ports	Default authentication	Supported authentication	Encryption supported?	Encrypted by default?
Hub Transport server to Hub Transport server	25/TCP (SMTP)	Kerberos	Kerberos	Yes, using Transport Layer Security (TLS)	Yes
Hub Transport server to Edge Transport server	25/TCP (SMTP)	Direct trust	Direct trust	Yes, using TLS	Yes
Edge Transport server to Hub Transport server	25/TCP (SMTP)	Direct trust	Direct trust	Yes, using TLS	Yes
Edge Transport server to Edge Transport server	25/TCP (SMTP)	Anonymous, Certificate	Anonymous, Certificate	Yes, using TLS	Yes
Mailbox server to Hub Transport server via the Microsoft Exchange Mail Submission Service	135/TCP (RPC)	NTLM. If the Hub Transport and the Mailbox server roles are on the same server, Kerberos is	NTLM/ Kerberos	Yes, using RPC encryption	Yes

		used.			
Hub Transport to Mailbox server via MAPI	135/TCP (RPC)	NTLM. If the Hub Transport and the Mailbox server roles are on the same server, Kerberos is used.	NTLM/ Kerberos	Yes, using RPC encryption	Yes
Unified Messaging server to Hub Transport server	25/TCP (SMTP)	Kerberos	Kerberos	Yes, using TLS	Yes
Microsoft Exchange EdgeSync service from Hub Transport server to Edge Transport server	50636/TCP (SSL)	Basic	Basic	Yes, using LDAP over SSL (LDAPS)	Yes
Active Directory access from Hub Transport server	389/TCP/UDP (LDAP), 3268/ TCP (LDAP GC), 88/TCP/ UDP (Kerberos), 53/TCP/UDP (DNS), 135/ TCP (RPC netlogon)	Kerberos	Kerberos	Yes, using Kerberos encryption	Yes
Active Directory Rights Management Services (AD RMS) access from Hub Transport server	443/TCP (HTTPS)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using SSL	Yes*
SMTP clients to Hub Transport server (for example, end-users using Windows Live Mail)	587 (SMTP) 25/TCP (SMTP)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using TLS	Yes

Notes on Transport Servers

- All traffic between Hub Transport servers is encrypted by using TLS with self-signed certificates that are installed by Exchange 2010 Setup.

Note:
In Exchange 2010, TLS can be disabled on Hub Transport servers for internal SMTP communication with other Hub Transport servers in the same Exchange organization. We don't recommend that you do this unless it is absolutely required. For more information, see Disabling TLS Between Active Directory Sites to Support WAN Optimization.

- All traffic between Edge Transport servers and Hub Transport servers is authenticated and encrypted. Mutual TLS is the underlying mechanism for authentication and encryption. Instead of using X.509 validation, Exchange 2010 uses *direct trust* to authenticate the certificates. Direct trust means that the presence of the certificate in Active Directory or Active Directory Lightweight Directory Services (AD LDS) acts as validation for the certificate. Active Directory is considered a trusted storage mechanism. When direct trust is used, it doesn't matter whether the certificate is self-signed or signed by a certification authority (CA). When you subscribe an Edge Transport server to the Exchange organization, the Edge Subscription publishes the Edge Transport server certificate in Active Directory for the Hub Transport servers to validate. The Microsoft Exchange EdgeSync service updates AD LDS together with the set of Hub Transport server certificates for the Edge Transport server to validate.
- EdgeSync uses a secure LDAP connection from the Hub Transport server to subscribed Edge Transport servers over TCP 50636. AD LDS also listens on TCP 50389. Connections to this port don't use SSL. You can use LDAP utilities to connect to the port and to check AD LDS data.
- By default, traffic between Edge Transport servers in two different organizations is encrypted. Exchange 2010 Setup creates a self-signed certificate, and TLS is enabled by default. This allows any sending system to encrypt the inbound SMTP session to Exchange. Also by default, Exchange 2010 tries TLS for all remote connections.
- Authentication methods for traffic between Hub Transport servers and Mailbox servers differ when the Hub Transport server roles and Mailbox server roles are installed on the same computer. When mail submission is local, Kerberos authentication is used. When mail submission is remote, NTLM authentication is used.
- Exchange 2010 also supports Domain Security. Domain Security refers to the functionality in Exchange 2010 and Microsoft Outlook 2010 that provides a low-cost alternative to S/MIME or other message-level, over-the-Internet security solutions. Domain Security provides you a way to manage secure message paths between domains over the Internet. After you configure these secure message paths, messages that have successfully traveled over the secure path from an authenticated sender are displayed to Outlook and Outlook Web Access users as "Domain Secured." For more information, see Understanding Domain Security.
- Many agents can run on Hub Transport servers and Edge Transport servers. Generally, anti-spam agents rely on information that's local to the computer on which the agents run. Therefore, a minimum of communication with remote computers is required. Recipient filtering is the exception. Recipient filtering requires calls to either AD LDS or Active Directory. As a best practice, run recipient filtering on the Edge Transport server. In this case, the AD LDS directory is on the same computer as the Edge Transport server. Therefore, no remote communication is required. When recipient filtering has been installed and configured on the Hub Transport server, recipient filtering accesses Active Directory.
- The Sender Reputation feature in Exchange 2010 uses the Protocol Analysis agent. This agent also makes various connections to outside proxy servers to determine inbound message paths for suspect connections.
- All other anti-spam functionality uses such data as safelist aggregation and recipient data for recipient filtering. This data is gathered, stored, and accessed only on the local computer. Frequently, the data is pushed to the

local AD LDS directory by using the Microsoft Exchange EdgeSync service.

- Information Rights Management (IRM) agents on Hub Transport servers make connections to Active Directory Rights Management Services (AD RMS) servers in the organization. AD RMS is a Web service that's secured by using SSL as a best practice. Communication with AD RMS servers occurs by using HTTPS, and Kerberos or NTLM is used for authentication, depending on the AD RMS server configuration.
- Journal rules, transport rules, and message classifications are stored in Active Directory and accessed by the Journaling agent and the Transport Rules agent on Hub Transport servers.

Mailbox Servers

Whether NTLM or Kerberos authentication is used for Mailbox servers depends on the user or process context that the Exchange Business Logic layer consumer is running under. In this context, the consumer is any application or process that uses the Exchange Business Logic layer. As a result, many entries in the **Default Authentication** column of the **Mailbox server data paths** table are listed as **NTLM/Kerberos**.

The Exchange Business Logic layer is used to access and communicate with the Exchange store. The Exchange Business Logic layer is also called from the Exchange store to communicate with external applications and processes.

If the Exchange Business Logic layer consumer is running as Local System, the authentication method is always Kerberos from the consumer to the Exchange store. Kerberos is used because the consumer must be authenticated by using the Local System computer account, and a two-way authenticated trust must exist.

If the Exchange Business Logic layer consumer isn't running as Local System, the authentication method is NTLM. For example, NTLM is used when you run an Exchange Management Shell cmdlet that uses the Exchange Business Logic layer.

The RPC traffic is always encrypted.

The following table provides information about ports, authentication, and encryption for data paths to and from Mailbox servers.

Mailbox server data paths

Data path	Required ports	Default authentication	Supported authentication	Encryption supported?	Encrypted by default?
Active Directory access	389/TCP/UDP (LDAP), 3268/TCP (LDAP GC), 88/TCP/UDP (Kerberos), 53/TCP/UDP (DNS), 135/TCP (RPC netlogon)	Kerberos	Kerberos	Yes, using Kerberos encryption	Yes
Admin remote access (Remote Registry)	135/TCP (RPC)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using IPsec	No
Admin remote access (SMB/	445/TCP (SMB)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using IPsec	No

File)					
Availability Web service (Client Access to Mailbox)	135/TCP (RPC)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using RPC encryption	Yes
Clustering	135/TCP (RPC) See Notes on Mailbox Servers after this table.	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using IPsec	No
Content indexing	135/TCP (RPC)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using RPC encryption	Yes
Log shipping	64327 (customizable)	NTLM/ Kerberos	NTLM/ Kerberos	Yes	No
Seeding	64327 (customizable)	NTLM/ Kerberos	NTLM/ Kerberos	Yes	No
Volume shadow copy service (VSS) backup	Local Message Block (SMB)	NTLM/ Kerberos	NTLM/ Kerberos	No	No
Mailbox Assistants	135/TCP (RPC)	NTLM/ Kerberos	NTLM/ Kerberos	No	No
MAPI access	135/TCP (RPC)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using RPC encryption	Yes
Microsoft Exchange Active Directory Topology service access	135/TCP (RPC)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using RPC encryption	Yes
Microsoft Exchange System Attendant service legacy access (Listen to requests)	135/TCP (RPC)	NTLM/ Kerberos	NTLM/ Kerberos	No	No
Microsoft Exchange System Attendant service legacy access to Active Directory	389/TCP/UDP (LDAP), 3268/ TCP (LDAP GC), 88/TCP/ UDP (Kerberos), 53/TCP/UDP (DNS), 135/ TCP (RPC netlogon)	Kerberos	Kerberos	Yes, using Kerberos encryption	Yes
Microsoft Exchange	135/TCP (RPC)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using RPC encryption	Yes

System Attendant service legacy access (As MAPI client)					
Offline address book (OAB) accessing Active Directory	135/TCP (RPC)	Kerberos	Kerberos	Yes, using RPC encryption	Yes
Recipient Update Service RPC access	135/TCP (RPC)	Kerberos	Kerberos	Yes, using RPC encryption	Yes
Recipient update to Active Directory	389/TCP/UDP (LDAP), 3268/TCP (LDAP GC), 88/TCP/UDP (Kerberos), 53/TCP/UDP (DNS), 135/TCP (RPC netlogon)	Kerberos	Kerberos	Yes, using Kerberos encryption	Yes

Notes on Mailbox Servers

- The **Clustering** data path listed in the preceding table uses dynamic RPC over TCP to communicate cluster status and activity between the different cluster nodes. The Cluster service (ClusSvc.exe) also uses UDP/3343 and randomly allocated, high TCP ports to communicate between cluster nodes.
- For intra-node communications, cluster nodes communicate over User Datagram Protocol (UDP) port 3343. Each node in the cluster periodically exchanges sequenced, unicast UDP datagrams with every other node in the cluster. The purpose of this exchange is to determine whether all nodes are running correctly, and also to monitor the health of network links.
- Port 64327/TCP is the default port used for log shipping. Administrators can specify a different port for log shipping.
- For HTTP authentication in which **Negotiate** is listed, Kerberos is tried first, and then NTLM.

Client Access Servers

Unless noted, client access technologies, such as Outlook Web App, POP3, or IMAP4 are described by the authentication and encryption from the client application to the Client Access server.

The following table provides information about ports, authentication, and encryption for data paths between Client Access servers and other servers and clients.

Client Access server data paths

Data path	Required ports	Default authentication	Supported authentication	Encryption supported?	Encrypted by default?
Active	389/TCP/UDP	Kerberos	Kerberos	Yes, using	Yes

Directory access	(LDAP), 3268/ TCP (LDAP GC), 88/TCP/ UDP (Kerberos), 53/TCP/UDP (DNS), 135/ TCP (RPC netlogon)			Kerberos encryption	
Autodiscover service	80/TCP, 443/ TCP (SSL)	Basic/ Integrated Windows authentication (Negotiate)	Basic, Digest, NTLM, Negotiate (Kerberos)	Yes, using HTTPS	Yes
Availability service	80/TCP, 443/ TCP (SSL)	NTLM/ Kerberos	NTLM, Kerberos	Yes, using HTTPS	Yes
Mailbox Replication Service (MRS)	808/TCP	Kerberos/ NTLM	Kerberos, NTLM	Yes, using RPC encryption	Yes
Outlook accessing OAB	80/TCP, 443/ TCP (SSL)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using HTTPS	No
Outlook Web App	80/TCP, 443/ TCP (SSL)	Forms Based Authentication	Basic, Digest, Forms Based Authentication , NTLM (v2 only), Kerberos, Certificate	Yes, using HTTPS	Yes, using a self-signed certificate
POP3	110/TCP (TLS), 995/ TCP (SSL)	Basic, Kerberos	Basic, Kerberos	Yes, using SSL, TLS	Yes
IMAP4	143/TCP (TLS), 993/ TCP (SSL)	Basic, Kerberos	Basic, Kerberos	Yes, using SSL, TLS	Yes
Outlook Anywhere (formerly known as RPC over HTTP)	80/TCP, 443/ TCP (SSL)	Basic	Basic or NTLM	Yes, using HTTPS	Yes
Exchange ActiveSync application	80/TCP, 443/ TCP (SSL)	Basic	Basic, Certificate	Yes, using HTTPS	Yes
Client Access server to Unified Messaging server	5060/TCP, 5061/TCP, 5062/TCP, a dynamic port	By IP address	By IP address	Yes, using Session Initiation Protocol (SIP) over TLS	Yes
Client Access server to a Mailbox server	80/TCP, 443/ TCP (SSL)	NTLM/ Kerberos	Negotiate (Kerberos with fallback to	Yes, using IPsec	No

that is running an earlier version of Exchange Server			NTLM or optionally Basic,) POP/ IMAP plain text		
Client Access server to Exchange 2010 Mailbox server	RPC. See Notes on Client Access Servers.	Kerberos	NTLM/ Kerberos	Yes, using RPC encryption	Yes
Client Access server to Client Access server (Exchange ActiveSync)	80/TCP, 443/ TCP (SSL)	Kerberos	Kerberos, Certificate	Yes, using HTTPS	Yes, using a self-signed certificate
Client Access server to Client Access server (Outlook Web Access)	80/TCP, 443/ TCP (HTTPS)	Kerberos	Kerberos	Yes, using SSL	Yes
Client Access server to Client Access server (Exchange Web Services)	443/TCP (HTTPS)	Kerberos	Kerberos	Yes, using SSL	Yes
Client Access server to Client Access server (POP3)	995 (SSL)	Basic	Basic	Yes, using SSL	Yes
Client Access server to Client Access server (IMAP4)	993 (SSL)	Basic	Basic	Yes, using SSL	Yes
Office Communications Server access to Client Access server (when Office Communications Server and Outlook Web App integration is enabled)	5075-5077/ TCP (IN), 5061/TCP (OUT)	mTLS (Required)	mTLS (Required)	Yes, using SSL	Yes

Note:
Integrated Windows authentication (NTLM) is not supported for POP3 or IMAP4 client connectivity. For more information, see the "Client Access Features" sections in

Discontinued Features.

Notes on Client Access Servers

- In Exchange 2010, MAPI clients such as Microsoft Outlook connect to Client Access servers.
- The Client Access servers use many ports to communicate with Mailbox servers. With some exceptions, those ports are determined by the RPC service, and they aren't fixed.
- For HTTP authentication where **Negotiate** is listed, Kerberos is tried first, and then NTLM.
- When an Exchange 2010 Client Access server communicates with a Mailbox server that runs Microsoft Exchange Server 2003, it's a best practice to use Kerberos and disable NTLM authentication and Basic authentication. It's also a best practice to configure Outlook Web App to use forms-based authentication with a trusted certificate. For Exchange ActiveSync clients to communicate through the Exchange 2010 Client Access server to the Exchange 2003 back-end server, Windows Integrated Authentication must be enabled on the Microsoft-Server-ActiveSync virtual directory on the Exchange 2003 back-end server. To use Exchange System Manager on an Exchange 2003 server to manage authentication on an Exchange 2003 virtual directory, download and install the hotfix referenced in Microsoft Knowledge Base article 937031, Event ID 1036 is logged on an Exchange 2007 server that is running the CAS role when mobile devices connect to the Exchange 2007 server to access mailboxes on an Exchange 2003 back-end server.

  Note:
  Although the Knowledge Base article is specific to MicrosoftExchange Server 2007, it's also applicable to Exchange 2010.

- When a Client Access server proxies POP3 requests to another Client Access server, the communication occurs over port 995/TCP. This is true regardless of whether the connecting client uses POP3 and requests TLS (on port 110/TCP) or connects on port 995/TCP using SSL. Similarly, for IMAP4 connections, the requesting server uses port 993/TCP to proxy requests regardless of whether the connecting client uses IMAP4 and requests TLS (on port 443/TCP) or connects to port 995 using IMAP4 with SSL encryption

Client Access Server Connectivity

In addition to having a Client Access server in every Active Directory site that contains a Mailbox server, it’s important to avoid restricting traffic between Exchange servers. Make sure that all defined ports that are used by Exchange are open in both directions between all source and destination servers. The installation of a firewall between Exchange servers or between an Exchange 2010 Mailbox or Client Access server and Active Directory isn’t supported. However, you can install a network device if traffic isn’t restricted and all available ports are open between the various Exchange servers and Active Directory.

Unified Messaging Servers

IP gateways and IP PBXs support only certificate-based authentication that uses mutual TLS for encrypting SIP traffic and IP-based authentication for Session Initiation Protocol (SIP)/TCP connections. IP gateways don't support either NTLM or Kerberos authentication. Therefore, when you use IP-based authentication, the connecting IP address or addresses are used to provide authentication mechanism for unencrypted (TCP) connections. When IP-based authentication is used in Unified Messaging (UM), the UM server verifies that the IP address is allowed to connect. The IP address is configured on the IP gateway or IP PBX.

IP gateways and IP PBXs support mutual TLS for encrypting SIP traffic. After you successfully import and export the required trusted certificates, the IP gateway or IP PBX

will request a certificate from the UM server, and then it will request a certificate from the IP gateway or IP PBX. Exchanging the trusted certificate between the IP gateway or IP PBX and the UM server enables the IP gateway or IP PBX and UM server to communicate over an encrypted connection by using mutual TLS.

The following table provides information about port, authentication, and encryption for data paths between UM servers and other servers.

Unified Messaging server data paths

Data path	Required ports	Default authentication	Supported authentication	Encryption supported?	Encrypted by default?
Active Directory access	389/TCP/UDP (LDAP), 3268/TCP (LDAP GC), 88/TCP/UDP (Kerberos), 53/TCP/UDP (DNS), 135/TCP (RPC netlogon)	Kerberos	Kerberos	Yes, using Kerberos encryption	Yes
Unified Messaging Phone interaction (IP PBX/VoIP Gateway)	5060/TCP , 5065/TCP, 5067/TCP (unsecured), 5061/TCP, 5066/TCP, 5068/TCP (secured), a dynamic port from the range 16000-17000/TCP (control), dynamic UDP ports from the range 1024-65535/UDP (RTP)	By IP address	By IP address, MTLS	Yes, using SIP/TLS, SRTP	No
Unified Messaging Web Service	80/TCP, 443/TCP (SSL)	Integrated Windows authentication (Negotiate)	Basic, Digest, NTLM, Negotiate (Kerberos)	Yes, using SSL	Yes
Unified Messaging server to Client Access server	5075, 5076, 5077 (TCP)	Integrated Windows authentication (Negotiate)	Basic, Digest, NTLM, Negotiate (Kerberos)	Yes, using SSL	Yes
Unified Messaging server to Client Access server (Play on Phone)	Dynamic RPC	NTLM/Kerberos	NTLM/Kerberos	Yes, using RPC encryption	Yes

Unified Messaging server to Hub Transport server	25/TCP (TLS)	Kerberos	Kerberos	Yes, using TLS	Yes
Unified Messaging server to Mailbox server	135/TCP (RPC)	NTLM/ Kerberos	NTLM/ Kerberos	Yes, using RPC encryption	Yes

Notes on Unified Messaging Servers

- When you create a UM IP gateway object in Active Directory, you must define the IP address of the physical IP gateway or IP PBX (Private Branch eXchange). When you define the IP address on the UM IP gateway object, the IP address is added to a list of valid IP gateways or IP PBXs (also called SIP peers) that the UM server is allowed to communicate with. When you create the UM IP gateway, you can associate it with a UM dial plan. Associating the UM IP gateway with a dial plan allows the Unified Messaging servers that are associated with the dial plan to use IP-based authentication to communicate with the IP gateway. If the UM IP gateway has not been created, or if it is not configured to use the correct IP address, authentication fails and the UM servers don't accept connections from that IP gateway's IP address. Also, when you implement mutual TLS and IP gateway or IP PBX and UM servers, the UM IP gateway must be configured to use the FQDN. After you configure the UM IP gateway with an FQDN, you must also add a host record to the DNS forward lookup zone for the UM IP gateway.
- In Exchange 2010, a UM server can either communicate on port 5060/TCP (unsecured) or on port 5061/TCP (secured), and can be configured to use both.

For more information, see Understanding Unified Messaging VoIP Security and Understanding Protocols, Ports, and Services in Unified Messaging.

Windows Firewall Rules Created by Exchange 2010 Setup

Windows Firewall with Advanced Security is a stateful, host-based firewall that filters inbound and outbound traffic based on firewall rules. Exchange 2010 Setup creates Windows Firewall rules to open the ports required for server and client communication on each server role. Therefore, you no longer have to use the Security Configuration Wizard (SCW) to configure these settings. To learn more about Windows Firewall with Advanced Security, see Windows Firewall with Advanced Security and IPsec.

This table lists the Windows Firewall rules created by Exchange Setup, including the ports opened on each server role. You can view these rules using the Windows Firewall with Advanced Security MMC snap-in.

Rule name	Server roles	Port	Program
MSExchangeADTopology - RPC (TCP-In)	Client Access, Hub Transport, Mailbox, Unified Messaging	Dynamic RPC	Bin \MSExchangeADTopologyService.exe
MSExchangeMonitoring - RPC (TCP-In)	Client Access, Hub Transport, Edge Transport, Unified Messaging	Dynamic RPC	Bin \Microsoft.Exchange.Management.Monitoring.exe

MSExchangeServiceHost - RPC (TCP-In)	All roles	Dynamic RPC	Bin\Microsoft.Exchange.ServiceHost.exe
MSExchangeServiceHost - RPCEPMap (TCP-In)	All roles	RPC-EPMap	Bin\Microsoft.Exchange.Service.Host
MSExchangeRPCEPMap (GFW) (TCP-In)	All roles	RPC-EPMap	Any
MSExchangeRPC (GFW) (TCP-In)	Client Access, Hub Transport, Mailbox, Unified Messaging	Dynamic RPC	Any
MSExchange - IMAP4 (GFW) (TCP-In)	Client Access	143, 993 (TCP)	All
MSExchangeIMAP4 (TCP-In)	Client Access	143, 993 (TCP)	ClientAccess\PopImap\Microsoft.Exchange.Imap4Service.exe
MSExchange - POP3 (FGW) (TCP-In)	Client Access	110, 995 (TCP)	All
MSExchange - POP3 (TCP-In)	Client Access	110, 995 (TCP)	ClientAccess\PopImap\Microsoft.Exchange.Pop3Service.exe
MSExchange - OWA (GFW) (TCP-In)	Client Access	5075, 5076, 5077 (TCP)	All
MSExchangeOWAAppPool (TCP-In)	Client Access	5075, 5076, 5077 (TCP)	Inetsrv\w3wp.exe
MSExchangeAB-RPC (TCP-In)	Client Access	Dynamic RPC	Bin\Microsoft.Exchange.AddressBook.Service.exe
MSExchangeAB-RPCEPMap (TCP-In)	Client Access	RPC-EPMap	Bin\Microsoft.Exchange.AddressBook.Service.exe
MSExchangeAB-RpcHttp (TCP-In)	Client Access	6002, 6004 (TCP)	Bin\Microsoft.Exchange.AddressBook.Service.exe
RpcHttpLBS (TCP-In)	Client Access	Dynamic RPC	System32\Svchost.exe
MSExchangeRPC - RPC (TCP-In)	Client Access, Mailbox	Dynamic RPC	Bin\Microsoft.Exchange.RpcClientAccess.Service.exe
MSExchangeRPC - PRCEPMap (TCP-In)	Client Access, Mailbox	RPC-EPMap	Bin\Microsoft.Exchange.RpcClientAccess.Service.exe

MSExchangeRPC (TCP-In)	Client Access, Mailbox	6001 (TCP)	Bin \Microsoft.Exchange.RpcClientAccess.Service.exe
MSExchangeMailboxReplication (GFW) (TCP-In)	Client Access	808 (TCP)	Any
MSExchangeMailboxReplication (TCP-In)	Client Access	808 (TCP)	Bin \MSExchangeMailboxReplication.exe
MSExchangeIS - RPC (TCP-In)	Mailbox	Dynamic RPC	Bin\Store.exe
MSExchangeIS RPCEPMap (TCP-In)	Mailbox	RPC-EPMap	Bin\Store.exe
MSExchangeIS (GFW) (TCP-In)	Mailbox	6001, 6002, 6003, 6004 (TCP)	Any
MSExchangeIS (TCP-In)	Mailbox	6001 (TCP)	Bin\Store.exe
MSExchangeMailboxAssistants - RPC (TCP-In)	Mailbox	Dynamic RPC	Bin \MSExchangeMailboxAssistants.exe
MSExchangeMailboxAssistants - RPCEPMap (TCP-In)	Mailbox	RPC-EPMap	Bin \MSExchangeMailboxAssistants.exe
MSExchangeMailSubmission - RPC (TCP-In)	Mailbox	Dynamic RPC	Bin \MSExchangeMailSubmission.exe
MSExchangeMailSubmission - RPCEPMap (TCP-In)	Mailbox	RPC-EPMap	Bin \MSExchangeMailSubmission.exe
MSExchangeMigration - RPC (TCP-In)	Mailbox	Dynamic RPC	Bin \MSExchangeMigration.exe
MSExchangeMigration - RPCEPMap (TCP-In)	Mailbox	RPC-EPMap	Bin \MSExchangeMigration.exe
MSExchangerepl - Log Copier (TCP-In)	Mailbox	64327 (TCP)	Bin \MSExchangeRepl.exe
MSExchangerepl - RPC (TCP-In)	Mailbox	Dynamic RPC	Bin \MSExchangeRepl.exe
MSExchangerepl - RPC-EPMap (TCP-In)	Mailbox	RPC-EPMap	Bin \MSExchangeRepl.exe
MSExchangeSearch - RPC (TCP-In)	Mailbox	Dynamic RPC	Bin \Microsoft.Exchange.Search.ExSearch.exe
MSExchangeThrottling	Mailbox	Dynamic RPC	Bin

- RPC (TCP-In)			\MSExchangeThrottling.exe
MSExchangeThrottling - RPCEPMap (TCP-In)	Mailbox	RPC-EPMap	Bin \MSExchangeThrottling.exe
MSFTED - RPC (TCP-In)	Mailbox	Dynamic RPC	Bin\MSFTED.exe
MSFTED - RPCEPMap (TCP-In)	Mailbox	RPC-EPMap	Bin\MSFTED.exe
MSExchangeEdgeSync - RPC (TCP-In)	Hub Transport	Dynamic RPC	Bin \Microsoft.Exchange.EdgeSyncSvc.exe
MSExchangeEdgeSync - RPCEPMap (TCP-In)	Hub Transport	RPC-EPMap	Bin \Microsoft.Exchange.EdgeSyncSvc.exe
MSExchangeTransportWorker - RPC (TCP-In)	Hub Transport	Dynamic RPC	Bin \edgetransport.exe
MSExchangeTransportWorker - RPCEPMap (TCP-In)	Hub Transport	RPC-EPMap	Bin \edgetransport.exe
MSExchangeTransportWorker (GFW) (TCP-In)	Hub Transport	25, 587 (TCP)	Any
MSExchangeTransportWorker (TCP-In)	Hub Transport	25, 587 (TCP)	Bin \edgetransport.exe
MSExchangeTransportLogSearch - RPC (TCP-In)	Hub Transport, Edge Transport, Mailbox	Dynamic RPC	Bin \MSExchangeTransportLogSearch.exe
MSExchangeTransportLogSearch - RPCEPMap (TCP-In)	Hub Transport, Edge Transport, Mailbox	RPC-EPMap	Bin \MSExchangeTransportLogSearch.exe
SESWorker (GFW) (TCP-In)	Unified Messaging	Any	Any
SESWorker (TCP-In)	Unified Messaging	Any	UnifiedMessaging \SESWorker.exe
UMService (GFW) (TCP-In)	Unified Messaging	5060, 5061	Any
UMService (TCP-In)	Unified Messaging	5060, 5061	Bin\UMService.exe
UMWorkerProcess (GFW) (TCP-In)	Unified Messaging	5065, 5066, 5067, 5068	Any
UMWorkerProcess (TCP-In)	Unified Messaging	5065, 5066, 5067, 5068	Bin \UMWorkerProcess.exe
UMWorkerProcess -	Unified Messaging	Dynamic RPC	Bin

RPC (TCP-In)			\UMWorkerProcess.exe

Notes on Windows Firewall Rules Created by Exchange 2010 Setup

- On servers that have Internet Information Services (IIS) installed, Windows opens the HTTP port (port 80, TCP) and HTTPS port (port 443, TCP). Exchange 2010 Setup doesn't open these ports. Therefore, these ports don't appear in the preceding table.
- In Windows Server 2008 and in Windows Server 2008 R2, Windows Firewall with Advanced Security allows you to specify the process or service for which a port is opened. This is more secure because it restricts usage of the port to the process or service specified in the rule. Exchange Setup creates firewall rules with the process name specified. In some cases, an additional rule that isn't restricted to the process is also created for compatibility. You can disable or remove the rules that aren't restricted to the processes, and then keep the corresponding rules restricted to processes if your deployment supports them. The rules that are not restricted to processes are distinguished by the word **(GFW)** in the rule name.
- Many Exchange services use remote procedure calls (RPCs) for communication. Server processes that use RPCs contact the RPC Endpoint Mapper to receive dynamic endpoints and register those endpoints in the Endpoint Mapper database. RPC clients contact the RPC Endpoint Mapper to determine the endpoints used by the server process. By default, the RPC Endpoint Mapper listens on port 135 (TCP). When it configures the Windows Firewall for a process that uses RPCs, Exchange 2010 Setup creates two firewall rules for the process. One rule allows communication with the RPC Endpoint Mapper, and the other rule allows communication with the dynamically assigned endpoint. To learn more about RPCs, see How RPC Works. For more information about creating Windows Firewall rules for dynamic RPC, see Allowing Inbound Network Traffic that Uses Dynamic RPC.

Note:
You can't modify the Windows Firewall rules created by Exchange 2010 Setup. You can create custom rules based on them, and then disable or delete them.

For more information, see Microsoft Knowledge Base article 179442, How to configure a firewall for domains and trusts.

1.12.3 Certificates

Certificates

Exchange Server 2010 > Security >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-01*

In Exchange 2010, digital certificates are used for authentication and encryption of the following:

- SMTP traffic (using Transport Layer Security) between transport servers
- HTTP traffic (using Secure Sockets Layer) for client access methods such as Outlook Web App , Outlook Anywhere, Exchange ActiveSync, and Exchange Web Services
- HTTP traffic for federation

The following topics explain how to use certificates:

Create a New Exchange Certificate

Import an Exchange Certificate

Assign Services to a Certificate

View Exchange Certificate Properties

Export an Exchange Certificate

Renew an Exchange Certificate

Additionally, the following topics explain how certificates are used for different services.

Understanding SSL for Outlook Anywhere

Understanding Redirection for Outlook Anywhere with a Single SSL Certificate

Configuring SSL and Exchange ActiveSync

Managing SSL for a Client Access Server

Configure SSL for Exchange ActiveSync

Configure SSL for Outlook Anywhere

Configuring TLS and SSL for POP3 and IMAP4 Access

Configure Outlook Web App Virtual Directories to Use SSL

Understanding TLS Certificates

Securing Unified Messaging Network Traffic

Understanding Federation

Trusted Root Certification Authorities for Federation Trusts

Certificate Cmdlets

Enable-ExchangeCertificate

Export-ExchangeCertificate

Get-ExchangeCertificate

New-ExchangeCertificate

Remove-ExchangeCertificate

Test-FederationTrustCertificate

1.12.3.1 Create a New Exchange Certificate

Create a New Exchange Certificate

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

After you have installed the Client Access server role, you'll need to create a Secure Sockets Layer (SSL) certificate for the various services in your organization.

Prerequisites

The Client Access server role has been installed.

What Do You Want to Do?

- Use the EMC to create a new Exchange certificate
- Use the Shell to create a new Exchange certificate

Use the EMC to create a new Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

1. In the console tree, click **Server Configuration**.
2. In the action pane, click **New Exchange Certificate** to open the New Exchange Certificate wizard. This wizard helps you determine what type of certificates you need for your Exchange organization.
3. On the **Introduction** page, enter a friendly name for your certificate.
4. On the **Domain Scope** page, select the **Enable wildcard certificate** check box, and then enter a root domain if you want to apply the certificate to all subdomains automatically by creating a wildcard certificate.
5. If you didn't choose to create a wildcard certificate, use the Exchange Configuration page to select the services and protocols that your certificate will need to support. Choose from the following options:
   - **Federated Sharing** If you will be using this certificate for Federated Sharing, select the **Use this certificate for Federated Sharing** check box.
   - **Client Access server (Outlook Web App)** If you'll be using this certificate for Outlook Web App, select the appropriate boxes for Outlook Web App on the Intranet or on the Internet and enter the domain name you use to access Outlook Web App.
   - **Client Access server (Exchange ActiveSync)** If you'll be using this certificate for Exchange ActiveSync, select the **Exchange ActiveSync is enabled** check box and enter the domain name you use to access Exchange ActiveSync.
   - **Client Access server (Exchange Web Services, Outlook Anywhere, and Autodiscover)** If you'll be using this certificate for Exchange Web Services, Outlook Anywhere, or the Autodiscover service, select the applicable check boxes and enter the external host name for your organization. For the Autodiscover service, choose whether you will be using the Long URL

format, the Short URL format, or a custom format. In the **Autodiscover URL to use** box, enter the full URL to the Autodiscover service.

- **Client Access server (POP/IMAP)** Select the check boxes to specify whether your users will be using POP and IMAP on the Intranet and the Internet. Enter the domain names to use for both POP and IMAP.
- **Unified Messaging Server** If you'll be using Unified Messaging, choose whether you'll use a self-signed certificate or a public certificate. You must use a public certificate if you are using Unified Messaging with Office Communications Server. For either option, enter the fully qualified domain name (FQDN) of your Unified Messaging server.
- **Hub Transport Server** Enter the FQDN of your Hub Transport server if you'll be using mutual TLS to help secure Internet mail or if you'll be using a Hub Transport server for POP and IMAP client submission.
- **Legacy Exchange Server** Select **Use legacy domains** and enter the legacy domain name if you're upgrading from a previous version of Exchange Server and will be operating in a coexistence scenario for a period of time during the upgrade.

6. Review the list of domains that will be added to the certificate on the **Certificate Domains** page. You can click **Add** to add another domain or click one of the domains listed and then click **Edit** if you need to make changes. Use the **Set as common name** option to choose one of the domains to be the common name of the certificate.

7. On the **Organization and Location** page, enter information about your Exchange organization. You'll need to enter the name of your Organization, the Organization unit, and location information including the Country/region, City/locality, and State/province. Under the **Certificate Request File Path** section, click **Browse** to select a location for the certificate request file, and then enter the file name you want to use.

8. On the **Certificate Completion** page, verify that all the information you've entered is correct. If it is, click **New**.

9. On the **Completion** page, follow the steps listed to complete your request. This page also contains the cmdlet syntax necessary to create a new certificate.

Use the Shell to create a new Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

The code example below outputs the certificate request in Base64 format to the command-line console. You must send the certificate request to a certification authority (CA) within the organization, a trusted CA outside the organization, or a commercial CA. You can do this by pasting the certificate request output into an e-mail message or into the appropriate field on the certificate request Web page of the CA. You can also save the certificate request to a file using a text editor such as Notepad.

The certificate that results has the following attributes associated with it:

- Subject name: c=<ES>,o=<Woodgrove Bank>,cn=mail1.woodgrovebank.com
- Subject alternate names: woodgrovebank.com and example.com
- An exportable private key

```
New-ExchangeCertificate -GenerateRequest -SubjectName "c=US, o=Woodgrove Bank, cn
```

1.12.3.2 Import an Exchange Certificate

Import an Exchange Certificate

[This topic is in progress.]

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-06-06*

You can use the Import Exchange Certificate wizard to import a certificate from a file with the extension of .pfx.

Prerequisites

The Client Access server role has been installed and you have previously exported a certificate with a private key as a file with the extension .pfx.

What Do You Want to Do?

- Use the EMC to import a new Exchange certificate
- Use the Shell to import a new Exchange certificate

Use the EMC to import a new Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

1. In the console tree, click **Server Configuration**.
2. From the action pane, click **Import Exchange Certificate** to open the Import Exchange Certificate wizard.
   - This wizard helps you import a certificate with a valid private key to your Exchange server. You must enter the password of the private key for a successful import.
3. On the **Introduction** page, click **Browse** to select the file that contains the exported certificate, and then enter the password for the certificate.
4. On the **Exchange Server Selection** page, select the Exchange server that you want to import the certificate to.
5. On the **Completion** page, verify that all previously selected options are correct.
6. On the final page, follow the steps listed to complete your request. This page also displays the Shell cmdlet syntax necessary to import the certificate.

Use the Shell to import a new Exchange certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

This example imports an Exchange certificate from a file named import.pfx.

```
Import-ExchangeCertificate -Path c:\certificates\import.pfx -Password:(Get-Creden
```


1.12.3.3 Assign Services to a Certificate

Assign Services to a Certificate

Exchange Server 2010 > Security > Certificates >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can assign specific services to your Secure Sockets Layer (SSL) certificate. The services you can assign include POP, IMAP, IIS, Unified Messaging, and SMTP.

Prerequisites

The Client Access server role has been installed and at least one certificate is installed on your Client Access server.

What Do You Want to Do?

- Use the EMC to assign services to a certificate
- Use the Shell to assign services to a certificate

Use the EMC to assign services to a certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

1. In the console tree, select **Server Configuration**.
2. In the action pane, click **Assign Services to Certificate** to open the Assign Services to Certificate wizard.
   - This wizard helps you assign the appropriate services to your certificate for your Exchange organization. For assistance creating a certificate, see Create a New Exchange Certificate.
3. On the **Assign Services** page, use the check boxes in the **Assign Services** section to choose the services you want to assign to your certificate. If you chose services during certificate creation, these services will already be checked. Click **Assign**.
4. On the **Completion** page, verify that all of the services were assigned properly.
   - If you attempt to assign the Unified Messaging service to the certificate and the certificate is running in TCP mode only, assignment will fail. In order to use a certificate for Unified Messaging, it must be set to run in TLS mode or Dual mode. For more information see Create a Certificate for Enabling Mutual TLS in Unified Messaging.

Use the Shell to assign services to a certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

This example assigns the IMAP, POP, IIS, and SMTP services to the certificate.

```
Enable-ExchangeCertificate -Server 'EXCH-H-868' -Services 'IMAP, POP, IIS, SMTP'
```


1.12.3.4 View Exchange Certificate Properties

View Exchange Certificate Properties

Exchange Server 2010 > Security > Certificates >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can view the properties of any existing Exchange certificate. The properties include the valid dates, serial number, and public key type.

Prerequisites

The Client Access server role has been installed and at least one certificate is installed on your Client Access server.

What Do You Want to Do?

- Use the EMC to view Exchange certificate properties
- Use the Shell to view Exchange certificate properties

Use the EMC to view Exchange certificate properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client Access Permissions topic.

1. In the console tree, click **Server Configuration**.
2. Select the server that contains the certificate, and then select the certificate you want to view.
3. From the action pane, click **Open**.
   - You can view information about the certificate on the **General**, **Details**, and **Certification Path** pages of the **Exchange Certificate** dialog box.

Use the Shell to view Exchange certificate properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Client Access server security settings" entry in the Client

Access Permissions topic.

This example displays all the properties for an Exchange certificate in a formatted list.

```
Get-ExchangeCertificate 0271A7F1CA9AD8A27152CCAE044F968F068B14B8 | fl
```


1.12.3.5 Clone an Existing Certificate

Clone an Existing Certificate

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-25*

Microsoft Exchange Server 2010 creates a self-signed certificate during installation that uses all the server and domain names that are known to Exchange at the time of installation. These certificates are valid for 12 months. In some cases, it may make sense to clone these certificates if the Subject and Subject Alternative Names can be used for other computers. Be aware that only the certificate metadata and not the key sets are cloned.

Looking for other management tasks related to certificates? See Certificates.

Use the Shell to clone an existing certificate

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Certificate management" entry in the Transport Permissions topic.

Note:
You can't use the EMC to clone an existing certificate.

To clone a new certificate from an existing certificate, you must first identify the current default certificate for the domain by using the **Get-ExchangeCertificate** cmdlet. The following example clones the self-signed Exchange certificate for the FQDN mail1.contoso.com. It first retrieves the certificates for mail1.contoso.com, and then filters the result for the self-signed certificate, and finally pipelines that result to the **New-ExchangeCertificate** cmdlet to clone a new certificate.

```
Get-ExchangeCertificate -DomainName mail1.contoso.com | Where {$_.IsSelfSigned -e
```

After you run this command, the Shell displays a prompt asking you if you want to overwrite the existing default SMTP certificate. Click **N** to clone the certificate without overwriting the default SMTP certificate.

The example above assumes that there is only a single self-signed Exchange certificate in your deployment, which is the case in a typical installation. However, if you have multiple self-signed certificates in your organization, you should first run the **Get-ExchangeCertificate** cmdlet and then use the thumbprint of the specific certificate you want to clone. The following example shows how to clone an existing certificate in this manner, assuming that the thumbprint value for the certificate you want to clone is c4248cd7065c87cb942d60f7293feb7d533a4afc. The first result of running **Get-ExchangeCertificate** is used to display the details of the self-signed certificates installed so you can determine which thumbprint to use.

```
Get-ExchangeCertificate -DomainName mail1.contoso.com | Where {$_.IsSelfSigned -e
Get-ExchangeCertificate -Thumbprint c4248cd7065c87cb942d60f7293feb7d533a4afc | Ne
```

For detailed syntax and parameter information, see Get-ExchangeCertificate and New-ExchangeCertificate.

1.12.3.6 Generate Request for Third-Party Certificate Services

Generate Request for Third-Party Certificate Services

Exchange Server 2010 > Security > Certificates >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-01*

Microsoft Exchange Server 2010 creates a self-signed certificate during installation that uses all the server and domain names known to Exchange at the time of installation. However, you can also use certificates signed by a certification authority (CA). If you are using a CA to generate certificates, you must provide a certificate request according to that CA's requirements.

To generate a certificate request, you can use the **New-ExchangeCertificate** cmdlet with the *GenerateRequest* parameter. You can then save the request in a file using the **Set-Content** cmdlet. The resulting file will be a PKCS #10 request (.req) file. PKCS #10 is the Certification Request Syntax Standard specified by RFC 2314. (For details, see http://www.ietf.org/rfc/rfc2314.txt.)

Looking for other management tasks related to certificates? Check out Certificates.

Prerequisites

You must contact your CA to determine its requirements for new certificate requests.

Use the Shell to generate a certificate request from a CA

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Certificate management" entry in the Transport Permissions topic.

Note:

For instructions on using the Exchange Management Shell to generate a certificate request, see Create a New Exchange Certificate.

This example generates a certificate request for the Contoso server, mail1. The common name (CN) of the Subject Name contains the fully qualified domain name (FQDN) of the server and the Subject Alternative Name contains all the accepted domains for Contoso.

```
$Data = New-ExchangeCertificate -GenerateRequest -SubjectName "c=us, o=contoso co
Set-Content -Path "c:\Certificates\mail1.contoso.com.req" -Value $Data
```

This example generates a certificate request for the Contoso server, mail1. The certificate request is similar to the preceding example, but the certificate request is saved as a DER-encoded certificate request file.

```
$Data = New-ExchangeCertificate -GenerateRequest -SubjectName "c=us, o=contoso co
Set-Content -Path "c:\Certificates\mail1.contoso.com.req" -Value $Data.FileData -
```

This example creates a certificate request from an existing Contoso.com certificate.

```
$Data = Get-ExchangeCertificate -Thumbprint c4248cd7065c87cb942d60f7293feb7d533a4
Set-Content -Path "c:\ certificates\mail1.contoso.com.req" -Value $Data
```

This example creates a certificate request with a wildcard character for all Contoso.com subdomains.

```
$Data = New-ExchangeCertificate -GenerateRequest -SubjectName "C=us, O=contoso co
Set-Content -Path "c:\certificates\mail1.contoso.com.req" -Value $Data
```

For detailed syntax and parameter information, see New-ExchangeCertificate.

Other Tasks

After you generate the certificate request, you may also want to install the certificate issued by the CA in your organization. For detailed steps, see Install Certificates Issued for Certificate Requests.

1.12.3.7 Install Certificates Issued for Certificate Requests

Install Certificates Issued for Certificate Requests

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-08-25*

Microsoft Exchange Server 2010 creates a self-signed certificate during installation that uses all the server and domain names that are known to it at the time of installation. However, you can also use certificates that are signed by a Certification Authority (CA). After you have sent the certificate request to a CA, the CA issues a certificate or chain of certificates. In both cases, the certificates are delivered as files that you must install with the **Import-ExchangeCertificate** cmdlet.

Important:

Do not use the Certificate Manager snap-in to import the certificates for any service on an Exchange server. Using the Certificate Manager snap-in to import certificates on Exchange servers will fail. Therefore, TLS or other Exchange certificate services will not work.

Looking for other management tasks related to certificates? Check out Certificates.

Prerequisites

- You must first generate a certificate request and send that request to your CA. For detailed steps, see Generate Request for Third-Party Certificate Services.
- You must place the certificates issued by your CA at a location accessible on your network.

Use the Shell to install certificates issued

by a CA

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Certificate management" entry in the Transport Permissions topic.

Note:
You can't use the EMC to install certificates issued by a CA.

You use the **Import-ExchangeCertificate** cmdlet to install a certificate issued by your CA. The following example shows how to import and enable a certificate for SMTP TLS:

```
Import-ExchangeCertificate -FileData ([Byte[]]$(Get-Content -Path c:\certificates
```

The following example shows how to import a certificate and enable it for a Client Access server that supports POP3 clients.

```
Import-ExchangeCertificate -FileData ([Byte[]]$(Get-Content -Path c:\certificates
```


1.13 Federation

Federation

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-17*

Understanding Federation

Learn about the Federation features in Exchange 2010, including the requirements for managing Federation in your organization.

Understanding Federated Delegation

Learn about federated delegation, which allows your organization and users to collaborate with users in external Exchange 2010 organizations by sharing their calendar availability (free/busy) and contact information.

Trusted Root Certification Authorities for Federation Trusts

Learn about which certification authorities (CAs) are trusted for federation trusts.

Federation Terminology in Exchange 2010

Learn about the federation terminology used in Exchange 2010.

Managing Federation

Learn how to manage federation trusts, including how to create a federation trust and configure the federated organization identifier (OrgId).

Managing Federated Delegation

Learn how to manage organization relationships and sharing policies.

1.13.1 Understanding Federation

Understanding Federation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-06*

Information workers frequently need to collaborate with external recipients, vendors, partners, and customers and share their free/busy (also known as calendar availability) and contact information. Federation in Microsoft Exchange Server 2010 helps with these collaboration efforts. *Federation* refers to the underlying trust infrastructure that supports *federated delegation*, an easy method for users to share calendar and contact information with recipients in other external federated organizations. To learn more about federated delegation, see Understanding Federated Delegation.

Looking for management tasks related to federation? Check out Managing Federation.

Contents

Microsoft Federation Gateway

The Microsoft Federation Gateway, a free cloud-based service offered by Microsoft, acts as the trust broker between your on-premises Exchange 2010 organization and other federated Exchange 2010 organizations. If you want to configure federation in your Exchange organization, you must establish a one-time federation trust with the Microsoft Federation Gateway, so that it can become a federation partner with your organization. With this trust in place, users authenticated by Active Directory (known as *identity providers*) are issued Security Assertion Markup Language (SAML) delegation tokens by the Microsoft Federation Gateway. These delegation tokens allow users from one federated organization to be trusted by another federated organization. With the Microsoft Federation Gateway acting as the trust broker, organizations aren't required to establish multiple individual trust relationships with other organizations, and users can access external resources using a single sign-on (SSO) experience. For more information, see Understanding the Microsoft Federation Gateway.

Return to top

Federation Trust

To use Exchange 2010 federated delegation features, you must establish a federation trust between your Exchange 2010 organization and the Microsoft Federation Gateway. Establishing a federation trust with the Microsoft Federation Gateway exchanges your

organization's digital security certificate with the Microsoft Federation Gateway and retrieves the Microsoft Federation Gateway certificate and federation metadata. You can establish a federation trust by using the New Federation Trust wizard in the Exchange Management Console (EMC) or the **New-FederationTrust** cmdlet in the Exchange Management Shell. A self-signed certificate is automatically created by the New Federation Trust wizard and is used for signing and encrypting delegation tokens that allow users to be trusted by external federated organizations. For details about certificate requirements, see Certificate Requirements for Federation later in this topic.

For details about how to create a federation trust, see Create a Federation Trust.

When you create a federation trust with the Microsoft Federation Gateway, an *application identifier* (AppID) is automatically generated for your Exchange organization and provided in the output of the New Federation Trust wizard or the **New-FederationTrust** cmdlet. The AppID is used by the Microsoft Federation Gateway to uniquely identify your Exchange organization. It's also used by the Exchange organization to provide proof that your organization owns the domain for use with the Microsoft Federation Gateway. This is done by creating a text (TXT) record in the Domain Name System (DNS) zone of each federated domain.

For details about how to create a TXT record, see Create a TXT Record for Federation.

Return to top

Federated Organization Identifier

The *federated organization identifier* (OrgID) defines which of the authoritative accepted domains configured in your organization are enabled for federation. Only recipients that have e-mail addresses with accepted domains configured in the OrgID are recognized by the Microsoft Federation Gateway and are able to use federated delegation features. When you create a new federation trust, an OrgID is automatically created with the Microsoft Federation Gateway. This OrgID is a combination of a pre-defined string and the first accepted domain selected for federation in the wizard. For example, in the Manage Federation wizard, if you specify the federated domain **contoso.com** as your organization's primary SMTP domain, the **FYDIBOHF25SPDLT.contoso.com** account namespace will be automatically created as the OrgID for the federation trust.

This subdomain doesn't have to be an accepted domain in your Exchange organization and doesn't require a domain name system (DNS) proof of ownership TXT record. The only requirement is that accepted domains selected to be federated are limited to a maximum of 32 characters. Additionally, if you use the Manage Hybrid Configuration wizard to create a federation trust associated with configuring a hybrid deployment between your on-premises organization and an Exchange Online organization, the OrgID for the federated trust is also automatically configured with the automated namespace. The only purpose of this subdomain is to serve as the federated namespace for the Microsoft Federation Gateway to maintain unique identifiers for recipients that request SAML delegation tokens. For more information about SAML tokens, see SAML Tokens and Claims

You can add or remove accepted domains at any time. If you want to enable or disable all federation features in your organization, all you have to do is enable or disable the OrgID.

Important:

If you change the OrgID, accepted domains, or the AppID used for federation, all federation features are affected in your organization. This also affects any external federated organizations, including Office 365 and hybrid deployment configurations. We recommend that you notify all external federated partners of any changes to these configuration settings.

For more information about configuring the federated OrgID, see the following topics:

- Manage Federation
- Configure Federated Delegation

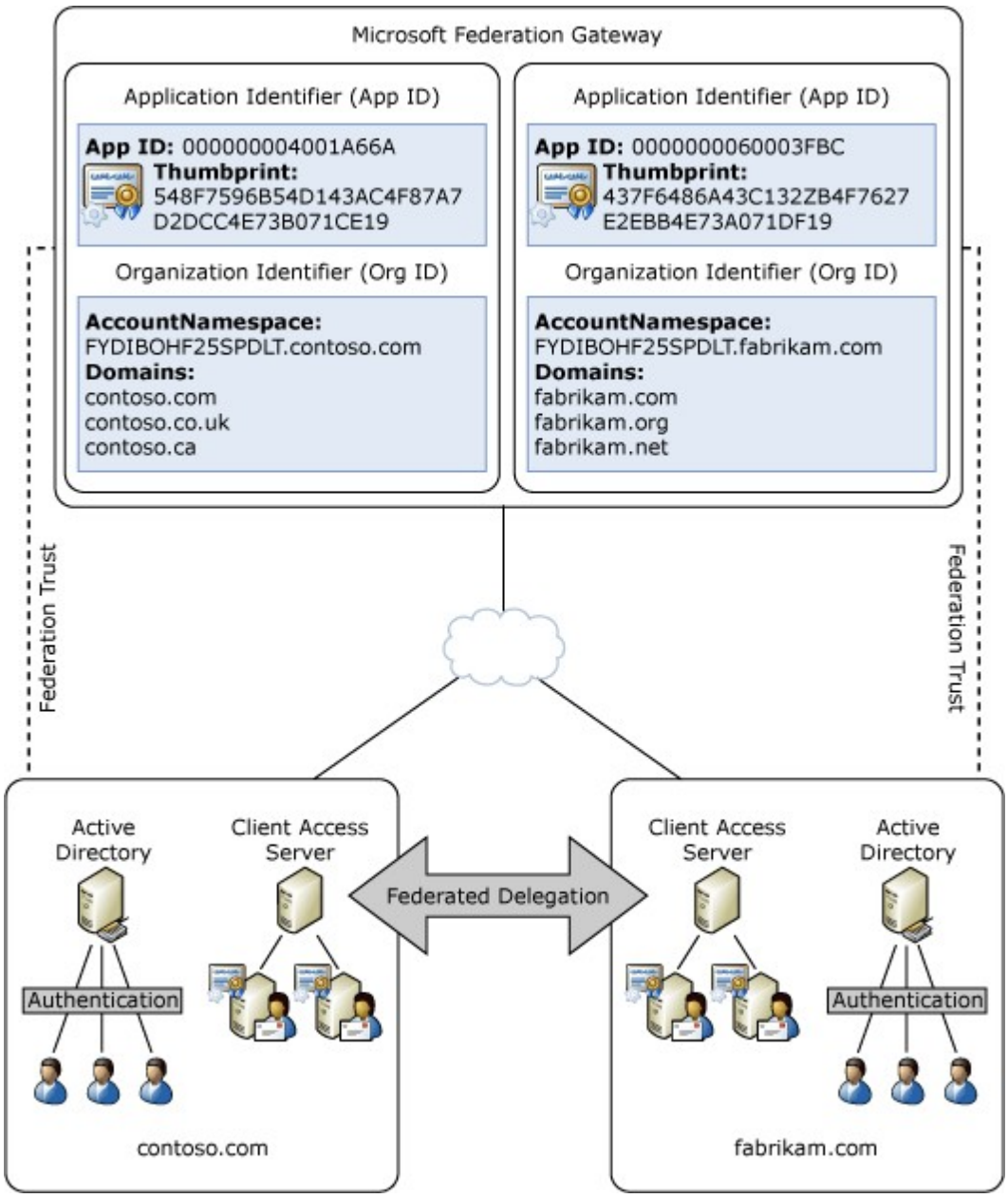
Return to top

Federation Example

Two Exchange organizations, Contoso, Ltd. and Fabrikam, Inc., want their users to be able to share free/busy information with each other. Each organization creates a federation trust with the Microsoft Federation Gateway and configures its account namespace to include the domain used for its user's e-mail address domain.

Contoso employees use one of the following e-mail address domains: contoso.com, contoso.co.uk, or contoso.ca. Fabrikam employees use one of the following e-mail address domains: fabrikam.com, fabrikam.org, or fabrikam.net. Both organizations make sure that all accepted e-mail domains are included in the account namespace for their federation trust with the Microsoft Federation Gateway. Rather than requiring a complex Active Directory forest or domain trust configuration between the two organizations, both organizations configure an organization relationship with each other to enable free/busy sharing.

The following figure illustrates the federation configuration between Contoso, Ltd. and Fabrikam, Inc.



Certificate Requirements for Federation

To establish a federation trust with the Microsoft Federation Gateway, either a self-signed certificate or an X.509 certificate signed by a certification authority (CA) must be created and installed on the Exchange 2010 server used to create the trust. We recommend using a self-signed certificate, which can be automatically created and installed using the New Federation Trust wizard in the EMC. This certificate is used only to sign and encrypt delegation tokens used for federated delegation. Only one certificate is required for the federation trust. Exchange 2010 automatically distributes the certificate to other Exchange 2010 servers in the organization.

If you want to use an X.509 certificate signed by an external CA, the certificate must meet the following requirements:

- **Trusted CA** If possible, the X.509 Secure Sockets Layer (SSL) certificate

should be issued from a CA trusted by Windows Live. However, you can use certificates issued by CAs that aren't currently certified by Microsoft. For a current list of trusted CAs, see Trusted Root Certification Authorities for Federation Trusts.

- **Subject key identifier** The certificate must have a subject key identifier field. Most X.509 certificates issued by commercial CAs have this identifier.
- **CryptoAPI cryptographic service provider (CSP)** The certificate must use a CryptoAPI CSP. Certificates that use Cryptography API: Next Generation (CNG) providers aren't supported for federation. If you use Exchange to create a certificate request, a CryptoAPI provider is used. For more information, see Cryptography API: Next Generation.
- **RSA signature algorithm** The certificate must use RSA as the signature algorithm.
- **Exportable private key** The private key used to generate the certificate must be exportable. You can specify that the private key be exportable when you create the certificate request using the New Exchange Certificate wizard in the EMC or the New-ExchangeCertificate cmdlet in the Shell.
- **Current certificate** The certificate must be current. You can't use an expired or revoked certificate to create a federation trust.
- **Enhanced key usage** The certificate must include the enhanced key usage (EKU) type **Client Authentication (1.3.6.1.5.5.7.3.2)**. This usage type is used to prove your identity to a remote computer. If you use the EMC or the Shell to generate a certificate request, this usage type is included by default.

Note:

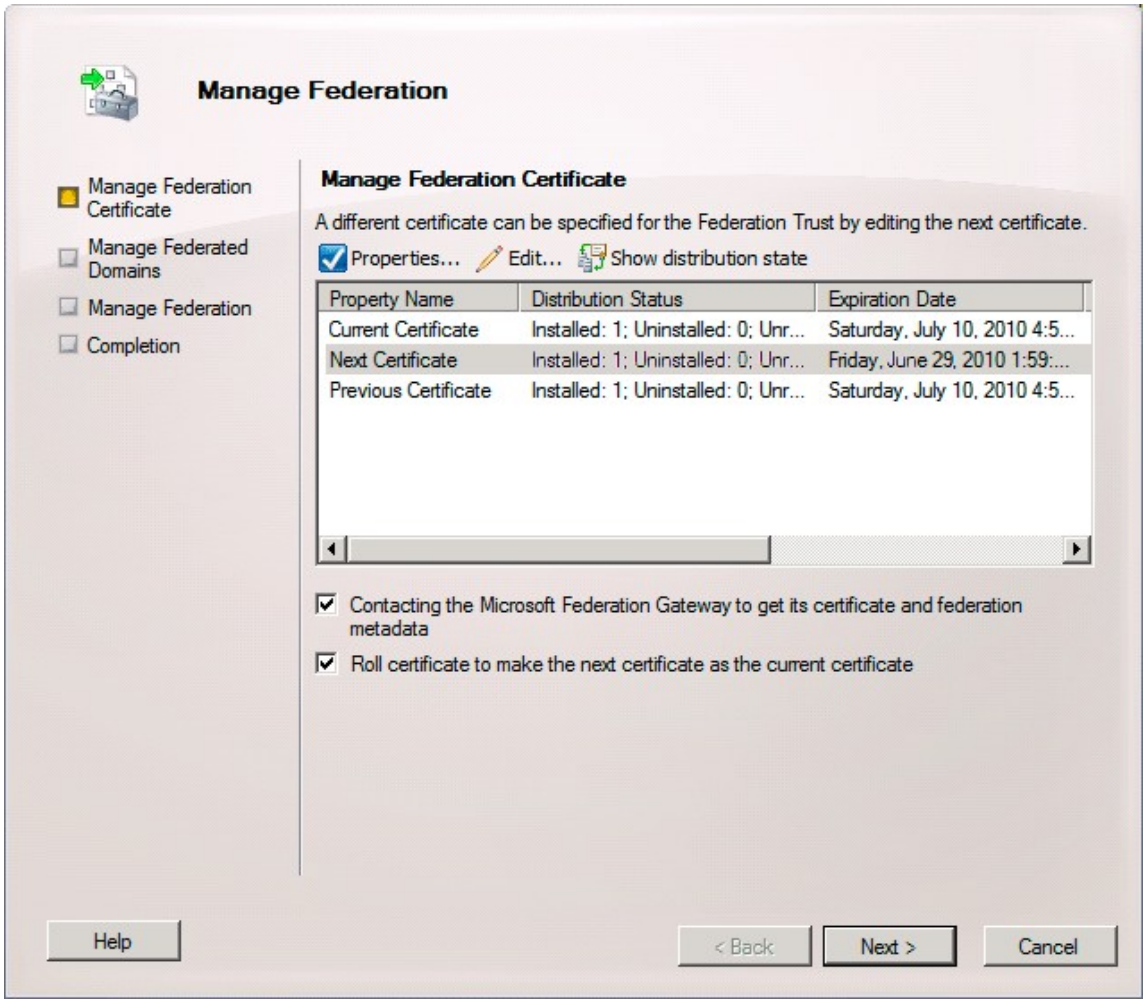
Because the certificate isn't used for authentication, it doesn't have any subject name or subject alternative name requirements. You can use a certificate with a subject name that's the same as the host name, the domain name, or any other name.

Return to top

Transitioning to a New Certificate

The certificate used to create the federation trust is designated as the current certificate. However, you may need to install and use a new certificate for the federation trust periodically. For example, you may need to use a new certificate if the current certificate expires or to meet a new business or security requirement. To ensure a seamless transition to a new certificate, you must install the new certificate on your Exchange 2010 server and configure the federation trust to designate it as the next certificate. Exchange 2010 automatically distributes the next certificate to other Exchange 2010 servers in the organization. Depending on your Active Directory topology, distribution of the certificate may take awhile. You can verify the certificate status using the Manage Federation wizard in the EMC or the Test-FederationTrustCertificate cmdlet in the Shell.

After you verify the certificate's distribution status, you can configure the trust to use the next certificate. After switching certificates, the current certificate is designated as the previous certificate, and the next certificate is designated as the current certificate. The new certificate is published to the Microsoft Federation Gateway, and all new tokens exchanged with the Microsoft Federation Gateway are encrypted using the new certificate. The following figure illustrates how you can use the Manage Federation wizard to configure this transition.



For more information about how to transition to a new certificate, see Manage Federation.

Note:
This certificate transition process is used only by federation. If you use the same certificate for other Exchange 2010 features that require certificates, you must take the feature requirements into consideration when planning to procure, install, or transition to a new certificate.

Return to top

1.13.2 Understanding Federated Delegation

Understanding Federated Delegation

Exchange Server 2010 > Federation >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-10-26*

Information workers frequently have to collaborate with partners, customers, vendors, or

other contacts outside their Exchange organization. For effective cross-organization collaboration, your users may have to share their free/busy (also known as calendar availability) information for scheduling meetings. Depending on the nature of the business relationship, users may have to share more detailed calendar information. Similarly, users may also have to share their contacts with these external recipients. In Microsoft Exchange Server 2010, federated delegation helps accomplish these goals.

Looking for management tasks related to federated delegation? See Managing Federated Delegation.

Contents

Collaboration Before Exchange 2010 and Federated Delegation

Earlier versions of Exchange had limited sharing capabilities and required complex set up and ongoing maintenance. For example, to share availability information with users in another Exchange organization, you had to use the Inter-Organization Replication tool to replicate public folders between Exchange organizations. This process required you to create Active Directory trusts between both organizations, as well as manage service account credentials.

For recipients to be visible in Exchange address lists, many organizations used different tools such as GALSync to synchronize one organization's recipients to another organization. Setting up trusts, managing credentials, and replication with multiple external organizations was difficult and cumbersome. Creating Active Directory forest or domain trusts and credential management also had security implications. Opening additional ports on firewalls between the two organizations or establishing a virtual private network (VPN) was also required.

With the introduction of Exchange Web Services, the Availability service, and the Client Access server role in Exchange Server 2007, the replication of public folder free/busy data wasn't necessary. However, trust or credential information and global address list (GAL) synchronization was still necessary to make free/busy information available to external organizations.

Sharing a Calendar or Contacts folder also involved assigning permissions to access the folder to users in trusted organizations. The only way to accomplish this was by creating Active Directory trusts between the two organizations, which had additional security implications.

For more information, see How to Configure the Availability Service for Cross-Forest Topologies.

Return to top

Federated Delegation

Using federated delegation in Exchange 2010, users can share information with recipients in external federated organizations by establishing a federation trust and creating organization relationships between Exchange 2010 organizations. Organizations can also use sharing policies to allow users to create individual sharing relationships with recipients in other organizations. Federated delegation uses the Microsoft Federation Gateway, a Microsoft cloud-based service, as the trust broker between two federated organizations. To enable federated delegation, the organizations between which you want to share information only have to establish a one-time federation trust with the Microsoft Federation Gateway and configure either an organization relationship or sharing policies with each other.

Important:

If you disable the federated organization identifier for your Exchange 2010 organization, all federation features are disabled for your organization.

To learn more about the Microsoft Federation Gateway and federation trusts, see the following:

- Microsoft Federation Gateway
- Understanding Federation
- Create a Federation Trust
- Manage Federation.

Federated delegation offers two ways for users to share calendar and contact information with external recipients: Organization relationships and sharing policies.

Organization Relationships

Organization relationships allow you to enable federated delegation with another federated organization for the purpose of sharing calendar free/busy information between users in both organizations. Organization relationships are one-to-one relationships between two organizations. Rather than requiring a complex Active Directory forest or domain trust configuration between the two organizations (which may also require opening multiple ports on firewalls in both organizations or establishment of a VPN), both organizations are required to establish only one federation trust with the Microsoft Federation Gateway and to configure their federated organization identifier prior to configuring the organization relationship with each other.

Requirements for Organization Relationships

The following are required for organization relationships:

- An Exchange 2010 Client Access server exists in each Exchange organization.
- Each Exchange organization has created a federation trust with the Microsoft Federation Gateway.
- Each Exchange organization has configured a federated organization identifier. Domains used for generating users' e-mail addresses have been added to the organization identifiers.
- An organization relationship exists in each corresponding organization.
- The Mailbox servers that are hosting user mailboxes can reach the Microsoft Federation Gateway servers and the federated partner organizations CAS servers.

Note:

Office Outlook 2007 users can't specify SMTP addresses of external recipients to display availability information. Recipients must be picked from the GAL, which requires GAL synchronization with the external organization. Outlook 2007 users with mailboxes on Exchange 2007 Service Pack 2 (SP2) Mailbox servers can use Office Outlook Web Access on an Exchange 2007 SP2 Client Access server.

Creating Organization Relationships

When you create an organization relationship with an external organization, users in the external organization can access your users' free/busy information. No replication of GAL information is required. With this configuration in place, Outlook 2010 and Office Outlook Web App users can simply enter the SMTP address of an external recipient when scheduling meetings.

When creating an organization relationship, you can specify one of the following three levels of calendar availability access:

- No free/busy access
- Free/busy access with time only
- Free/busy access with time, plus subject and location

For users in your organization to have access to external users' free/busy information or to allow for one-way sharing of their free/busy information with the external organization, the administrator in the external organization must also create an organization relationship with your organization. However, the external administrator can specify a different level of access for their users that's different from the level you specified. In a one-way sharing example, the external administrator would configure their organization relationship so that their users' free/busy information isn't shared with users in your organization, but the free/busy information for your users would be visible to the users in the external organization based on your organization relationship settings.

Note:

If users don't want to share their free/busy information with others, they can modify the Default permission entry in Outlook. To do this, users navigate to the **Calendar Properties** > **Permissions** tab, select the **Default** permission, and select **None** from the **Permission Level** list. Their free/busy information won't be visible to internal or external users, even if an organization relationship exists with an external organization. The organization relationship honors the permissions set by the user.

When you create an organization relationship, Exchange 2010 connects to the Autodiscover Web service published by the external organization to obtain the Availability service endpoint. You can also specify the external organization's Availability service endpoint manually when creating the relationship.

To create an organization relationship with an external organization, you can use the New Organization Relationship wizard in the Exchange Management Console (EMC) or the New-OrganizationRelationship cmdlet in the Exchange Management Shell.

For details instructions about how to create an organization relationship, see Create an Organization Relationship.

Sharing Policies

Unlike organization relationships, which only enable sharing of free/busy information with recipients in other federated Exchange organizations, sharing policies enable user-established, people-to-people sharing of both calendar and contact information with different types of external users. Sharing polices allow your users to share both their free/busy and contact information (including the Calendar and Contacts folders) with recipients in other external federated organizations. For recipients that aren't in an external federated organization or are in non-Exchange organizations, sharing policies allow people-to-people sharing of their calendar information with anonymous users through the use of Internet Calendar Publishing.

With sharing policies, you won't need to manage your users' collaboration relationships. Instead, they get to decide which external recipients they want to collaborate with. Using Outlook 2010 or Outlook Web App, users can invite external recipients in other federated domains to access their Calendar or Contacts folder and also request that they share theirs in return. Users can also grant anonymous access to their calendar information to any individual who has Internet access. With sharing policies, you only control what types of users they can share information with and how much information they can share. If

necessary, you can also disable a user's or group's sharing policy.

Sharing policies are assigned to mailbox users. The default sharing policy applied to users allows availability information to be shared with all external federated domains. After you create a federation trust with the Microsoft Federation Gateway and configure the federated organization identifier, users can invite users in any external federated organization to share their calendar and contact information.

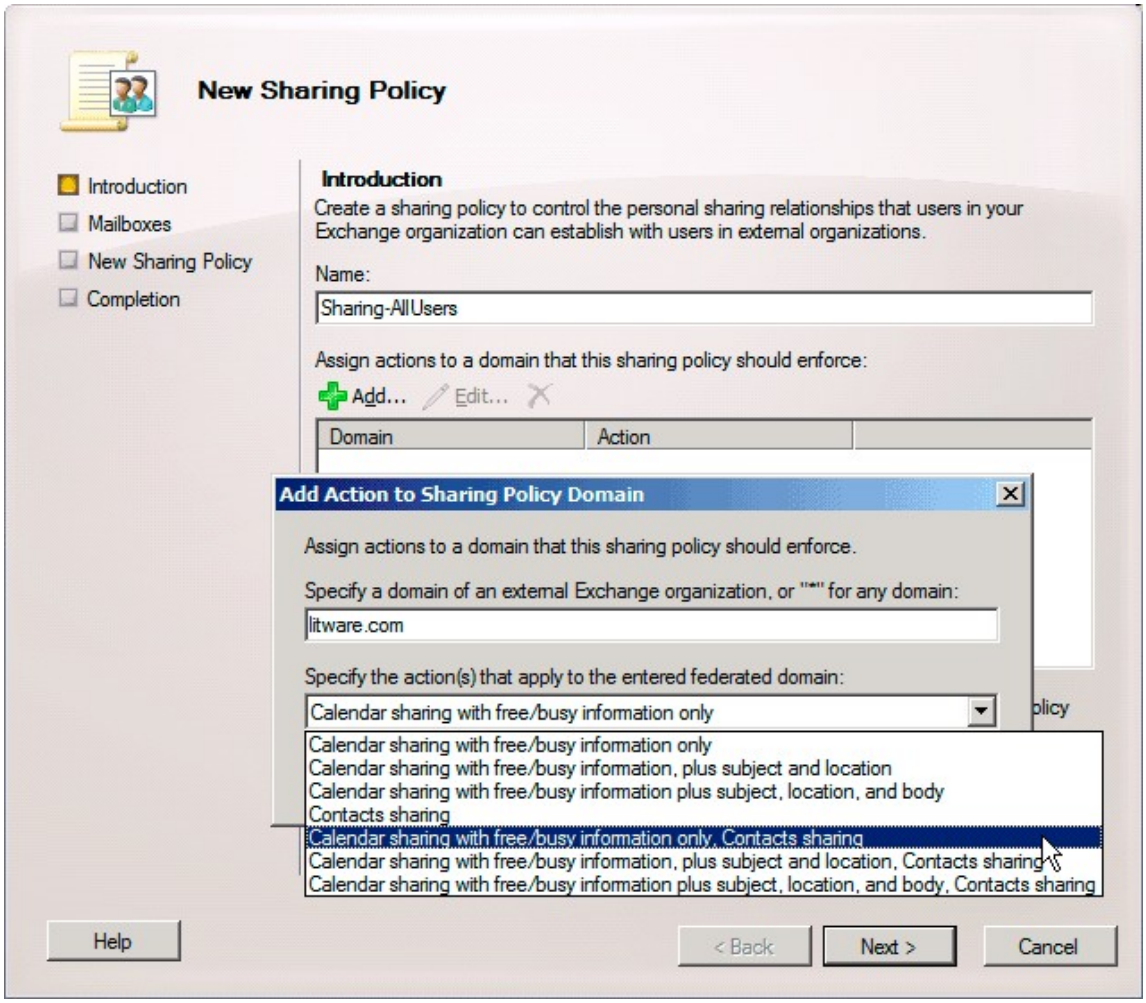
Important:

To participate in federated delegation, the external user's organization must also have a federation trust established with the Microsoft Federation Gateway, and the federated organization identifier must be configured.

To allow access to user's calendars by recipients in non-federated domain organizations, such as family members, friends, or users in non-Exchange organizations, a separate sharing policy should be created that allows for anonymous calendar access through the use of Internet Calendar Publishing. For details, see Enable Internet Calendar Publishing.

Sharing policies can contain pairs of domain names and the sharing actions allowed for users from those domains. As shown in the following figure, you can specify the following actions that apply to the external domain specified in a sharing policy:

- Calendar sharing with free/busy information only
- Calendar sharing with free/busy information, plus subject and location
- Calendar sharing with free/busy information plus subject, location and body
- Contacts sharing
- Calendar sharing with free/busy information only, Contacts sharing
- Calendar sharing with free/busy information, plus subject and location, Contacts sharing
- Calendar sharing with free/busy information plus subject, location, and body, Contacts sharing



When creating a sharing invitation, your users can select the information they want to share, provided that the action is allowed by the user's sharing policy. For example, let's say you create a sharing policy with the following settings for Fabrikam and other federated domain organizations:

- **Calendar sharing with free/busy information, plus subject and location** for external users in Fabrikam.com
- **Calendar sharing with free/busy information only** for external users in all other federated domain organizations (represented by the asterisk [*] symbol)

Users who have this policy applied can either share their calendar free/busy information with other federated domain organizations or can also share additional limited details if they invite users from Fabrikam.com.

For details about how to create a sharing policy, see Create a Sharing Policy.

For details about how to apply a sharing policy to users, see Apply a Sharing Policy to Mailboxes.

Requirements for Federated Sharing Policies

The following are required for sharing policies between federated domain organizations:

- An Exchange 2010 Client Access server exists in each Exchange organization.
- Each Exchange organization has created a federation trust with the Microsoft Federation Gateway.

- Each Exchange organization has configured a federated organization identifier. Domains used for generating users' e-mail addresses have been added to the organization identifiers.
- User mailboxes are located on Exchange 2010 Mailbox servers in each Exchange organization.
- Only Outlook 2010 and Outlook Web App users can create sharing invitations.

Requirements for Non-Federated Sharing Policies

The following are required for sharing policies with non-federated domain organizations or individual anonymous access:

- An Exchange 2010 Client Access server exists in the Exchange organization that's sharing user's calendar information.
- User mailboxes are located on Exchange 2010 Mailbox servers in the Exchange organization that's sharing user's calendar information.
- The Client Access server must be enabled for Outlook Web App access.

Comparing Organization Relationships and Sharing Policies

Although organization relationships and sharing policies allow sharing of free/busy information with external users, they're intended for different scenarios. Organization relationships are created to collaborate with external federated organizations and are limited to sharing only free/busy information. Sharing policies govern what calendar and contact information your users can share with users in external federated organizations, non-federated Exchange organizations, non-Exchange organizations, and anonymous users.

The following table lists the differences between organization relationships and sharing policies.

Organization relationships vs. sharing policies

Functionality	Organization relationship	Sharing policy
Requires a federation trust for your organization	Yes	Yes when sharing with other federated domain organizations. Not required for Internet sharing policies.
Recommends that the external domain be federated	Yes	Yes when sharing with other federated domain organizations. Not required for Internet sharing policies.
Allows sharing of free/busy information (including subject and location) with external organizations for a set of many users.	Yes	No
Allows sharing of Calendar folders with free/busy information	No	Yes
Allows sharing of Calendar folders with free/busy information, including subject and body	No	Yes
Allows sharing of contacts	No	Yes when sharing with other federated domain organizations. Not required for Internet sharing policies.

Requires users to send a sharing invitation to external recipients	No	Yes
Provides an access method	Your Client Access server accesses the Client Access server of the external organization and retrieves free/busy information for the external user when requested.	Your Client Access server accesses the Client Access server of the external organization and subscribes to the external user's Calendar or Contacts folder for federated domain organizations. For Internet sharing policies, external users access either a restricted or public URL on the Client Access server.
Can be applied to all external domains	No (a one-to-one relationship between two Exchange 2010 organizations)	Yes
Provides users with different sharing experiences with external recipients	No	Yes, based on the sharing policy that's applied
Disables sharing for some users	Yes, by specifying a security distribution group for the organization relationship	Yes, by disabling the sharing policy that's applied
Requires that the mailbox reside on an Exchange 2010 Mailbox server	No	Yes

Return to top

Firewall Considerations for Federated Delegation

Federated delegation features require that the Client Access servers in your organization have outbound access to the Internet by using HTTPS. You must allow outbound HTTPS access (port 443 for TCP) to all Exchange 2010 Client Access servers in the organization.

For an external organization to access your organization's free/busy information, you must publish one Client Access server to the Internet. This requires inbound HTTPS access from the Internet to the Client Access server. Client Access servers in Active Directory sites that don't have a Client Access server published to the Internet can use Client Access servers in other Active Directory sites that are accessible from the Internet. The Client Access servers that aren't published to the Internet must have the external URL of the Web services virtual directory set with the URL that's visible to external organizations.

Return to top

Coexistence with Exchange 2007

In organizations that contain both Exchange 2010 and Exchange 2007 servers, users who have a mailbox on an Exchange 2007 Mailbox server can use organization relationships to share free/busy information with recipients in external federated domain

organizations. The Mailbox server must be running Exchange 2007 SP2 or later, and you must have at least one Exchange 2010 Client Access server in the Exchange organization. You can use organization relationships by introducing a single Exchange 2010 Client Access server in the organization, providing a more robust solution than solutions that synchronize free/busy information and require GAL synchronization.

When using Outlook 2010 or Outlook Web App to scheduling a meeting on an Exchange 2007 server, a user who has a mailbox on an Exchange 2007 server can see free/busy information for a user in the external organization. Free/busy information for Exchange 2007 mailboxes is visible to recipients in the external organization.

Sharing policies are assigned to Exchange 2010 mailbox users. To use sharing policies, a mailbox must be located on an Exchange 2010 Mailbox server. Only Outlook 2010 and Outlook Web App clients can be used to generate or respond to sharing invitations.

Return to top

Coexistence with Exchange 2003

In organizations that contain both Exchange 2010 and Exchange 2003 servers, users who have a mailbox on an Exchange 2003 server can use organization relationships to share free/busy information with recipients in external federated domain organizations. The Mailbox server must be running Exchange Server 2003 SP2 or later, and you must have at least one Exchange 2010 Client Access and public folder server in the Exchange 2003 organization. The Client Access server acts as a proxy for all inbound and outbound free/busy requests and is used to configure organization relationship properties. The public folder server contains and manages a replica of Exchange 2003 public folder data for access of free/busy information by other federated Exchange 2010 organizations.

Internal and external Exchange mailbox users can view free/busy information in the Exchange 2003 organization by using Outlook 2003, Outlook 2007, Outlook 2010 or Outlook Web App. Sharing policies are assigned only to Exchange 2010 mailbox users. To use sharing policies, mailboxes must be located on an Exchange 2010 Mailbox server. You can't apply sharing policies to mailboxes located on Exchange 2003 servers.

Return to top

Establishing an Organization Relationship and a Sharing Policy

In this example, you're the administrator for Contoso, Ltd. Your organization entered into an agreement with Fabrikam, Inc. to develop a product that will be jointly marketed and sold by both organizations. To enable collaboration between the two organizations, users from the Marketing and Engineering departments of both organizations need to access each other's availability information. This collaboration should occur with minimal or no effort by users.

Contoso also collaborates with Litware, Inc. This collaboration is limited to a small subset of users. Users from both organizations should be able to establish sharing relationships with each other. Sharing of contacts and free/busy information should be allowed. No additional calendar information should be shared.

Additionally, Contoso users want to share their calendar information with family members to help coordinate outside activities that they manage in Outlook.

Lastly, sharing should occur without having to:

- Create any Active Directory forest or domain trusts.

- Exchange credentials between the organizations or individuals.
- Establish a VPN between the organizations or individuals.

To accomplish this scenario, take the following steps:

1. To configure federated delegation with Fabrikam and Litware, create a federation trust with the Microsoft Federation Gateway (if one hasn't already been created). This isn't required for sharing information with Contoso users' family members. This one-time procedure is required to use Exchange 2010 federation features. The process requires that an X.509 certificate be issued by a certification authority trusted by the Microsoft Federation Gateway. For details, see Create a Federation Trust.
2. Configure the federated organization identifier (if it isn't already configured). This process requires that you add the organization's accepted domains for which you want to enable federation to the organization identifier. This one-time procedure is required to use Exchange 2010 federation features. For details, see Manage Federation.
3. Create an organization relationship with Fabrikam, Inc. For details, see Create an Organization Relationship. Do the following:
   - To determine if the Fabrikam organization already has federation established, use the Get-FederationInformation cmdlet.
   - Select a distribution group that includes members from the Marketing and Engineering departments. Availability information for these users will be visible to Fabrikam users.
4. To allow users in both organizations to see availability information for each other, the administrator from Fabrikam, Inc. must also create an organization relationship with your organization.
5. Create a sharing policy for users who need to collaborate with users in the Litware.com domain. For details, see Create a Sharing Policy. Create the sharing policy with the following specifications:
   - To determine if the Litware organization already has federation established, use the Get-FederationInformation cmdlet.
   - Add the Litware.com domain to the sharing policy.
   - Select the **Calendar sharing with free/busy information only, Contacts sharing** action for the policy.
   - Assign the policy to users in your organization who need to collaborate with users from Litware. For details, see Apply a Sharing Policy to Mailboxes.
6. Create an anonymous sharing policy for Contoso users who need to collaborate with their family members. For details, see Create a Sharing Policy. Create the sharing policy with the following specifications:
   - Set the publishing virtual directory on the Client Access server. For details, see Set-OwaVirtualDirectory
   - Set the Webproxy URL for the Mailbox server. To do this, use the Set-ExchangeServer cmdlet with the *InternetWebProxy* parameter.
   - Enable the Client Access server virtual directory for anonymous publishing.

After you create the organization relationship with Fabrikam, Inc. and the sharing policy for Litware, Inc. and Contoso users, the following functionality will be available:

- All users will be able to view the availability information for users in the Marketing and Engineering departments of Fabrikam.
- Users in your organization who have the new sharing policy applied will be able send individual sharing invitations to users from Litware, Inc.
- Contoso users can invite their friends and family to view their calendar information by providing a link to their published calendar. Family members won't need special credentials to access the information.

Return to top

1.13.3 Trusted Root Certification Authorities for Federation Trusts

Trusted Root Certification Authorities for Federation Trusts

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-10-26*

To establish a federation trust between your Microsoft Exchange Server 2010 organization and the Microsoft Federation Gateway, you need a digital certificate installed on the Exchange server used to create the trust. We recommend using a self-signed certificate. A self-signed certificate is created and installed automatically when using the New Federation Trust wizard in the Exchange Management Console (EMC).

If you don't want to use the recommended self-signed certificate, you should request and install an X.509 Secure Sockets Layer (SSL) certificate from a certification authority (CA) trusted by Windows Live. Although certificates issued by other CAs may also be used to establish a federation trust with the Microsoft Federation Gateway, they aren't certified by Microsoft to date.

The following table lists CAs currently trusted by Windows Live. These CAs have been tested for use with Exchange 2010.

CA friendly name	Issued by	Intended purposes
Comodo	Comodo Certification Authority	Server authentication, client authentication
Digicert	Digicert Global Root Certification Authority	Server authentication, client authentication
Digicert High Assurance EV	Digicert Global Root Certification Authority	Server authentication, client authentication
Entrust	Entrust.net Secure Server Certification Authority	Server authentication, client authentication
Entrust (2048)	Entrust.net Secure Server Certification Authority	Server authentication, client authentication
Equifax	Equifax Secure Certification Authority	Server authentication, client authentication
GlobalSign	GlobalSign Certification Authority	Server authentication, client authentication
Go Daddy	Go Daddy Class 2 Certification Authority	Server authentication, client authentication
Network Solutions	Network Solutions Certification Authority	Server authentication, client authentication
PositiveSSL	Comodo Certification Authority	Server authentication, client authentication
UTN-UserFirst-Hardware	Comodo Certification Authority	Server authentication, client authentication
VeriSign	Class 3 Public Primary Certification Authority	Server authentication, client authentication

VeriSign	VeriSign Trust Network	Server authentication, client authentication

Are you successfully using a certificate for Federation with Exchange 2010 that isn't on this list? If so, you can assist in the CA verification process. Simply click **Click to Rate and Give Feedback** at the top of this topic and include the CA name and thumbprint information.

For more information about certificate requirements for Federation, see Understanding Federation.

1.13.4 Federation Terminology in Exchange 2010

Federation Terminology in Exchange 2010

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-03-06*

Federation is a technology in Microsoft Exchange Server 2010 that helps organizations share information with other Exchange organizations. Federation makes it easier to share free/busy (calendar availability) and contact information with users in other Exchange organizations. The following table defines the core components associated with federation in Exchange 2010.

account namespace domain

The combination of the first selected accepted domain namespace and a pre-defined string that's automatically added to the organization identifier (OrgID) as a federated domain. The account namespace domain is formatted as FYDIBOHF25SPDLT.< *your domain*>, is used in delegation tokens, and is unique to your Exchange organization.

application identifier (AppID)

A unique number generated by the Microsoft Federation Gateway to identify Exchange organizations. The AppID is generated when you create a federation trust with the Microsoft Federation Gateway.

delegation token

A Security Assertion Markup Language (SAML) token issued by the Microsoft Federation Gateway that allows users from one federated organization to be trusted by another federated organization. A delegation token contains the user's e-mail address, an immutable identifier, and information associated with the offer for which the token is issued for action.

external federated organization

An external Exchange organization that's established a federation trust with the Microsoft Federation Gateway.

federated delegation

A group of Exchange features that leverage a federation trust with the Microsoft Federation Gateway to work across Exchange organizations, including cross-premise Exchange deployments. Together, these features are used to make authenticated requests between servers on behalf of users across multiple Exchange organizations.

federated domain

An accepted authoritative domain that's added to the organization identifier (OrgID) for an Exchange organization.

domain proof encryption string

A cryptographically secure string used by an Exchange organization to provide proof that the organization owns the domain used with the Microsoft Federation Gateway. The string is generated by using the **Get-FederatedDomainProof** cmdlet.

federated sharing policy

An organization-level policy that enables and controls user-established, person-to-person sharing of both calendar and contact information.

federation

A trust-based agreement between two Exchange organizations to achieve a common purpose. With federation, both organizations want authentication assertions from one organization to be recognized by the other.

federation trust

A relationship with the Microsoft Federation Gateway that defines the following components for your Exchange organization:

- Account namespace
- Application identifier (AppID)
- Organization identifier (OrgID)
- Federated domains

To configure federated delegation with other federated Exchange organizations, a federation trust must be established with the Microsoft Federation Gateway.

Microsoft Federation Gateway

A free identity service that runs in the cloud (over the Internet and beyond a corporate network domain). The Microsoft Federation Gateway acts as the trust broker between federated Microsoft Exchange Server 2010 organizations. It's responsible for issuing delegation tokens to Exchange recipients when they request information from recipients in other federated Exchange organizations.

non-federated organization

Organizations that don't have a federation trust established with the Microsoft Federation Gateway.

organization identifier (OrgID)

Defines which of the authoritative accepted domains configured in an organization are enabled for federation. Only recipients that have e-mail addresses with federated domains configured in the OrgID are recognized by the Microsoft Federation Gateway and able to use federated delegation features.

organization relationship

A one-to-one relationship between two federated Exchange organizations that allows recipients to share free/busy (calendar availability) information. An organization relationship requires a federation trust with the Microsoft Federation Gateway and replaces the need to use Active Directory forest or domain trusts between Exchange organizations.

1.13.5 Managing Federation

Managing Federation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-07*

Create a Federation Trust

Create a TXT Record for Federation

Manage Federation

Remove a Federation Trust

1.13.5.1 Create a Federation Trust

Create a Federation Trust

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-04-27*

A federation trust establishes a trust relationship between a Microsoft Exchange Server 2010 organization and the Microsoft Federation Gateway.

Note:

Creating a federation trust is one of several steps in setting up federated delegation in your Exchange organization. To review all the steps, see Configure Federated Delegation.

Looking for other management tasks related to federation? Check out Managing Federation.

Prerequisites

- The domain used for establishing a federation trust should be resolvable from the Internet. This requires that the domain be registered with a domain registrar and the Domain Name System (DNS) zone for the domain to be hosted on a DNS server accessible from the Internet. If the organization receives Internet e-mail for the domain, these requirements are already met.
- Both Exchange organizations in a federated delegation relationship must use the same Microsoft Federation Gateway instance for their federation trusts. This requirement applies when configuring federated delegation between two on-premises Exchange organizations or between an on-premises Exchange organization and an Exchange organization hosted by Microsoft Online Services or Microsoft Live@edu.
  When you create a federation trust with the Microsoft Federation Gateway for your Exchange organization, the federation trust will use either the business or consumer instance of the Microsoft Federation Gateway.
  The following Exchange organizations use the business instance of the Microsoft Federation Gateway by default:

- Exchange 2010 Service Pack 2 (SP2) organizations using self-signed certificates for a federation trust
- Exchange organizations hosted by Microsoft Online Services, such as the Exchange Online service offered in the Microsoft Business Productivity Online Standard Suite

The following Exchange organizations use the consumer instance of the Microsoft Federation Gateway by default:

- Release to manufacturing (RTM) version of Exchange 2010 organizations using certificates issued by third-party certification authorities
- Exchange organizations hosted by Microsoft Live@edu

We recommend that all Exchange organizations use the business instance of the Microsoft Federation Gateway for federation trusts. Before configuring federated delegation between the two organizations, you need to verify which Microsoft Federation Gateway instance each Exchange organization is using for any existing federation trusts. To determine which Microsoft Federation Gateway instance an Exchange organization is using for an existing federation trust, run the following Shell command.

```
Get-FederationInformation -DomainName <the hosted Exchange domain names
```

The business instance returns a value of **<uri:federation:MicrosoftOnline>** for the *TokenIssuerURIs* parameter.

The consumer instance returns a value of **<uri:WindowsLiveID>** for the *TokenIssuerURIs* parameter.

To configure federated delegation with an Exchange organization that has an existing federation trust that's using the business instance of the Microsoft Federation Gateway, follow the steps in Use the EMC to create a federation trust or Use the Shell to create a federation trust steps in this topic. These steps are all you need to perform to create federation trusts that can be used to enable federated delegation between two Exchange 2010 SP2 organizations.

To configure federated delegation between your Exchange 2010 SP2 organization and an Exchange organization that has an existing federation trust that's using the consumer instance of the Microsoft Federation Gateway, select from the following methods:

- **Recommended method** The Exchange organization using the consumer instance of the Microsoft Federation Gateway should install Exchange 2010 SP2. After installing SP2, the existing federated domains and federation trusts should be removed and re-created using the EMC. When the federation trusts are re-created, the business instance of the Microsoft Federation Gateway will be used. You should also test all existing organization relationships to verify that they're functioning properly. For details about how to remove federation trusts, see Remove a Federation Trust.
- **Alternative method** To create a federation trust using the consumer instance of the Microsoft Federation Gateway, the Exchange 2010 SP2 organization can use the procedure Use the Shell to create a federation trust that uses the consumer instance of the Microsoft Federation Gateway. This method should be used only when you need to enable federated delegation with another Exchange organization that can't install Exchange 2010 SP2.

What Do You Want to Do?

- Use the EMC to create a federation trust
- Use the Shell to create a federation trust
- Use the Shell to create a federation trust that uses the consumer instance of the Microsoft Federation Gateway

Use the EMC to create a federation trust

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Federation trusts" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In the console tree, click **Organization Configuration**.
2. In the action pane, click **New Federation Trust**.
3. On the **New Federation Trust** page, click **New**. This automatically creates a self-signed certificate for the federation trust with the Microsoft Federation Gateway and deploys the self-signed certificate to the Exchange servers in your organization. The default name of the new federation trust is **Microsoft Federation Gateway**.
4. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Note:

The new federation trust appears on the **Federation Trust** tab.

Note:

To complete the federation configuration, you must add a text (TXT) record in DNS for the domain you want to use as the account namespace and for any other domain you want to add as a federated domain on the Microsoft Federation Gateway. After the TXT records are available in DNS, complete the federation trust configuration by using the Manage Federation wizard in the EMC or the Set-FederatedOrganizationIdentifier cmdlet in the Shell. For details, see Create a TXT Record for Federation or Managing Federation.

Use the Shell to create a federation trust

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Federation trusts" entry in the Exchange and Shell Infrastructure Permissions topic.

1. This example creates a unique subject key identifier to be used with the certificate.

```
$ski = [System.Guid]::NewGuid().ToString("N")
```

2. This example creates a self-signed certificate for the federation trust with the Microsoft Federation Gateway.

```
New-ExchangeCertificate -FriendlyName "Exchange Federated Delegation"
```

3. This example retrieves the self-signed certificate and creates the federation trust "Microsoft Federation Gateway". This automatically deploys the self-signed certificate to the Exchange servers in your organization.

```
Get-ExchangeCertificate | ?{$_.friendlyname -eq "Exchange Federated De
```

For detailed syntax and parameter information, see the following topics:

- New-ExchangeCertificate
- Get-ExchangeCertificate
- New-FederationTrust

Use the Shell to create a federation trust

that uses the consumer instance of the Microsoft Federation Gateway

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Federation trusts" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:
You can't use the EMC to create a federation trust that uses the consumer instance of the Microsoft Federation Gateway.

Prerequisite

To create a federation trust that uses the consumer instance of the Microsoft Federation Gateway, you need a valid X.509 certificate that meets the requirements for federation trusts. The certificate must be issued by a certification authority (CA) trusted by the Microsoft Federation Gateway. This certificate will be deployed automatically to all Client Access and Hub Transport servers accessible by the federation trust task. For more details, see Trusted Root Certification Authorities for Federation Trusts.

1. This example gets a list of certificates and their thumbprints.

```
Get-ExchangeCertificate | where {$_.IsSelfSigned -eq $false} | Format-
```

`where` is an alias for the **Where-Object** cmdlet. It can also be replaced by the alias ? (question mark). To get a list of all aliases available in the Shell, run the **Get-Alias** cmdlet.
If there's only one certificate on the server that's not self-signed, you can simplify this task by combining commands from this step and the next step. You can pipeline results from the **Get-ExchangeCertificate** cmdlet to the **New-FederationTrust** cmdlet, as shown in this example.

```
Get-ExchangeCertificate | where {$_.IsSelfSigned -eq $false} | New-Fed
```

2. This example creates the federation trust Microsoft Federation Gateway.

```
New-FederationTrust -Name "Microsoft Federation Gateway" -Thumbprint 6
```

Important:
After you create a federation trust, the next step in configuring federation delegation is to create a separate TXT record in the DNS zone for both the federated delegation subdomain and each primary e-mail or SMTP proxy domain you want to federate. Because you've created a federation trust that uses the consumer instance of the Microsoft Federation Gateway, you must follow the steps outlined in the Exchange 2010 RTM version of the topic Create a TXT Record for Federation. After the TXT records are available in DNS, complete the federation trust configuration by using the Manage Federation wizard in the EMC or the Set-FederatedOrganizationIdentifier cmdlet in the Shell.

For detailed syntax and parameter information, see Get-ExchangeCertificate or New-FederationTrust.

Other Tasks

After you create a federation trust, you may also want to:

- Create a TXT Record for Federation
- Create an Organization Relationship
- Create a Sharing Policy

1.13.5.2 Create a TXT Record for Federation

Create a TXT Record for Federation

[This topic is in progress.]

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Microsoft Exchange Server 2010 uses Federation for federated delegation. Federation requires a federation trust with the Microsoft Federation Gateway. After you create the trust, you must configure the federated organization identifier with any accepted domains you want to federate.

To provide proof of ownership of the registered Internet domain, you must create a text (TXT) record in the Domain Name System (DNS) zone of each accepted domain you want to federate. The TXT record contains the federated domain proof encryption string generated when you run the Get-FederatedDomainProof cmdlet for each domain.

You can create a TXT record by using DNS Manager on a server running Windows Server 2008 that has the DNS server role installed. Your organization may use DNS server software from another vendor or use a service provider to host the DNS zone for the domain. Many Internet domain registrars host DNS zones for customers and most service providers offer Web-based management tools so that customers can manage DNS records for their domains. To learn more about the DNS server role, see DNS Server Role.

Note:

Creating a TXT record is one of several steps in setting up federated delegation in your Exchange 2010 organization. To review all the steps, see Configure Federated Delegation.

Looking for other management tasks related to Federation? Check out Managing Federation.

Prerequisites

- A federation trust has been created between your Exchange 2010 organization and the Microsoft Federation Gateway. For details, see Create a Federation Trust.
- Your Exchange organization uses one or more Internet domains registered with a domain registrar.
- The domains have a DNS zone accessible from the Internet.
- The DNS server role or the DNS Server service is installed. You can install the DNS server role by using Server Manager in Windows Server 2008. For information about using Server Manager, see Server Manager.

Step 1: Use the Shell to create the federated domain proof encryption strings

Run the **Get-FederatedDomainProof** cmdlet for any domains to be federated.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Federation trusts" entry in the Exchange and Shell Infrastructure Permissions topic.

This example generates the domain proof string used for the TXT record for contoso.com.

```
Get-FederatedDomainProof -DomainName contoso.com
```

For detailed syntax and parameter information, see Get-FederatedDomainProof.

Step 2: Create a TXT record

Use DNS Manager

1. In DNS Manager, expand the DNS server you want, and then expand **Forward Lookup Zones**.
2. Select the forward lookup zone in which you want to create the TXT record.
3. From the menu bar, navigate to **Action** > **Other New Records**.
4. In **Resource Record Type**, select **Text (TXT)**, and then click **Create Record**.
5. In **New Resource Record**, complete the following fields:
   - **Record name (uses parent domain if left blank)** Leave this field blank, allowing it to create a record with the same name as the domain name.
   - **Fully qualified domain name type (FQDN)** This read-only field displays the FQDN created by concatenating the record name to the domain name.
   - **Text** Type the federated domain proof string that was generated when you ran the **Get-FederatedDomainProof** cmdlet. For example, if the federated domain proof string is `7Zyr2i/fE/M/T3AwCpitDbF30Fk/TdzXME6f7d1lDaKGthPdoS+UF94t43D2nU5hLNnIAP+5A3jJR2ik9HDPgg==`, you would enter the entire string in the **Text** field.

     Important:

     The federated domain proof is a string of alphanumeric characters. To avoid input errors, we recommend that you copy the string from the Shell, paste it into a text editor such as Notepad, copy it from the text editor to the Clipboard, and then paste it into the **Text** field of the TXT record. If the TXT record is created by using an incorrect federated domain proof string, the Microsoft Federation Gateway won't be able to verify proof of domain ownership, and you won't be able to add it to the federated organization identifier.
6. Click **OK**, and then click **Done** to create the record.

Use the DNSCmd command

This example creates a TXT record in the forward lookup zone `contoso.com` with the federated domain proof string `7Zyr2i/fE/M/T3AwCpitDbF30Fk/TdzXME6f7d1lDaKGthPdoS+UF94t43D2nU5hLNnIAP+5A3jJR2ik9HDPgg==` on DNS server NS1.

```
DNSCmd NS1 /RecordAdd contoso.com "@" TXT "7Zyr2i/fE/M/T3AwCpitDbF30Fk/TdzXME6f7d
```

For detailed syntax and parameter information, see Dnscmd.

Other Tasks

After you create a TXT record for Federation, you may also want to:

- Add a federated domain. For details, see Manage Federation.
- Create an Organization Relationship

1.13.5.3 Manage Federation

Manage Federation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Use the Manage Federation wizard to manage certificates used for a federation trust, refresh the Microsoft Federation Gateway certificate and metadata, add or change the organization contact for federation, and disable or enable federation for the Exchange organization. In addition to the wizard in the EMC, you can also use the Shell to manage a federation trust.

Looking for other management tasks related to federation? Check out Managing Federation.

Prerequisites

Before you use the Manage Federation wizard or the corresponding cmdlets to modify a federation trust, a federated organization identifier, or federated domains, we recommend you understand how federation works and the impact of modifying federation configuration. For more information, see Understanding Federation.

What Do You Want to Do?

- Use the EMC to manage federation
- Use the Shell to manage federation

Use the EMC to manage federation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Federation trusts" entry in the Exchange and Shell Infrastructure Permissions topic.

Note:

The Manage Federation wizard is a comprehensive way of managing the federation trust and its associated federated organization identifier. The wizard includes multiple tasks.

1. In the console tree, navigate to **Organization Configuration**.
2. In the result pane, click the **Federation Trust** tab, and then select the federation trust you want to manage. By default, the trust is named Microsoft Federation Gateway.
3. In the action pane, click **Manage Federation**.
4. On the **Manage Federation Certificate** page, information is displayed for the certificates used for the federation trust. This includes information for the current certificate, the next certificate, and the previous certificate. The current certificate is the active certificate used for the federation trust. The next certificate is a replacement certificate that will be used if the current certificate expires or needs to be replaced. The previous certificate is the certificate that was used for the federation trust immediately before the

current certificate. You can take the following actions:

- **Properties** Select the current, next, or previous certificate from the **Property Name** column, and then click **Properties** to view the certificate's properties.
- **Edit** Select the **Next Certificate** from the **Property Name** column, and then click **Edit** to select another certificate as the next certificate.
- **Show distribution state** Click this button to display the distribution state of the certificate in your Exchange organization.
- **Contact the Microsoft Federation Gateway to get its certificate and federation metadata** This check box is selected by default. When you use this option, Exchange retrieves the certificate and federation metadata from the Microsoft Federation Gateway. Clear this check box if you don't want to perform this refresh.
- **Roll certificate to mark the next certificate as the current certificate** Select this check box to configure the federation trust to use the next certificate as the current certificate.

Important:

Before you configure the federation trust to use the next certificate, you must make sure the certificate is installed on all Microsoft Exchange Server 2010 servers. To check the certificate status, click **Show distribution state**. The distribution state of the certificate is displayed in the **Distribution State** column. Expand the column width to display all text in the column.

5. On the **Manage Federated Domains** page, you can take the following actions:
   - **Add** Click this button to add a domain as a federated domain. The **Select Accepted Domain** dialog box displays all accepted domains in the Exchange 2010 organization.

     Note:

     To add an accepted domain to this list, use the New-AcceptedDomain cmdlet.

   - Select a domain from the **Domain** column, and then click this button to remove the domain.
   - **E-mail address of organization contact** Use this box to enter the e-mail address of the designated organization contact for federation.
   - **Enable Federation** Select this check box to enable federation. Clear this check box to disable federation for the Exchange organization.

   Note:

   Configuring domains is one of several steps in setting up federated delegation in your Exchange 2010 organization. To review all the steps, see Configure Federated Delegation.

6. On the **Manage Federation** page, review the **Configuration Summary**, and then click **Manage** to execute the changes.

7. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to manage federation

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Federation trusts" entry in the Exchange and Shell Infrastructure Permissions topic.

View federation certificates

This example displays the previous, current, and next certificates used by the federation trust MyFederationTrust.

```
Get-FederationTrust -Identity MyFederationTrust | Select Org*certificate
```

For detailed syntax and parameter information, see Get-FederationTrust.

Check federation certificate status

This example displays the state of federation certificates on all Hub Transport and Client Access servers in the organization.

```
Test-FederationTrustCertificate
```

For detailed syntax and parameter information, see Test-FederationTrustCertificate.

Configure the federation trust to use a certificate as the next certificate

This example configures the federation trust MyFederationTrust to use the certificate with the provided thumbprint as the next certificate. After the certificate is deployed to all Exchange servers in the organization, you can use the *PublishCertificate* switch to configure the trust to use this certificate as the current certificate.

```
Set-FederationTrust -Identity MyFederationTrust -Thumbprint AC00F35CBA8359953F412
```

For detailed syntax and parameter information, see Set-FederationTrust.

Configure the federation trust to use the next certificate as the current certificate

This example configures the federation trust MyFederationTrust to use the next certificate as the current certificate and publishes it to the Microsoft Federation Gateway.

```
Set-FederationTrust "MyFederationTrust" -PublishFederationCertificate
```

Caution:

Before configuring the federation trust to use the next certificate as the current federation certificate, make sure that the certificate is deployed on all Exchange servers in your organization. Use the Test-FederationTrustCertificate cmdlet or the Manage Federation wizard to check the deployment status of the certificate.

For detailed syntax and parameter information, see Set-FederationTrust.

Refresh federation metadata and certificate from the Microsoft Federation Gateway

This example refreshes the federation metadata and certificate of the Microsoft Federation Gateway for the federation trust MyFederationTrust.

```
Set-FederationTrust MyFederationTrust -RefreshMetadata
```

For detailed syntax and parameter information, see Set-FederationTrust.

View federated organization identifier and federated domains

This example displays the Exchange organization's federated organization identifier and related information, including federated domains and status.

```
Get-FederatedOrganizationIdentifier
```

For detailed syntax and parameter information, see Get-FederatedOrganizationIdentifier.

Add a domain as a federated domain

This example adds the domain contoso.co.uk as a federated domain. The domain must exist as an accepted domain in the Exchange organization.

```
Add-FederatedDomain contoso.co.uk
```

For detailed syntax and parameter information, see Add-FederatedDomain.

Remove a federated domain

This example removes the domain contoso.co.uk as a federated domain.

```
Remove-FederatedDomain contoso.co.uk
```

For detailed syntax and parameter information, see Remove-FederatedDomain.

Enable federation for the Exchange organization

This example enables federation for the Exchange organization.

```
Set-FederatedOrganizationIdentifier -Enabled $true
```

For detailed syntax and parameter information, see Set-FederatedOrganizationIdentifier.

Disable federation for the Exchange organization

This example disables federation for the Exchange organization.

```
Set-FederatedOrganizationIdentifier -Enabled $false
```

For detailed syntax and parameter information, see Set-FederatedOrganizationIdentifier.

1.13.5.4 Remove a Federation Trust

Remove a Federation Trust

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

Removing a federation trust disables Federation for the Exchange organization. All federated domains, including the domain used for the account namespace, should be removed. To retrieve the list of federated domains and the account namespace, use the Get-AcceptedDomain cmdlet. The federated domains are also listed in the Remove Federation Trust wizard in the Exchange Management Console (EMC).

Looking for other tasks related to Federation? Check out Managing Federation.

Use the EMC to remove a federation trust

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Federation trusts" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In the console tree, click **Organization Configuration**.
2. In the result pane, select the federation trust you want to remove.
3. In the action pane, click **Remove Federation Trust**.

4. On the **Remove Federation Trust** page, review the federated domains configured to use the trust.
5. Click **Remove** to remove the trust.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to remove a federation trust

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Federation trusts" entry in the Exchange and Shell Infrastructure Permissions topic.

This example removes the federated domain contoso.co.uk with the account namespace domain contoso.com.

```
Remove-FederatedDomain -DomainName contoso.co.uk
Remove-FederatedDomain -DomainName contoso.com
```

This example removes the federation trust Microsoft Federation Gateway.

```
Remove-FederationTrust "Microsoft Federation Gateway"
```

For detailed syntax and parameter information, see Remove-FederatedDomain or Remove-FederationTrust.

1.13.6 Managing Federated Delegation

Managing Federated Delegation

Exchange Server 2010 > Federation >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-29*

Managing Organization Relationships

Configure Federated Delegation

Create an Organization Relationship

Configure Organization Relationship Properties

Remove an Organization Relationship

Managing Sharing Policies

Create a Sharing Policy

Configure Sharing Policy Properties

Enable a Sharing Policy

Disable a Sharing Policy

Apply a Sharing Policy to Mailboxes

Remove a Sharing Policy

Configure Free/Busy Sharing Between Exchange Organizations

1.13.6.1 Configure Federated Delegation

Configure Federated Delegation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can set up federated delegation (formerly known as federated sharing) in a Microsoft Exchange Server 2010 on-premises environment.

Using federated delegation, users in your on-premises Exchange organization can share information with recipients in other Exchange organizations that are also configured for federated delegation. This connection is established by creating organization relationships between the two organizations or by using a sharing policy, which allows users to create sharing relationships on an individual basis.

Federated delegation uses the Microsoft Federation Gateway, a cloud-based service offered by Microsoft, as the trust broker between your on-premises Exchange 2010 organization and other federated Exchange 2010 organizations.

Looking for other management tasks related to federated delegation? Check out Managing Federated Delegation.

Domain Namespace Requirements

To set up federated delegation for your on-premises Exchange 2010 organization, you must configure a domain proof of ownership record for any domains used for user e-mail accounts or for hosting user accounts in Microsoft Outlook Live or Microsoft Online Services.

Step 1: Create a federation trust with the Microsoft Federation Gateway

You can use the EMC or the Shell to create a federation trust. For detailed instructions, see Create a Federation Trust.

Step 2: Create TXT records for federated delegation

To provide proof of ownership of a registered Internet domain, you must create a text (TXT) record in the public Domain Name System (DNS) zone for each primary e-mail or SMTP proxy domain you want to federate. For example, if your primary SMTP domain is contoso.com, you would create a TXT record for contoso.com.

You can use DNS Manager or the **DNSCmd** command to create a TXT record for federation. For detailed instructions, see Create a TXT Record for Federation.

Step 3: Configure the domains for federated delegation

You also need to add the primary SMTP domain as a federated domain for your Exchange organization.

Note:
To participate in federated delegation, users who aren't using contoso.com as their e-mail address domain need to have contoso.com added as a proxy address domain to their account or have their e-mail address domain added as an additional federated domain.

This command uses the Shell to add the domain used in the contoso.com example.

```
Add-FederatedDomain -DomainName contoso.com
```

You can use the EMC or the Shell to configure domains for federated delegation. For detailed instructions, see Manage Federation.

Step 4: Create an Autodiscover DNS record

You need to add an alias canonical name (CNAME) resource record to your public-facing DNS. The new CNAME record should point to an Internet-facing Client Access server that's running the Autodiscover service.

In the previous Contoso example, the new CNAME record would specify autodiscover.contoso.com as the host name. For organizations using Microsoft DNS, you can add a CNAME record by using either DNS Manager or the **DNSCmd** command. For detailed instructions, see Add an Alias (CNAME) Resource Record to a Zone.

Step 5: Create an organization relationship

You can use the EMC or the Shell to create an organization relationship. For detailed instructions, see Create an Organization Relationship.

1.13.6.2 Create an Organization Relationship

Create an Organization Relationship

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-10*

You can create an organization relationship with an external federated Microsoft Exchange Server 2010 organization for the purpose of sharing calendar availability (free/busy) information.

Note:

Creating an organization relationship is one of several steps in setting up federated delegation in your Microsoft Exchange Server 2010 organization. To review all the steps, see Configure Federated Delegation.

Looking for other management tasks related to federated delegation? Check out Managing Federated Delegation.

Prerequisites

Before you can create an organization relationship, you must first set up a federation trust with the Exchange Federation Gateway. For more information, see Create a Federation Trust.

What Do You Want to Do?

- Use the EMC to create an organization relationship
- Use the Shell to create an organization relationship

Use the EMC to create an organization relationship

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Organization relationships" entry in the Mailbox Permissions topic.

1. In the console tree, click **Organization Configuration**.
2. In the action pane, click **New Organization Relationship**.
3. On the **Introduction** page, complete the following fields:
   - **Name** Type a name for the organization relationship.
   - **Enable this organization relationship** Select this check box to enable this organization relationship.
   - **Enable free/busy information access** Select this check box to specify whether this organization relationship should be used for retrieving free/busy information from the external Exchange organization.
   - **Specify free/busy data access level** If you selected the **Enable free/busy information access** check box, you can select one of the following options from this list to specify what type of free/busy information should be retrieved from the external Exchange organization:
     No free/busy access
     Free/busy access with time only
     Free/busy access with time, plus subject and location
   - **Specify a security distribution group that indicates what internal users free/busy data is accessible** Select this check box if you want to specify a distribution group to list your users who can have their free/busy information accessed by the external Exchange organization. Use the corresponding box to type the SMTP address of a security distribution group within your organization, or click **Browse** to search for the group.
4. On the **External Organization** page, complete the following fields:

- **Automatically discover configuration information** Click this button to have Exchange locate the configuration information of the external Exchange organization by using Autodiscover.
  Specify a federated domain of the external Exchange organization If you clicked **Automatically discover configuration information**, use this box to specify a federated domain of the external Exchange organization (for example, contoso.com). You can't specify more than one domain. Information about domains federated by the remote organization is published by using the Exchange Autodiscover Web service endpoints.
- **Manually enter the configuration information** Click this button if you want to manually provide the configuration information for the external Exchange organization.
  Federated domains of the external Exchange organization Use this box to type the federated domain names of the external Exchange organization. The organization you're establishing an organization relationship with may have more than one federated domain. After you type each name, click **Add** to add the name to the list of domains.
  Edit Select a federated domain name from the list, and then click **Edit** to modify the domain name.
   Select a federated domain name from the list, and then click this button to remove the domain.
  Application URI of the external Exchange organization Use this box to type the Uniform Resource Identifier (URI) of the external Exchange organization's application server (for example, mail.contoso.com). A URI is a string of characters used to identify or name a resource. In this case, the application URI is used when requesting a delegated token for the external Exchange organization to retrieve free/busy information.
  Autodiscover endpoint of the external Exchange organization Use this box to type the Autodiscover URL of the external Exchange organization's Exchange Web Services (for example, https://contoso.com/autodiscover/autodiscover.svc/wssecurity). Exchange uses the Autodiscover service to automatically detect the correct Client Access server endpoint.

5. On the **New Organization Relationship** page, review your configuration settings. Click **New** to create the organization relationship. Click **Back** to make changes.

6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create an organization relationship

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Organization relationships" entry in the Mailbox Permissions topic.

This example creates an organization relationship with Contoso, Ltd with the following

conditions:

- The organization relationship is enabled for contoso.com, northamerica.contoso.com, and europe.contoso.com.
- Free/busy access is enabled.
- The requesting organization receives free/busy time, subject, and location information from the target organization.

```
New-OrganizationRelationship -Name "Contoso" -DomainNames "contoso.com","northame
```

For detailed syntax and parameter information, see New-OrganizationRelationship.

This example attempts to automatically discover configuration information from the external Exchange organization Contoso.com by using the domain names provided in the **Get-FederationInformation** cmdlet. If you use this method to create your organization relationship, you must first make sure that you've created an organization identifier by using the Set-FederatedOrganizationIdentifier cmdlet.

```
Get-FederationInformation -DomainName Contoso.com | New-OrganizationRelationship
```

For detailed syntax and parameter information, see Get-FederationInformation and New-OrganizationRelationship.

This example creates an organization relationship with Fourth Coffee. In this example, the connection settings with the external Exchange organization are provided. The following conditions apply:

- The organization relationship is established by using “fourthcoffee.com” as the domain that has been set up as a federated domain by Fourth Coffee.
- If fourthcoffee.com is on Microsoft Exchange Server 2010 Service Pack 1 (SP1), the **ApplicationUri** property is exchangedelegation.fourthcoffee.com. If fourthcoffee.com is on Microsoft Exchange Server 2010 Service Pack 2 (SP2), the **ApplicationUri** property is FYDIBOHF25SPDLT.fourthcoffee.com.
- The Autodiscover URL is https://mail.fourthcoffee.com/autodiscover/autodiscover.svc/wssecurity.
- Free/busy access is enabled.
- The requesting organization only receives free/busy information with the time.

In Exchange 2010 SP1, run the following command:

```
New-OrganizationRelationship -Name "Fourth Coffee" -DomainNames "fourthcoffee.com
```

In Exchange 2010 SP2, run the following command:

```
New-OrganizationRelationship -Name "Fourth Coffee" -DomainNames "fourthcoffee.com
```

For detailed syntax and parameter information, see New-OrganizationRelationship.

1.13.6.3 Configure Organization Relationship Properties

Configure Organization Relationship Properties

Exchange Server 2010 > Federation > Managing Federated Delegation >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-07-21*

You can use organization relationships to securely share calendar availability (free/busy) information with recipients outside your Microsoft Exchange Server 2010 organization.

Looking for other management tasks related to federated delegation? Check out Managing Federated Delegation.

Prerequisites

Before organization relationships can work, you must first configure a federation trust with the Microsoft Federation Gateway. For more information, see Understanding Federation.

What Do You Want to Do?

- Use the EMC to configure organization relationship properties
- Use the Shell to configure organization relationship properties

Use the EMC to configure organization relationship properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Organization relationships" entry in the Mailbox Permissions topic.

1. In the console tree, click **Organization Configuration**.
2. In the result pane, click the **Organization Relationships** tab, and then select the organization relationship you want to configure.
3. In the action pane, under the organization relationship name, click **Properties**.
4. Use the **General** tab to view or modify general organization relationship settings:
   - **Name** This unlabeled box displays the name of the organization relationship. You can modify this name.
   - **Modified** This read-only field indicates the date and time when the organization policy was created or modified.
   - **Enable this organization relationship** Clear this check box to disable the organization relationship.
   - **Enable free/busy information access** Clear this check box to specify that this organization relationship shouldn't be used for retrieving free/busy information from the external Exchange organization.
   - **Specify free/busy data access level** If you selected the **Enable free/busy information access** check box, you can select one of the following options from this list to specify what type of free/busy information should be retrieved from the external Exchange organization:
     No free/busy access
     Free/busy access with time only
     Free/busy access with time, plus subject and location
   - **Specify a security distribution group that indicates what internal users free/busy data is accessible** Select this check box if you want to specify a distribution group to list your users who can have their free/busy information accessed by the external Exchange organization. Use the corresponding box to type the SMTP address of a security distribution group within your organization, or click **Browse** to search for the group.
5. Use the **External Organization** tab to view or modify the information required to set up the organization relationship with an external federated Exchange organization using the following fields:
   - **Automatically discover configuration information** Click this button to have Exchange locate the configuration information of the external

Exchange organization by using Autodiscover.

Specify a federated domain of the external Exchange organization If you clicked **Automatically discover configuration information**, use this box to specify a federated domain of the external Exchange organization (for example, contoso.com). You can't specify more than one domain. Information about domains federated by the remote organization is published by using the Exchange 2010 Autodiscover Web service endpoints.

- **Manually enter the configuration information** Click this button if you want to manually provide the configuration information for the external Exchange organization.

  Federated domains of the external Exchange organization Use this box to type the federated domain names of the external Exchange organization. The organization you're establishing an organization relationship with may have more than one federated domain. After you type each domain name, click **Add** to add the name to the list of domains. The organization relationship applies to only the federated domains listed on this tab.

  Edit Select a domain name from the list, and then click this button to modify it.

   Select a domain name from the list, and then click this button to remove it from the organization relationship.

  Application URI of the external Exchange organization Use this box to type the Uniform Resource Identifier (URI) of the external Exchange organization's application server (for example, mail.contoso.com). A URI is a string of characters used to identify or name a resource. In this case, the application URI is used when requesting a delegated token for the external Exchange organization to retrieve free/busy information.

  Autodiscover endpoint of the external Exchange organization Use this box to type the Autodiscover URL of the external Exchange organization's Exchange Web Services (for example, https://contoso.com/autodiscover/autodiscover.svc/wssecurity). Exchange uses the Autodiscover service to automatically detect the correct Client Access server endpoint.

Use the Shell to configure organization relationship properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Organization relationships" entry in the Mailbox Permissions topic.

This example adds the domain name woodgrovebank.co.uk to the organization relationship WoodgroveBank.

```
$domains = (Get-OrganizationRelationship WoodgroveBank).DomainNames
$domains += 'woodgrovebank.co.uk'
Set-OrganizationRelationship -Identity WoodgroveBank -DomainNames $domains
```

This example disables the organization relationship WoodgroveBank.

```
Set-OrganizationRelationship -Identity WoodgroveBank -Enabled $false
```

This example enables calendar availability (free/busy) information access for the organization relationship WoodgroveBank and sets the access level to **Free/busy access with time only**.

```
Set-OrganizationRelationship -Identity WoodgroveBank -FreeBusyAccessEnabled $true
```

For detailed syntax and parameter information, see Set-OrganizationRelationship and Get-OrganizationRelationship.

1.13.6.4 Remove an Organization Relationship

Remove an Organization Relationship

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Removing an organization relationship disables all features enabled for the relationship, including federated delegation.

Note:

To stop sharing information with a remote federated Exchange organization without removing the organization relationship, you can disable the organization relationship by using the EMC or the Set-OrganizationRelationship cmdlet in the Shell.

Looking for other management tasks related to federated delegation? Check out Managing Federated Delegation.

Use the EMC to remove an organization relationship

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Organization relationships" entry in the Mailbox Permissions topic.

1. In the console tree, click **Organization Configuration**.
2. In the result pane, select the **Organization Relationships** tab, and then select the organization relationship you want to remove.
3. In the action pane, click **Remove**.

Use the Shell to remove an organization relationship

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Organization relationships" entry in the Mailbox Permissions topic.

This example removes the organization relationship Contoso.

```
Remove-OrganizationRelationship -Identity "Contoso"
```

For detailed syntax and parameter information, see Remove-OrganizationRelationship.

1.13.6.5 Create a Sharing Policy

Create a Sharing Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use sharing policies to control how users in your organization can share calendar and contact information with users outside your Exchange organization. Sharing policies support the sharing of calendar and contact information with external federated organizations, external non-federated organizations, and individuals with Internet access. To configure recipients to use a specific sharing policy, see Apply a Sharing Policy to Mailboxes.

Note:

For sharing policies between federated organizations, only Microsoft Outlook 2010 and Microsoft Office Outlook Web App users can create sharing invitations.

Looking for other management tasks related to sharing policies? Check out Managing Federated Delegation.

Prerequisites for Sharing Policies Between Federated Organizations

- An Exchange 2010 Client Access server exists in each Exchange organization.
- A federation trust with the Microsoft Federation Gateway is established for each Exchange organization. For details, see Create a Federation Trust.
- The federated organization identifier is configured for each Exchange organization. Also, any primary and secondary SMTP domains used for generating users' e-mail addresses have been added to the Microsoft Federation Gateway as accepted domains for both Exchange organizations. For details, see Configure Federated Delegation.
- User mailboxes are on Exchange 2010 Mailbox servers in each Exchange organization.

Prerequisites for Sharing Policies Between Non-Federated Organizations or Individuals

- An Exchange 2010 Client Access server exists in the Exchange organization that's sharing user's calendar information.
- User mailboxes are on Exchange 2010 Mailbox servers in the Exchange organization that's sharing user's calendar information.
- The Client Access server is enabled for Outlook Web App access and a publishing virtual directory is enabled. For details, see Set-OwaVirtualDirectory.
- The Mailbox server's Web proxy URL is configured. For details, see Set-ExchangeServer.

What Do You Want to Do?

- Use the EMC to create a sharing policy

- Use the Shell to create a sharing policy

Use the EMC to create a sharing policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

1. In the console tree, expand the forest you want, and then navigate to **Organization Configuration** > **Mailbox**.
2. In the action pane, click **New Sharing Policy**.
3. On the **Introduction** page, complete the following fields:
   - **Name** Use this box to type a name for the new sharing policy.
   - **Add** Click this button to open the **Add Action to Sharing Policy Domain** dialog box. Use this dialog box to specify the domains and actions that this sharing policy applies to. Complete the following fields:
     Specify a domain of an external Exchange organization, or "*" for any domain Use this box to type the fully qualified domain name (FQDN) of an external Exchange organization, for example, **Contoso.com**.
     Specify the actions that apply to the federated domain Use this list to select one of the following sharing levels you want to enforce:
     Calendar sharing with free/busy information only
     Calendar sharing with free/busy information, plus subject and location
     Calendar sharing with free/busy information, plus subject, location, and body
     Contacts sharing
     Calendar sharing with free/busy information only, Contacts sharing
     Calendar sharing with free/busy information, plus subject and location, Contacts sharing
     Calendar sharing with free/busy information plus subject, location, and body, Contacts sharing
   - **Edit** Select a domain, and then click this button to edit the domain name or action.
   -  Select a domain, and then click this button to remove the domain from the sharing policy.
   - **Enable sharing policy** Select this check box to enable the sharing of calendar and contact information with recipients in the external domains that you specified in the policy. If you clear this check box, mailboxes assigned this policy won't be able to share calendar and contact information with the external domains or users specified in the policy. Additionally, existing shared calendar and contacts folders will no longer be shared with the external domains or users specified in the policy.
4. On the **Mailboxes** page, click **Add** to select the mailboxes to which you want to apply this sharing policy.

   Note:
   After creating the sharing policy, you can apply it to more mailboxes by using the **Mailboxes** tab in the sharing policy's property page or by using the **Mailbox Settings** tab in the mailbox's property page.
5. On the **New Sharing Policy** page, review your configuration settings. Click **New** to create the sharing policy. Click **Back** to make configuration changes.
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:

- A status of **Completed** indicates that the wizard completed the task successfully.
- A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to create a sharing policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

This example creates the sharing policy Contoso for the external federated domain contoso.com. This policy allows users in the contoso.com domain to see your user's detailed calendar availability (free/busy) information and contacts. By default, this policy is enabled.

```
New-SharingPolicy -Name "Contoso" -Domains contoso.com: CalendarSharingFreeBusyDe
```

This example creates the sharing policy SharingPolicy01 for two different federated domains (contoso.com and woodgrovebank.com) with different sharing actions configured for each domain. The policy is disabled.

```
New-SharingPolicy -Name "SharingPolicy01" -Domains 'contoso.com: CalendarSharingF
```

This example creates the sharing policy Anonymous for an Exchange organization with the Client Access server CAS01 and the Mailbox server MAIL01 with the sharing action configured for limited calendar free/busy availability information. This policy allows users in your Exchange organization to invite users with Internet access to view their calendar availability information by sending them a link. The policy is enabled.

1. Set the Web proxy URL for MAIL01.

   ```
   Set-ExchangeServer -Identity "Mail01" -InternetWebProxy "<Webproxy URL
   ```

2. Enable the publishing virtual directory on CAS01.

   ```
   Set-OwaVirtualDirectory -Identity "CAS01" -ExternalURL "<URL for CAS01
   ```

3. Create the sharing policy Anonymous and configure limited calendar information sharing.

   ```
   New-SharingPolicy -Name "Anonymous" -Domains 'Anonymous: CalendarShari
   ```

For detailed syntax and parameter information, see the following topics:

- New-SharingPolicy
- Set-ExchangeServer
- Set-OwaVirtualDirectory

1.13.6.6 Configure Sharing Policy Properties

Configure Sharing Policy Properties

Exchange Server 2010 > Federation > Managing Federated Delegation >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-03-19*

You can use sharing policies to control how users in your organization can share calendar and contact information with users outside your Exchange organization. Sharing policies

support the sharing of calendar and contact information with external federated organizations, external non-federated organizations, and individuals with Internet access.

Note:
For sharing policies between federated organizations, only Microsoft Outlook 2010 and Microsoft Office Outlook Web App users can create sharing invitations.

Looking for other management tasks related to sharing policies? Check out Managing Federated Delegation.

Prerequisites for Sharing Policies Between Federated Organizations

- An Exchange 2010 Client Access server exists in each Exchange organization.
- A federation trust with the Microsoft Federation Gateway is established for each Exchange organization. For details, see Create a Federation Trust.
- The federated organization identifier is configured for each Exchange organization. Also, any primary and secondary SMTP domains used for generating users' e-mail addresses have been added to the Microsoft Federation Gateway as accepted domains for both Exchange organizations. For details, see Configure Federated Delegation.
- User mailboxes are on Exchange 2010 Mailbox servers in each Exchange organization.

Prerequisites for Sharing Policies Between Non-Federated Organizations or Individuals

- An Exchange 2010 Client Access server exists in the Exchange organization that's sharing user's calendar information.
- User mailboxes are on Exchange 2010 Mailbox servers in the Exchange organization that's sharing user's calendar information.
- The Client Access server is enabled for Outlook Web App access, and a publishing virtual directory is enabled. For details, see Set-OwaVirtualDirectory.
- The Mailbox server's Web proxy URL is configured. For details, see Set-ExchangeServer.

What Do You Want to Do?

- Use the EMC to configure sharing policy properties
- Use the Shell to configure sharing policy properties

Use the EMC to configure sharing policy properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Sharing Policies** tab, and then click the sharing policy you want to view or configure.
3. In the action pane, under the sharing policy name, click **Properties**.

4. Use the **General** tab to view or modify the following sharing policy information.
   - **Name** This unlabeled box lists the name of the sharing policy. You can modify this field.
   - **Add** Click this button to open the **Add Action to Sharing Policy Domain** dialog box. Use this dialog box to specify the domains and actions that this sharing policy applies to. Complete the following fields:
     Specify a domain of an external Exchange organization, or "*" for any domain Use this box to type the fully qualified domain name (FQDN) of an external Exchange organization, for example Contoso.com.
     Specify the actions that apply to the federated domain Use this list to select one of the following sharing levels you want to enforce:
     Calendar sharing with free/busy information only
     Calendar sharing with free/busy information, plus subject and location
     Calendar sharing with free/busy information plus subject, location, and body
     Contacts sharing
     Calendar sharing with free/busy information only, Contacts sharing
     Calendar sharing with free/busy information, plus subject and location, Contacts sharing
     Calendar sharing with free/busy information plus subject, location, and body, Contacts sharing
   - **Edit** Select a domain, and then click this button to edit the domain name or action.
   -  Select a domain, and then click this button to remove the domain from the sharing policy.
   - **Enable sharing policy** Select this check box to enable the sharing of calendar and contact information with recipients in the external domains that you specified in the policy. If you clear this check box, mailboxes assigned this policy won't be able to share calendar and contact information with the external domains or users specified in the policy. Additionally, existing shared calendar and contacts folders will no longer be shared with the external domains or users specified in the policy.

5. Use the **Mailboxes** tab to add or remove the mailboxes in your organization that this sharing policy applies to.
   - **Add** Click this button to select the mailboxes to which you want to apply this sharing policy.

     Note:
     You can also apply the sharing policy to mailboxes by using the **Mailbox Settings** tab in the mailbox's property page.

   -  Select mailboxes from the list, and then click this button to remove the sharing policy from the specified mailboxes.

Use the Shell to configure sharing policy properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

This example modifies the sharing policy Contoso for the external federated domain contoso.com. This policy allows users in the Contoso domain to see your users' basic calendar availability (free/busy) information and contacts.

```
Set-SharingPolicy -Identity Contoso -Domains 'contoso.com: CalendarSharingFreeBus
```

This example adds a second federated domain to the sharing policy SharingPolicy01. When you add a domain to an existing policy, you must include any previously included domains.

```
Set-SharingPolicy -Identity SharingPolicy01 -Domains 'contoso.com: CalendarSharin
```

This example modifies the sharing policy for the non-federated Anonymous domain. This policy allows users in the Anonymous domain to see your users' detailed calendar availability (free/busy) information. The policy is enabled.

```
Set-SharingPolicy -Name "Anonymous" -Domains 'Anonymous: CalendarSharingFreeBusyD
```

For detailed syntax and parameter information, see Set-SharingPolicy.

1.13.6.7 Enable a Sharing Policy

Enable a Sharing Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

You can enable a disabled sharing policy. You can also create a sharing policy in a disabled state, and then enable it when you want the policy to be applied to the recipients provisioned to use the policy. When you enable the sharing policy, users provisioned to use the policy won't be able to share information until the Sharing Policy Assistant runs. To specify how often the Sharing Policy Assistant runs, use the Set-MailboxServer cmdlet with the *SharingPolicySchedule* parameter.

Looking for other management tasks related to sharing policies? Check out Managing Federated Delegation.

Use the EMC to enable a sharing policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Sharing Policies** tab, and then select the disabled sharing policy that you want to enable.
3. In the action pane, click **Properties**.
4. On the **General** tab, select the **Enable sharing policy** check box.
5. Click **Apply** to apply the sharing policy.

Use the Shell to enable a sharing policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

This example enables the sharing policy Fabrikam.

```
Set-SharingPolicy -Identity "Fabrikam" -Enabled $true
```

For detailed syntax and parameter information, see Set-SharingPolicy.

1.13.6.8 Disable a Sharing Policy

Disable a Sharing Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you disable a sharing policy, users who are provisioned to use the sharing policy won't be able to view or share calendar and contact information with the domains specified in the policy. However, you can't remove a sharing policy until all the users who are provisioned to use the policy have the sharing policy setting removed from their mailboxes.

Note:

When the sharing policy is disabled, users provisioned to use the policy will continue to share information until the Sharing Policy Assistant runs. To specify how often the Sharing Policy Assistant runs, use the Set-MailboxServer cmdlet with the *SharingPolicySchedule* parameter.

Looking for other management tasks related to sharing policies? Check out Managing Federated Delegation.

Use the EMC to disable a sharing policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Sharing Policies** tab, and then select the sharing policy you want to disable.
3. In the action pane, click **Properties**.
4. On the **General tab**, clear the **Enable sharing policy** check box.
5. Click **Apply** to disable the sharing policy.

Use the Shell to disable a sharing policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

This example disables the sharing policy Fabrikam.

```
Set-SharingPolicy -Identity "Fabrikam" -Enabled $False
```


1.13.6.9 Apply a Sharing Policy to Mailboxes

Apply a Sharing Policy to Mailboxes

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

After creating a sharing policy, you must apply the sharing policy to mailboxes so users

can create sharing relationships with users in other external federated Exchange organizations or with individuals in non-Exchange organizations.

Looking for other management tasks related to sharing policies? Check out Managing Federated Delegation.

Prerequisites

A sharing policy exists. For details, see Create a Sharing Policy.

Use the EMC to apply a sharing policy to a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Applying sharing policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the recipient that you want.
3. In the action pane, click **Properties**.
4. On the **Mailbox Settings** tab, select **Sharing**, and then click **Properties**.
5. In **Sharing**, click **Browse.**
6. In **Select Sharing Policy**, select the sharing policy you want to use, and then click **OK**.
7. In **Sharing**, click **OK**.
8. In **<Mailbox> Properties**, click **Apply**.

Use the Shell to apply a sharing policy to a mailbox

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Applying sharing policies" entry in the Mailbox Permissions topic.

This example applies the Fabrikam sharing policy to Tony's mailbox.

```
Set-Mailbox -Identity Tony -SharingPolicy "Fabrikam"
```

This example specifies that all user mailboxes in the Marketing department use the Contoso Marketing sharing policy.

```
Get-Mailbox -Filter {Department -eq "Marketing"} | Set-Mailbox -SharingPolicy "Co
```

For detailed syntax and parameter information, see Set-Mailbox and Get-Mailbox.

Use the Shell to retrieve mailboxes provisioned with a sharing policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Applying sharing policies" entry in the Mailbox Permissions topic.

This example returns all the mailboxes that have the Fabrikam sharing policy applied, and it sorts the users into a table that displays only their aliases and e-mail addresses.

```
Get-Mailbox -ResultSize unlimited | Where {$_.SharingPolicy -eq "Fabrikam" } | fo
```

For detailed syntax and parameter information, see Get-Mailbox.

1.13.6.10 Remove a Sharing Policy

Remove a Sharing Policy

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

When you remove a sharing policy, the policy object is permanently removed from Active Directory. If you want to prevent a sharing policy from being used but retain the policy definition, you can disable the policy instead of removing it. When you disable a sharing policy, users associated with the sharing policy won't be able to share calendar or contact information with recipients from the domains specified in the sharing policy.

Before you remove a sharing policy, you must remove the policy from all users who have the policy applied.

Note:

The default sharing policy applies to all mailbox users who don't have an explicit sharing policy applied. The default sharing policy is enabled by default and allows users to share limited calendar availability (free/busy) information with recipients in all external federated domains. For more information about how to remove a sharing policy from a user mailbox, see Set-Mailbox.

Looking for other management tasks related to sharing policies? Check out Managing Federated Delegation.

Prerequisites

Make sure no users are provisioned to use the sharing policy. You can use the **Get-Mailbox** cmdlet to retrieve mailboxes provisioned with a sharing policy. For details, see Apply a Sharing Policy to Mailboxes

Use the EMC to remove a sharing policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Sharing Policies** tab, and then select the sharing policy you want to remove.
3. In the action pane, click **Remove**. A dialog box appears asking if you want to remove the sharing policy. Click **Yes**.

Use the Shell to remove a sharing policy

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Sharing policies" entry in the Mailbox Permissions topic.

This example removes the sharing policy Fabrikam.

```
Remove-SharingPolicy -Identity Fabrikam
```

This example removes the sharing policy Contoso and suppresses the confirmation that you want to remove the policy.

```
Remove-SharingPolicy -Identity Contoso -Confirm
```

For detailed syntax and parameter information, see Remove-SharingPolicy.

1.13.6.11 Configure Free/Busy Sharing Between Exchange Organizations

Configure Free/Busy Sharing Between Exchange Organizations

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP1*

Topic Last Modified: *2011-10-12*

Using federated delegation, users in your on-premises Exchange organization can share free/busy calendar information with recipients in other Exchange organizations that are also configured for federated delegation. Free/busy sharing can be enabled between two organizations running Exchange Server 2010 and also between organizations with a mixed Exchange deployment. For more information, see Understanding Federated Delegation.

This topic provides a summary of the requirements and configuration steps necessary to enable free/busy sharing between different types of the following common Exchange deployments:

- Two Exchange 2010 Service Pack 1 (SP1) organizations.
- An Exchange 2007 organization (or mixed Exchange 2007 and Exchange 2010 organization) and an Exchange 2010 organization.
- An Exchange Server 2003 organization (or mixed Exchange 2003 and Exchange 2007 organization) and an Exchange 2010 organization.

In addition, this topic discusses the limitations of sharing free/busy information between federated Exchange organizations.

Free/Busy Sharing Between Exchange 2010 Organizations

To configure free/busy sharing between two federated Exchange 2010 organizations, complete the steps in Configure Federated Delegation for both organizations.

Free/Busy Sharing Between Exchange 2007 and Exchange 2010 Organizations

To configure free/busy sharing between Exchange 2007 and Exchange 2010 organizations, follow the steps listed below for each Exchange organization.

1. **Add Exchange 2010 SP1 server** An Exchange 2010 SP1 server with the Client Access server (CAS) role must be installed in the Exchange 2007 organization. If you have other existing Exchange 2010 servers, they should also be updated to Exchange 2010 SP1. Learn more about installing Exchange 2010 in an Exchange 2007 organization at Exchange 2007 -

Planning Roadmap for Upgrade and Coexistence.

2. **Federated delegation** Configure federated delegation between the Exchange 2007 and Exchange 2010 organizations by completing the steps in Configure Federated Delegation for both organizations.
3. **Active Directory synchronization** Active Directory synchronization must be configured for all users that need to share free/busy information between the organizations. You can either configure the Active Directory synchronization manually or use an automated Active Directory synchronization service. Learn about Active Directory synchronization at Forefront Identity Management.
4. **Availability address space** Create a new availability address space for the remote Exchange 2010 organization that directs availability requests from Exchange 2007 mailbox users to the Exchange 2010 Client Access server in the Exchange 2007 organization. This setting enables user availability requests from Exchange 2007 users for users in the remote Exchange 2010 organization to be proxied through the Exchange 2010 CAS server in the Exchange 2007 organization. The Exchange 2010 Client Access server uses the federation trust and organization relationship to send the availability requests to the remote Exchange 2010 organization forest availability endpoint.
   Run the following command in the Exchange Management Shell on the Exchange 2010 Client Access server in the Exchange 2007 organization to configure the availability address space:

```
Add-AvailabilityAddressSpace -AccessMethod InternalProxy -ProxyUrl htt
```

Free/Busy Sharing Between Exchange 2003 and Exchange 2010 Organizations

To configure free/busy sharing between Exchange 2003 and Exchange 2010 organizations, follow the steps listed below for each Exchange organization.

1. **Add Exchange 2010 SP1 server** An Exchange 2010 SP1 server with the Client Access and Mailbox server roles must be installed in the Exchange 2003 organization. If you have other existing Exchange 2010 servers, they should also be updated to Exchange 2010 SP1. Learn more about installing Exchange 2010 in an Exchange 2003 organization at Exchange 2003 - Planning Roadmap for Upgrade and Coexistence.
2. **Configure federated delegation** Configure federated delegation between the Exchange 2003 and Exchange 2010 organizations by completing the steps in Configure Federated Delegation for both organizations.
3. **Configure Active Directory synchronization** Active Directory synchronization must be configured for all users that need to share free/busy information between the organizations. You can either configure the Active Directory synchronization manually or use an automated Active Directory synchronization service. Learn about Active Directory synchronization at Forefront Identity Management.

   Important:

   The **OU=EXTERNAL (FYDIBOHF25SPDLT)** public folder is only created on the Exchange 2010 CAS/Mailbox server if the option to create the public folders is selected during the Exchange 2010 setup. Additionally, this option is only presented during the setup process if the Exchange 2010 CAS/Mailbox server is the first Mailbox server installed in the organization. If the **OU=EXTERNAL (FYDIBOHF25SPDLT)** database wasn't created during setup, you will need to manually create this folder. Learn more at: How to troubleshoot Free/Busy issues when you use Exchange Federation in the Microsoft Office 365 for enterprises environment
4. Follow the steps below to configure public folders for free/busy sharing in your Exchange 2003 organization.
   4.a.In Exchange System Manager, navigate to **Administrative Groups** > **First**

Administrative Group > **Servers**.

4.b.Select your Exchange 2003 server and navigate to **First Storage Group** > **Public Folder Store** > **Public Folders** > **Schedule+ FREE BUSY**.

4.c.In the action pane, select the **OU=EXTERNAL (FYDIBOHF25SPDLT)** folder for the **First Administrative Group**.

4.d.Right-click the **OU=EXTERNAL (FYDIBOHF25SPDLT)** folder, and then click **Properties**.

4.e.In **OU=EXTERNAL (FYDIBOHF25SPDLT) Properties**, select the **Replication** tab.

4.f.To replicate the **OU=EXTERNAL (FYDIBOHF25SPDLT)** folder to the Exchange 2010 CAS/Mailbox server, click **Add**.

4.g.In **Select a Public Folder Store**, select the **Public Folder Database** for the Exchange 2010 CAS/Mailbox server and then click **OK**.

Note:

By default, Exchange uses the replication schedule set on the public folder database.

4.h.Click **OK** to close **OU=EXTERNAL (FYDIBOHF25SPDLT) Properties** and save your changes.

4.i.Complete the same steps above for the **OU=Exchange Administrative Group (FYDIBOHF23SPDLT)** folder.

Warning:

Depending on the size of your public folders, this replication could take several hours to complete.

4.j.After the **OU=EXTERNAL (FYDIBOHF25SPDLT)** and **OU=Exchange Administrative Group (FYDIBOHF23SPDLT)** public folders have replicated to the Exchange 2010 CAS/Mailbox server, you must remove the replicas for these public folders on the Exchange 2003 server.

5. **Modify the LegacyExchangeDN parameter** Modify the *LegacyExchangeDN* parameter on all mail-enabled objects in the Exchange 2003 organization that reference the remote Exchange 2010 organization. Change the existing organizational unit (OU) value for the mail-enabled object to External (FYDIBOHF25SPDLT). For example, LegacyExchangeDN=/o=First Organization/ou=External (FYDIBOHF25SPDLT)/cn=Recipients/cn=User Name

Limitations of Free/Busy Sharing

The following limitations apply when sharing free/busy information between federated Exchange organizations:

- **Outlook Web Access 2003** When a user in an Exchange 2003 organization uses Outlook Web Access to access free/busy for users in a remote Exchange 2010 organization, the request will fail. Outlook Web Access connections from Exchange 2003 can't make WebDAV (Web-based Distributed Authoring and Versioning) connections to a free/busy system folder to retrieve the free/busy information for remote users. Because Exchange 2010 does not support WebDAV connections, the Exchange 2003 server can't connect to External (FYDIBOHF25SPDLT) on the Exchange 2010 CAS/Mailbox server for Outlook Web Access requests. Outlook clients don't experience this limitation because they use MAPI instead of WebDAV when connecting to External (FYDIBOHF25SPDLT).
- **Wide Area Network (WAN) latency** In Exchange 2003 organizations, the replicas for all free/busy folders must reside on Exchange 2010 SP1 Mailbox servers. In environments where Exchange 2003 public folder databases are located in multiple physical sites, there may be excessive latency and performance issues if internal free/busy queries have to traverse WAN links to access Exchange 2010 public folder databases not located in the same physical site.
- **Free/busy information period** Free/busy information requests to an Exchange 2007 organization from an Exchange 2010 organization may fail due

to a mismatch in the requested free/busy information period. By default, Exchange 2007 accepts availability requests for 42 days of free/busy information and Exchange 2010 may request 62 days of free/busy information. If the request exceeds the default 42 limit imposed by Exchange 2007, the request will fail.
Follow the steps below to configure your Exchange 2007 CAS servers to accept longer period free/busy information requests:

.1.On all your Exchange 2007 CAS servers, open the following file with a text editor such as Notepad.
<Exchange Installation Path>\V14\ClientAccess\ExchWeb\EWS\web.config

Caution:
Before you make any changes to the web.config file, make a copy of the file and store it in a safe location.

.2.Locate the **appSettings** section in the web.config file.
.3.Add a new key "<add key="maximumQueryIntervalDays" value="62" />" and save the web.config file.

Note:
The maximumQueryIntervalDays value isn't present by default. When this value isn't present, Exchange 2007 uses the default interval of 42 days.

.4.Stop and restart the Microsoft Internet Information Services (IIS) on all the Exchange 2007 CAS servers.

- **Exchange organizations that have both on-premises and cloud users** If you configure federated delegation with another Exchange organization that is configured in a hybrid deployment with a cloud service such as Microsoft Office 365, free/busy availability lookups for cloud-based or remote users that have been moved to the cloud will fail. Because the organization relationship for your Exchange organization is with the remote on-premises Exchange organization, not the cloud-based Exchange organization, the free/busy request can't query the cloud-based users. Exchange 2010 doesn't support functionality to proxy these availability requests through the on-premises organization to the cloud service.

1.14 Hybrid Deployments

Hybrid Deployments

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-02-26*

Understanding Hybrid Deployments with Exchange 2010 SP3

Understanding Upgrading Office 365 Tenants for Exchange 2010-based Hybrid Deployments

Understanding Single Sign-On with Hybrid Deployments

Understanding Certificate Requirements for Hybrid Deployments

1.14.1 Understanding Hybrid Deployments with Exchange 2010 SP3

Understanding Hybrid Deployments with Exchange 2010 SP3

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-01-25*

A hybrid deployment offers organizations the ability to extend the feature-rich experience and administrative control of their existing on-premises Microsoft Exchange organization to the cloud. A hybrid deployment provides the seamless look and feel of a single Exchange organization between an on-premises Exchange organization and Exchange Online in Microsoft Office 365. In addition, a hybrid deployment can serve as an intermediate step to moving completely to an Exchange Online organization.

Hybrid Deployment Features

A hybrid deployment enables the following features:

- Secure mail routing between on-premises and Exchange Online organizations.
- Mail routing with a shared domain namespace. For example, both on-premises and cloud-based organizations use the @contoso.com SMTP domain.
- A unified global address list, also called a "shared address book".
- Free/busy and calendar sharing between on-premises and Exchange Online organizations.
- Centralized control of outbound mail flow. You can configure Exchange Online to route all messages to Internet recipients through the on-premises Exchange organization.
- A single Outlook Web App URL for both the on-premises and Exchange Online organizations.
- The ability to move existing on-premises mailboxes to the Exchange Online organization.
- Centralized mailbox management using the on-premises Exchange Management Console.
- Message tracking, MailTips, and multi-mailbox search between on-premises and Exchange Online organizations.
- Cloud-based message archiving for on-premises Exchange mailboxes. Exchange Online Archiving can be used with a hybrid deployment. For more information, see Understanding Exchange Online Archiving.

Hybrid Deployment Components

A hybrid deployment involves several different services and components:

- **Microsoft Office 365** Office 365 provides a cloud-based Exchange Online organization as a part of its subscription service. Organizations configuring a hybrid deployment must create and configure this cloud-based Exchange organization.
- **Hybrid Configuration wizard** Service Pack 3 (SP3) for Exchange Server 2010 includes Hybrid Configuration wizards which provide you with a streamlined process to configure a hybrid deployment between on-premises Exchange and Exchange Online organizations.
  Learn more at: Understanding the Hybrid Configuration Wizard
- **Hybrid server** When the Hybrid Configuration wizards complete the configuration of an Exchange 2010 SP3 server in your existing Exchange organization, that Exchange 2010 SP3 server is now referred to as a *hybrid server*. Hybrid servers are required for hybrid deployments. They enable messaging features and message delivery between your on-premises Exchange and Exchange Online organizations.
- **Microsoft Federation Gateway** The Microsoft Federation Gateway is a free cloud-based service offered by Microsoft that acts as the trust broker between your on-premises Exchange 2010 organization and the Exchange Online organization.
  On-premises organizations configuring a hybrid deployment must have a federation trust with the Microsoft Federation Gateway. The Hybrid Configuration wizard checks to see if there is an existing federation trust with the Microsoft Federation Gateway for the on-premises organization. If present, the existing federation trust is used to support the hybrid deployment. If not present, the wizard creates a federation trust for the on-premises organization with the Microsoft Federation Gateway. A federation trust with the Microsoft Federation Gateway for your Office 365 tenant is automatically configured when you activate your Office 365 service account.
  Learn more at: Microsoft Federation Gateway
- **Active Directory synchronization** Active Directory synchronization replicates on-premises Active Directory information for mail-enabled objects to the Office 365 organization to support the unified global address list (GAL).
  Organizations configuring a hybrid deployment must deploy Active Directory synchronization on a separate on-premises server.
  Learn more at: Active Directory synchronization: Roadmap

1.14.2 Understanding Upgrading Office 365 Tenants for Exchange 2010-based Hybrid Deployments

Understanding Upgrading Office 365 Tenants for Exchange 2010-based Hybrid Deployments

Topic Last Modified: *2013-02-21*

Organizations that have configured a hybrid deployment with Microsoft Office 365 using Microsoft Exchange Server 2010 servers need to consider several factors when upgrading an Office 365 tenant to the next service version. Organizations with an existing hybrid deployment should evaluate whether to remain configured as an Exchange 2010-based hybrid deployment or upgrade their on-premises organization to an Exchange 2013-based hybrid deployment.

Organizations with on-premises Exchange 2010-only hybrid deployments need to make

this evaluation, as well as Exchange Server 2007 and Exchange Server 2003 on-premises organizations that have added Exchange 2010 servers as part of the hybrid deployment configuration process. Organizations with existing Exchange 2010-based hybrid deployments should also be aware that some administrative tasks are necessary to ensure full hybrid feature functionality. This topic focuses on Exchange 2010-based hybrid deployments and the Office 365 tenant upgrade process.

Exchange Hybrid Deployment Types and Compatibility with Office 365

Hybrid deployments between your on-premises and Office 365 organizations can be configured using either Exchange 2013 or Exchange 2010 servers. Depending on which version of Exchange you deploy in your on-premises organization to configure hybrid, your hybrid deployment will be either an *Exchange 2010-based hybrid deployment* or an *Exchange 2013-based hybrid deployment*. Following is a brief description of each deployment type:

- **Exchange 2010-based hybrid deployment** Exchange 2010-based hybrid deployments use Exchange 2010 servers to connect to the Microsoft Exchange Online Protection (EOP) service (formerly known as Forefront Online Protection for Exchange) included with all Office 365 tenants. Exchange 2010-based hybrid deployments can either be on-premises organizations that are homogenous Exchange 2010 organizations, or Exchange 2003 and Exchange 2007 on-premises organizations that have added Exchange 2010 servers as part of configuring a hybrid deployment with Office 365. This includes adding servers with either the Exchange 2010 Client Access or Edge Transport server roles.

  Exchange 2010-based hybrid deployments are compatible with the newest version of Office 365, provided some requirements are met. Compatibility with Office 365 allows organizations to remain configured as Exchange 2010-based hybrid deployments if they choose not to use the new features of Exchange 2013.

- **Exchange 2013-based hybrid deployment** Exchange 2013-based hybrid deployments use Exchange 2013 servers to connect to the EOP service included with all Office 365 tenants. Exchange 2013-based hybrid deployments can either be on-premises organizations that are homogenous Exchange 2013 organizations, or Exchange 2007 and Exchange 2010 on-premises organizations that have added Exchange 2013 servers as part of configuring a hybrid deployment with Office 365. All on-premises Exchange 2013 servers must have installed Cumulative Update 1 (CU1) or greater for Exchange 2013 to support hybrid functionality with Office 365. For more information, see Cumulative Updates for Exchange 2013.

  Exchange 2013-based hybrid deployment also includes scenarios where on-premises organizations add servers with the Exchange 2010 SP3 Edge Transport server role to Exchange 2013 organizations to use the benefits of a perimeter network. For more information about Exchange 2013-based hybrid deployments, see Exchange Server 2013 Hybrid Deployments.

Important:

Exchange 2003 on-premises organizations can't configure a hybrid deployment using Exchange 2013 servers. These organizations must use Exchange 2010-based hybrid deployments to configure coexistence with Office 365.

Office 365 Tenant Upgrade Process

Microsoft initiates Office 365 tenant upgrades. When their Office 365 tenant is eligible for upgrade to the newest version of the service, Office 365 administrators receive an email notification from Microsoft. While the Office 365 tenant upgrade process is fully automated and doesn't require any additional deployment requirements for cloud-only organizations, organizations with Exchange 2010-based hybrid deployments do require a few basic checks and actions as part of the Office 365 upgrade process.

For more information, see Office 365 Service Upgrade Center for Enterprise.

Exchange 2010-based Hybrid Deployments and Office 365 Tenant Upgrades

As part of the Office 365 tenant upgrade process, administrators need to conduct two administrative steps in order for Exchange 2010-based organizations to be fully functional when the Office 365 tenant is upgraded to version v15:

- **Exchange 2010 Service Pack 3** Exchange Server 2010 SP3 is required for all Exchange 2010 Client Access and Hub Transport servers in an Exchange 2010-based hybrid deployment that are Internet-facing and connect to Office 365 tenant version v15 or higher. This requirement also includes any Exchange 2010 Edge Transport servers that are configured to connect with Office 365 as part of a hybrid deployment.

  We recommend installing Exchange 2010 SP3 on your Exchange 2010 servers and management workstations in your on-premises organization before you accept the Office 365 update invitation. Exchange 2010 SP3 contains updates to the Exchange Management Console (EMC) that allow it to connect to the remote Exchange Online organization, as well as updating the management experience for the remote Exchange Online organization.

  Important:
  If you don't install Exchange 2010 SP3 prior to your Office 365 tenant upgrading to version v15, don't worry. Your hybrid deployment-related features and secure mail between your on-premises and Exchange Online organizations will continue to function normally. You'll receive a prompt to upgrade to Exchange 2010 SP3 when you try to access the remote Exchange Online organization node in the EMC. If you need to manage the organization configuration setting for the Exchange Online organization prior to updating to Exchange 2010 SP3, you can use the Exchange admin center (EAC) in the Office 365 tenant.
  To learn more about hybrid management and the version v15 Office 365 tenant, see Understanding Hybrid Management in Exchange 2010 Hybrid Deployments.
  To learn more about other updates included with Exchange 2010 SP3, see What's New in Exchange 2010 SP3.

- **Hybrid Configuration wizard** After you've installed Exchange 2010 SP3 and completed the update to your Office 365 tenant, you must run the Hybrid Configuration wizard again. You don't need to make any hybrid configuration changes if there aren't any changes to be made, but the wizard still needs to run to properly update the *HybridConfiguration* Active Directory object.

Version Information for Office 365 and Exchange Online

The Exchange Online service included as part of an Office 365 tenant is based on Exchange Server. When the Office 365 tenant is upgraded and the tenant version changes, the version of Exchange Online also changes. Following is specific information about tenant versions currently available:

- **Office 365 tenant version v14** Office 365 tenant version 14 includes the Exchange Online service that is based on Exchange 2010. This tenant version is identified by version number 14.0.000.0 and higher.
- **Office 365 tenant version v15** Office 365 tenant version 15 includes the Exchange Online service that is based on Exchange 2013. This tenant version is identified by version number 15.0.000.0 and higher.

Note:

If you're unsure what version of the Office 365 tenant is configured as part of your hybrid deployment, see the Verify Office 365 tenant version and status section later in this topic.

The Office 365 tenant version and each Exchange-based hybrid deployment requirements are listed in the following table.

On-premises environment	Exchange 2010-based hybrid with tenant version v14	Exchange 2010-based hybrid with tenant version v15	Exchange 2013-based hybrid with tenant version v15
Exchange 2013 (CU1)	Not supported[1]	Not applicable	Supported
Exchange 2010 SP3	Supported	Supported	Supported[5]
Exchange 2010 SP2	Supported	Not supported[2]	Not supported
Exchange 2010 SP1	Supported	Not supported[2]	Not supported
Exchange 2007 SP3 RU10	Supported[3]	Supported[4]	Supported[5]
Exchange 2007 SP3	Supported[3]	Not Supported	Not supported
Exchange 2003 SP2	Supported[3]	Supported[4]	Not supported

Note:

[1] Blocked in Exchange 2013 setup
[2] Tenant upgrade notification provided in Exchange Management Console
[3] Requires at least one on-premises Exchange 2010 SP2 server
[4] Requires at least one on-premises Exchange 2010 SP3 server
[5] Requires at least one on-premises Exchange 2013 (CU1) or greater server

Verify Office 365 Tenant Version and Status

If you're not sure which version of the Office 365 tenant is currently configured with your hybrid deployment, follow the steps below to verify the version of your Office 365 tenant:

1. Connect to the Office 365 tenant using remote Windows PowerShell. For step-by-step connection instructions, see Connect Windows PowerShell to the Service.
2. After connecting to the Office 365 tenant, run the following command.

```
Get-OrganizationConfig | Format-List AdminDisplayVersion
```

   Note the version of your Office 365 tenant:
   - *AdminDisplayVersion* parameter value displays the current Office tenant version. For example, "0.10 (14.0.500.5)" for a v14 tenant or "0.20 (15.0.100.1)" for a v15 tenant.
3. Disconnect from the Office 365 tenant remote PowerShell session. For step-by-step disconnection instructions, see Connect Windows PowerShell to the Service.

1.14.3 Understanding Single Sign-On with Hybrid Deployments

Understanding Single Sign-On with Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-02-14*

Single sign-on enables users to access both the on-premises and Microsoft Office 365 organizations with a single user name and password. Single sign-on provides users with a familiar sign-on experience and allows administrators to easily control account policies for cloud-based organization mailboxes by using on-premises Active Directory management tools. Deploying single sign-on includes several components that configure the trust relationship between the on-premises Active Directory Federation Services (AD FS) server and the Microsoft Federation Gateway.

Although not a requirement for hybrid deployments, we strongly recommend deploying single sign-on in your on-premises organization to make the account authentication experience seamless and familiar for your users. In addition to users not having to sign in multiple times and having to remember additional passwords when accessing the Office 365 organization, single sign-on also offers the following benefits:

- **Exchange Online Archiving** When single sign-on is deployed in Exchange 2010 organizations, on-premises Microsoft Outlook users aren't prompted for their credentials when accessing archived content in the Exchange Online organization. If single sign-on isn't deployed in Exchange 2010 organizations and Exchange Online Archiving is enabled, the on-premises user principal name (UPN) must match their Exchange Online account. In this scenario, the user will be prompted for their on-premises credentials when initially accessing their archive. A user can temporarily avoid future credential prompting by choosing "save password", but the user will be prompted again when their on-premises account password is changed.
- **Policy control** The administrator can control account policies through Active Directory, which gives the administrator the ability to manage password policies, workstation restrictions, lock-out controls, and more, without having to perform additional tasks in the cloud.
- **Access control** The administrator can restrict access to Office 365 so that the services can be accessed through the corporate environment, through online servers, or both.
- **Reduced support calls** Forgotten passwords are a common source of support calls in all companies. If users have fewer passwords to remember, they are less likely to forget them.
- **Security** User identities and information are protected because all the servers and services used in single sign-on are administered and controlled on-premises.
- **Support for strong authentication** You can use strong authentication (also called two-factor authentication) with Office 365. However, if you use strong authentication, you must use single sign-on. There are restrictions on the use of strong authentication. For more information, see Configuring Advanced Options for AD FS 2.0 and Office 365.

Learn more at: Prepare for single sign-on

1.14.4 Understanding Certificate Requirements for Hybrid Deployments

Understanding Certificate Requirements for Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

Digital certificates are an important part of securing the communication between the on-premises Exchange organization and the Microsoft Office 365 service, other on-premises Exchange servers, and your clients. Certificates enable one entity to trust the identity of another. This helps to ensure that a client or server is communicating to the right source.

In a hybrid deployment, several services make use of certificates:

- **Active Directory Federation Services (AD FS)** A certificate issued by a trusted third-party certificate authority (CA) is used to establish a trust between Web clients and federation server proxies, to sign security tokens, and to decrypt security tokens.
  Learn more at: Certificates
- **Exchange federation** A self-signed certificate is used to create a secure connection between the on-premises Service Pack 3 (SP3) for Exchange Server 2010 servers configured for the hybrid deployment (that is, "hybrid servers") and the Microsoft Federation Gateway.
  Learn more at: Understanding Federated Delegation
- **Exchange services** Certificates issued by a trusted third-party CA are used to increase the security for Secure Sockets Layer (SSL) communication between Exchange servers and clients. Services that use certificates include Outlook Web App, Exchange ActiveSync, Outlook Anywhere, and message transport.
- **Existing Exchange servers** Your existing Exchange servers may make use of certificates to help secure Outlook Web App communication, message transport, and so on. Depending on how you use certificates on your Exchange servers, you might use self-signed certificates or certificates issued by a trusted third-party CA.
  Learn more at: Understanding Digital Certificates and SSL

Certificate Requirements for a Hybrid Deployment

When configure a hybrid deployment, you must configure certificates. You must purchase certificates from a trusted third-party CA. Multiple services, such as AD FS, Exchange 2010 federation, Exchange 2010 services, and Exchange, each require certificates. Depending on your organization, you may decide to do one of the following:

- Use a third-party certificate that's used by all services across multiple servers.
- Use a third-party certificate for each server that provides services.

Whether you choose to use the same certificate for all services, or dedicate a certificate for each service, depends on your organization and the service you're implementing. Here are some things to consider about each option:

- **Third-party certificate across multiple servers** Third-party certificates that are used by services across multiple servers may be slightly cheaper to obtain, but they may complicate renewal and replacement. The complication occurs

because, when a certificate needs replacement, you need to replace the certificate on every server where it's installed.

- **Third-party certificate for each server** Using a dedicated certificate for each server that hosts services allows you to configure the certificate specifically for the services on that server. If you need to replace the certificate or renew it, you only need to replace it on the server where the services are installed. Other servers aren't impacted.

We recommend that you use a dedicated third-party certificate for the AD FS server, another certificate for the Exchange services on your hybrid servers, and if needed, a certificate on your Exchange server. The on-premises federated trust configured as part of federated delegation uses a self-signed certificate by default. Unless you have specific requirements, there's no need to use a third-party certificate with the federation trust configured as part of federated delegation.

The services that are installed on a single server may require that you configure multiple fully qualified domain names (FQDNs) for the server. Purchase a certificate that allows for the required number of FQDNs. Certificates consistent of the subject, or principal, name, and one or more subject alternative names (SAN). The subject name is the FQDN that the certificate is issued to. SANs are additional FQDNs that can be added to a certificate in addition to the subject name. If you need a certificate to support five FQDNs, purchase a certificate that allows for five domains to be added to the certificate: one subject name and four SANs.

Service	Server	Suggested FQDN
Active Directory Federation Services (AD FS) (if you've chosen to configure AD FS)	ADFS	sts.contoso.com
Autodiscover	Hybrid servers	autodiscover.contoso.com
Transport	Hybrid servers	Label that matches the external FQDN of your Exchange 2010 SP3 hybrid servers, such as hybrid.contoso.com.
Outlook Anywhere	Hybrid servers	Label that matches the internal FQDN of your Exchange 2010 SP3 hybrid servers, such as Ex2010.corp.contoso.com. Label that matches the internal host name of your Exchange 2010 SP3 hybrid servers, such as Ex2010.
Outlook Web App (Exchange 2010)	Hybrid servers	owa.contoso.com
Outlook Web App (existing Exchange server)	Existing Exchange server	Label that matches the external FQDN of your existing Exchange server, such as mail.contoso.com.

1.14.5 Understanding Hybrid Deployment Permissions with Exchange 2010 SP3

Understanding Hybrid Deployment Permissions with Exchange 2010 SP3

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2011-11-09*

The Exchange Online in Microsoft Office 365 organization is based on Exchange 2010 and, like on-premises organizations, uses Role Based Access Control (RBAC) to control permissions. Administrators are granted permissions using management role groups, and end users are granted permissions using management role assignment policies.

Learn more about RBAC at: Understanding Permissions

Administrator Permissions

By default, the user that was used to create the Office 365 service is made a member of the Organization Management role group in the Exchange Online organization. This user can manage the entire Office 365 organization, including configuration of organization-level settings and management of Exchange Online recipients.

You can add additional administrators in the Office 365 organization, depending on the management that needs to take place. You can add additional organization administrators and recipient administrators enable specialist users to perform compliance tasks such as discovery, configure custom permissions, and more. All permissions management for Office 365 administrators must be performed in the Exchange Online organization using either the Exchange Control Panel (ECP) or remote PowerShell.

However, it's important to note that there is no transfer of permissions between the on-premises organization and the Office 365 organization. Any permissions that you've defined in the on-premises organization must be re-created in the Office 365 organization.

See the following topics for more information:

- Create a Role Group
- Add a Role to a Role Group
- Remove a Role from a Role Group
- Copy a Role Group
- Add Members to a Role Group
- Remove Members from a Role Group

End User Permissions

As with administrator permissions, end users in Exchange Online can be granted permissions. By default, end users are granted permissions via the default role assignment policy. This policy is applied to every mailbox in the Exchange Online organization. If the permissions granted by default are sufficient, you don't need to change anything.

If you do want to customize end user permissions, you can either modify the existing default role assignment policy, or you can create new assignment policies. If you create multiple assignment policies, you can assign different policies to different groups of mailboxes, enabling you to control permissions granted to each group depending on their requirements. All permissions management for cloud-based end users must be performed in the Exchange Online organization using either the ECP or remote PowerShell.

Like administrator permissions, end user permissions aren't transferred between the on-premises organization and the Exchange Online organization. Any permissions that you've defined in the on-premises organization must be re-created in the Exchange Online organization.

The following table lists the permissions granted by the default role assignment policies in the Exchange Online organization.

Default role assignment policy permissions

Management role	Description
MyBaseOptions	The `MyBaseOptions` management role enables individual users to view and modify the basic configuration of their own mailbox and associated settings.
MyContactInformation	The `MyContactInformation` management role enables individual users to modify their contact information, including address and phone numbers.
MyDistributionGroupMembership	The `MyDistributionGroupMembership` management role enables individual users to view and modify their membership in distribution groups in an organization, provided that those distribution groups allow manipulation of group membership.
MyDistributionGroups	The `MyDistributionGroups` management role enables individual users to create, modify, and view distribution groups, and to modify, view, remove, and add members to distribution groups they own.
MyMailSubscription	The `MyMailSubscription` role enables individual users to view and modify their e-mail subscription settings such as message format and protocol defaults.
MyProfileInformation	The `MyProfileInformation` management role enables individual users to modify their name.
MyRetentionPolicies	The `MyRetentionPolicies` management role enables individual users to view their retention tags, and to view and modify their retention tag settings and defaults.
MyTextMessaging	The `MyTextMessaging` management role enables individual users to create, view, and modify their text messaging settings.
MyVoiceMail	The `MyVoiceMail` management role enables individual users to view and modify their voice mail settings.

See the following topics for more information:

- Add an Assignment Policy
- Remove an Assignment Policy

- Add a Role to an Assignment Policy
- Remove a Role from an Assignment Policy
- Change the Assignment Policy on a Mailbox
- Change the Default Assignment Policy

1.14.6 Understanding Cloud-Only Deployments with Exchange 2010 SP3

Understanding Cloud-Only Deployments with Exchange 2010 SP3

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2011-11-09*

A cloud-only deployment is one where your organization in the Exchange Online service isn’t connected with your on-premises directory and Exchange organization in a hybrid deployment. Exchange Online is part of Microsoft Office 365 . In a cloud-only deployment:

- If you have an on-premises Exchange organization, the Exchange Online organization looks like an external mail system.
- Users need to use different credentials to access their Exchange Online-based mailboxes.
- Your on-premises directory isn't synchronized with the Office 365 organization. Exchange Online mailboxes and distribution groups are managed separately from on-premises mailboxes and distribution groups.

A cloud-only deployment is most often used when you want to migrate from your existing on-premises e-mail system to Exchange Online. If you've already signed up for Office 365, you can click the **Cloud Only** button in the Exchange Server Deployment Assistant. If you haven't chosen to sign up for Office 365 yet, here's planning information that may help you: Exchange Hybrid Deployment and Migration with Office 365.

If you don’t want any of the functionality mentioned in the list above, you need to configure a hybrid deployment between your on-premises Exchange organization and the Exchange Online organization. With a hybrid deployment, you get the following capabilities:

- Active Directory synchronization
- Single sign-on
- Transport Layer Security (TLS) transport
- Free/busy and calendar sharing
- And more.

If you want to learn more about hybrid deployments, see Understanding Hybrid Deployments with Exchange 2010 SP3.

1.14.7 Hybrid Deployments with the Hybrid Configuration Wizard

Hybrid Deployments with the Hybrid Configuration Wizard

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-02*

Service Pack 2 (SP2) for Microsoft Exchange Server 2010 includes the *New Hybrid Configuration* and *Manage Hybrid Configuration* wizards, new components designed to help you configure hybrid deployments. These wizards provide Exchange administrators with a streamlined process to create and configure a hybrid deployment between on-premises Exchange and Microsoft Office 365 organizations.

When configuring a new hybrid deployment for your Exchange organization, follow these general deployment and configuration steps:

1. Read Understanding the Hybrid Configuration Wizard.
2. Configure all hybrid deployment prerequisites listed in Hybrid Configuration Wizard Prerequisites.
3. Create a new `HybridConfiguration` Active Directory object by following the steps in Create a New Hybrid Deployment.
4. Configure the options and properties of your hybrid deployment by following the steps in Manage a Hybrid Deployment.

1.14.7.1 Understanding the Hybrid Configuration Wizard

Understanding the Hybrid Configuration Wizard

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-12-13*

This topic gives you an overview of the Hybrid Configuration wizards, the hybrid deployment configuration process, and the Hybrid Configuration Engine.

For more information about hybrid deployments, check out Understanding Hybrid Deployment. Looking for management tasks related to hybrid deployments? See Hybrid Deployments with the Hybrid Configuration Wizard.

Contents

Hybrid Configuration Process

Creating and configuring your hybrid deployment with the Hybrid Configuration Wizards is

a two-step process. To begin, you use the New Hybrid Configuration wizard to create the foundation for the hybrid deployment. Then, you use the Manage Hybrid Configuration wizard to configure your Exchange organization for the hybrid deployment.

In the first step of the hybrid configuration process, the New Hybrid Configuration wizard creates the **HybridConfiguration** object in your on-premises Active Directory. This Active Directory object stores the hybrid configuration information for the hybrid deployment and is updated using the Manage Hybrid Configuration wizard.

In the second step of the hybrid configuration process, the Manage Hybrid Configuration wizard gathers existing Exchange and Active Directory topology configuration data, defines several organization parameters, and then runs an extensive sequence of configuration tasks. The general phases of the process run in the following order:

1. **Test account credentials** Designated on-premises and cloud organization hybrid management accounts access the on-premises and cloud organizations to gather prerequisite verification information and to make organization parameter configuration changes to enable hybrid deployment functionality. The Manage Hybrid Configuration wizard checks that the accounts have the appropriate credentials and can connect to the on-premises and Exchange Online organizations. The hybrid deployment management accounts for the on-premises and cloud organizations must be members of the Organization Management role group for the Hybrid Configuration wizard to complete these tasks successfully.
2. **Verify prerequisites and perform topology checks** The Manage Hybrid Configuration wizard verifies that your on-premises and cloud organizations can support a hybrid deployment. Some of the items that the wizard verifies and checks are Exchange server versions, the presence of Active Directory synchronization in the on-premises organization, and the presence of registered domains on the Office 365 service.
3. **Run the hybrid configuration changes** After testing the hybrid management accounts, conducting the verification and topology checks, and gathering configuration information defined by the Exchange administrator in the wizard process, the Manage Hybrid Configuration wizard makes the configuration changes to create and enable the hybrid deployment. All changes to the hybrid configuration are automatically logged in the hybrid configuration log. By default, the hybrid configuration log is located at C:\Program Files \Microsoft\Exchange Server\V14\Logging\Update-HybridConfiguration. The table below outlines the main areas that the Hybrid Configuration wizards modify and configure.

Configuration area	Description
Recipients	The wizard adds an accepted domain to the on-premises organization for hybrid mail flow and Autodiscover requests for the cloud organization. This domain, referred to as the "coexistence domain", is added as a secondary proxy domain to any e-mail address policies which have *PrimarySmtpAddress* templates for domains selected in the Hybrid Configuration wizard. By default, this domain is <domain>.mail.onmicrosoft.com. You can view the accepted domain by running the following command in the Shell on the cloud organization. `Get-AcceptedDomain | FL DomainName, IsCoexistenceDomain`
Exchange federation	The wizard checks to see if there is an existing federation trust with the Microsoft Federation Gateway for the on-premises organization. If present, the existing federation trust is used to support the hybrid deployment. If not present, the wizard creates a federation trust for the on-premises organization with the Microsoft Federation

	Gateway. The wizard also adds any domains selected within the hybrid configuration wizard to the federation trust. In addition to the federation trust configuration, the wizard also creates and configures organizational relationships for both the on-premises and cloud organizations. These organization relationships allow the wizard to enable several hybrid deployment features, including free/busy sharing, Outlook Web App redirection, message tracking, and MailTips.
Mailbox moves	The wizard enables the Mailbox Replication Service (MRS) proxy on the on-premises Client Access servers included in the hybrid deployment to enable mailbox moves from the on-premises organization to the cloud organization.
Mail flow	The wizard configures on-premises Hub Transport servers and Forefront Online Protection for Exchange (FOPE) on your Office 365 organization for hybrid mail routing. By configuring new and existing Send and Receive connectors in the on-premises organization and Inbound and Outbound connectors in FOPE, the wizard allows you to choose whether outbound messages delivered to the Internet from the Office 365 organization will be sent directly to external mail recipients or routed through your on-premises Hub Transport servers included in the hybrid deployment. Learn more at: • For Exchange 2003 hybrid deployments: Understanding Transport Options • For Exchange 2007 hybrid deployments: Understanding Transport Options for an Exchange 2007 Hybrid Deployment • For Exchange 2010 hybrid deployments: Understanding Transport Options for an Exchange 2010 Hybrid Deployment

Important:

Inbound mail flow is controlled by your organization's MX record. Inbound Internet e-mail for a hybrid deployment isn't configured by the Hybrid Configuration wizard.

Hybrid Configuration Features

The Manage Hybrid Configuration wizard automatically enables all hybrid deployment features by default. If you want to enable or disable specific hybrid configuration features, you can run the Manage Hybrid Configuration wizard again, or use the Exchange Management Console and the Exchange Management Shell to update hybrid deployment parameters. The following hybrid deployment features are enabled by default by the wizard:

- **Free/busy sharing** The free/busy sharing feature enables calendar information to be shared between on-premises and cloud-based organization users. Free/busy sharing is enabled as part of the federated delegation and organization relationship configuration for the on-premises and cloud-based Exchange organizations. Learn more at Understanding Federated Delegation.
- **Mailbox moves** The mailbox move feature enables on-premises mailboxes to be moved to the cloud organization while preserving user's Microsoft Office Outlook profiles and offline .ost folders. Mailbox move also enables moving cloud mailboxes to the on-premises organization.
- **Message tracking** The message tracking feature records the SMTP transport activity of all messages transferred to and from the hybrid Hub Transport servers between the on-premises and cloud-based organizations. You can use message tracking logs for message forensics, mail flow analysis, reporting, and troubleshooting. Learn more at Understanding Message Tracking.

- **MailTips** MailTips are informative messages displayed to users while they're composing a message. By enabling MailTips in the hybrid deployment, on-premises and cloud-based senders can adjust messages they're composing to avoid undesirable situations or non-delivery reports (NDRs) between the organizations. Learn more at Understanding MailTips.
- **Online archiving** Online archiving enables the cloud-based organization to host user e-mail archives for both on-premises and cloud-based users. Learn more at Configure Exchange Online Archiving.
- **Outlook Web App redirection** Outlook Web App redirection provides a single, common URL to access both on-premises and cloud-based Exchange mailboxes. The hybrid server automatically redirects Outlook Web App requests to the on-premises mailbox server or provides a link to users for their mailbox in the cloud-based organization. Learn more at:
  - For Exchange 2003 hybrid deployments: Understanding Access to Outook Web App with a Single URL
  - For Exchange 2007 hybrid deployments: Understanding Access to Outlook Web App with a Single URL for an Exchange 2007 Hybrid Deployment
  - For Exchange 2010 hybrid deployments: Understanding Access to Outlook Web App with a Single URL for an Exchange 2010 Hybrid Deployment
- **Secure mail** Secure mail enables secure message delivery between the on-premises and cloud organization via Transport Layer Security (TLS) protocol. The on-premises and cloud organizations are mutually authenticated through digital certificate subjects and e-mail headers and rich-text message formatting are preserved across the organizations.

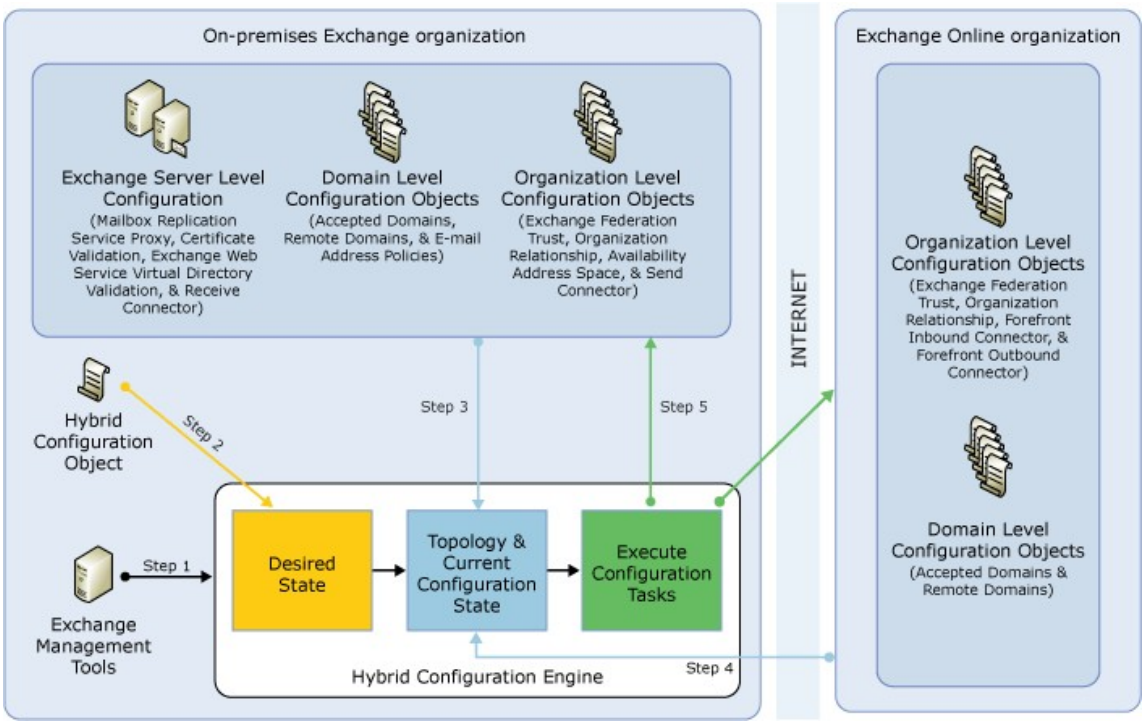
Hybrid Configuration Engine

The Hybrid Configuration Engine executes the core actions necessary for configuring and updating a hybrid deployment. Responsible for processing the `Update-HybridConfiguration` cmdlet actions, the Hybrid Configuration Engine compares the state of the *HybridConfiguration* Active Directory object with current on-premises Exchange and Exchange Online configuration settings and then executes tasks to match the deployment configuration settings to the parameters defined in the *HybridConfiguration* Active Directory object. If the current on-premises Exchange and Exchange Online deployment configuration states already match the settings defined in the *HybridConfiguration* Active Directory object, no changes are made by the Hybrid Configuration Engine to either the on-premises or Exchange Online organizations.

When updating an existing hybrid deployment, the Hybrid Configuration Engine performs the following steps:

- **Step 1** The *Update-HybridConfiguration* cmdlet triggers the Hybrid Configuration Engine to start.
- **Step 2** The Hybrid Configuration Engine reads the "desired state" stored on the `HybridConfiguration` Active Directory object.
- **Step 3** The Hybrid Configuration Engine discovers topology data and current configuration from the on-premises Exchange organization.
- **Step 4** The Hybrid Configuration Engine discovers topology data and current configuration from the Exchange Online organization.
- **Step 5** Based on the desired state, topology data, and current configuration, across both the on-premises Exchange and Exchange Online organizations, the Hybrid Configuration Engine establishes the "difference" and then executes configuration tasks to establish the "desired state."

The following figure shows a summary of how the Hybrid Configuration Engine retrieves and modifies on-premises Exchange server and Exchange Online in Office 365 configuration settings during the hybrid deployment process.



1.14.7.2 Hybrid Configuration Wizard Prerequisites

Hybrid Configuration Wizard Prerequisites

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-02-21*

Before you create and configure a hybrid deployment using the Hybrid Configuration wizards, your existing on-premises Exchange organization must meet certain requirements. If you don't meet these requirements, you won't be able to complete the steps within the Hybrid Configuration wizards and you won't be able to configure a hybrid deployment between your on-premises Exchange organization and the Exchange Online organization in Microsoft Office 365.

Prerequisites for Hybrid Deployment

The following prerequisites are required for configuring a hybrid deployment:

1. **On-premises Exchange organization** On-premises Exchange 2003-based organizations or later are required for a hybrid deployment. For Exchange 2003 and Exchange 2007 organizations, at least one Exchange 2010 Service Pack 2 (SP2) server must be installed in the on-premises organization to run the Hybrid Configuration wizards and support hybrid deployment functionality. All other on-premises Exchange servers must have the latest service packs installed.
   Learn more at: What's New in Exchange 2010 SP2.
2. **Install Exchange rollup packages** You must install the latest Exchange 2010 SP2 rollup packages on all hybrid servers to properly configure and avoid problems when configuring a hybrid deployment. Microsoft releases

update rollup packages approximately every six to eight weeks. The rollup packages are available via Microsoft Update and also through the Microsoft Download Center. In the Search box on the Microsoft Download Center, type "Exchange 2010 SP2 update rollup" to find links to the Exchange 2010 SP2 rollup packages.
Find update rollup packages at: Microsoft Download Center

3. **Office 365 for enterprises** An Office 365 for enterprises tenant and administrator account and user licenses available on the cloud service to configure a hybrid deployment.
   Learn more at: Sign up for Office 365
4. **Custom domains** Register any custom domains you want to use in your hybrid deployment with Office 365. You can do this by using the Office 365 Administrative portal, or by optionally configuring Active Directory Federation Services (AD FS) in your on-premises organization.
   Learn more at: Add your domain to Office 365
5. **Active Directory synchronization** Deploy Office 365 Active Directory synchronization in your on-premises organization.

   Important:
   If you signed up for your Office 365 tenant organization during the Office 365 beta program and enabled Active Directory synchronization, you must run the following Shell command in your Office 365 organization to create a coexistence domain (<domain>.mail.onmicrosoft.com) for your organization.
   ```
   Set-MsolDirsyncEnabled -EnableDirsync $true
   ```

   Learn more at: Active Directory synchronization: Roadmap
6. **Client Access and Hub Transport servers** Install one or more Exchange 2010 SP2 Client Access and Hub Transport servers in your on-premises organization. If you're configuring a hybrid deployment for an Exchange 2003 on-premises organization, you must also install the Mailbox Server role on at least one Exchange 2010 SP2 server added for the hybrid deployment.
7. **Autodiscover DNS records** Configure the Autodiscover public DNS records for your existing SMTP domains to point to an on-premises Exchange 2010 SP2 Client Access server.
8. **Office 365 organization in the Exchange Management Console (EMC)** Add the Office 365 organization to the EMC. This will allow you to manage both the on-premises and cloud Exchange organizations from a single management console. Learn more at: Add an Exchange Forest
9. **Exchange Web Services** Configure the *ExternalURL* parameter for the default Exchange Web Services (EWS) virtual directory with the externally accessible, fully qualified domain name (FQDN) of the hybrid Exchange 2010 SP2 Client Access server included in your hybrid deployment. Learn more at: Understanding Exchange Web Services Virtual Directories

   Important:
   Pre-authentication connections to the /EWS/exchange.asmx/wssecurity, /autodiscover/autodiscover.svc/wssecurity, and /EWS/MRSProxy.svc/wssecurity virtual directories must be turned off. Authentication for these virtual directories must use the Exchange federation trust certificate and federation claims.
10. **Certificates** Install and assign Exchange services to a valid digital certificate purchased from a trusted certificate authority (CA). Although self-signed certificates can be used for the on-premises federation trust with the Microsoft Federation Gateway, self-signed certificates can't be used for Exchange services in a hybrid deployment. The Internet Information Services (IIS) instance on the Client Access servers configured in the hybrid deployment must have a valid digital certificate purchased from a trusted certificate authority (CA). Additionally, the EWS external URL and the Autodiscover endpoint specified in your public DNS must be listed in Subject Alternative Name (SAN) of the certificate. The Hub Transport servers used for mail transport in the hybrid deployment must all use the same certificate (have matching certificate thumbprints).

After you've made sure your Exchange organization meets these requirements, you're ready to use the New Hybrid Deployment wizard. For detailed guidance, see Create a New Hybrid Deployment.

Recommended Tools and Services

In addition to the required prerequisites described earlier, other tools and services are beneficial when you're configuring hybrid deployments with the Hybrid Configuration wizards:

- **Remote Connectivity Analyzer tool** The Microsoft Remote Connectivity Analyzer tool checks the external connectivity of your on-premises Exchange organization and makes sure that you're ready to configure your hybrid deployment. We strongly recommend that you check your on-premises organization with the Remote Connectivity Analyzer tool prior to configuring your hybrid deployment with the Hybrid Configuration wizard.
  Learn more at: Remote Connectivity Analyzer Tool
- **Single sign-on** Although not a requirement for hybrid deployments, single sign-on enables users to access both the on-premises and cloud-based organizations with a single user name and password. Single sign-on provides users with a familiar sign-on experience and allows administrators to easily control account policies for cloud-based organization mailboxes by using on-premises Active Directory management tools. If you decide to deploy single sign-on with your hybrid deployment, we recommend that you deploy it in conjunction with Active Directory synchronization and before using the Hybrid Configuration wizards.
  Learn more at: Prepare for single sign-on

1.14.7.3 Create a New Hybrid Deployment

Create a New Hybrid Deployment

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-23*

A hybrid deployment offers organizations the ability to extend the feature-rich experience and administrative control they have with their existing on-premises Microsoft Exchange organization to the cloud. A hybrid deployment provides the seamless look and feel of a single Exchange organization between an on-premises organization and a cloud-based organization. The New Hybrid Configuration wizard helps simplify the creation of a hybrid deployment between your on-premises and Microsoft Office 365 Exchange organizations. After you have created a hybrid deployment, see Manage a Hybrid Deployment, which describes how to use the Manage Hybrid Deployment wizard.

Important:

Creating a hybrid deployment requires careful planning and affects several areas of your on-premises and cloud-based organizations. We strongly recommend that you review Hybrid Deployments with the Hybrid Configuration Wizard and Hybrid Configuration Wizard Prerequisites prior to creating your hybrid deployment using the New Hybrid Configuration Wizard.

Use the EMC to create a hybrid deployment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hybrid configuration" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In the console on-premises organization tree, select the **Organization Configuration** node and then select the **Hybrid Configuration** tab.
2. In the action pane, click **New Hybrid Configuration**.
3. In the **New Hybrid Configuration** wizard, click **New**. The wizard creates the *HybridConfiguration* object. The default name of the new hybrid configuration is **Hybrid Configuration**.
4. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Now that you've finished these steps, you're ready to complete the hybrid deployment configuration by following the steps described in Manage a Hybrid Deployment.

Use the Shell to create a hybrid deployment

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hybrid configuration" entry in the Exchange and Shell Infrastructure Permissions topic.

Run the following command in the Shell to create the *HybridConfiguration* object in Active Directory in the on-premises organization.

```
New-HybridConfiguration
```

Important:

If there is already an existing federation trust with the Microsoft Federation Gateway configured for your on-premises Exchange organization, the Hybrid Configuration wizard will use the existing federation trust for your hybrid deployment configuration. If there isn't an existing federation trust, you must manually create a new federation trust before the hybrid deployment configuration process can continue. Learn more at Create a Federation Trust.

Now that you've finished this step, you're ready to complete the hybrid deployment configuration by following the steps described in Manage a Hybrid Deployment.

1.14.7.4 Manage a Hybrid Deployment

Manage a Hybrid Deployment

Exchange Server 2010 > Hybrid Deployments > Hybrid Deployments with the Hybrid Configuration Wizard >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-04-12*

You can use a hybrid deployment to extend the feature-rich experience and administrative control for an existing on-premises Microsoft Exchange organization to the cloud. A hybrid deployment provides the seamless look and feel of a single Exchange organization between an on-premises organization and an Exchange Online organization.

For more information about hybrid deployments, see Hybrid Deployments with the Hybrid Configuration Wizard and Hybrid Deployments.

Prerequisites

A hybrid configuration for your on-premises and cloud-based organizations, created with the New Hybrid Configuration wizard. The wizard creates a **HybridConfiguration** object that must be accessible to manage and configure changes in your hybrid deployment. For more information, see Create a New Hybrid Deployment.

Use the EMC to configure hybrid configuration properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hybrid configuration" entry in the Exchange and Shell Infrastructure Permissions topic.

1. In the console on-premises organization tree, select the **Organization Configuration** node and then select the **Hybrid Configuration** tab.
2. In the **Organization Configuration** pane on the **Hybrid Configuration** tab, select the **Hybrid Configuration** object.
3. In the action pane, click **Manage Hybrid Configuration**.
4. On the **Introduction** page of the **Manage Hybrid Configuration** wizard, click **Next**.
5. On the **Credentials** page, complete the following fields:
   - For the on-premises organization:
     - **Username** Type the domain and user name for an account that is a member of the Organization Management role group in the on-premises organization. For example, "corp\administrator".
     - **Password** Type the password for the on-premises account you entered in the **Username** text box.
     - **Remember my credentials** Select this check box to allow the wizard to automatically use this on-premises account while configuring the hybrid deployment. If you do not select this check box, you'll have to manually enter the on-premises account credentials later when the hybrid configuration changes are executed.
   - For the Microsoft Office 365 organization:
     - **Username** Type the new domain and user name for an account that is a member of the Organization Management role group in the Office 365 organization. For example, "administrator@contoso.onmicrosoft.com".
     - **Password** Type the password for the Office 365 account you entered in the previous step.
     - **Remember my credentials** Select this check box to allow the wizard to automatically use this Office 365 account while configuring the hybrid deployment. If you do not select this check box, you'll have to manually enter the Office 365 account credentials later when the hybrid

configuration changes are executed.

6. Click **Next**.

7. On the **Domains** page, complete the following fields:
   - Click **Add** to add hybrid domains for your organization.
   - In the **Select Accepted Domain** dialog box, select accepted domains for the hybrid configuration. You should select the primary SMTP domain for your organization and any other accepted domains that will be used in the hybrid deployment. For example, select "contoso.com" and "sales.contoso.com".
   - Click **OK** on the **Select Accepted Domain** dialog box.
   -  To remove a domain from the hybrid configuration, select a hybrid domain name from the list and then click this button to remove it from the hybrid configuration.

   Note:
   At least one domain is required in a hybrid deployment.

8. Click **Next**.

9. On the **Domain Proof of Ownership** page, note the values listed in the **Record Value** field for each of the new hybrid domains you selected in the previous step. You must create a TXT record for each new domain in your public DNS so that the domain can be added to the Exchange federation trust for your organization. If you have kept a domain from your previous hybrid configuration and the TXT record for this domain has already been created on your public DNS, you don't need to re-create the TXT record on your public DNS. For example, you would only need to create additional TXT records in your public DNS for the new domains similar to the following:

Domain	DNS record type	Text
contoso.com	TXT	7Zyr2i/fE/M/T3AwCpitDbF30Fk/TdzXME6f7d1lDaKGthPdoS+UF94t43D2nU5hLNnIAP+5A3jJR2ik9HDPgg==
sales.contoso.com	TXT	Eh/po5qT098GMPklJU2DShrYO9mPseTn5i9wWKOKebmceLPuLCpaejYj83W53H/YcuzPy2VSo621BHO4DNS7jg==

Warning:
The federated domain proof is a lengthy string of alphanumeric characters. To avoid input errors, we recommend that you copy the domain string from the wizard by pressing CTRL+C, paste it into a text editor such as Notepad, copy it from the text editor to the Clipboard, and then paste the string into the **Text** field of the TXT record. If the TXT record is created with an incorrect federated domain proof string, the Microsoft Federation Gateway won't be able to verify proof of domain ownership, and you won't be able to add it to the federated organization identifier or complete the hybrid configuration.

After you have created the TXT records for the new hybrid domains in your public DNS and the DNS zone file has replicated, select the **Check to confirm that the TXT records have been created in public DNS for the domains above** check box.

10. Click **Next**.

11. On the **Servers** page, complete the following fields:
    - For the Client Access servers:
      - Click **Add** to select the Client Access servers in your on-premises organization that will be configured for your hybrid deployment.
      - In the **Select Client Access Server** dialog box, select one or more servers that have the Exchange 2010 SP2 Client Access server role installed.
      - Click **OK** on the **Select Client Access Server** dialog box.
      -  To remove a Client Access server from the hybrid configuration, select the Client Access server from the list and then click this button to remove it from the hybrid configuration.

        Note:
        At least one Exchange 2010 SP2 Client Access server is required in a hybrid deployment.
    - For the Hub Transport servers:
      - Click **Add** to select the Hub Transport servers in your on-premises organization that will be configured for mail flow in your hybrid deployment.
      - In the **Select Hub Transport Server** dialog box, select one or more servers that have the Exchange 2010 SP2 Hub Transport server role installed.
      - Click **OK** on the **Select Hub Transport Server** dialog box.
      -  To remove a Hub Transport server from the hybrid configuration, select the Hub Transport server from the list and then click this button to remove it from the hybrid configuration.

        Note:
        At least one Exchange 2010 SP2 Hub Transport server is required in a hybrid deployment.
12. Click **Next**.

13. On the **Mail Flow Settings** page, complete the following fields:
    - For the Forefront Online Protection for Exchange inbound connector:
      - Click **Add** and enter the publicly accessible IP address for a Hub Transport server in your hybrid deployment. Repeat this step to enter IP addresses for multiple Hub Transport servers in your hybrid deployment.

        Note:
        If you're using a network firewall device in your on-premises organization, you may have to enter the external IP address of the firewall for the FOPE inbound connector instead of the external IP address of you hybrid Hub Transport servers. FOPE examines the sending IP address for messaging traffic originating from the on-premises organization and verifies that it matches the IP addresses configured for this inbound connector. If these IP addresses don't match, FOPE refuses the message traffic and messages sent from recipients in the on-premises organization to recipients in the Exchange Online organization aren't delivered. Additionally, be sure to use IPv4-based IP addresses because IPv6-based IP addresses aren't supported.
    - For the Forefront Online Protection for Exchange outbound connector:
      - In the **Specify the FQDN of the on-premises hybrid Hub Transport servers** field, enter the FQDN of a Hub Transport server in your hybrid deployment. For example, enter "mail.contoso.com".
14. Click **Next**.

15. On the **Mail Flow Security** page, complete the following fields:
    - For **Select Transport Certificate**, select the drop-down arrow for the **Select transport certificate** field and then select a valid digital certificate from a trusted certificate authority (CA) that has been installed on all Hub Transport servers in your hybrid deployment.
    - For **Mail Flow Path**, select one of the following hybrid mail routing options for outbound messages for your Office 365-based mailboxes:
        - **Deliver Internet-bound messages directly using the external recipient's DNS settings** Select this option if you want Office 365 to bypass your on-premises transport servers when routing outbound messages to external recipients.
        - **Route all Internet-bound messages through your on-premises Exchange servers** Select this option if you want Office 365 to send all outbound messages to external recipients to your on-premises transport servers. The on-premises hybrid transport servers will be responsible for delivering the messages to external recipients.

16. On the **Progress** page, review the properties for the hybrid configuration changes. Click **Manage** to update the hybrid configuration.

17. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

Use the Shell to configure hybrid deployment properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Hybrid configuration" entry in the Exchange and Shell Infrastructure Permissions topic.

This example updates a default hybrid deployment and disables the secure mail and centralized transport hybrid deployment features. All other default hybrid deployment features, such as free/busy sharing, MailTips, and message tracking, remain enabled.

1. Use the following command to disable the secure mail and centralized transport hybrid deployment features.

```
Set-HybridConfiguration -Features FreeBusy,MoveMailbox,MailTips,OWARed
```

2. Use the following command to specify your on-premises credentials. For example, run this command and then enter "admin@contoso.com" and the associated account password in the credentials dialog when prompted.

```
$OnPremisesCreds = Get-Credential
```

3. Use the following command to specify your cloud-based service credentials. For example, run this command and then enter "admin@contoso.onmicrosoft.com"and the associated account password in the credentials dialog when prompted.

```
$TenantCreds = Get-Credential
```

4. Use the following command to define the specified credentials that will be used when updating the hybrid configuration object and connecting to the cloud-based service.

```
Update-HybridConfiguration -OnPremisesCredentials $OnPremisesCreds -Te
```

For more information about these hybrid deployment cmdlets, see Set-HybridConfiguration and Update-HybridConfiguration.

1.14.8 Hybrid Deployments with Exchange 2010 SP3 and Exchange 2003

Hybrid Deployments with Exchange 2010 SP3 and Exchange 2003

Exchange Server 2010 > Hybrid Deployments >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-01-28*

Understanding Hybrid Servers in Exchange 2003 Hybrid Deployments

Understanding Prerequisites for Exchange 2003 Hybrid Deployments

Understanding Hybrid Management in Exchange 2003 Hybrid Deployments

Understanding Edge Transport Servers in Exchange 2003 Hybrid Deployments

Understanding Shared Free/Busy in Exchange 2003 Hybrid Deployments

Understanding Transport Options in Exchange 2003 Hybrid Deployments

Understanding Transport Routing in Exchange 2003 Hybrid Deployments

1.14.8.1 Understanding Hybrid Servers in Exchange 2003 Hybrid Deployments

Understanding Hybrid Servers in Exchange 2003 Hybrid Deployments

Exchange Server 2010 > Hybrid Deployments > Hybrid Deployments with Exchange 2010 SP3 and Exchange 2003 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

When configuring a hybrid deployment, you have to install at least one hybrid server in your existing Exchange organization. Hybrid servers are additional servers configured with Exchange 2010 SP3 server roles that coordinate communication between your existing Exchange 2003 organization and the Exchange Online organization. This communication includes message transport and messaging features between the on-premises and Exchange Online organizations. We highly recommend installing more than one hybrid server in your on-premises organization to help increase reliability and availability of hybrid deployment features.

Hybrid Deployment Server Roles

Depending on the hybrid deployment configuration that you want, a hybrid server requires one or more of the following Exchange 2010 server roles to be installed. If you choose to install a single hybrid server in your on-premises organization, you'll need to

install all the following server roles on the single hybrid server. If you choose to install more than one hybrid server in your on-premises organization, you may choose to install the server roles on separate servers in your on-premises organization. For example, you could install one hybrid server that has both the Client Access and Mailbox server roles installed and install another hybrid server that only has the Hub Transport server role installed. However, the best practice and recommended hybrid server configuration is to install the Client Access, Mailbox, and Hub Transport servers on each hybrid server deployed in your on-premises organization.

Here is a quick overview of the server roles in a hybrid deployment:

- **Client Access server role** The Client Access server role on a hybrid server provides the functionality typically provided by a front-end server in Exchange 2003. All client connectivity, including Outlook client access, Outlook Web App, and Outlook Anywhere goes through the Client Access server role. Organization relationship features between the on-premises and Exchange Online organizations, such as free/busy sharing, are also handled by the Client Access server role.
  Learn more at: Understanding Client Access
- **Hub Transport server role** The Hub Transport server role on a hybrid server handles all mail flow between the on-premises and Exchange Online organizations and between the on-premises organization and the Internet. It helps to secure transport communication between the on-premises and Exchange Online organizations, as well as handling transport rules, journaling policies, and message delivery to user mailboxes in a hybrid deployment.
  Learn more at: Overview of the Hub Transport Server Role
- **Mailbox server role** The Mailbox server role on a hybrid server hosts a replica of the **OU=EXTERNAL (FYDIBOHF25SPDLT)** public folder that enables calendar free/busy information sharing between the on-premises and Exchange Online organizations. Mailboxes should not be created on a hybrid server in a typical hybrid deployment between an on-premises Exchange 2003 organization and an Exchange Online organization.
  Learn more at: Overview of the Mailbox Server Role

Hybrid Server Functionality

A hybrid server provides several important functions for your on-premises organization in a hybrid deployment:

- **Federation** Hybrid servers enable you to create a federation trust for your on-premises organization with the Microsoft Federation Gateway. The Microsoft Federation Gateway is a free, cloud-based service offered by Microsoft that acts as the trust broker between your on-premises organization and the Office 365 tenant organization. Federation is a requirement for creating an organization relationship between the on-premises and the Exchange Online organizations.
  Learn more at: Understanding Federation
- **Organization relationships** Hybrid Client Access servers enable you to create organization relationships between the on-premises and Exchange Online organizations. Organization relationships are required for many other services in a hybrid deployment, including calendar free/busy information sharing, message tracking, and mailbox moves between the on-premises and Exchange Online organizations.
  Learn more at: Understanding Federated Delegation
- **Message transport** Hybrid Hub Transport servers are responsible for message transport in a hybrid deployment. Using Send and Receive connectors, they replace the on-premises Exchange 2003 server as the connection endpoint for incoming external messages and also provide outbound message delivery to the Internet and the Exchange Online organization.
  Learn more at: Understanding Transport
- **Message transport security** Hybrid Hub Transport servers help to secure

message communication between the on-premises and Exchange Online organizations by using the Domain Security functionality in Exchange 2010. Security can be increased by using mutual transport layer security authentication and encryption for message communications.
Learn more at: Understanding Domain Security

- **Outlook Web App** Hybrid Client Access servers support configuring a single URL endpoint for external connections to on-premises and Exchange Online mailboxes. For on-premises mailboxes, hybrid Client Access servers are configured to automatically redirect user Outlook Web App requests to your Exchange 2003 mailbox server. For Exchange Online organization mailboxes, hybrid Client Access servers are configured to automatically display a link to the Outlook Web App endpoint on the Exchange Online organization.
- Learn more at: Understanding Outlook Web App

Hybrid Server Topology

A hybrid server is deployed much like an Exchange 2010 server would be deployed to your existing Exchange 2003 organization. Using the Client Access, Mailbox, and Hub Transport server roles, hybrid servers are responsible for many services for your on-premises organization that are currently provided by your existing Exchange 2003 server. The following table describes briefly the changes in services after configuring a hybrid deployment.

Service	Before hybrid server deployment	After hybrid server deployment	Description
Message transport (inbound and outbound)	Exchange 2003 server	Hybrid Hub Transport server(s)	The MX (mail exchanger) record for the domain may be updated to point to hybrid Hub Transport servers.
OU=EXTERNAL (FYDIBOHF25SPDLT) public folder replica	Exchange 2003 server	Hybrid Mailbox server (s)	All other public folder replicas remain on the Exchange 2003 server.
Outlook Web App public URL	Exchange 2003 server	Hybrid Client Access server(s)	Hybrid Client Access servers redirect Outlook Web App requests to the publicly accessible endpoint on the Exchange 2003 server.

Hybrid Server Software

Service Pack 3 (SP3) for Exchange Server 2010 enables hybrid deployment functionality with the Hybrid Configuration wizards. You can use any Exchange 2010 SP3 media when installing the hybrid server.

Additionally, we recommend that you install future Update Rollups for Exchange 2010 SP3 on all your hybrid servers. Microsoft releases update rollup packages approximately every six to eight weeks. The rollup packages are available via Microsoft Update and the Microsoft Download Center. In the Search box on the Microsoft Download Center, type "Exchange 2010 SP3 update rollup" to find links to the rollup packages for Exchange 2010 SP3.

Download Exchange Server 2010 SP3 at: Exchange 2010 Service Pack 3 (SP3)

Important:
You need to provide an Exchange 2010 Hybrid Edition product key on the hybrid server when you configure a hybrid deployment with Office 365. To obtain a Hybrid Edition product key, contact Office 365 support.

1.14.8.2 Understanding Prerequisites for Exchange 2003 Hybrid Deployments

Understanding Prerequisites for Exchange 2003 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Before you can really start to use the Deployment Assistant, your system and servers must meet requirements. If they don't meet these requirements, you won't be able to complete the steps within the tool and you won't be able to configure a hybrid deployment between your on-premises Exchange 2003 and Exchange Online organizations. This topic provides information about the following:

- The Exchange Pre-Deployment Analyzer
- Permissions needed to install and manage Exchange 2010
- Requirements for directory servers, hardware, software, clients, and other elements, including:
  - Windows Server 2008 Service Pack 2 (SP2) or later or Windows Server 2008 R2 operating system prerequisites that are required for all Exchange 2010 server roles
- Language support for Exchange 2010
- The Exchange Management Shell, the command-line interface for Exchange 2010, and the Exchange Management Console, the GUI management tool for Exchange 2010

Note:
Before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Exchange Pre-Deployment Analyzer

You can use the Exchange Pre-Deployment Analyzer (ExPDA) to perform an overall topology readiness scan of your environment. This scan focuses on overall topology readiness and not the ability to run Exchange 2010 on the local computer. ExPDA provides a detailed report that will alert you if there are any issues within your organization, which could prevent you from deploying Exchange 2010. For example, ExPDA will notify you if you haven't deployed the minimum required Exchange service pack on all your Exchange servers. If your organization passes the ExPDA readiness scan, you can go ahead and use the Exchange Deployment Assistant.

To get ExPDA from the Microsoft Download Center, see: Exchange Pre-Deployment Analyzer

Permissions to Install and Manage

Exchange 2010

Exchange 2010 requires different permissions to install and to manage your server roles. When you're installing Exchange 2010 servers in your organization, the account you use might not be the same account that you use for administering and managing your server roles. To manage your server roles, Exchange 2010 uses the Role Based Access Control (RBAC) permissions model.

Exchange 2010 uses RBAC to manage permissions on the Exchange 2010 hybrid server. With RBAC, you can control what resources administrators can configure and what features users can access. The RBAC model in Exchange 2010 is flexible and provides you with several ways to customize the default permissions.

RBAC has two primary ways of assigning permissions to users in your organization, depending on whether the user is an administrator or specialist user, or an end-user: management role groups and management role assignment policies. Each method associates users with the permissions they need to perform their jobs. The following sections list the tasks found in the Deployment Assistant and the permissions required to complete the task.

Note:

Some features may require that you have local administrator permissions on the server you want to manage. To manage these features, you must be a member of the Local Administrators group on that server.

Installation Permissions

By default, the account that's used to install Exchange 2010 in the organization is added as a member of the Organization Management role group.

When you install the first hybrid server into your Exchange 2003 organization, Exchange Setup will prepare your Active Directory schema if you have the correct permissions. If you want to separate your Active Directory schema preparation from a hybrid server installation, see: Prepare Active Directory and Domains

For information about how to add permissions, see: Add Members to a Role Group

The following permissions are required to install the hybrid server in your organization:

- Local Administrator on the server on which Exchange 2010 will be installed
- Enterprise Administrator in the Active Directory forest where Exchange 2010 will be installed
- Schema Administrator in the Active Directory forest where Exchange 2010 will be installed

Exchange Management Permissions

The table below lists the configuration permissions that you need to successfully use the Deployment Assistant and the Hybrid Configuration wizards. Some tasks need to be performed only in the on-premises organization while some tasks also need to be performed in the Office 365 tenant organization. If a task needs to be performed in the Office 365 tenant organization, you must ensure that you have the required permissions in that organization. Permissions in the on-premises organization aren't replicated to the Office 365 tenant organization.

Note:

The user account used to create the Office 365 tenant organization has all the permissions required to perform the tasks in this checklist.

Learn more at: Understanding Hybrid Deployment Permissions

Some procedures require you to perform tasks on your Exchange 2003 servers. For

information about how to manage permissions in an organization with Exchange 2003 and Exchange 2010 installed, see: Understanding Permissions Coexistence with Exchange 2003

Task	Permissions required	On-premises or Office 365 tenant organization
Import digital certificates	Local Administrator	On-premises organization
Configure settings on virtual directories	Server Management	On-premises organization
Configure virtual directories	Organization Management Server Management	On-premises organization
Create accepted domains	Organization Management	On-premises and Office 365 tenant organization
Create and modify Send and Receive connectors	Organization Management	On-premises organization
Create routing group connectors	Organization Management Server Management	On-premises organization
Create a federation trust	Organization Management	On-premises organization
Create organization relationships	Organization Management	On-premises and Exchange Online organization
Configure Mailbox Replication Service (MRS) proxy	Local Administrator	On-premises organization
Move mailboxes	Organization Management Recipient Management	On-premises and Exchange Online organization
Configure Exchange 2003 authentication	Local Administrator	On-premises organization
Configure Exchange 2003 e-mail address policies	Exchange Administrator	On-premises organization

Directory Servers

Here are the requirements for the directory servers in your organization:

- **Schema master** The latest 32-bit or 64-bit edition of the Windows Server 2003 SP2 Standard or Enterprise operating system or the Windows Server 2008 Standard or Enterprise operating system.
- **Global catalog server** In every Active Directory site where you plan to install Exchange 2010, you must have at least one global catalog server that is either the latest 32-bit or 64-bit edition of: Windows Server 2003 SP2 Standard or Enterprise; Windows Server 2008 Standard or Enterprise; or Windows Server 2008 R2 Standard or Enterprise.
- **Active Directory Forest** The Active Directory forest must be Windows Server 2003 forest functional mode or higher.
- **Domain Controller** You must have the latest 32-bit or 64-bit Windows Server 2003 Standard Edition or Enterprise Edition with Service Pack 2 (SP2) operating system or the latest 32-bit or 64-bit edition of the Windows Server

2008 Standard or Enterprise operating system or the Windows Server 2008 R2 Standard or Enterprise operating system.

Hardware

The recommended hardware requirements for Exchange 2010 servers vary depending on several factors including the server role(s) that are installed and the anticipated load that will be placed on the servers.

- **Processor** x64 architecture-based computer with processor that supports 64-bit architecture
- **Memory** Minimum 4GB with a recommended maximum of 2GB per core (8GB minimum). Learn more at: Understanding Memory Configurations and Exchange Performance
- **Disk space** At least 1.2 GB on the drive on which you install Exchange and additional 200 MB of available space on the system drive.
- **Drive** DVD-ROM drive, local or network accessible
- **File format** Disk partitions formatted as NTFS file systems

Operating System

Here are the supported operating systems for Exchange 2010:

- 64-bit edition of Windows Server 2008 Standard Service Pack 2
- 64-bit edition of Windows Server 2008 Enterprise Service Pack 2
- 64-bit edition of Windows Server 2008 Standard R2
- 64-bit edition of Windows Server 2008 Enterprise R2

Exchange 2010 Management tools can use the operating systems listed above plus:

- 64-bit edition of Windows Vista
- 64-bit edition of Windows 7

Install Hotfixes for Windows Server 2008 SP2

The following hotfixes are required for Windows Server 2008 SP2:

- Install the update described in Microsoft Knowledge Base article 977624, AD RMS clients do not authenticate federated identity providers in Windows Server 2008 or in Windows Vista. Without this update, Active Directory Rights Management Services (AD RMS) features may stop working.
- Install the update described in Knowledge Base article 979744, A .NET Framework 2.0-based Multi-AppDomain application stops responding when you run the application.
- Install the update described in Knowledge Base article 979917, Two issues occur when you deploy an ASP.NET 2.0-based application on a server that is running IIS 7.0 or IIS 7.5 in Integrated mode. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB979917 - QFE for Sharepoint issues - Perf Counter fix & User Impersonation.
  - For the available downloads, see KB979917 - QFE for Sharepoint issues - Perf Counter fix & User Impersonation.
- Install the update described in Knowledge Base article 973136, FIX: ArgumentNullException exception error message when a .NET Framework 2.0 SP2-based application tries to process a response with zero-length content to an asynchronous ASP.NET Web service request: "Value cannot be null".
- Install the update described in Knowledge Base article 977592, RPC over HTTP clients cannot connect to the Windows Server 2008 RPC over HTTP servers that have RPC load balancing enabled.

Install Hotfixes for Windows Server 2008 R2

The following hotfixes are required for Windows Server 2008 R2:

Important:
The following hotfixes only apply to Windows Server 2008 R2 RTM. If you're installing Exchange on Windows Server 2008 R2 SP1, you don't need to apply these hotfixes.

- Install the update described in Knowledge Base article 979099, An update is available to remove the application manifest expiry feature from AD RMS clients. Without this update, the AD RMS features may stop working.
- Install the update described in Knowledge Base article 979744, A .NET Framework 2.0-based Multi-AppDomain application stops responding when you run the application.
- Install the update described in Knowledge Base article 983440, An ASP.NET 2.0 hotfix rollup package is available for Windows 7 and for Windows Server 2008 R2. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB983440 - Win7 rollup package (PR for QFE 810219).
  - For the available downloads, see KB983440 - Win7 rollup package (PR for QFE 810219).
- Install the update described in Knowledge Base article 977020, FIX: An application that is based on the Microsoft .NET Framework 2.0 Service Pack 2 and that invokes a Web service call asynchronously throws an exception on a computer that is running Windows 7.

Install Hotfixes for Windows 7 and Windows Vista

The following hotfixes are required for Windows 7 and Windows Vista computers where you install the Exchange Management Console

- Install the update described in Knowledge Base article 977020, FIX: An application that is based on the Microsoft .NET Framework 2.0 Service Pack 2 and that invokes a Web service call asynchronously throws an exception on a computer that is running Windows 7.
- Install the update described in Knowledge Base article 983440, An ASP.NET 2.0 hotfix rollup package is available for Windows 7 and for Windows Server 2008 R2. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB983440 - Win7 rollup package (PR for QFE 810219).
  - For the available downloads, see KB983440 - Win7 rollup package (PR for QFE 810219).

Install the Windows Server 2008 SP2 prerequisites

1. Install the Microsoft Filter Pack. For details, see: 2007 Office System Converter: Microsoft Filter Pack
2. Open an elevated command prompt, navigate to the Scripts folder on the Exchange 2010 installation media and use the following command to install the necessary operating system components:

```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

Install the Exchange 2010 SP1 Hotfixes for Windows Server 2008 SP2

The following hotfix is required for Windows Server 2008 SP2 and must be installed after the operating system prerequisites have been installed:

- Install the hotfix described in Knowledge Base article 982867, WCF services that are hosted by computers together with a NLB fail in .NET Framework 3.5 SP1. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.
  - For the available downloads, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.

After installing the preceding prerequisites and hotfix, and before installing Exchange

2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Install the Windows Server 2008 R2 prerequisites

1. Install the Microsoft Filter Pack. For details, see: 2007 Office System Converter: Microsoft Filter Pack
2. On the Start Menu, navigate to **All Programs**, then **Accessories**, then **Windows PowerShell**. Open an elevated Windows PowerShell console, and run the following command:

```
Import-Module ServerManager
```

3. Use the **Add-WindowsFeature** cmdlet to install the necessary operating system components using the following command:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,W
```

4. After the system has restarted, log on as an administrator, open an elevated Windows PowerShell console, and configure the Net.Tcp Port Sharing Service for Automatic startup by running the following command:

```
Set-Service NetTcpPortSharing -StartupType Automatic
```

Install the Exchange 2010 SP1 Hotfixes for Windows Server 2008 R2

The following hotfix is required for Windows Server 2008 R2 and must be installed after the operating system prerequisites have been installed:

- Install the hotfix described in Knowledge Base article 982867, WCF services that are hosted by computers together with a NLB fail in .NET Framework 3.5 SP1. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.
  - For the available downloads, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.

After installing the preceding prerequisites and hotfix, and before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Windows Management Framework

- Windows PowerShell V2.0
- Windows Remote Management V2.0
- .NET Framework 3.5 SP1
- Internet Information Services (IIS)

Language Support

An Exchange 2010 SP2 language pack contains the necessary resources for a supported Exchange language. Language packs are installed automatically during deployment of Exchange 2010 SP2. Client and server language packs come grouped into a single bundle containing both client and server resource and support files. There are no performance issues with installing all the languages because they're just stored when not in use.

Learn more at: Exchange 2010 Language Support

Exchange Management Shell

The Exchange Management Shell, built on Windows PowerShell technology, provides a powerful command-line interface for Exchange 2010 that enables automation of

administrative tasks.

With the Shell, you can manage every aspect of Exchange 2010; the Shell can perform every task that can be performed by the Exchange Management Console (EMC) and the Exchange Control Panel (ECP) in addition to tasks that can't be performed in those interfaces. In fact, when a task is performed in the EMC or the ECP, those interfaces use the Shell to perform the task.

Learn more at: Overview of Exchange Management Shell

Exchange Management Console

The Exchange Management Console (EMC) is a Microsoft Management Console (MMC) 3.0-based tool that provides you with a GUI to manage the configuration of your Exchange 2010 organization. You can also add the EMC snap-in to custom MMC-based tools.

Learn more at: Exchange Management Console

1.14.8.3 Understanding Hybrid Management in Exchange 2003 Hybrid Deployments

Understanding Hybrid Management in Exchange 2003 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-31*

Both your on-premises organization and the Exchange Online organization are based on Microsoft Exchange. In particular, hybrid servers in your on-premises organization are based on Microsoft Exchange Server 2010 and the Exchange Online organization Exchange servers are based on Exchange Server 2013. Service Pack 3 (SP3) for Exchange 2010 enables hybrid features to function correctly between these two types of hybrid deployment servers.

When you install a hybrid server, Exchange 2010 management tools are automatically installed on the server. You'll use the management tools to configure and manage both the hybrid server(s) and some recipient management features for the Exchange Online organization. These tools include the Exchange Management Console (EMC), a graphical administrative interface, and the Exchange Management Shell, a Windows PowerShell-based command-line interface. You'll also use the Exchange Administration Center (EAC) in the Exchange Online section of the Office 365 management portal to manage most of the properties of the Exchange Online recipients and organization.

Exchange Management Console

The EMC enables you to perform many deployment tasks and most common day-to-day administrative tasks. Additionally, the EMC allows you to administer both the on-premises hybrid servers and some recipient management features for mailboxes in the Exchange Online organization. It's installed by default on every Exchange 2010 server, but you can also install it on a computer running any of the following 64-bit operating systems:

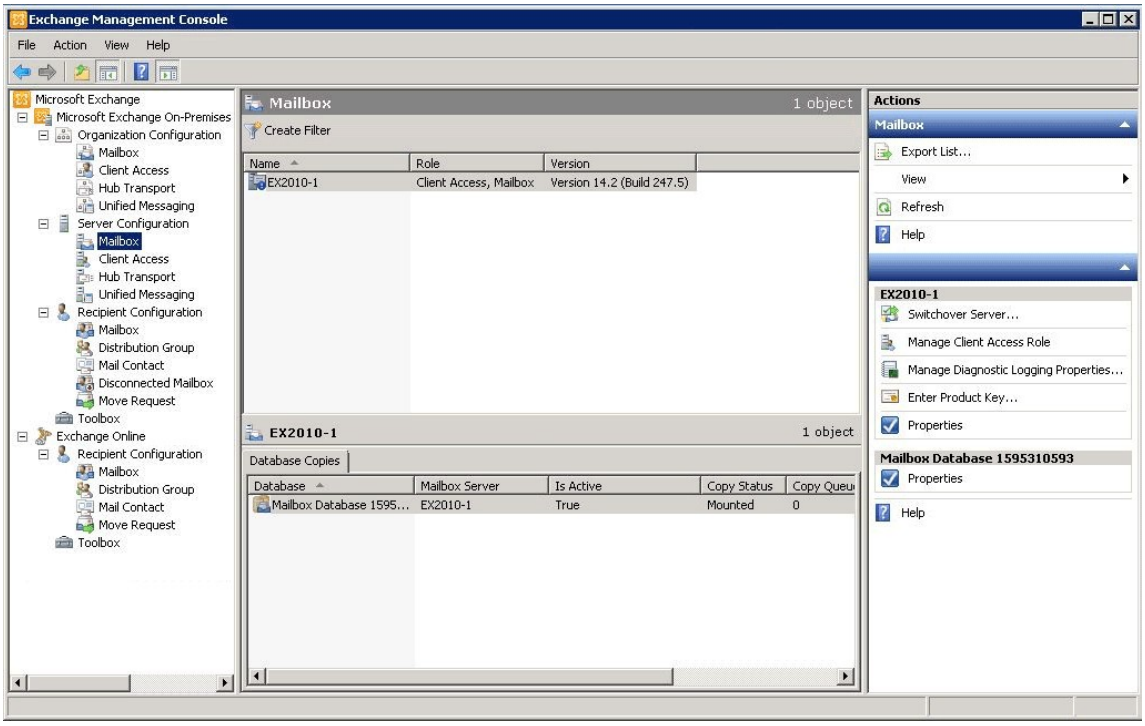
- Windows Server 2008 SP2 Standard and Enterprise
- Windows Server 2008 R2 Standard and Enterprise
- Windows 8

- Windows 7
- Windows Vista Service Pack (SP) 2

Adding the Exchange Online organization to the EMC is similar to adding another Exchange 2010 forest to the EMC. When the Exchange Online organization is added to the EMC, it appears as another node in the navigation tree. From there you can select the Exchange Online organization and configure some properties of Exchange Online recipient objects. To fully manage organization-level features and objects for the Exchange Online organization, you'll be redirected by the EMC and provided a link to connect to the EAC in the Office 365 management portal.

The following screenshot shows the on-premises organization and Exchange Online organization in the same console.

Exchange on-premises and Exchange Online organizations in the Exchange Management Console



Important:

You can't use the EMC to administer Exchange 2003 servers or recipients. For more information, see "Administering Exchange 2003" later in this topic.

Learn more at: Exchange Management Console

Exchange Management Shell

The Shell enables you to perform any task that the EMC does and some additional tasks that can only be performed in the Shell. The Shell is a collection of Windows PowerShell scripts and cmdlets that are installed on a computer when the Exchange 2010 management tools are installed. These scripts and cmdlets are only loaded when you open the Shell using the Exchange Management Shell icon. If you open Windows PowerShell directly, the Exchange scripts and cmdlets aren't loaded and you won't be able to manage your on-premises organization.

Note:
You can create a manual Windows PowerShell connection to your local on-premises organization, similar to how you manually connect to the Exchange Online organization below. However, we strongly recommend that you use the Exchange Management Shell icon to open the Shell to manage your on-premises hybrid servers.

When you open the Shell using the Exchange Management Shell icon on a computer that has the management tools installed, you can manage your on-premises organization. However, you can't manage the Exchange Online organization when you open the Shell using this icon. This is because opening the Shell using the Exchange Management Shell icon automatically connects you to a local hybrid server.

If you want to manage the Exchange Online organization using Windows PowerShell, you must open Windows PowerShell directly and not via the Exchange Management Shell icon. When you open Windows PowerShell, you can then manually specify where you want to connect. When you create a manual connection, you specify an administrator account in the Office 365 tenant organization, and then you run a command to create a connection. When the connection is established, the Exchange cmdlets you have permissions to run are made available to you.

Learn more at: Use Windows PowerShell

If you're new to the Shell, check out the following topic to learn the basics about how the Shell works, command syntax, and more.

Learn more at: Exchange Management Shell

You can't use the Shell to administer Exchange 2003 servers or recipients. For more information, see "Administering Exchange 2003" later in this topic.

Administering Exchange 2003

You can't use the EMC or the Shell to administer Exchange 2003 servers or recipients. To manage Exchange 2003 servers, use Exchange System Manager on a computer that has Exchange 2003 installed. To manage Exchange 2003 recipients, use Active Directory Users and Computers on a computer that has Exchange 2003 installed.

1.14.8.4 Understanding Edge Transport Servers in Exchange 2003 Hybrid Deployments

Understanding Edge Transport Servers in Exchange 2003 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

Edge Transport servers in Exchange 2010 are deployed in your organization's on-premises perimeter network. They're non-domain-joined computers that handle Internet-facing mail flow and act as an SMTP relay and smart host for Exchange servers in your internal network. In hybrid deployments, you have the option of deploying Edge Transport servers running Service Pack 3 (SP3) for Exchange 2010 if you don't want to expose internal hybrid Hub Transport servers directly to the Internet.

Learn more at: Overview of the Edge Transport Server Role

Adding an Edge Transport Server to a Hybrid Deployment

Deploying an Edge Transport server in your on-premises organization when you configure a hybrid deployment is an optional step. During the initial run of the Manage Hybrid Configuration wizard, the wizard requires that you select one or more Hub Transport servers. However, after the initial run of the wizard, you can add an Edge Transport server to your organization, configure it, run the Manage Hybrid Configuration wizard again, and then manually update the on-premises Send connectors and Edge Transport Receive connector to add it to the hybrid deployment.

When you add an Edge Transport server to your hybrid deployment, it communicates with Microsoft Exchange Online Protection (EOP) on behalf of the internal hybrid Hub Transport servers. The Edge Transport server acts as a relay between the on-premises hybrid Hub Transport server and EOP. All connection security previously handled by the hybrid Hub Transport server is handled by the Edge Transport server. Recipient lookup, compliance policies, and other message inspection, continue to be done on the hybrid Hub Transport servers.

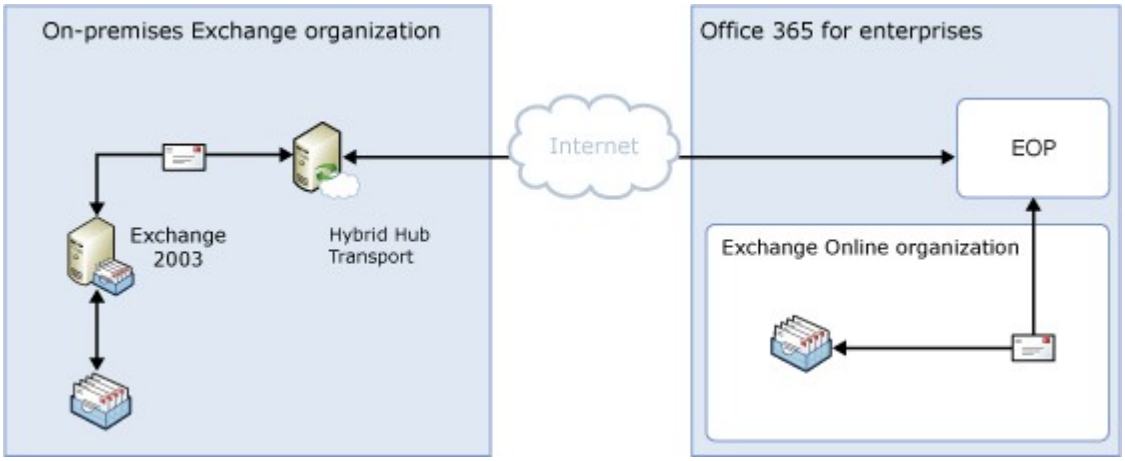
If you add an Edge Transport server to your hybrid deployment, you don't need to route mail sent between on-premises users and Internet recipients through it. Only messages sent between the on-premises and Exchange Online organizations will be routed through the Edge Transport server.

Mail Flow without an Edge Transport Server

The following process and diagram describe the path messages take between an on-premises organization and Exchange Online when there is no Edge Transport server deployed:

1. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from the Exchange 2003 server to a hybrid Hub Transport server.
2. The Hub Transport server sends the message directly to the Exchange Online EOP company.
3. EOP delivers the message to the Exchange Online organization.
4. Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

Mail flow in a hybrid deployment without an Edge Transport server deployed

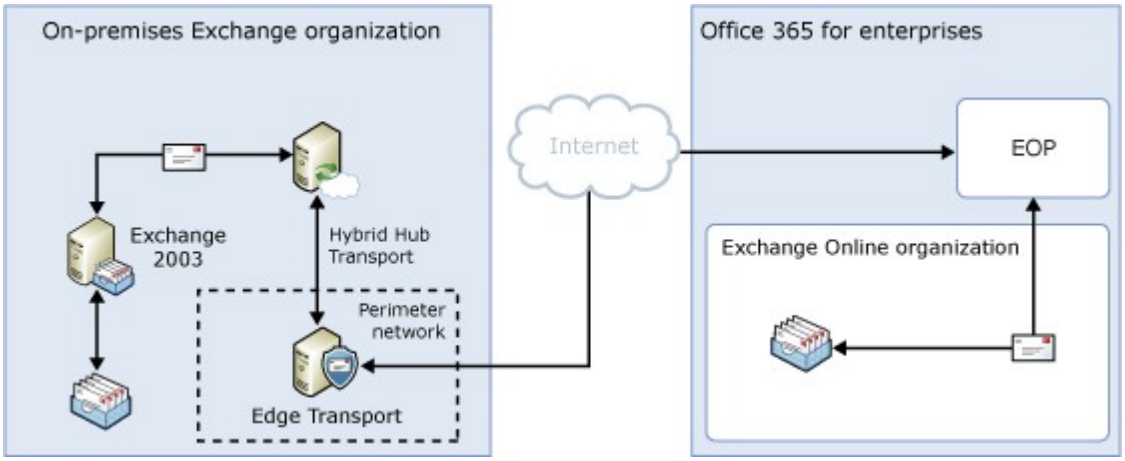


Mail Flow with an Edge Transport Server

The following diagram shows the path messages take between an on-premises organization and Exchange Online when there is an Edge Transport server deployed. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from the Exchange 2003 server:

1. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from the Exchange 2003 server to a hybrid Hub Transport server.
2. The Hub Transport server sends the message to an Edge Transport server.
3. The Edge Transport server sends the message to the Exchange Online EOP company.
4. EOP delivers the message to the Exchange Online organization.
5. Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

Mail flow in a hybrid deployment with an Edge Transport server deployed



1.14.8.5 Understanding Shared Free/Busy in Exchange 2003 Hybrid Deployments

Understanding Shared Free/Busy in Exchange 2003 Hybrid Deployments

Exchange Server 2010 > Hybrid Deployments > Hybrid Deployments with Exchange 2010 SP3 and Exchange 2003 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

Sharing free/busy (calendar availability) information between users located on-premises and in the Microsoft Exchange Online organization is one of the primary benefits of a hybrid deployment. Users in both organizations can view each other's calendars just as if they were located in the same physical organization. This makes scheduling meetings and resources easy and efficient.

Several components in a hybrid deployment are required to enable the shared free/busy feature in a Microsoft Exchange Server 2003 deployment:

- **Federation trust** Both the on-premises and Microsoft Office 365 service organizations need to have a federation trust established with the Microsoft Federation Gateway. A federation trust is a one-to-one relationship with the Microsoft Federation Gateway that defines parameters for your Exchange organization. The gateway uses these parameters when acting as a trust broker between your on-premises and Office 365 service organization to

exchange free/busy information between on-premises and Exchange Online organization users.
By default, a federation trust with the gateway is automatically configured for your Office 365 service organization when the account is created. The Manage Hybrid Configuration wizard automatically checks to see if there is an existing federation trust with the Microsoft Federation Gateway for the on-premises organization. If present, the existing federation trust is used to support the hybrid deployment. If not present, the wizard creates a federation trust for the on-premises organization with the Microsoft Federation Gateway. The wizard also adds any domains selected within the Manage Hybrid Configuration wizard to the on-premises organization federation trust.
Learn more at: Understanding Federated Delegation

- **Organization relationships** Organization relationships are needed for both the on-premises and Exchange Online organization and are configured automatically by the Manage Hybrid Configuration wizard. An organization relationship defines the level of free/busy information shared for an organization.
  By default, the free/busy data access sharing level is **Free/busy access with time, plus subject and location** for both the on-premises and Exchange Online organization relationships. If you want to modify the free/busy sharing access between your on-premises and Exchange Online organization users, you can manually configure the organization relationship access level after the Manage Hybrid Configuration wizard has completed.
  Learn more at: Understanding Federated Delegation
- **Hybrid Mailbox server** Exchange 2003 organizations must have a hybrid server with the Service Pack 3 (SP3) for Exchange 2010 Mailbox server role installed to support free/busy sharing between on-premises and Exchange Online mailboxes. Free/busy information for Exchange 2003 mailboxes is stored in public folders and the free/busy information in your existing public folders must be replicated to the hybrid Mailbox servers. Client requests for free/busy information are automatically directed to the hybrid Mailbox servers for processing for both on-premises and Exchange Online organization users after the hybrid deployment is configured by the Manage Hybrid Configuration wizard. To avoid a single point of failure for these public folder replicas, you should consider adding more than one hybrid Mailbox server to your on-premises organization for redundancy.

When configuring your organization for a hybrid deployment, configuring shared free/busy calendar access is automatically configured by the Manage Hybrid Configuration wizard in all scenarios. Creating a federation trust with the Microsoft Federation Gateway and configuring organization relationships for the on-premises and Exchange Online organization are hybrid deployment requirements. If you don't want to allow free/busy sharing between your on-premises and Exchange Online organization users in the hybrid deployment, you can manually disable free/busy sharing by using the Shell and the Set-HybridConfiguration cmdlet after the Manage Hybrid Configuration wizard has completed.

The hybrid deployment features shown in the following table have a dependency on federation trusts and organization relationships.

Messaging area	Feature
E-mail client	• Message tracking • MailTips • Multi-mailbox search
Transport	• Mailbox moves • Secure intra-organization message delivery
Compliance	• Exchange Online Archiving

1.14.8.6 Understanding Transport Options in Exchange 2003 Hybrid Deployments

Understanding Transport Options in Exchange 2003 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

In hybrid deployments, you can have mailboxes that reside in your on-premises organization and also in an Exchange Online organization. A critical component of making these two separate organizations appear as one combined organization to users and messages exchanged between them is hybrid transport. With hybrid transport, messages sent between recipients in either organization are authenticated, transferred using Transport Layer Security (TLS), and appear as "internal" to Exchange components such as transport rules, journaling, and anti-spam policies. Hybrid transport is automatically configured by the Manage Hybrid Configuration wizard in Service Pack 3 (SP3) for Exchange 2010.

For hybrid transport configuration to work with the Manage Hybrid Configuration wizard, the on-premises SMTP endpoint that accepts connections from Exchange Online Protection (EOP), which handles transport for the Exchange Online organization, must be an Exchange 2010 SP3 Hub Transport or Edge Transport server. Hybrid transport makes use of new features provided in Exchange 2010 SP3 to secure messages and make them appear as "internal." While an on-premises Exchange 2010 SP3 server is required for hybrid transport between the on-premises and Exchange Online organizations, you don't need to route the mail to and from on-premises mailboxes and Internet recipients through an Exchange 2010 server.

Important:

There can be no other SMTP hosts, services, or appliances between the on-premises Exchange 2010 SP3 Hub Transport or Edge Transport server and EOP. Information added to messages that enables hybrid transport features is removed when they pass through a non-Exchange 2010 SP3 server or SMTP host. This includes earlier versions of Exchange.
Hub Transport and Edge Transport servers must run Exchange 2010 SP3 to use the Manage Hybrid Deployment wizard for hybrid deployment configuration.

Inbound messages sent to recipients in both organizations from external Internet senders follow a common inbound route. Outbound messages sent from the organizations to external Internet recipients can either follow a common outbound route or can be sent via independent routes.

You'll need to choose how to route inbound and outbound mail when you configure your hybrid deployment. The route taken by inbound and outbound messages sent to and from recipients in the on-premises and Exchange Online organizations depends on the following:

- Do you want to route inbound Internet mail for both your on-premises and Exchange Online mailboxes through Microsoft Office 365 and EOP or through your on-premises organization?
  You can choose to route inbound Internet mail for both organizations through your on-premises organization or through EOP and the Exchange Online organization. The route that inbound messages for both organizations take depends on whether you enable centralized mail transport in your hybrid deployment.
- Do you want to route outbound mail to external recipients from your Exchange Online organization through your on-premises organization (centralized mail

transport), or do you want to route it directly to the Internet?
Known as centralized mail transport, you can route all mail from mailboxes in the Exchange Online organization through the on-premises organization before they're delivered to the Internet. This approach is helpful in compliance scenarios where all mail to and from the Internet must be processed by on-premises servers. Alternately, you can configure Exchange Online to deliver messages for external recipients directly to the Internet.

Note:
Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- Do you want to deploy an Edge Transport server in your on-premises organization?
  If you don't want to expose your domain-joined internal hybrid Hub Transport servers directly to the Internet, you can deploy Edge Transport servers in your perimeter network. For more information about adding an Edge Transport server to your hybrid deployment: see: Understanding Edge Transport Servers in Exchange 2003 Hybrid Deployments

Regardless of how you route messages to and from the Internet, all messages sent between the on-premises and Exchange Online organizations are sent using secure transport. For more information, see "Trusted Communication" later in this topic.

To learn more about how these options affect message routing in your organization, see Understanding Transport Routing in Exchange 2003 Hybrid Deployments.

Exchange Online Protection in Hybrid Deployments

EOP is an online service provided by Microsoft that's used by many companies to protect their on-premises organizations from viruses, spam, phishing scams, and policy violations. In Office 365, EOP is used to protect Exchange Online organizations from the same threats. When you sign up for Office 365, an EOP company is automatically created that's tied to your Exchange Online organization.

An EOP company contains several of the mail transport settings that can be configured for your Exchange Online organization. You can specify which SMTP domains must come from specific IP addresses, require a TLS and a Secure Sockets Layer (SSL) certificate, can bypass anti-spam filtering or compliance policies, and more. EOP is the front door to your Exchange Online organization. All messages, regardless of their origin, must pass through EOP before they reach mailboxes in your Exchange Online organization. And, all messages sent from your Exchange Online organization must go through EOP before they reach the Internet.

When you configure a hybrid deployment with the Manage Hybrid Configuration wizard, all transport settings are automatically configured in your on-premises organization and in the EOP company set up for your Exchange Online organization. The Manage Hybrid Configuration wizard configures all inbound and outbound connectors and other settings in this EOP company to secure messages sent between the on-premises and Exchange Online organizations and route messages to the right destination. If you want to configure custom transport settings for your Exchange Online organization, you'll configure them in this EOP company also.

Trusted Communication

To help protect recipients in both the on-premises and Exchange Online organizations, and to help ensure that messages sent between the organizations aren't intercepted and

read, transport between the on-premises organization and EOP is configured to use forced TLS. TLS transport uses Secure Sockets Layer (SSL) certificates provided by a trusted third-party Certificate Authority (CA). Messages between FOPE and the Exchange Online organization also use TLS.

When using forced TLS transport, the sending and receiving servers examine the certificate configured on the other server. The subject name, or one of the subject alternative names (SANs), configured on the certificates must match the FQDN that an administrator has explicitly specified on the other server. For example, if EOP is configured to accept and secure messages sent from the hybrid.contoso.com FQDN, the sending on-premises hybrid server must have an SSL certificate with hybrid.contoso.com in either the subject name or SAN. If this requirement isn't met, the connection is refused.

Note:

The FQDN used doesn't need to match the e-mail domain name of the recipients. The only requirement is that the FQDN in the certificate subject name or SAN must match the FQDN that the receiving or sending servers are configured to accept.

In addition to using TLS, messages between the organizations are treated as "internal". This approach allows messages to bypass anti-spam settings and other services.

Learn more about SSL certificates and domain security at: Understanding Certificate Requirements for Hybrid Deployments, Understanding TLS Certificates

1.14.8.7 Understanding Transport Routing in Exchange 2003 Hybrid Deployments

Understanding Transport Routing in Exchange 2003 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-29*

This topic discusses your routing options for inbound messages from the Internet and outbound messages to the Internet.

Note:

The examples in this topic don't include the addition of Edge Transport servers into the hybrid deployment. The routes messages take between the on-premises organization, the Exchange Online organization, and the Internet don't change with the addition of an Edge Transport server. The routing only changes within the on-premises organization. For more information about adding Edge Transport servers to a hybrid deployment, see Understanding Edge Transport Servers in Exchange 2003 Hybrid Deployments.

Inbound Messages from the Internet

As part of planning and configuring your hybrid deployment, you need to decide whether you want all messages from Internet senders to be routed through your on-premises organization or through the Exchange Online organization. All messages from Internet senders will initially be delivered to the organization you select and then routed according to where the recipient's mailbox is located. Whether you choose to have messages routed through your on-premises organization or the Exchange Online organization depends on various factors, including whether you want to apply compliance policies to all messages sent to both organizations, how many mailboxes are in each organization, and so on.

The path messages sent to recipients in your on-premises and Exchange Online organizations take depends on how you decide to configure your MX record in your hybrid deployment. The Manage Hybrid Configuration wizard doesn't configure the routing for inbound Internet messages for either the on-premises or Exchange Online organizations. You must manually configure your MX record if you want to change how your inbound Internet mail is delivered.

- If you keep your MX record pointed to your on-premises organization: All messages sent to any recipient in either organization will be routed through your on-premises organization first. A message addressed to a recipient that's located in Exchange Online will be routed first through your on-premises organization and then delivered to the recipient in Exchange Online. This route can be helpful for organizations where you have compliance policies that require messages sent to and from an organization be examined by a journaling solution. This route is also recommended if you have more recipients in your on-premises organization than in your Exchange Online organization.
- If you decide to change your MX record to point to the Microsoft Exchange Online Protection (EOP) service in Office 365: All messages sent to any recipient in either organization will be routed through the Exchange Online organization first. A message addressed to a recipient that's located in your on-premises organization will be routed first through your Exchange Online organization and then delivered to the recipient in your on-premises organization. This route is recommended if you have more recipients in your Exchange Online organization than in your on-premises organization.

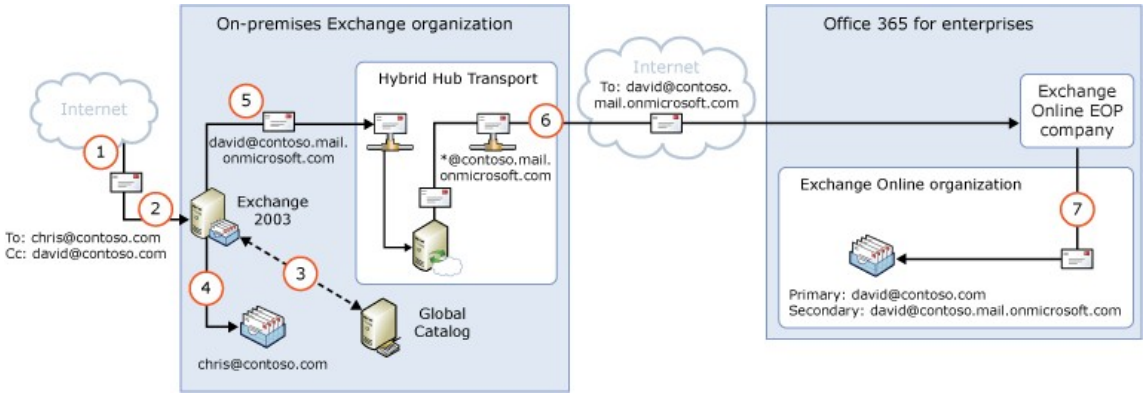
Read the section below that matches how you plan to route messages sent from Internet recipients to your on-premises and Exchange Online recipients.

Route Incoming Internet Messages Through Your On-Premises Organization

The following steps and diagram illustrate the inbound Internet message path that will occur in your hybrid deployment if you decide to keep your MX record pointed to your on-premises organization.

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2003 server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to the on-premises organization, the message is delivered to an Exchange 2003 server.
3. The Exchange 2003 server performs a lookup for each recipient using an on-premises global catalog server. Through the global catalog lookup, it determines that Chris's mailbox is located on the Exchange 2003 server while David's mailbox is located in the Exchange Online organization and has a hybrid routing address of david@contoso.mail.onmicrosoft.com.
4. The Exchange 2003 server splits the message into two copies. One copy of the message is delivered to Chris's mailbox.
5. The second copy of the message is sent through the routing group connector that's configured between the hybrid servers and the Exchange 2003 server.
6. A hybrid Hub Transport server sends the message to EOP, which receives messages sent to the Exchange Online organization, using a Send connector configured to use TLS.
7. EOP sends the message to the Exchange Online organization where the message is scanned for viruses and delivered to David's mailbox.

Route mail through the on-premises organization for both on-premises and Exchange Online organizations



Route Incoming Internet Messages Through the Exchange Online Organization

The following steps and diagrams illustrate the inbound message path that occur in your hybrid deployment if you decide to point your MX record to the EOP service in the Office 365 organization. The message path differs depending on whether you choose to enable centralized mail transport.

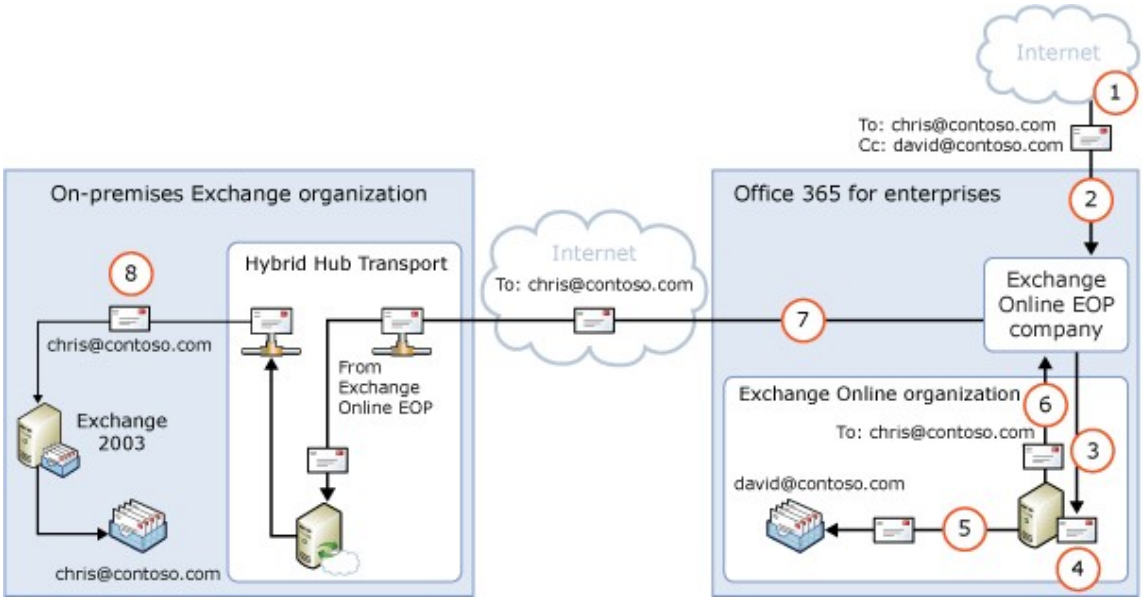
Important:

You may need to purchase EOP licenses for each on-premises mailbox that receives messages that are first delivered to EOP and then routed through the Exchange Online organization. Contact your Microsoft reseller for more information.

When centralized mail transport is *disabled* (default configuration), incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2003 server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to EOP, the message is delivered to EOP.
3. EOP routes the messages for both recipients to Exchange Online.
4. Exchange Online scans the messages for viruses and performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. Exchange Online splits the message into two copies. One copy of the message is delivered to David's mailbox.
6. The second copy is sent from Exchange Online back to EOP.
7. EOP sends the message to the hybrid Exchange 2010 Hub Transport servers in the on-premises organization.
8. A hybrid Hub Transport server sends the message through th routing group connector that’s configured between the hybrid servers and the Exchange 2003 server where it’s delivered to Chris's mailbox.

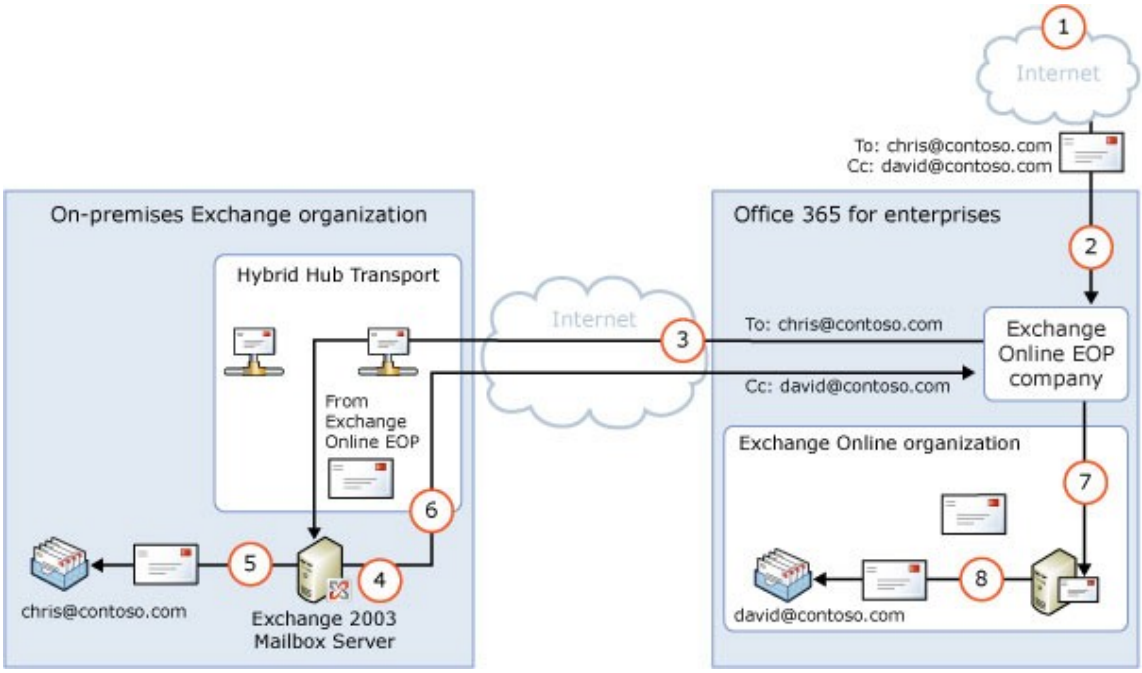
Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport disabled (default configuration)



When centralized mail transport is *enabled*, incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2003 server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to EOP, the message is delivered to EOP and scanned for viruses.
3. Since centralized mail transport is enabled, EOP routes the messages for both recipients to the on-premises hybrid Exchange 2010 Hub Transport server.
4. The hybrid Hub Transport server performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. The hybrid Hub Transport server splits the message into two copies. One copy of the message is delivered to Chris’s mailbox in the on-premises Exchange 2003 server.
6. The second copy is sent from the hybrid Hub Transport server back to EOP.
7. EOP sends the message to Exchange Online.
8. Exchange delivers the message to David's mailbox.

Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport enabled



Outbound Messages to the Internet

In addition to choosing how inbound messages addressed to recipients to your organizations are routed, you can also choose how outbound messages sent from Exchange Online recipients are routed. When you run the Hybrid Configuration wizard, you can select one of two options:

- **Enable centralized mail transport** Selecting this option routes outbound messages sent from the Exchange Online organization through your on-premises organization. Except for messages sent to other recipients in the same Exchange Online organization, all messages sent from recipients in the Exchange Online organization are sent through the on-premises organization. This enables you to apply compliance rules to these messages and any other processes or requirements that must be applied to all of your recipients, regardless of whether they're located in the Exchange Online organization or the on-premises organization.

  Note:
  Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- **Don’t enable centralized mail transport** Selected by default in the Manage Hybrid Configuration wizard, this option routes outbound messages sent from the Exchange Online organization directly to the Internet. Use this option if you don't need to apply any on-premises compliance policies or other processing rules to messages that are sent from recipients in the Exchange Online organization.

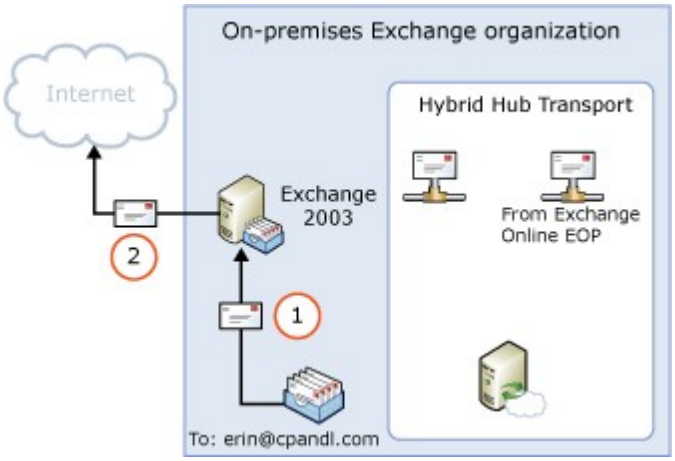
Messages sent from on-premises recipients are always sent to directly to Internet recipients using DNS regardless of which of the above choices you select in the Manage Hybrid Configuration wizard.

The following steps and diagram illustrate the outbound message path for messages sent from on-premises recipients.

1. Chris, who has a mailbox on the on-premises Exchange 2003 server, sends a message to an external Internet recipient, erin@cpandl.com.

2. The Exchange 2003 server looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

Messages from on-premises senders to Internet recipients



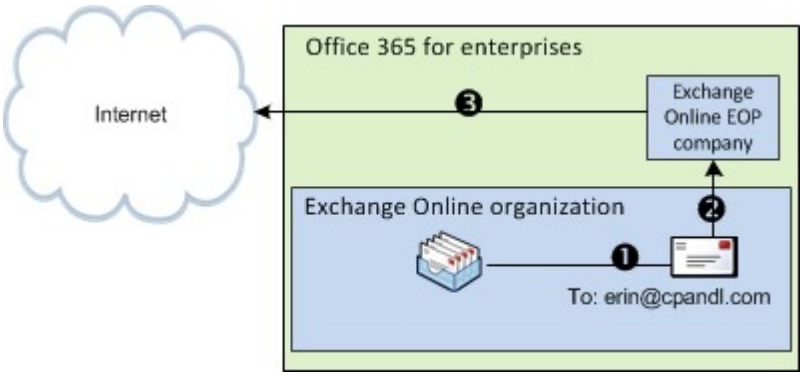
Read the section below that matches how you plan to route messages sent from recipients in the Exchange Online organization to Internet recipients.

Deliver Internet-bound Messages from Exchange Online using DNS (Centralized Mail Transport Disabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when **Enable centralized mail transport** is not selected in the Manage Hybrid Configuration wizard, which is the default configuration.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to the Exchange Online EOP company.
3. EOP looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

Mail from Exchange Online senders routed directly to the Internet with centralized mail transport disabled (default configuration)



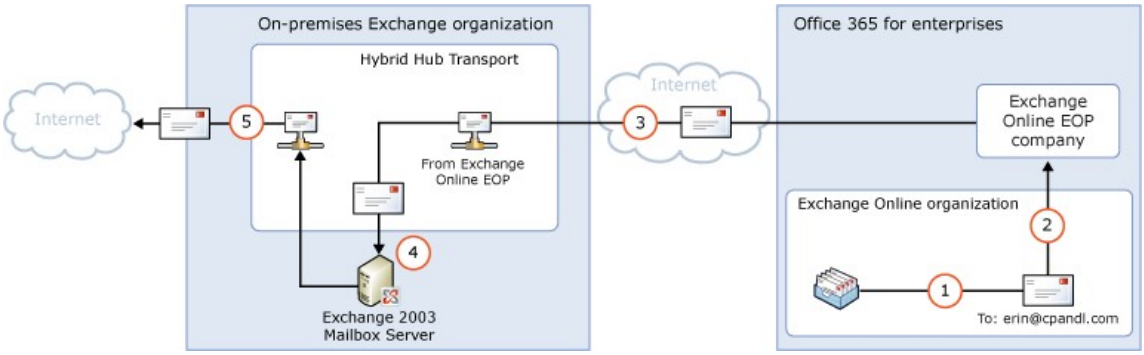
Route Internet-bound messages from Exchange Online Through Your on-Premises Organization (Centralized Mail Transport Enabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when you select

Enable centralized mail transport in the Manage Hybrid Configuration wizard.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to EOP.
3. EOP is configured to send all Internet-bound messages to an on-premises server, so the message is routed to a hybrid Hub Transport server. The message is sent using TLS.
4. An hybrid Hub Transport server performs compliance and any other processes configured by the administrator on David's message.
5. The hybrid Hub Transport server looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

Mail from Exchange Online senders routed through on-premises organization with centralized mail transport enabled



1.14.9 Hybrid Deployments with Exchange 2010 SP3 and Exchange 2007

Hybrid Deployments with Exchange 2010 SP3 and Exchange 2007

Exchange Server 2010 > Hybrid Deployments >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-01-28*

Understanding Hybrid Servers in Exchange 2007 Hybrid Deployments

Understanding Prerequisites for Exchange 2007 Hybrid Deployments

Understanding Hybrid Management in Exchange 2007 Hybrid Deployments

Understanding Edge Transport Servers in Exchange 2007 Hybrid Deployments

Understanding Shared Free/Busy in Exchange 2007 Hybrid Deployments

Understanding Transport Options in Exchange 2007 Hybrid Deployments

Understanding Transport Routing in Exchange 2007 Hybrid Deployments

Understanding IRM in Exchange 2007 Hybrid Deployments

1.14.9.1 Understanding Hybrid Servers in Exchange 2007 Hybrid Deployments

Understanding Hybrid Servers in Exchange 2007 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

When configuring a hybrid deployment, you have to install at least one hybrid server in your existing Microsoft Exchange organization. Hybrid servers are additional servers configured with Service Pack 3 (SP3) for Exchange Server 2010 server roles that coordinate communication between your existing Exchange 2007 organization and the Exchange Online organization. This communication includes message transport and messaging features between the on-premises and Exchange Online organizations. We highly recommend installing more than one hybrid server in your on-premises organization to help increase reliability and availability of hybrid deployment features.

Server Roles in a Hybrid Deployment

Here is a quick overview of the Exchange 2010 server roles in a hybrid deployment:

- **Client Access server role** The Client Access server role on a hybrid server provides essentially the same functionality typically provided by other Client Access servers in your Exchange 2007 organization with a few additions required to support a hybrid deployment. All client connectivity, including Outlook client access, Outlook Web App, and Outlook Anywhere goes through the hybrid Client Access server role. Organization relationship features between the on-premises and Exchange Online organizations, such as free/busy sharing, are also handled by the hybrid Client Access server role. Learn more at: Understanding Client Access
- **Hub Transport server role** The Hub Transport server role on a hybrid server handles all mail flow between the on-premises and Exchange Online organizations and between the on-premises organization and the Internet. It helps to secure transport communication between the on-premises and Exchange Online organizations, as well as handling transport rules, journaling policies, and message delivery to user mailboxes in a hybrid deployment. Learn more at: Overview of the Hub Transport Server Role

Depending on the hybrid deployment configuration that you want, a hybrid server requires one or more of the server roles to be installed on it:

- **Single hybrid server** If you choose to install a single hybrid server in your on-premises organization, you'll need to install the Client Access and Hub Transport server roles on the single hybrid server.
- **More than one hybrid server** If you choose to install more than one hybrid server in your on-premises organization, you can install the server roles on separate servers in your on-premises organization. For example, you could install one hybrid server that has the Client Access role installed and also install another hybrid server that has only the Hub Transport server role installed. However, the best practice and recommended hybrid server configuration is to install the Client Access and Hub Transport servers on *each* hybrid server deployed in your on-premises organization.

If you also decide to install the optional Exchange 2010 Mailbox server role in your hybrid deployment, you should add the Mailbox server role to each hybrid server that has the Client Access and Hub Transport server roles installed. Learn more about the Mailbox server role at: Overview of the Mailbox Server Role

Hybrid Server Functionality

A hybrid server provides several important functions for your on-premises organization in a hybrid deployment:

- **Federation** Hybrid servers enable you to create a federation trust for your on-premises organization with the Microsoft Federation Gateway. The Microsoft Federation Gateway is a free, cloud-based service offered by Microsoft that acts as the trust broker between your on-premises organization and the Office 365 tenant organization. Federation is a requirement for creating an organization relationship between the on-premises and the Exchange Online organizations.
  Learn more at: Understanding Federation
- **Organization relationships** Hybrid Client Access servers enable the creation of organization relationships between the on-premises and Exchange Online organizations. Organization relationships are required for many other services in a hybrid deployment, including calendar free/busy information sharing, message tracking, and mailbox moves between the on-premises and Exchange Online organizations.
  Learn more at: Understanding Federated Delegation
- **Message transport** Hybrid Hub Transport servers are responsible for message transport in a hybrid deployment. Using Send and Receive connectors, they replace the on-premises Exchange 2007 Hub Transport server as the connection endpoint for incoming external messages and also provide outbound message delivery to the Internet and the Exchange Online organization.
  Learn more at: Understanding Transport
- **Message transport security** Hybrid Hub Transport servers help to secure message communication between the on-premises and Exchange Online organizations by using the Domain Security functionality in Exchange 2010. Security can be increased by using mutual transport layer security authentication and encryption for message communications.
  Learn more at: Understanding Domain Security
- **Outlook Web App** Hybrid Client Access servers support configuring a single URL endpoint for external connections to on-premises and Exchange Online mailboxes. For on-premises mailboxes, hybrid Client Access servers are configured to automatically redirect user Outlook Web App requests to your Exchange 2007 Client Access server. For Exchange Online organization mailboxes, hybrid Client Access servers are configured to automatically display a link to the Outlook Web App endpoint on the Exchange Online organization.
- Learn more at: Understanding Outlook Web App

Hybrid Server Topology

A hybrid server is deployed much like an Exchange 2010 server would be deployed to your existing Exchange 2007 organization. Using the Client Access, Mailbox, and Hub Transport server roles, hybrid servers are responsible for many services for your on-premises organization that are currently provided by your existing Exchange 2007 servers. The following table describes briefly the changes in services after configuring a hybrid deployment.

Service	Before hybrid server deployment	After hybrid server deployment	Description
Message transport (inbound and outbound)	Exchange 2007 Client Access server	Hybrid Hub Transport server(s)	The MX (mail exchanger) record for the domain may be updated to point to hybrid Hub Transport

			servers.
Outlook Web App public URL	Exchange 2007 Client Access server	Hybrid Client Access server(s)	Hybrid Client Access servers redirect Outlook Web App requests to the publicly accessible endpoint on the Exchange 2007 Client Access server.

Hybrid Server Software

Service Pack 3 (SP3) for Exchange Server 2010 enables hybrid deployment functionality with the Hybrid Configuration wizards. You can use any Exchange 2010 SP3 media when installing the hybrid server.

Additionally, we recommend that you install future Update Rollups for Exchange 2010 SP3 on all your hybrid servers. Microsoft releases update rollup packages approximately every six to eight weeks. The rollup packages are available via Microsoft Update and the Microsoft Download Center. In the Search box on the Microsoft Download Center, type "Exchange 2010 SP3 update rollup" to find links to the rollup packages for Exchange 2010 SP3.

Download Exchange Server 2010 SP3 at: Exchange 2010 Service Pack 3 (SP3)

Find update rollup packages at: Microsoft Download Center

Important:
You need to provide an Exchange 2010 Hybrid Edition product key on the hybrid server when you configure a hybrid deployment with Office 365. To obtain a Hybrid Edition product key, contact Office 365 support.

1.14.9.2 Understanding Prerequisites for Exchange 2007 Hybrid Deployments

Understanding Prerequisites for Exchange 2007 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Before you can really start to use the Deployment Assistant, your system and servers must meet requirements. If they don't meet these requirements, you won't be able to complete the steps within the tool and you won't be able to configure a hybrid deployment between your on-premises Exchange 2007 and Exchange Online organizations. This topic provides information about the following:

- The Exchange Pre-Deployment Analyzer
- Permissions needed to install and manage Exchange 2010
- Requirements for directory servers, hardware, software, clients, and other elements, including:
  - Windows Server 2008 Service Pack 2 (SP2) or later or Windows Server 2008 R2 operating system prerequisites that are required for all Exchange 2010 server roles

- Language support for Exchange 2010
- The Exchange Management Shell, the command-line interface for Exchange 2010, and the Exchange Management Console, the GUI management tool for Exchange 2010

Note:
Before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Exchange Pre-Deployment Analyzer

You can use the Exchange Pre-Deployment Analyzer (ExPDA) to perform an overall topology readiness scan of your environment. This scan focuses on overall topology readiness and not the ability to run Exchange 2010 on the local computer. ExPDA provides a detailed report that will alert you if there are any issues within your organization, which could prevent you from deploying Exchange 2010. For example, ExPDA will notify you if you haven't deployed the minimum required Exchange service pack on all your Exchange servers. If your organization passes the ExPDA readiness scan, you can go ahead and use the Exchange Deployment Assistant.

To get ExPDA from the Microsoft Download Center, see: Exchange Pre-Deployment Analyzer

Permissions to Install and Manage Exchange 2010

Exchange 2010 requires different permissions to install and to manage your server roles. When you're installing Exchange 2010 servers in your organization, the account you use might not be the same account that you use for administering and managing your server roles. To manage your server roles, Exchange 2010 uses the Role Based Access Control (RBAC) permissions model.

Exchange 2010 uses RBAC to manage permissions on the Exchange 2010 hybrid server. With RBAC, you can control what resources administrators can configure and what features users can access. The RBAC model in Exchange 2010 is flexible and provides you with several ways to customize the default permissions.

RBAC has two primary ways of assigning permissions to users in your organization, depending on whether the user is an administrator or specialist user, or an end-user: management role groups and management role assignment policies. Each method associates users with the permissions they need to perform their jobs. The following sections list the tasks found in the Deployment Assistant and the permissions required to complete the task.

Note:
Some features may require that you have local administrator permissions on the server you want to manage. To manage these features, you must be a member of the Local Administrators group on that server.

Installation Permissions

By default, the account that's used to install Exchange 2010 in the organization is added as a member of the Organization Management role group.

When you install the first hybrid server into your Exchange 2007 organization, Exchange Setup will prepare your Active Directory schema if you have the correct permissions. If you want to separate your Active Directory schema preparation from a hybrid server installation, see: Prepare Active Directory and Domains

For information about how to add permissions, see: Add Members to a Role Group

The following permissions are required to install the hybrid server in your organization:

- Local Administrator on the server on which Exchange 2010 will be installed
- Enterprise Administrator in the Active Directory forest where Exchange 2010 will be installed
- Schema Administrator in the Active Directory forest where Exchange 2010 will be installed

Exchange Management Permissions

The table below lists the configuration permissions that you need to successfully use the Deployment Assistant and the Hybrid Configuration wizards. Some tasks need to be performed only in the on-premises organization while some tasks also need to be performed in the Office 365 tenant organization. If a task needs to be performed in the Office 365 tenant organization, you must ensure that you have the required permissions in that organization. Permissions in the on-premises organization aren't replicated to the Office 365 tenant organization.

Note:

The user account used to create the Office 365 tenant organization has all the permissions required to perform the tasks in this checklist.

Learn more at: Understanding Hybrid Deployment Permissions with Exchange 2010 SP3

Some procedures require you to perform tasks on your Exchange 2007 servers. For information about how to manage permissions in an organization with Exchange 2007 and Exchange 2010 installed, see: Understanding Permissions Coexistence with Exchange 2007

Task	Permissions required	On-premises or Office 365 tenant organization
Import digital certificates	Local Administrator	On-premises organization
Configure settings on virtual directories	Server Management	On-premises organization
Configure virtual directories	Organization Management Server Management	On-premises organization
Create accepted domains	Organization Management	On-premises and Office 365 tenant organization
Create and modify Send and Receive connectors	Organization Management	On-premises organization
Create routing group connectors	Organization Management Server Management	On-premises organization
Create a federation trust	Organization Management	On-premises organization
Create organization relationships	Organization Management	On-premises and Exchange Online organization
Configure Mailbox Replication Service (MRS) proxy	Local Administrator	On-premises organization
Move mailboxes	Organization Management	On-premises and Exchange Online organization

	Recipient Management	
Configure Exchange 2007 authentication	Local Administrator	On-premises organization
Configure Exchange 2007 e-mail address policies	Exchange Administrator	On-premises organization

Directory Servers

Here are the requirements for the directory servers in your organization:

- **Schema master** The latest 32-bit or 64-bit edition of the Windows Server 2003 SP2 Standard or Enterprise operating system or the Windows Server 2008 Standard or Enterprise operating system.
- **Global catalog server** In every Active Directory site where you plan to install Exchange 2010, you must have at least one global catalog server that is either the latest 32-bit or 64-bit edition of: Windows Server 2003 SP2 Standard or Enterprise; Windows Server 2008 Standard or Enterprise; or Windows Server 2008 R2 Standard or Enterprise.
- **Active Directory Forest** The Active Directory forest must be Windows Server 2003 forest functional mode or higher.
- **Domain Controller** You must have the latest 32-bit or 64-bit Windows Server 2003 Standard Edition or Enterprise Edition with Service Pack 2 (SP2) operating system or the latest 32-bit or 64-bit edition of the Windows Server 2008 Standard or Enterprise operating system or the Windows Server 2008 R2 Standard or Enterprise operating system.

Hardware

The recommended hardware requirements for Exchange 2010 servers vary depending on several factors including the server role(s) that are installed and the anticipated load that will be placed on the servers.

- **Processor** x64 architecture-based computer with processor that supports 64-bit architecture
- **Memory** Minimum 4GB with a recommended maximum of 2GB per core (8GB minimum). Learn more at: Understanding Memory Configurations and Exchange Performance
- **Disk space** At least 1.2 GB on the drive on which you install Exchange and additional 200 MB of available space on the system drive.
- **Drive** DVD-ROM drive, local or network accessible
- **File format** Disk partitions formatted as NTFS file systems

Operating System

Here are the supported operating systems for Exchange 2010:

- 64-bit edition of Windows Server 2008 Standard Service Pack 2
- 64-bit edition of Windows Server 2008 Enterprise Service Pack 2
- 64-bit edition of Windows Server 2008 Standard R2
- 64-bit edition of Windows Server 2008 Enterprise R2

Exchange 2010 Management tools can use the operating systems listed above plus:

- 64-bit edition of Windows Vista
- 64-bit edition of Windows 7

Install Hotfixes for Windows Server 2008 SP2

The following hotfixes are required for Windows Server 2008 SP2:

- Install the update described in Microsoft Knowledge Base article 977624, AD RMS clients do not authenticate federated identity providers in Windows Server 2008 or in Windows Vista. Without this update, Active Directory Rights Management Services (AD RMS) features may stop working.
- Install the update described in Knowledge Base article 979744, A .NET Framework 2.0-based Multi-AppDomain application stops responding when you run the application.
- Install the update described in Knowledge Base article 979917, Two issues occur when you deploy an ASP.NET 2.0-based application on a server that is running IIS 7.0 or IIS 7.5 in Integrated mode. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB979917 - QFE for Sharepoint issues - Perf Counter fix & User Impersonation.
  - For the available downloads, see KB979917 - QFE for Sharepoint issues - Perf Counter fix & User Impersonation.
- Install the update described in Knowledge Base article 973136, FIX: ArgumentNullException exception error message when a .NET Framework 2.0 SP2-based application tries to process a response with zero-length content to an asynchronous ASP.NET Web service request: "Value cannot be null".
- Install the update described in Knowledge Base article 977592, RPC over HTTP clients cannot connect to the Windows Server 2008 RPC over HTTP servers that have RPC load balancing enabled.

Install Hotfixes for Windows Server 2008 R2

The following hotfixes are required for Windows Server 2008 R2:

Important:

The following hotfixes only apply to Windows Server 2008 R2 RTM. If you're installing Exchange on Windows Server 2008 R2 SP1, you don't need to apply these hotfixes.

- Install the update described in Knowledge Base article 979099, An update is available to remove the application manifest expiry feature from AD RMS clients. Without this update, the AD RMS features may stop working.
- Install the update described in Knowledge Base article 979744, A .NET Framework 2.0-based Multi-AppDomain application stops responding when you run the application.
- Install the update described in Knowledge Base article 983440, An ASP.NET 2.0 hotfix rollup package is available for Windows 7 and for Windows Server 2008 R2. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB983440 - Win7 rollup package (PR for QFE 810219).
  - For the available downloads, see KB983440 - Win7 rollup package (PR for QFE 810219).
- Install the update described in Knowledge Base article 977020, FIX: An application that is based on the Microsoft .NET Framework 2.0 Service Pack 2 and that invokes a Web service call asynchronously throws an exception on a computer that is running Windows 7.

Install Hotfixes for Windows 7 and Windows Vista

The following hotfixes are required for Windows 7 and Windows Vista computers where you install the Exchange Management Console

- Install the update described in Knowledge Base article 977020, FIX: An application that is based on the Microsoft .NET Framework 2.0 Service Pack 2 and that invokes a Web service call asynchronously throws an exception on a computer that is running Windows 7.
- Install the update described in Knowledge Base article 983440, An ASP.NET 2.0 hotfix rollup package is available for Windows 7 and for Windows Server 2008 R2. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB983440 - Win7 rollup package (PR for QFE 810219).

- For the available downloads, see KB983440 - Win7 rollup package (PR for QFE 810219).

Install the Windows Server 2008 SP2 prerequisites

1. Install the Microsoft Filter Pack. For details, see: 2007 Office System Converter: Microsoft Filter Pack
2. Open an elevated command prompt, navigate to the Scripts folder on the Exchange 2010 installation media and use the following command to install the necessary operating system components:

```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

Install the Exchange 2010 SP1 Hotfixes for Windows Server 2008 SP2

The following hotfix is required for Windows Server 2008 SP2 and must be installed after the operating system prerequisites have been installed:

- Install the hotfix described in Knowledge Base article 982867, WCF services that are hosted by computers together with a NLB fail in .NET Framework 3.5 SP1. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.
  - For the available downloads, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.

After installing the preceding prerequisites and hotfix, and before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Install the Windows Server 2008 R2 prerequisites

1. Install the Microsoft Filter Pack. For details, see: 2007 Office System Converter: Microsoft Filter Pack
2. On the Start Menu, navigate to **All Programs**, then **Accessories**, then **Windows PowerShell**. Open an elevated Windows PowerShell console, and run the following command:

```
Import-Module ServerManager
```

3. Use the **Add-WindowsFeature** cmdlet to install the necessary operating system components using the following command:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,W
```

4. After the system has restarted, log on as an administrator, open an elevated Windows PowerShell console, and configure the Net.Tcp Port Sharing Service for Automatic startup by running the following command:

```
Set-Service NetTcpPortSharing -StartupType Automatic
```

Install the Exchange 2010 SP1 Hotfixes for Windows Server 2008 R2

The following hotfix is required for Windows Server 2008 R2 and must be installed after the operating system prerequisites have been installed:

- Install the hotfix described in Knowledge Base article 982867, WCF services that are hosted by computers together with a NLB fail in .NET Framework 3.5 SP1. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.
  - For the available downloads, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.

After installing the preceding prerequisites and hotfix, and before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Windows Management Framework

- Windows PowerShell V2.0
- Windows Remote Management V2.0
- .NET Framework 3.5 SP1
- Internet Information Services (IIS)

Language Support

An Exchange 2010 SP2 language pack contains the necessary resources for a supported Exchange language. Language packs are installed automatically during deployment of Exchange 2010 SP2. Client and server language packs come grouped into a single bundle containing both client and server resource and support files. There are no performance issues with installing all the languages because they're just stored when not in use.

Learn more at: Exchange 2010 Language Support

Exchange Management Shell

The Exchange Management Shell, built on Windows PowerShell technology, provides a powerful command-line interface for Exchange 2010 that enables automation of administrative tasks.

With the Shell, you can manage every aspect of Exchange 2010; the Shell can perform every task that can be performed by the Exchange Management Console (EMC) and the Exchange Control Panel (ECP) in addition to tasks that can't be performed in those interfaces. In fact, when a task is performed in the EMC or the ECP, those interfaces use the Shell to perform the task.

Learn more at: Overview of Exchange Management Shell

Exchange Management Console

The Exchange Management Console (EMC) is a Microsoft Management Console (MMC) 3.0-based tool that provides you with a GUI to manage the configuration of your Exchange 2010 organization. You can also add the EMC snap-in to custom MMC-based tools.

Learn more at: Exchange Management Console

1.14.9.3 Understanding Hybrid Management in Exchange 2007 Hybrid Deployments

Understanding Hybrid Management in Exchange 2007 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-02-01*

Both your on-premises organization and the Exchange Online organization are based on Microsoft Exchange. In particular, hybrid servers in your on-premises organization are based on Microsoft Exchange Server 2010 and the Exchange Online organization

Exchange servers are based on Exchange Server 2013. Service Pack 3 (SP3) for Exchange 2010 enables hybrid features to function correctly between these two types of hybrid deployment servers.

When you install a hybrid server, Exchange 2010 management tools are automatically installed on the server. You'll use the management tools to configure and manage both the hybrid server(s) and some recipient management features for the Exchange Online organization. These tools include the Exchange Management Console (EMC), a graphical administrative interface, and the Exchange Management Shell, a Windows PowerShell-based command-line interface. You'll also use the Exchange Administration Center (EAC) in the Exchange Online section of the Office 365 management portal to manage most of the properties of the Exchange Online recipients and organization.

Exchange Management Console

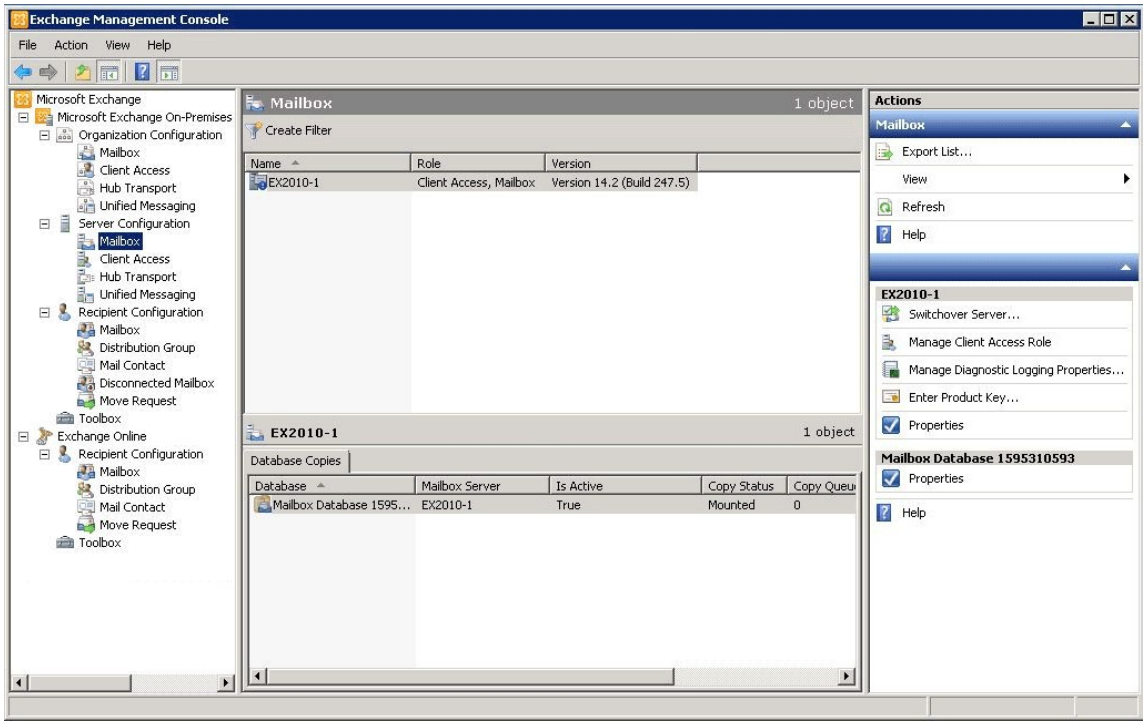
The EMC enables you to perform many deployment tasks and most common day-to-day administrative tasks. Additionally, the EMC allows you to administer both the on-premises hybrid servers and some recipient management features for mailboxes in the Exchange Online organization. It's installed by default on every Exchange 2010 server, but you can also install it on a computer running any of the following 64-bit operating systems:

- Windows Server 2008 SP2 Standard and Enterprise
- Windows Server 2008 R2 Standard and Enterprise
- Windows 8
- Windows 7
- Windows Vista Service Pack (SP) 2

Adding the Exchange Online organization to the EMC is similar to adding another Exchange 2010 forest to the EMC. When the Exchange Online organization is added to the EMC, it appears as another node in the navigation tree. From there you can select the Exchange Online organization and configure some properties of Exchange Online recipient objects. To fully manage organization-level features and objects for the Exchange Online organization, you'll be redirected by the EMC and provided a link to connect to the EAC in the Office 365 management portal.

The following screenshot shows the on-premises organization and Exchange Online organization in the same console.

Exchange on-premises and Exchange Online organizations in the Exchange Management Console



Learn more at: Exchange Management Console

Exchange Management Shell

The Shell enables you to perform any task that the EMC does and some additional tasks that can only be performed in the Shell. The Shell is a collection of Windows PowerShell scripts and cmdlets that are installed on a computer when the Exchange 2010 management tools are installed. These scripts and cmdlets are only loaded when you open the Shell using the Exchange Management Shell icon. If you open Windows PowerShell directly, the Exchange scripts and cmdlets aren't loaded and you won't be able to manage your on-premises organization.

Note:

You can create a manual Windows PowerShell connection to your local on-premises organization, similar to how you manually connect to the Exchange Online organization below. However, we strongly recommend that you use the Exchange Management Shell icon to open the Shell to manage your on-premises hybrid servers.

When you open the Shell using the Exchange Management Shell icon on a computer that has the management tools installed, you can manage your on-premises organization. However, you can't manage the Exchange Online organization when you open the Shell using this icon. This is because opening the Shell using the Exchange Management Shell icon automatically connects you to a local hybrid server.

If you want to manage the Exchange Online organization using Windows PowerShell, you must open Windows PowerShell directly and not via the Exchange Management Shell icon. When you open Windows PowerShell, you can then manually specify where you want to connect. When you create a manual connection, you specify an administrator account in the Office 365 tenant organization, and then you run a command to create a connection. When the connection is established, the Exchange cmdlets you have permissions to run are made available to you.

Learn more at: Use Windows PowerShell

If you're new to the Shell, check out the following topic to learn the basics about how the Shell works, command syntax, and more.

Learn more at: Exchange Management Shell

1.14.9.4 Understanding Edge Transport Servers in Exchange 2007 Hybrid Deployments

Understanding Edge Transport Servers in Exchange 2007 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

Edge Transport servers in Exchange 2010 are deployed in your organization's on-premises perimeter network. They're non-domain-joined computers that handle Internet-facing mail flow and act as an SMTP relay and smart host for Exchange servers in your internal network. In hybrid deployments, you have the option of deploying Edge Transport servers running Service Pack 3 (SP3) for Exchange 2010 if you don't want to expose internal hybrid Hub Transport servers directly to the Internet. If you have Exchange 2007 Edge Transport servers and want to use them for hybrid transport, you need to upgrade them to Exchange 2010 SP2.

Learn more at: Overview of the Edge Transport Server Role

Exchange 2007 Edge Transport Servers

Messages routed between on-premises and Exchange Online organizations require that Exchange Online Protection (EOP), on behalf of Exchange Online, connects directly to on-premises Hub Transport or Edge Transport servers that run Exchange 2010 SP2. If you've deployed Exchange 2007 Edge Transport servers, you must upgrade the servers you want to use for hybrid transport to Exchange 2010 SP3. Only the Edge Transport servers that handle hybrid transport between the on-premises organization and Exchange Online need to be upgraded to Exchange 2010 SP3. If you have other Edge Transport servers in other locations that won't handle hybrid transport, they don't need to be upgraded to Exchange 2010 SP3. If, in the future, you want EOP to connect to additional Edge Transport servers for hybrid transport, they must be upgraded to Exchange 2010 SP3.

Important:

If you keep Exchange 2007 Edge Transport servers in your organization, make sure that EOP connects to an on-premises Exchange 2010 SP3 Hub Transport or Edge Transport server for hybrid transport. If EOP connects to a server running a version other than Exchange 2010 SP3, messages may not be handled correctly. For more information, see: Understanding Transport Options in Exchange 2007 Hybrid Deployments

Upgrading an existing Exchange 2007 Edge Transport server isn't covered in the Exchange Server Deployment Assistant. For more information about upgrading an Edge Transport server from Exchange 2007 to Exchange 2010 SP3, see: Upgrade from Exchange 2007 Transport

Adding an Edge Transport Server to a

Hybrid Deployment

Deploying an Edge Transport server in your on-premises organization when you configure a hybrid deployment is an optional step. During the initial run of the Manage Hybrid Configuration wizard, the wizard requires that you select one or more Hub Transport servers. However, after the initial run of the wizard, you can add an Edge Transport server to your organization, configure it, run the Manage Hybrid Configuration wizard again, and then manually update the on-premises Send connectors and Edge Transport Receive connector to add it to the hybrid deployment.

When you add an Edge Transport server to your hybrid deployment, it communicates with EOP on behalf of the internal hybrid Hub Transport servers. The Edge Transport server acts as a relay between the on-premises hybrid Hub Transport server and EOP. All connection security previously handled by the hybrid Hub Transport server is handled by the Edge Transport server. Recipient lookup, compliance policies, and other message inspection, continue to be done on the hybrid Hub Transport servers.

If you add an Edge Transport server to your hybrid deployment, you don't need to route mail sent between on-premises users and Internet recipients through it. Only messages sent between the on-premises and Exchange Online organizations will be routed through the Edge Transport server.

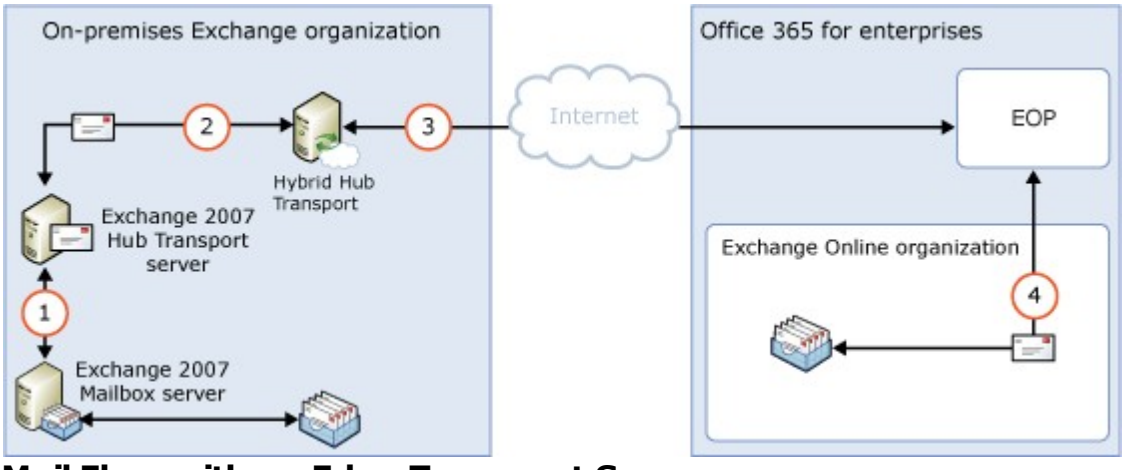
Mail Flow without an Edge Transport Server

The following process and diagram describe the path messages take between an on-premises organization and Exchange Online when there is no Edge Transport server deployed:

1. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from an Exchange 2007 Mailbox server to an Exchange 2007 Hub Transport server.
2. The Exchange 2007 Hub Transport server sends the message to an Exchange 2010 hybrid Hub Transport server.
3. The Hub Transport server sends the message directly to the Exchange Online EOP company.
4. EOP delivers the message to the Exchange Online organization.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

Mail flow in a hybrid deployment without an Edge Transport server deployed



Mail Flow with an Edge Transport Server

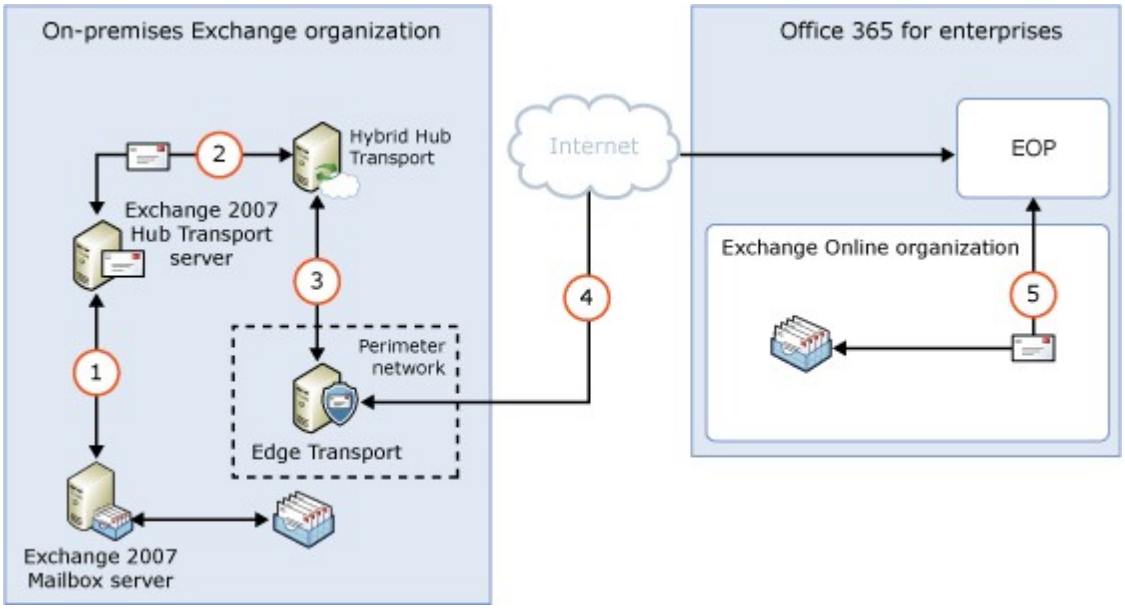
The following diagram shows the path messages take between an on-premises organization and Exchange Online when there is an Edge Transport server deployed.

Messages from the on-premises organization to recipients in the Exchange Online organization are sent from the Exchange 2007 server:

1. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from an Exchange 2007 Mailbox server to an Exchange 2007 Hub Transport server.
2. The Exchange 2007 Hub Transport server sends the message to an Exchange 2010 hybrid Hub Transport server.
3. The hybrid Hub Transport server sends the message to an Exchange 2010 Edge Transport server.
4. The Edge Transport server sends the message to the Exchange Online EOP company.
5. EOP delivers the message to the Exchange Online organization.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

Mail flow in a hybrid deployment with an Edge Transport server deployed



1.14.9.5 Understanding Shared Free/Busy in Exchange 2007 Hybrid Deployments

Understanding Shared Free/Busy in Exchange 2007 Hybrid Deployments

Exchange Server 2010 > Hybrid Deployments > Hybrid Deployments with Exchange 2010 SP3 and Exchange 2007 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-04-05*

Sharing free/busy (calendar availability) information between users located on-premises and in the Exchange Online organization is one of the primary benefits of a hybrid deployment. Users in both organizations can view each other's calendars just as if they were located in the same physical organization. This makes scheduling meetings and resources easy and efficient.

Several components in a hybrid deployment are required to enable the shared free/busy

feature in an Exchange 2007 deployment:

- **Federation trust** Both the on-premises and Microsoft Office 365 service organizations need to have a federation trust established with the Microsoft Federation Gateway. A federation trust is a one-to-one relationship with the Microsoft Federation Gateway that defines parameters for your Exchange organization. The gateway uses these parameters when acting as a trust broker between your on-premises and Office 365 service organization to exchange free/busy information between on-premises and Exchange Online organization users.
  By default, a federation trust with the gateway is automatically configured for your Office 365 service organization when the account is created. The Manage Hybrid Configuration wizard automatically checks to see if there is an existing federation trust with the Microsoft Federation Gateway for the on-premises organization. If present, the existing federation trust is used to support the hybrid deployment. If not present, the wizard creates a federation trust for the on-premises organization with the Microsoft Federation Gateway. The wizard also adds any domains selected within the Manage Hybrid Configuration wizard to the on-premises organization federation trust.
  Learn more at: Understanding Federated Delegation
- **Organization relationships** Organization relationships are needed for both the on-premises and Exchange Online organization and are configured automatically by the Manage Hybrid Configuration wizard. An organization relationship defines the level of free/busy information shared for an organization.
  By default, the free/busy data access sharing level is **Free/busy access with time, plus subject and location** for both the on-premises and Exchange Online organization relationships. If you want to modify the free/busy sharing access between your on-premises and Exchange Online organization users, you can manually configure the organization relationship access level after the Manage Hybrid Configuration wizard has completed.
  Learn more at: Understanding Federated Delegation

When configuring your organization for a hybrid deployment, configuring shared free/busy calendar access is automatically configured by the Manage Hybrid Configuration wizard in all scenarios. Creating a federation trust with the Microsoft Federation Gateway and configuring organization relationships for the on-premises and Exchange Online organization are hybrid deployment requirements. If you don't want to allow free/busy sharing between your on-premises and Exchange Online organization users in the hybrid deployment, you can manually disable free/busy sharing by using the Shell and the Set-HybridConfiguration cmdlet after the Manage Hybrid Configuration wizard has completed.

The hybrid deployment features shown in the following table have a dependency on federation trusts and organization relationships.

Messaging area	Feature
E-mail client	• Message tracking • MailTips • Multi-mailbox search
Transport	• Mailbox moves • Secure intra-organization message delivery
Compliance	• Exchange Online Archiving

1.14.9.6 Understanding Transport Options in Exchange 2007 Hybrid Deployments

Understanding Transport Options in Exchange 2007 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

In hybrid deployments, you can have mailboxes that reside in your on-premises organization and also in an Exchange Online organization. A critical component of making these two separate organizations appear as one combined organization to users and messages exchanged between them is hybrid transport. With hybrid transport, messages sent between recipients in either organization are authenticated, transferred using Transport Layer Security (TLS), and appear as "internal" to Exchange components such as transport rules, journaling, and anti-spam policies. Hybrid transport is automatically configured by the Manage Hybrid Configuration wizard in Service Pack 3 (SP3) for Exchange 2010.

For hybrid transport configuration to work with the Manage Hybrid Configuration wizard, the on-premises SMTP endpoint that accepts connections from Exchange Online Protection (EOP), which handles transport for the Exchange Online organization, must be an Exchange 2010 SP3 Hub Transport or Edge Transport server. Hybrid transport makes use of new features provided in Exchange 2010 SP3 to secure messages and make them appear as "internal." While an on-premises Exchange 2010 SP3 server is required for hybrid transport between the on-premises and Exchange Online organizations, you don't need to route the mail to and from on-premises mailboxes and Internet recipients through an Exchange 2010 server.

Important:

There can be no other SMTP hosts, services, or appliances between the on-premises Exchange 2010 SP3 Hub Transport or Edge Transport server and EOP. Information added to messages that enables hybrid transport features is removed when they pass through a non-Exchange 2010 SP3 server or SMTP host. This includes earlier versions of Exchange. If you have Exchange 2007 Edge Transport servers deployed in your organization, and you want to use them for hybrid transport, they must be upgraded to Exchange 2010 SP3.
Hub Transport and Edge Transport servers must run Exchange 2010 SP3 to use the Manage Hybrid Deployment wizard for hybrid deployment configuration.

Inbound messages sent to recipients in both organizations from external Internet senders follow a common inbound route. Outbound messages sent from the organizations to external Internet recipients can either follow a common outbound route or can be sent via independent routes.

You'll need to choose how to route inbound and outbound mail when you configure your hybrid deployment. The route taken by inbound and outbound messages sent to and from recipients in the on-premises and Exchange Online organizations depends on the following:

- Do you want to route inbound Internet mail for both your on-premises and Exchange Online mailboxes through Microsoft Office 365 and EOP or through your on-premises organization?
  You can choose to route inbound Internet mail for both organizations through your on-premises organization or through EOP and the Exchange Online organization. The route that inbound messages for both organizations take depends on whether you enable centralized mail transport in your hybrid deployment.

- Do you want to route outbound mail to external recipients from your Exchange Online organization through your on-premises organization (centralized mail transport), or do you want to route it directly to the Internet?
  Known as centralized mail transport, you can route all mail from mailboxes in the Exchange Online organization through the on-premises organization before they're delivered to the Internet. This approach is helpful in compliance scenarios where all mail to and from the Internet must be processed by on-premises servers. Alternately, you can configure Exchange Online to deliver messages for external recipients directly to the Internet.

  Note:
  Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- Do you want to deploy an Edge Transport server in your on-premises organization?
  If you don't want to expose your domain-joined internal hybrid Hub Transport servers directly to the Internet, you can deploy Edge Transport servers in your perimeter network. For more information about adding an Edge Transport server to your hybrid deployment: see: Understanding Edge Transport Servers in Exchange 2007 Hybrid Deployments

Regardless of how you route messages to and from the Internet, all messages sent between the on-premises and Exchange Online organizations are sent using secure transport. For more information, see "Trusted Communication" later in this topic.

To learn more about how these options affect message routing in your organization, see Understanding Transport Routing in Exchange 2007 Hybrid Deployments.

Exchange Online Protection in Hybrid Deployments

EOP is an online service provided by Microsoft that's used by many companies to protect their on-premises organizations from viruses, spam, phishing scams, and policy violations. In Office 365, EOP is used to protect Exchange Online organizations from the same threats. When you sign up for Office 365, an EOP company is automatically created that's tied to your Exchange Online organization.

An EOP company contains several of the mail transport settings that can be configured for your Exchange Online organization. You can specify which SMTP domains must come from specific IP addresses, require a TLS and a Secure Sockets Layer (SSL) certificate, can bypass anti-spam filtering or compliance policies, and more. FOPE is the front door to your Exchange Online organization. All messages, regardless of their origin, must pass through EOP before they reach mailboxes in your Exchange Online organization. And, all messages sent from your Exchange Online organization must go through EOP before they reach the Internet.

When you configure a hybrid deployment with the Manage Hybrid Configuration wizard, all transport settings are automatically configured in your on-premises organization and in the EOP company set up for your Exchange Online organization. The Manage Hybrid Configuration wizard configures all inbound and outbound connectors and other settings in this EOP company to secure messages sent between the on-premises and Exchange Online organizations and route messages to the right destination. If you want to configure custom transport settings for your Exchange Online organization, you'll configure them in this EOP company also.

Trusted Communication

To help protect recipients in both the on-premises and Exchange Online organizations, and to help ensure that messages sent between the organizations aren't intercepted and read, transport between the on-premises organization and EOP is configured to use forced TLS. TLS transport uses Secure Sockets Layer (SSL) certificates provided by a trusted third-party Certificate Authority (CA). Messages between EOP and the Exchange Online organization also use TLS.

When using forced TLS transport, the sending and receiving servers examine the certificate configured on the other server. The subject name, or one of the subject alternative names (SANs), configured on the certificates must match the FQDN that an administrator has explicitly specified on the other server. For example, if EOP is configured to accept and secure messages sent from the hybrid.contoso.com FQDN, the sending on-premises hybrid server must have an SSL certificate with hybrid.contoso.com in either the subject name or SAN. If this requirement isn't met, the connection is refused.

Note:

The FQDN used doesn't need to match the e-mail domain name of the recipients. The only requirement is that the FQDN in the certificate subject name or SAN must match the FQDN that the receiving or sending servers are configured to accept.

In addition to using TLS, messages between the organizations are treated as “internal”. This approach allows messages to bypass anti-spam settings and other services.

Learn more about SSL certificates and domain security at: Understanding Certificate Requirements for Hybrid Deployments, Understanding TLS Certificates

1.14.9.7 Understanding Transport Routing in Exchange 2007 Hybrid Deployments

Understanding Transport Routing in Exchange 2007 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-29*

This topic discusses your routing options for inbound messages from the Internet and outbound messages to the Internet.

Note:

The examples in this topic don’t include the addition of Edge Transport servers into the hybrid deployment. The routes messages take between the on-premises organization, the Exchange Online organization, and the Internet don’t change with the addition of an Edge Transport server. The routing only changes within the on-premises organization. For more information about adding Edge Transport servers to a hybrid deployment, see Understanding Edge Transport Servers in Exchange 2007 Hybrid Deployments.

Inbound Messages from the Internet

As part of planning and configuring your hybrid deployment, you need to decide whether you want all messages from Internet senders to be routed through your on-premises organization or through the Exchange Online organization. All messages from Internet senders will initially be delivered to the organization you select and then routed according to where the recipient’s mailbox is located. Whether you choose to have messages routed through your on-premises organization or the Exchange Online organization depends on various factors, including whether you want to apply compliance policies to all

messages sent to both organizations, how many mailboxes are in each organization, and so on.

The path messages sent to recipients in your on-premises and Exchange Online organizations take depends on how you decide to configure your MX record in your hybrid deployment. The Manage Hybrid Configuration wizard doesn't configure the routing for inbound Internet messages for either the on-premises or Exchange Online organizations. You must manually configure your MX record if you want to change how your inbound Internet mail is delivered.

- If you keep your MX record pointed to your on-premises organization: All messages sent to any recipient in either organization will be routed through your on-premises organization first. A message addressed to a recipient that's located in Exchange Online will be routed first through your on-premises organization and then delivered to the recipient in Exchange Online. This route can be helpful for organizations where you have compliance policies that require messages sent to and from an organization be examined by a journaling solution. This route is also recommended if you have more recipients in your on-premises organization than in your Exchange Online organization.
- If you decide to change your MX record to point to the Microsoft Exchange Online Protection (EOP) service in Office 365: All messages sent to any recipient in either organization will be routed through the Exchange Online organization first. A message addressed to a recipient that's located in your on-premises organization will be routed first through your Exchange Online organization and then delivered to the recipient in your on-premises organization. This route is recommended if you have more recipients in your Exchange Online organization than in your on-premises organization.

Read the section below that matches how you plan to route messages sent from Internet recipients to your on-premises and Exchange Online recipients.

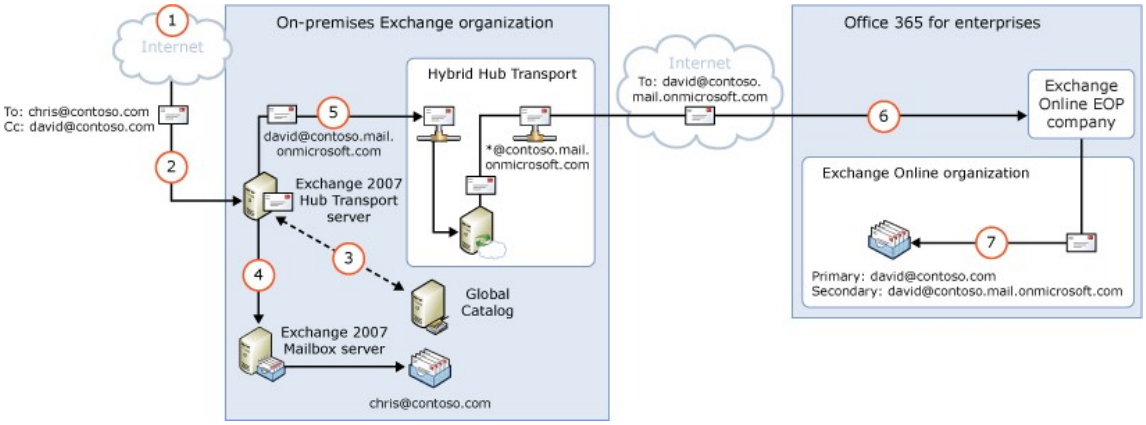
Route Incoming Internet Messages Through Your On-Premises Organization

The following steps and diagram illustrate the inbound Internet message path that will occur in your hybrid deployment if you decide to keep your MX record pointed to your on-premises organization.

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2007 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to the on-premises organization, the message is delivered to an Exchange 2007 Mailbox server.
3. The Exchange 2007 Mailbox server performs a lookup for each recipient using an on-premises global catalog server. Through the global catalog lookup, it determines that Chris's mailbox is located on the Exchange 2007 Mailbox server while David's mailbox is located in the Exchange Online organization and has a hybrid routing address of david@contoso.mail.onmicrosoft.com.
4. The Exchange 2007 Mailbox server splits the message into two copies. One copy of the message is delivered to Chris's mailbox.
5. The second copy of the message is sent through the routing group connector that's configured between the hybrid servers and the Exchange 2007 server.
6. A hybrid Hub Transport server sends the message to EOP, which receives messages sent to the Exchange Online organization, using a Send connector configured to use TLS.
7. EOP sends the message to the Exchange Online organization where the message is scanned for viruses and delivered to David's mailbox.

Route mail through the on-premises organization for both on-premises and Exchange

Online organizations



Route Incoming Internet Messages Through the Exchange Online Organization

The following steps and diagrams illustrate the inbound message path that occur in your hybrid deployment if you decide to point your MX record to the EOP service in the Office 365 organization. The message path differs depending on whether you choose to enable centralized mail transport.

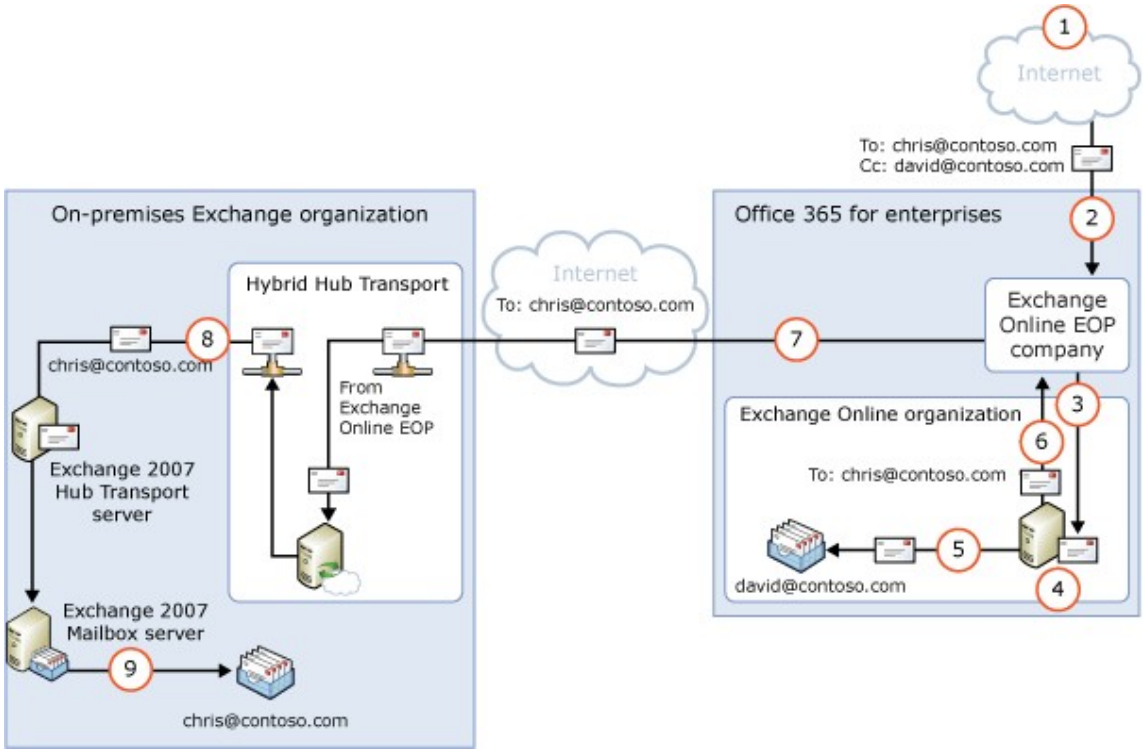
Important:

You may need to purchase EOP licenses for each on-premises mailbox that receives messages that are first delivered to EOP and then routed through the Exchange Online organization. Contact your Microsoft reseller for more information.

When centralized mail transport is *disabled* (default configuration), incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2007 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to EOP, the message is delivered to EOP.
3. EOP routes the messages for both recipients to Exchange Online.
4. Exchange Online scans the messages for viruses and performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. Exchange Online splits the message into two copies. One copy of the message is delivered to David's mailbox.
6. The second copy is sent from Exchange Online back to EOP.
7. EOP sends the message to the hybrid Exchange 2010 Hub Transport servers in the on-premises organization.
8. A hybrid Hub Transport server sends the message through the routing group connector that’s configured between the hybrid servers and the Exchange 2007 server to the Exchange 2007 Mailbox server.
9. The Exchange 2007 server delivers the message to Chris's mailbox.

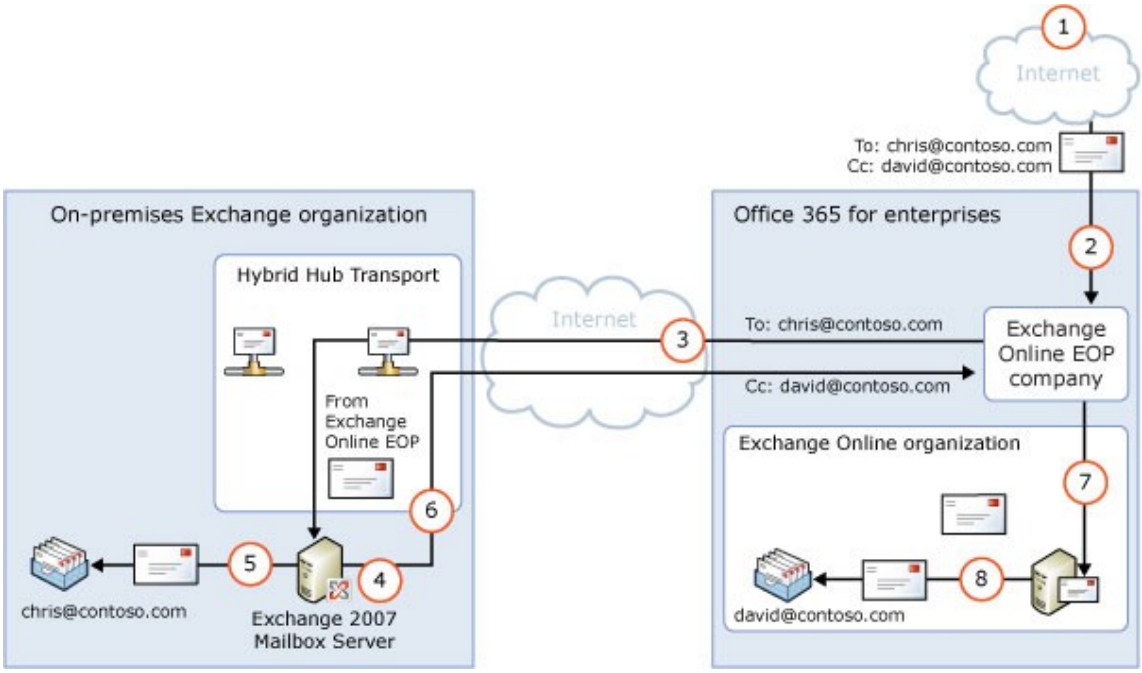
Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport disabled (default configuration)



When centralized mail transport is *enabled*, incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2007 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to EOP, the message is delivered to EOP and scanned for viruses.
3. Since centralized mail transport is enabled, EOP routes the messages for both recipients to the on-premises hybrid Exchange 2010 Hub Transport server.
4. The hybrid Hub Transport server performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. The hybrid Hub Transport server splits the message into two copies. One copy of the message is delivered to Chris’s mailbox in the on-premises Exchange 2007 server.
6. The second copy is sent from the hybrid Hub Transport server back to EOP.
7. EOP sends the message to Exchange Online.
8. Exchange delivers the message to David's mailbox.

Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport enabled



Outbound Messages to the Internet

In addition to choosing how inbound messages addressed to recipients to your organizations are routed, you can also choose how outbound messages sent from Exchange Online recipients are routed. When you run the Hybrid Configuration wizard, you can select one of two options:

- **Enable centralized mail transport** Selecting this option routes outbound messages sent from the Exchange Online organization through your on-premises organization. Except for messages sent to other recipients in the same Exchange Online organization, all messages sent from recipients in the Exchange Online organization are sent through the on-premises organization. This enables you to apply compliance rules to these messages and any other processes or requirements that must be applied to all of your recipients, regardless of whether they're located in the Exchange Online organization or the on-premises organization.

  Note:
  Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- **Don’t enable centralized mail transport** Selected by default in the Manage Hybrid Configuration wizard, this option routes outbound messages sent from the Exchange Online organization directly to the Internet. Use this option if you don't need to apply any on-premises compliance policies or other processing rules to messages that are sent from recipients in the Exchange Online organization.

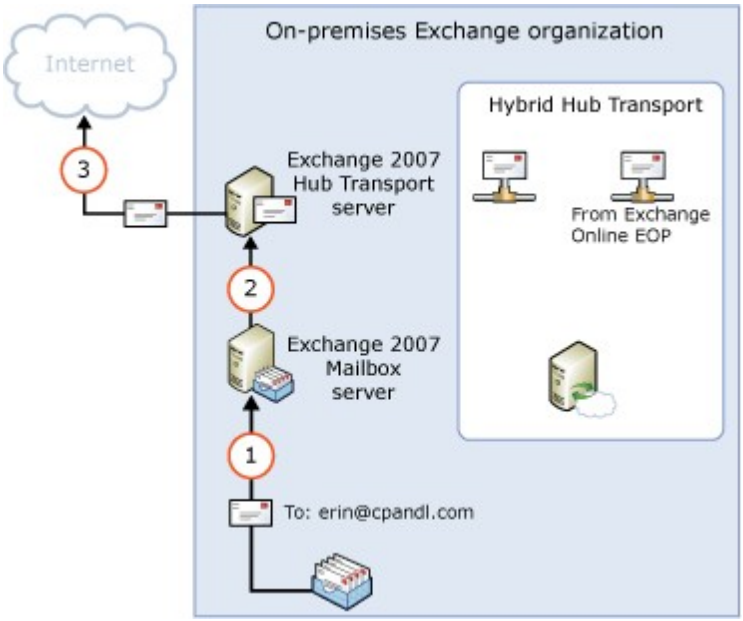
Messages sent from on-premises recipients are always sent to directly to Internet recipients using DNS regardless of which of the above choices you select in the Manage Hybrid Configuration wizard.

The following steps and diagram illustrate the outbound message path for messages sent from on-premises recipients.

1. Chris, who has a mailbox on the on-premises Exchange 2007 Mailbox server, sends a message to an external Internet recipient, erin@cpandl.com.

2. The Exchange 2007 server looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

Messages from on-premises senders to Internet recipients



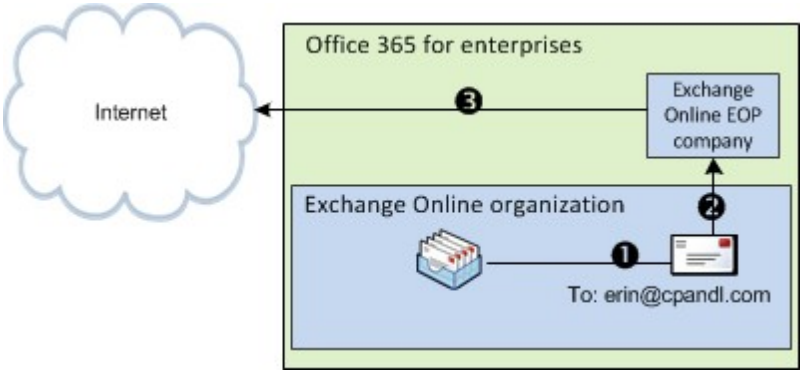
Read the section below that matches how you plan to route messages sent from recipients in the Exchange Online organization to Internet recipients.

Deliver Internet-Bound Messages from Exchange Online Using DNS (Centralized Mail Transport Disabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when **Enable centralized mail transport** is not selected in the Manage Hybrid Configuration wizard, which is the default configuration.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to the Exchange Online EOP company.
3. EOP looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

Mail from Exchange Online senders routed directly to the Internet with centralized mail transport disabled (default configuration)

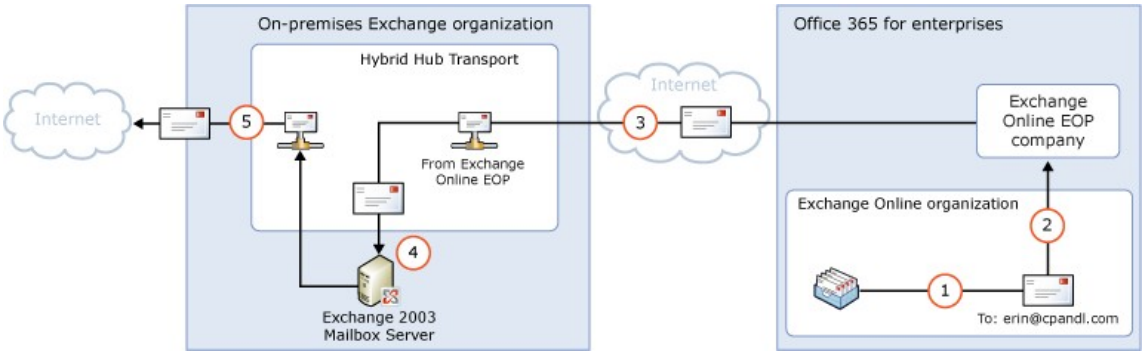


Route Internet-Bound Messages from Exchange Online Through Your On-Premises Organization (Centralized Mail Transport Enabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when you select **Enable centralized mail transport** in the Manage Hybrid Configuration wizard.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to EOP.
3. EOP is configured to send all Internet-bound messages to an on-premises server, so the message is routed to a hybrid Hub Transport server. The message is sent using TLS.
4. A hybrid Hub Transport server performs compliance and any other processes configured by the administrator on David's message.
5. The hybrid Hub Transport server looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

Mail from Exchange Online senders routed through on-premises organization with centralized mail transport enabled



1.14.9.8 Understanding IRM in Exchange 2007 Hybrid Deployments

Understanding IRM in Exchange 2007 Hybrid Deployments

Exchange Server 2010 > Hybrid Deployments > Hybrid Deployments with Exchange 2010 SP3 and Exchange 2007 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-04-05*

Information Rights Management (IRM) helps you to protect against leakage of sensitive information by providing persistent online and offline protection of e-mail messages and attachments. Both Exchange 2007, in your on-premises organization, and Exchange Online, in Office 365 for Enterprises, support IRM. However, there are differences between the two implementations, and you must configure IRM in the Exchange Online organization before users in that organization can use it.

IRM uses Active Directory Rights Management Services (AD RMS), which is a component of Windows Server 2008 R2. AD RMS allows users to create rights-protected content, such as e-mail messages and attachments, and then control how that content is used, and to whom it’s distributed. Users can specify templates that determine how content can be used. For example, a user may specify that an e-mail message can't be forwarded to other recipients or that information in the message can't be copied.

Learn more about IRM in Exchange 2007 at: Understanding the AD RMS Prelicensing Agent

Learn more about IRM in Exchange 2010 at: Understanding Information Rights Management

Learn more about AD RMS at: Active Directory Rights Management Services Overview

Learn more about configuring IRM at: Configure IRM in Exchange 2007 Hybrid Deployments

Differences between IRM in Exchange 2007 and Exchange Online

Exchange Online is based on Exchange 2010, which includes several new IRM features. IRM functionality that's available in your on-premises Exchange 2007 organization is different than the functionality available in your Exchange Online organization. The following table provides a summary of features and functionality available in each organization. (Learn more about these features at: Understanding Information Rights Management)

Available IRM features

Feature	Available in Exchange 2007	Available in Exchange Online
Manual protection of messages in Outlook	Yes	Yes
Manual protection of messages in Outlook Web App	No	Yes
View IRM-protected messages in Outlook	Yes	Yes
View IRM-protected messages in Outlook Web App	Yes*	Yes
IRM Pre-licensing agent	Yes	Yes
RMS policy templates	No	Yes
Transport decryption	No	Yes
Journal report decryption	No	Yes
Exchange Search and discovery decryption	No	Yes
Automatic Outlook protection rules	No	Yes
Automatic transport protection rules	No	Yes

* Internet Explorer with Rights Management add-in required

IRM in Hybrid Deployments

Exchange uses AD RMS servers in the Active Directory forest in which the Exchange server is installed. For your on-premises Exchange 2007 servers, the on-premises AD RMS server is used. For your Exchange Online organization, AD RMS servers that are maintained within the Microsoft Office 365 datacenters are used. The AD RMS configuration that each Exchange organization uses is independent of any other AD RMS deployment.

AD RMS configuration, and therefore IRM configuration, isn't automatically replicated between your on-premises Exchange organization and the Exchange Online organization. Any AD RMS templates that you've defined aren't automatically copied to the Exchange Online organization. If you want the same AD RMS templates to be available in the Exchange Online organization, you must manually export the templates from your on-premises organization and apply them to the cloud-based organization. See the IRM Configuration in Hybrid Deployments section later in this topic.

User Experience

The IRM configuration that's applied to a user depends on the client the user uses and the location of the user's mailbox. The following table shows the AD RMS server a user will use.

Active AD RMS server

Client	On-premises mailbox	Cloud-based mailbox
Outlook 2007 or Outlook 2010	On-premises AD RMS	On-premises AD RMS
Outlook Web App	On-premises AD RMS	Exchange Online AD RMS
ActiveSync device	On-premises AD RMS	Exchange Online AD RMS

It's possible that, depending on the AD RMS configuration you configure in your on-premises and Exchange Online organizations, a user who uses Outlook 2007 and Outlook Web App may see different AD RMS templates. For this reason, we strongly recommend that you apply the same templates to both your on-premises and Exchange Online organizations.

There should be no difference in the IRM experience for Outlook client users, regardless of whether their mailbox is located in the on-premises or Exchange Online organization.

An Outlook Web App user whose mailbox is located on an Exchange 2007 server can only open rights-protected messages after installing the Rights Management for Internet Explorer add-in. They can't reply to or create new rights-protected messages.

An Outlook Web App user whose mailbox is located in Exchange Online can open rights-protected messages without any additional software and can reply to, and create, new rights-protected messages.

Server Functionality

On-premises Exchange 2007 servers use the AD RMS pre-licensing agent to decrypt rights-protected messages so that users don't need to supply credentials when they open those messages. The on-premises Exchange 2007 server contacts the on-premises AD RMS server to check usage policies and rights, and to request authorization to decrypt the message.

The Exchange Online organization provides several additional IRM-related features that make use of Exchange Online AD RMS. These features, such as journal report decryption, make the content of right-protected messages available to Exchange services for

additional processing. For example, the decrypted contents of a journaled message can be saved, along with the original rights-protected message, to allow for easier discovery. Additionally, IRM templates can automatically be applied to messages using either Outlook protection rules or transport rules to ensure that messages adhere to organization policies regarding information protection.

IRM Configuration in Hybrid Deployments

IRM in Exchange relies on AD RMS being deployed in the Active Directory forest in which the Exchange server resides. AD RMS configuration isn't automatically synchronized between the on-premises and Exchange Online organizations. You must manually export the AD RMS configuration, known as a trusted publishing domain (TPD), from your on-premises AD RMS server, and import that configuration into the Exchange Online organization. The TPD contains the AD RMS configuration, including templates, which the Exchange Online organization needs to use IRM.

Learn more at: AD RMS Trusted Publishing Domain Considerations

In addition to applying your on-premises AD RMS configuration to the Exchange Online organization, you must ensure that your AD RMS servers can be contacted by Outlook and ActiveSync clients outside of your on-premises network. You must do this if you want these clients to access rights-protected messages outside of your on-premises network.

After you've configured your on-premises network and exported the TPD data, you need to configure the Exchange Online organization by importing the TPD data and enabling IRM.

Note:

Any time you modify your on-premises AD RMS configuration, you must manually apply the new configuration in the Exchange Online organization. To do so, export the TPD data from your on-premises AD RMS server and import it into the Exchange Online organization.

Learn more at: Configure IRM in Exchange 2007 Hybrid Deployments

1.14.9.8.1 Configure IRM in Exchange 2007 Hybrid Deployments

Configure IRM in Exchange 2007 Hybrid Deployments

Hybrid Deployments > Hybrid Deployments with Exchange 2010 SP3 and Exchange 2007 > Understanding IRM in Exchange 2007 Hybrid Deployments >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you use Information Rights Management (IRM) in your on-premises Exchange organization and you want your Exchange Online users to also use IRM, you need to do the following:

1. Configure your on-premises Active Directory Rights Management Services (AD RMS) server.
2. Enable IRM in your Exchange Online organization.
3. Distribute the imported AD RMS templates to users in the Exchange Online organization.

Learn more at: Understanding IRM in an Exchange 2007 Hybrid Deployment

How do I configure on-premises AD RMS servers?

To configure IRM in a hybrid deployment, you need to use Windows PowerShell to access your on-premises AD RMS server. Learn more at: Using Windows PowerShell to Administer AD RMS

Do the following to export trusted publishing domain (TPD) data from your on-premises AD RMS server and then configure access to the AD RMS server for external clients.

1. Export TPD data from your on-premises organization. Learn more at: Exporting a Trusted Publishing Domain
2. Configure access to AD RMS servers from external clients. Learn more at: Adding an Extranet Cluster URL

How do I enable IRM in the Exchange Online organization?

After you export the TPD data from your on-premises AD RMS servers, you need to import that data into the Exchange Online organization and then enable IRM.

1. In the Exchange Online organization, import the TPD data.

```
Import-RMSTrustedPublishingDomain -FileData $( [Byte[]] (Get-Content -
```

2. Enable IRM in the Exchange Online organization.

```
Set-IRMConfiguration -InternalLicensingEnabled $True
```

How do I distribute AD RMS templates in the Exchange Online organization?

After you've enabled IRM in the Exchange Online organization, you must distribute the imported AD RMS templates. The following Exchange Online users and features use AD RMS templates:

- Outlook Web App users
- Exchange ActiveSync users
- Transport rules
- Journal report decryption
- Outlook protection rules

1. In the Exchange Online organization, retrieve a list of AD RMS templates.

```
Get-RMSTemplate -Type All
```

2. Distribute the AD RMS templates to users and features in the Exchange Online organization.

```
Set-RMSTemplate <template name> -Type Distributed
```

Note:
You can't modify the "Do Not Forward" AD RMS template.

3. Repeat step 2 for each AD RMS template you want to distribute.

How do I know this worked?

Outlook Web App users should be able to apply AD RMS templates to new messages. Outlook Web App and Exchange ActiveSync users should be able to read messages that have AD RMS templates applied to them. In addition, all the AD RMS templates that were imported from your on-premises organization should be listed when you run the **Get-**

RMSTemplate cmdlet.

Run the following command in the Exchange Online organization.

```
Get-RMSTemplate
```

Learn more at: Understanding Information Rights Management in Outlook Web App

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

1.14.10 Hybrid Deployments with Exchange 2010 SP3

Hybrid Deployments with Exchange 2010 SP3

Exchange Server 2010 > Hybrid Deployments >

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-02-01*

Understanding Hybrid Servers in Exchange 2010 Hybrid Deployments

Understanding Prerequisites for Exchange 2010 Hybrid Deployments

Understanding Hybrid Management in Exchange 2010 Hybrid Deployments

Understanding Edge Transport Servers in Exchange 2010 Hybrid Deployments

Understanding Shared Free/Busy in Exchange 2010 Hybrid Deployments

Understanding Transport Options in Exchange 2010 Hybrid Deployments

Understanding Transport Routing in Exchange 2010 Hybrid Deployments

Understanding IRM in Exchange 2010 Hybrid Deployments

1.14.10.1 Understanding Hybrid Servers in Exchange 2010 Hybrid Deployments

Understanding Hybrid Servers in Exchange 2010 Hybrid Deployments

Exchange Server 2010 > Hybrid Deployments > Hybrid Deployments with Exchange 2010 SP3 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

When configuring a hybrid deployment in an Exchange 2010 organization, you aren't required to install additional Exchange servers in your existing Exchange organization. As long as your Client Access and Hub Transport servers are updated to Exchange 2010 Service Pack 3 (SP3) with the latest update roll up, these servers can coordinate communications between your existing Exchange 2010 organization and the Exchange Online organization. This communication includes message transport and messaging features between the on-premises and Exchange Online organizations. We highly

recommend installing more than one Exchange server in your on-premises organization to help increase reliability and availability of hybrid deployment features.

Server Roles in a Hybrid Deployment

Here is a quick overview of the Exchange 2010 server roles in a hybrid deployment:

- **Client Access server role** The Client Access server role continues to provide essentially the same functionality typically provided by Client Access servers in your Exchange 2010 organization with a few additions required to support a hybrid deployment. All client connectivity, including Outlook client access, Outlook Web App, and Outlook Anywhere goes through the Client Access server role. Organization relationship features between the on-premises and Exchange Online organizations, such as free/busy sharing, are also handled by the Client Access server role.
  Learn more at: Understanding Client Access
- **Hub Transport server role** The Hub Transport server role handles all mail flow between the on-premises and Exchange Online organizations and between the on-premises organization and the Internet. It helps to secure transport communication between the on-premises and Exchange Online organizations, as well as handling transport rules, journaling policies, and message delivery to user mailboxes in a hybrid deployment.
  Learn more at: Overview of the Hub Transport Server Role

Depending on the hybrid deployment configuration that you want, an Exchange 2010 SP3 server requires one or more of the server roles to be installed on it:

- **Single Exchange server** If you choose to install a single Exchange server in your on-premises organization, you'll need to install the Mailbox, Client Access, and Hub Transport server roles on the single server.
- **More than one Exchange server** If you choose to install more than one Exchange server in your on-premises organization, you can install the server roles on separate servers in your on-premises organization. For example, you could install one Exchange server that has the Mailbox and Client Access roles installed and also install another Exchange server that has only the Hub Transport server role installed. However, the best practice and recommended server configuration is to install the Client Access and Hub Transport servers on *each* server deployed in your on-premises organization.

If you also decide to install the optional Exchange 2010 Mailbox server role in your hybrid deployment, you should add the Mailbox server role to each Exchange server that has the Client Access and Hub Transport server roles installed. Learn more about the Mailbox server role at Overview of the Mailbox Server Role and learn more about Exchange capacity planning at Understanding Multiple Server Role Configurations in Capacity Planning.

Exchange Server Functionality in Hybrid Deployments

A hybrid Exchange server provides several important functions for your on-premises organization in a hybrid deployment:

- **Federation** Exchange servers enable you to create a federation trust for your on-premises organization with the Microsoft Federation Gateway. The Microsoft Federation Gateway is a free, cloud-based service offered by Microsoft that acts as the trust broker between your on-premises organization and the Office 365 tenant organization. Federation is a requirement for creating an organization relationship between the on-premises and the Exchange Online organizations.

Learn more at: Understanding Federation

- **Organization relationships** Exchange servers with the Client Access server role enable the creation of organization relationships between the on-premises and Exchange Online organizations. Organization relationships are required for many other services in a hybrid deployment, including calendar free/busy information sharing, message tracking, and mailbox moves between the on-premises and Exchange Online organizations.
  Learn more at: Understanding Federated Delegation
- **Message transport** Exchange servers with the Hub Transport server role are responsible for message transport in a hybrid deployment. Using Send and Receive connectors, they serve as the connection endpoint for incoming external messages and also provide outbound message delivery to the Internet and the Exchange Online organization.
  Learn more at: Understanding Transport
- **Message transport security** Exchange servers with the Hub Transport server role help to secure message communication between the on-premises and Exchange Online organizations by using the Domain Security functionality in Exchange 2010. Security can be increased by using mutual transport layer security authentication and encryption for message communications.
  Learn more at: Understanding Domain Security
- **Outlook Web App** Exchange servers with the Client Access server role support configuring a single URL endpoint for external connections to on-premises and Exchange Online mailboxes. For on-premises mailboxes, Client Access servers are configured to service Outlook Web App requests.. For Exchange Online organization mailboxes, Client Access servers are configured to automatically display a link to the Outlook Web App endpoint on the Exchange Online organization.
  Learn more at: Understanding Outlook Web App

Exchange Server Topology

If you choose to add additional Exchange servers to support your hybrid deployment, the Exchange server would be deployed much like any other Exchange 2010 server would be deployed to your existing Exchange 2010 organization. Configuring your existing on-premises Exchange 2010 organization for a hybrid deployment doesn't require any special Exchange server topology. The following table describes briefly the changes in services after configuring a hybrid deployment.

Service	Before hybrid server deployment	After hybrid server deployment	Description
Message transport (inbound and outbound)	Exchange 2010 Hub Transport server	Exchange 2010 Hub Transport server or Exchange Online Protection (EOP) included with Office 365	The MX (mail exchanger) record for the domain may remain unchanged or be updated to point to EOP.
Outlook Web App public URL	Exchange 2010 Client Access server	Exchange 2010 Client Access server	Client Access servers continue to handle Outlook Web App requests for on-premises mailboxes. Outlook Web App requests for mailboxes hosted on Exchange Online are provided with a link to the Exchange Online Outlook Web App

			URL.

Exchange Server Software

Exchange 2010 SP3 enables hybrid deployment functionality with the Hybrid Configuration wizards. You can use any Exchange 2010 SP3 media when installing additional Exchange 2010 servers.

Additionally, we recommend installing future Update Rollups 4 for Exchange 2010 SP3 on all your hybrid servers. Microsoft releases update rollup packages approximately every six to eight weeks. The rollup packages are available via Microsoft Update and the Microsoft Download Center. In the Search box on the Microsoft Download Center, type "Exchange 2010 SP3 update rollup" to find links to the rollup packages for Exchange 2010 SP3.

Download Exchange Server 2010 SP3 at: Exchange 2010 Service Pack 3 (SP3)

Find update rollup packages at: Microsoft Download Center

Important:

You need to provide an Exchange 2010 Hybrid Edition product key on the hybrid server when you configure a hybrid deployment with Office 365. To obtain a Hybrid Edition product key, contact Office 365 support.

1.14.10.2 Understanding Prerequisites for Exchange 2010 Hybrid Deployments

Understanding Prerequisites for Exchange 2010 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

Before you can really start to use the Deployment Assistant, your system and servers must meet requirements. If they don't meet these requirements, you won't be able to complete the steps within the tool and you won't be able to configure a hybrid deployment between your on-premises Exchange 2010 and Exchange Online organizations. This topic provides information about the following:

- The Exchange Pre-Deployment Analyzer
- Permissions needed to install and manage Exchange 2010
- Requirements for directory servers, hardware, software, clients, and other elements, including:
  - Windows Server 2008 Service Pack 2 (SP2) or later or Windows Server 2008 R2 operating system prerequisites that are required for all Exchange 2010 server roles
- Language support for Exchange 2010
- The Exchange Management Shell, the command-line interface for Exchange 2010, and the Exchange Management Console, the GUI management tool for Exchange 2010

Note:

Before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Exchange Pre-Deployment Analyzer

You can use the Exchange Pre-Deployment Analyzer (ExPDA) to perform an overall topology readiness scan of your environment. This scan focuses on overall topology readiness and not the ability to run Exchange 2010 on the local computer. ExPDA provides a detailed report that will alert you if there are any issues within your organization, which could prevent you from deploying Exchange 2010. For example, ExPDA will notify you if you haven't deployed the minimum required Exchange service pack on all your Exchange servers. If your organization passes the ExPDA readiness scan, you can go ahead and use the Exchange Deployment Assistant.

To get ExPDA from the Microsoft Download Center, see: Exchange Pre-Deployment Analyzer

Permissions to Install and Manage Exchange 2010

Exchange 2010 requires different permissions to install and to manage your server roles. When you're installing Exchange 2010 servers in your organization, the account you use might not be the same account that you use for administering and managing your server roles. To manage your server roles, Exchange 2010 uses the Role Based Access Control (RBAC) permissions model.

Exchange 2010 uses RBAC to manage permissions on an Exchange 2010 server. With RBAC, you can control what resources administrators can configure and what features users can access. The RBAC model in Exchange 2010 is flexible and provides you with several ways to customize the default permissions.

RBAC has two primary ways of assigning permissions to users in your organization, depending on whether the user is an administrator or specialist user, or an end-user: management role groups and management role assignment policies. Each method associates users with the permissions they need to perform their jobs. The following sections list the tasks found in the Deployment Assistant and the permissions required to complete the task.

Note:

Some features may require that you have local administrator permissions on the server you want to manage. To manage these features, you must be a member of the Local Administrators group on that server.

Installation Permissions

By default, the account that's used to install Exchange 2010 in the organization is added as a member of the Organization Management role group.

For information about how to add permissions, see: Add Members to a Role Group

The following permissions are required to install the hybrid server in your organization:

- Local Administrator on the server on which Exchange 2010 will be installed
- Enterprise Administrator in the Active Directory forest where Exchange 2010 will be installed
- Schema Administrator in the Active Directory forest where Exchange 2010 will be installed

Exchange Management Permissions

The table below lists the configuration permissions that you need to successfully use the Deployment Assistant and the Hybrid Configuration wizards. Some tasks need to be performed only in the on-premises organization while some tasks also need to be

performed in the Office 365 tenant organization. If a task needs to be performed in the Office 365 tenant organization, you must ensure that you have the required permissions in that organization. Permissions in the on-premises organization aren't replicated to the Office 365 tenant organization.

Note:

The user account used to create the Office 365 tenant organization has all the permissions required to perform the tasks in this checklist. Additionally, you must use an on-premises account that's a member of the Organization Management role group for the on-premises section in the Credentials page in the Manage Hybrid Configuration wizard for these tasks to complete successfully.

Learn more at: Understanding Hybrid Deployment Permissions with Exchange 2010 SP3

Task	Permissions required	On-premises or Office 365 tenant organization
Import digital certificates	Local Administrator	On-premises organization
Configure settings on virtual directories	Server Management	On-premises organization
Configure virtual directories	Organization Management Server Management	On-premises organization
Create accepted domains	Organization Management	On-premises and Office 365 tenant organization
Create and modify Send and Receive connectors	Organization Management	On-premises organization
Create routing group connectors	Organization Management Server Management	On-premises organization
Create a federation trust	Organization Management	On-premises organization
Create organization relationships	Organization Management	On-premises and Exchange Online organization
Move mailboxes	Organization Management Recipient Management	On-premises and Exchange Online organization
Configure Exchange 2010 authentication	Local Administrator	On-premises organization
Configure Exchange 2010 e-mail address policies	Exchange Administrator	On-premises organization

Directory Servers

Here are the requirements for the directory servers in your organization:

- **Schema master** The latest 32-bit or 64-bit edition of the Windows Server 2003 SP2 Standard or Enterprise operating system or the Windows Server 2008 Standard or Enterprise operating system.
- **Global catalog server** In every Active Directory site where you plan to install Exchange 2010, you must have at least one global catalog server that is either the latest 32-bit or 64-bit edition of: Windows Server 2003 SP2 Standard or Enterprise; Windows Server 2008 Standard or Enterprise; or

Windows Server 2008 R2 Standard or Enterprise.

- **Active Directory Forest** The Active Directory forest must be Windows Server 2003 forest functional mode or higher.
- **Domain Controller** You must have the latest 32-bit or 64-bit Windows Server 2003 Standard Edition or Enterprise Edition with Service Pack 2 (SP2) operating system or the latest 32-bit or 64-bit edition of the Windows Server 2008 Standard or Enterprise operating system or the Windows Server 2008 R2 Standard or Enterprise operating system.

Hardware

The recommended hardware requirements for Exchange 2010 servers vary depending on several factors including the server role(s) that are installed and the anticipated load that will be placed on the servers.

- **Processor** x64 architecture-based computer with processor that supports 64-bit architecture
- **Memory** Minimum 4GB with a recommended maximum of 2GB per core (8GB minimum). Learn more at: Understanding Memory Configurations and Exchange Performance
- **Disk space** At least 1.2 GB on the drive on which you install Exchange and additional 200 MB of available space on the system drive.
- **Drive** DVD-ROM drive, local or network accessible
- **File format** Disk partitions formatted as NTFS file systems

Operating System

Here are the supported operating systems for Exchange 2010:

- 64-bit edition of Windows Server 2008 Standard Service Pack 2
- 64-bit edition of Windows Server 2008 Enterprise Service Pack 2
- 64-bit edition of Windows Server 2008 Standard R2
- 64-bit edition of Windows Server 2008 Enterprise R2

Exchange 2010 Management tools can use the operating systems listed above plus:

- 64-bit edition of Windows Vista
- 64-bit edition of Windows 7

Install Hotfixes for Windows Server 2008 SP2

The following hotfixes are required for Windows Server 2008 SP2:

- Install the update described in Microsoft Knowledge Base article 977624, AD RMS clients do not authenticate federated identity providers in Windows Server 2008 or in Windows Vista. Without this update, Active Directory Rights Management Services (AD RMS) features may stop working.
- Install the update described in Knowledge Base article 979744, A .NET Framework 2.0-based Multi-AppDomain application stops responding when you run the application.
- Install the update described in Knowledge Base article 979917, Two issues occur when you deploy an ASP.NET 2.0-based application on a server that is running IIS 7.0 or IIS 7.5 in Integrated mode. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB979917 - QFE for Sharepoint issues - Perf Counter fix & User Impersonation.
  - For the available downloads, see KB979917 - QFE for Sharepoint issues - Perf Counter fix & User Impersonation.
- Install the update described in Knowledge Base article 973136, FIX: ArgumentNullException exception error message when a .NET Framework 2.0 SP2-based application tries to process a response with zero-length content to an asynchronous ASP.NET Web service request: "Value cannot be null".
- Install the update described in Knowledge Base article 977592, RPC over HTTP

clients cannot connect to the Windows Server 2008 RPC over HTTP servers that have RPC load balancing enabled.

Install Hotfixes for Windows Server 2008 R2

The following hotfixes are required for Windows Server 2008 R2:

Important:
The following hotfixes only apply to Windows Server 2008 R2 RTM. If you're installing Exchange on Windows Server 2008 R2 SP1, you don't need to apply these hotfixes.

- Install the update described in Knowledge Base article 979099, An update is available to remove the application manifest expiry feature from AD RMS clients. Without this update, the AD RMS features may stop working.
- Install the update described in Knowledge Base article 979744, A .NET Framework 2.0-based Multi-AppDomain application stops responding when you run the application.
- Install the update described in Knowledge Base article 983440, An ASP.NET 2.0 hotfix rollup package is available for Windows 7 and for Windows Server 2008 R2. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB983440 - Win7 rollup package (PR for QFE 810219).
  - For the available downloads, see KB983440 - Win7 rollup package (PR for QFE 810219).
- Install the update described in Knowledge Base article 977020, FIX: An application that is based on the Microsoft .NET Framework 2.0 Service Pack 2 and that invokes a Web service call asynchronously throws an exception on a computer that is running Windows 7.

Install Hotfixes for Windows 7 and Windows Vista

The following hotfixes are required for Windows 7 and Windows Vista computers where you install the Exchange Management Console

- Install the update described in Knowledge Base article 977020, FIX: An application that is based on the Microsoft .NET Framework 2.0 Service Pack 2 and that invokes a Web service call asynchronously throws an exception on a computer that is running Windows 7.
- Install the update described in Knowledge Base article 983440, An ASP.NET 2.0 hotfix rollup package is available for Windows 7 and for Windows Server 2008 R2. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB983440 - Win7 rollup package (PR for QFE 810219).
  - For the available downloads, see KB983440 - Win7 rollup package (PR for QFE 810219).

Install the Windows Server 2008 SP2 prerequisites

1. Install the Microsoft Filter Pack. For details, see: 2007 Office System Converter: Microsoft Filter Pack
2. Open an elevated command prompt, navigate to the Scripts folder on the Exchange 2010 installation media and use the following command to install the necessary operating system components:

```
sc config NetTcpPortSharing start= auto
ServerManagerCmd -ip Exchange-Typical.xml -Restart
```

Install the Exchange 2010 SP1 Hotfixes for Windows Server 2008 SP2

The following hotfix is required for Windows Server 2008 SP2 and must be installed after the operating system prerequisites have been installed:

- Install the hotfix described in Knowledge Base article 982867, WCF services that are hosted by computers together with a NLB fail in .NET Framework 3.5 SP1. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB982867 - WCF: Enable

WebHeader settings on the RST/SCT.
- For the available downloads, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.

After installing the preceding prerequisites and hotfix, and before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Install the Windows Server 2008 R2 prerequisites

1. Install the Microsoft Filter Pack. For details, see: 2007 Office System Converter: Microsoft Filter Pack
2. On the Start Menu, navigate to **All Programs**, then **Accessories**, then **Windows PowerShell**. Open an elevated Windows PowerShell console, and run the following command:

```
Import-Module ServerManager
```

3. Use the **Add-WindowsFeature** cmdlet to install the necessary operating system components using the following command:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,W
```

4. After the system has restarted, log on as an administrator, open an elevated Windows PowerShell console, and configure the Net.Tcp Port Sharing Service for Automatic startup by running the following command:

```
Set-Service NetTcpPortSharing -StartupType Automatic
```

Install the Exchange 2010 SP1 Hotfixes for Windows Server 2008 R2

The following hotfix is required for Windows Server 2008 R2 and must be installed after the operating system prerequisites have been installed:

- Install the hotfix described in Knowledge Base article 982867, WCF services that are hosted by computers together with a NLB fail in .NET Framework 3.5 SP1. For more information, see these MSDN Code Gallery pages:
  - For additional background information, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.
  - For the available downloads, see KB982867 - WCF: Enable WebHeader settings on the RST/SCT.

After installing the preceding prerequisites and hotfix, and before installing Exchange 2010, we recommend that you install any critical or recommended updates from Microsoft Update.

Windows Management Framework

- Windows PowerShell V2.0
- Windows Remote Management V2.0
- .NET Framework 3.5 SP1
- Internet Information Services (IIS)

Language Support

An Exchange 2010 SP2 language pack contains the necessary resources for a supported Exchange language. Language packs are installed automatically during deployment of Exchange 2010 SP2. Client and server language packs come grouped into a single bundle containing both client and server resource and support files. There are no performance issues with installing all the languages because they're just stored when not in use.

Learn more at: Exchange 2010 Language Support

Exchange Management Shell

The Exchange Management Shell, built on Windows PowerShell technology, provides a powerful command-line interface for Exchange 2010 that enables automation of administrative tasks.

With the Shell, you can manage every aspect of Exchange 2010; the Shell can perform every task that can be performed by the Exchange Management Console (EMC) and the Exchange Control Panel (ECP) in addition to tasks that can't be performed in those interfaces. In fact, when a task is performed in the EMC or the ECP, those interfaces use the Shell to perform the task.

Learn more at: Overview of Exchange Management Shell

Exchange Management Console

The Exchange Management Console (EMC) is a Microsoft Management Console (MMC) 3.0-based tool that provides you with a GUI to manage the configuration of your Exchange 2010 organization. You can also add the EMC snap-in to custom MMC-based tools.

Learn more at: Exchange Management Console

1.14.10.3 Understanding Hybrid Management in Exchange 2010 Hybrid Deployments

Understanding Hybrid Management in Exchange 2010 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-02-01*

Both your on-premises organization and the Exchange Online organization are based on Exchange. In particular, hybrid servers in your on-premises organization are based on Microsoft Exchange Server 2010 and the Exchange Online organization Exchange servers are based on Exchange Server 2013. Service Pack 3 (SP3) for Exchange 2010 enables hybrid features to function correctly between these two types of hybrid deployment servers.

When you install a hybrid server, Exchange 2010 management tools are automatically installed on the server. You'll use the management tools to configure and manage both the hybrid server(s) and some recipient management features for the Exchange Online organization. These tools include the Exchange Management Console (EMC), a graphical administrative interface, and the Exchange Management Shell, a Windows PowerShell-based command-line interface. You'll also use the Exchange Administration Center (EAC) in the Exchange Online section of the Office 365 management portal to manage most of the properties of the Exchange Online recipients and organization.

Exchange Management Console

The EMC enables you to perform many deployment tasks and most common day-to-day administrative tasks. Additionally, the EMC allows you to administer both the on-premises hybrid servers and some recipient management features for mailboxes in the Exchange Online organization. It's installed by default on every Exchange 2010 server, but you can

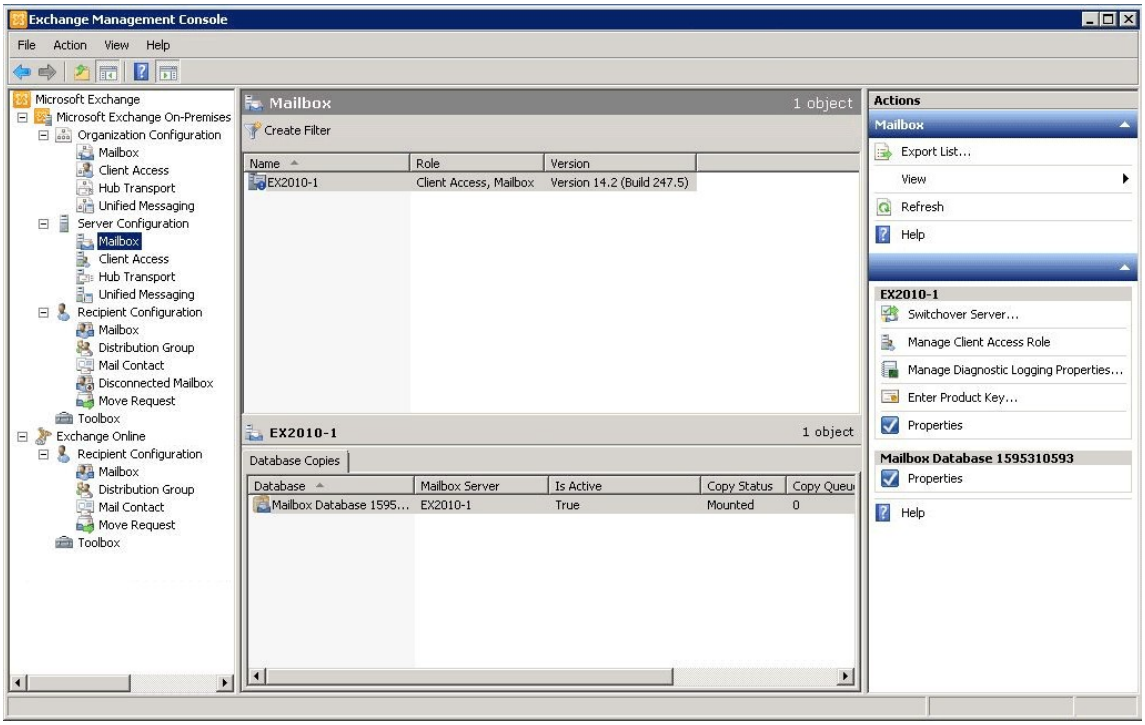
also install it on a computer running any of the following 64-bit operating systems:

- Windows Server 2008 SP2 Standard and Enterprise
- Windows Server 2008 R2 Standard and Enterprise
- Windows 8
- Windows 7
- Windows Vista Service Pack (SP) 2

Adding the Exchange Online organization to the EMC is similar to adding another Exchange 2010 forest to the EMC. When the Exchange Online organization is added to the EMC, it appears as another node in the navigation tree. From there you can select the Exchange Online organization and configure some properties of Exchange Online recipient objects. To fully manage organization-level features and objects for the Exchange Online organization, you'll be redirected by the EMC and provided a link to connect to the EAC in the Office 365 management portal.

The following screenshot shows the on-premises organization and Exchange Online organization in the same console.

Exchange on-premises and Exchange Online organizations in the Exchange Management Console



Learn more at: Exchange Management Console

Exchange Management Shell

The Shell enables you to perform any task that the EMC does and some additional tasks that can only be performed in the Shell. The Shell is a collection of Windows PowerShell scripts and cmdlets that are installed on a computer when the Exchange 2010 management tools are installed. These scripts and cmdlets are only loaded when you open the Shell using the Exchange Management Shell icon. If you open Windows PowerShell directly, the Exchange scripts and cmdlets aren't loaded and you won't be able to manage your on-premises organization.

Note:
You can create a manual Windows PowerShell connection to your local on-premises organization, similar to how you manually connect to the Exchange Online organization below. However, we strongly recommend that you use the Exchange Management Shell icon to open the Shell to manage your on-premises Exchange servers.

When you open the Shell using the Exchange Management Shell icon on a computer that has the management tools installed, you can manage your on-premises organization. However, you can't manage the Exchange Online organization when you open the Shell using this icon. This is because opening the Shell using the Exchange Management Shell icon automatically connects you to a local Exchange server.

If you want to manage the Exchange Online organization using Windows PowerShell, you must open Windows PowerShell directly and not via the Exchange Management Shell icon. When you open Windows PowerShell, you can then manually specify where you want to connect. When you create a manual connection, you specify an administrator account in the Office 365 tenant organization, and then you run a command to create a connection. When the connection is established, the Exchange cmdlets you have permissions to run are made available to you.

Learn more at: Use Windows PowerShell

If you're new to the Shell, check out the following topic to learn the basics about how the Shell works, command syntax, and more.

Learn more at: Exchange Management Shell

1.14.10.4 Understanding Edge Transport Servers in Exchange 2010 Hybrid Deployments

Understanding Edge Transport Servers in Exchange 2010 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3*

Topic Last Modified: *2013-01-25*

Edge Transport servers in Exchange 2010 are deployed in your organization's on-premises perimeter network. They're non-domain-joined computers that handle Internet-facing mail flow and act as an SMTP relay and smart host for Exchange servers in your internal network. In hybrid deployments, you have the option of deploying Edge Transport servers running Service Pack 3 (SP3) for Exchange 2010 if you don't want to expose internal Hub Transport servers directly to the Internet.

Learn more at: Overview of the Edge Transport Server Role

Exchange 2010 Edge Transport Servers

Messages routed between on-premises and Exchange Online organizations require that Exchange Online Protection (EOP), on behalf of Exchange Online, connects directly to on-premises Hub Transport or Edge Transport servers that run Exchange 2010 SP3. If you've deployed Exchange 2010 SP2 Edge Transport servers, you must upgrade the Edge Transport servers you want to use for hybrid transport to Exchange 2010 SP3. Only the Edge Transport servers that handle hybrid transport between the on-premises organization and Exchange Online need to be upgraded to Exchange 2010 SP3.

If you have other Edge Transport servers in other locations that won't handle hybrid transport, they don't need to be upgraded to Exchange 2010 SP3. If, in the future, you want EOP to connect to additional Edge Transport servers for hybrid transport, they must be upgraded to Exchange 2010 SP3.

Important:

If you prefer to keep Exchange 2010 SP2 Edge Transport servers in your organization, make sure that EOP connects to an on-premises Exchange 2010 SP3 Hub Transport or Edge Transport server for hybrid transport. If EOP connects to a server running a version other than Exchange 2010 SP3, messages may not be handled correctly. For more information, see: Understanding Transport Options in Exchange 2010 Hybrid Deployments

Adding an Edge Transport Server to a Hybrid Deployment

Deploying an Edge Transport server in your on-premises organization when you configure a hybrid deployment is an optional step. During the initial run of the Manage Hybrid Configuration wizard, the wizard requires that you select one or more Hub Transport servers. However, after the initial run of the wizard, you can add an Edge Transport server to your organization, configure it, run the Manage Hybrid Configuration wizard again, and then manually update the on-premises Send connectors and Edge Transport Receive connector to add it to the hybrid deployment.

When you add an Edge Transport server to your hybrid deployment, it communicates with EOP on behalf of the internal Hub Transport servers. The Edge Transport server acts as a relay between the on-premises Hub Transport server and EOP. All connection security previously handled by the Hub Transport server is handled by the Edge Transport server. Recipient lookup, compliance policies, and other message inspection, continue to be done on the Hub Transport servers.

If you add an Edge Transport server to your hybrid deployment, you don't need to route mail sent between on-premises users and Internet recipients through it. Only messages sent between the on-premises and Exchange Online organizations will be routed through the Edge Transport server.

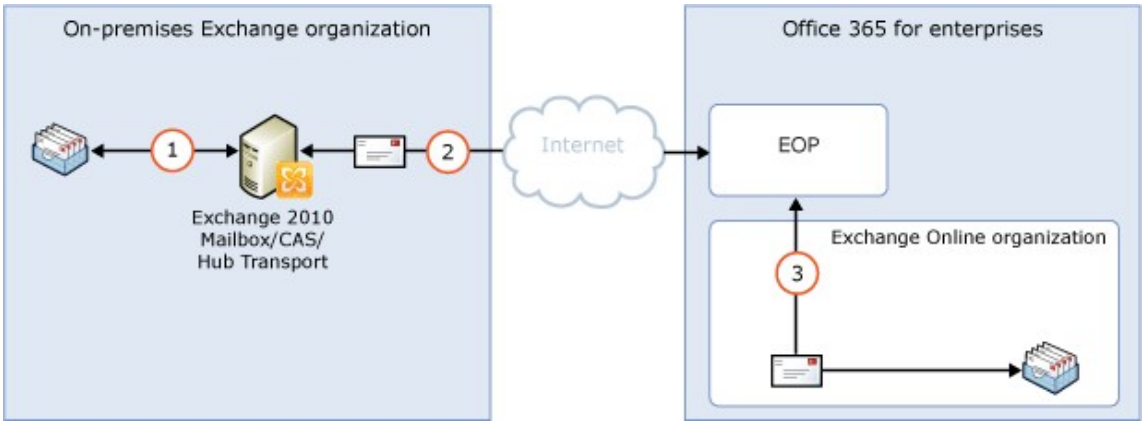
Mail Flow without an Edge Transport Server

The following process and diagram describe the path messages take between an on-premises organization and Exchange Online when there is no Edge Transport server deployed:

1. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from an Exchange 2010 Mailbox server to an Exchange 2010 Hub Transport server. In this example, the Mailbox and Hub Transport server roles are installed on the same Exchange 2010 server.
2. The Hub Transport server sends the message directly to the Exchange Online EOP company.
3. EOP delivers the message to the Exchange Online organization.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

Mail flow in a hybrid deployment without an Edge Transport server deployed



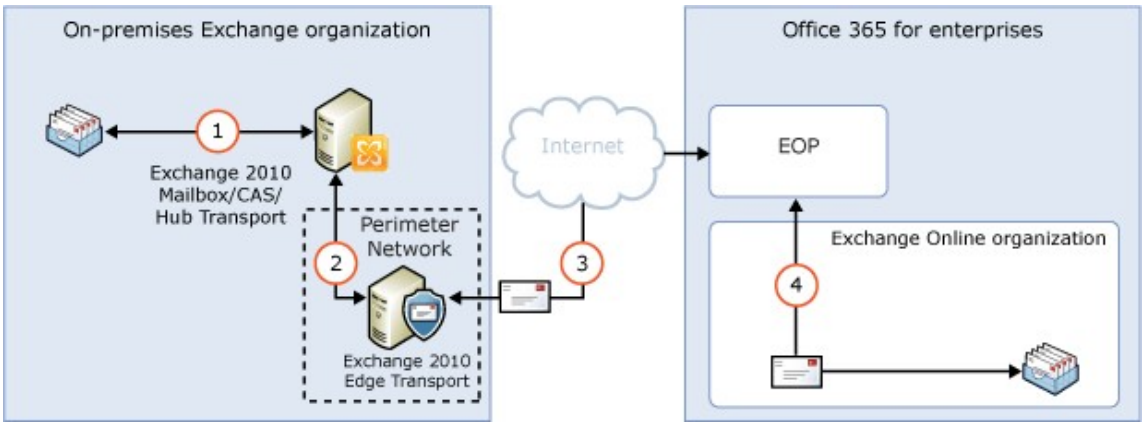
Mail Flow with an Edge Transport Server

The following diagram shows the path messages take between an on-premises organization and Exchange Online when there is an Edge Transport server deployed. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from the Exchange 2010 servers:

1. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from an Exchange 2010 Mailbox server to an Exchange 2010 Hub Transport server. In this example, the Mailbox and Hub Transport server roles are installed on the same Exchange 2010 server.
2. The Exchange 2010 Hub Transport server sends the message to an Exchange 2010 Edge Transport server.
3. The Edge Transport server sends the message to the Exchange Online EOP company.
4. EOP delivers the message to the Exchange Online organization.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

Mail flow in a hybrid deployment with an Edge Transport server deployed



1.14.10.5 Understanding Shared Free/Busy in Exchange 2010 Hybrid Deployments

Understanding Shared Free/Busy in Exchange 2010 Hybrid Deployments

Exchange Server 2010 > Hybrid Deployments > Hybrid Deployments with Exchange 2010 SP3 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-11*

Sharing free/busy (calendar availability) information between users located on-premises and in the Exchange Online organization is one of the primary benefits of a hybrid deployment. Users in both organizations can view each other's calendars just as if they were located in the same physical organization. This makes scheduling meetings and resources easy and efficient.

Several components in a hybrid deployment are required to enable the shared free/busy feature in an Exchange 2010 deployment:

- **Federation trust** Both the on-premises and Microsoft Office 365 service organizations need to have a federation trust established with the Microsoft Federation Gateway. A federation trust is a one-to-one relationship with the Microsoft Federation Gateway that defines parameters for your Exchange organization. The gateway uses these parameters when acting as a trust broker between your on-premises and Office 365 service organization to exchange free/busy information between on-premises and Exchange Online organization users.
  By default, a federation trust with the gateway is automatically configured for your Office 365 service organization when the account is created. The Manage Hybrid Configuration wizard automatically checks to see if there is an existing federation trust with the Microsoft Federation Gateway for the on-premises organization. If present, the existing federation trust is used to support the hybrid deployment. If not present, the wizard creates a federation trust for the on-premises organization with the Microsoft Federation Gateway. The wizard also adds any domains selected within the Manage Hybrid Configuration wizard to the on-premises organization federation trust.
  Learn more at: Understanding Federated Delegation
- **Organization relationships** Organization relationships are needed for both the on-premises and Exchange Online organization and are configured automatically by the Manage Hybrid Configuration wizard. An organization relationship defines the level of free/busy information shared for an organization.
  By default, the free/busy data access sharing level is **Free/busy access with time, plus subject and location** for both the on-premises and Exchange Online organization relationships. If you want to modify the free/busy sharing access between your on-premises and Exchange Online organization users, you can manually configure the organization relationship access level after the Manage Hybrid Configuration wizard has completed.
  Learn more at: Understanding Federated Delegation

When configuring your organization for a hybrid deployment, configuring shared free/busy calendar access is automatically configured by the Manage Hybrid Configuration wizard in all scenarios. Creating a federation trust with the Microsoft Federation Gateway and configuring organization relationships for the on-premises and Exchange Online organization are hybrid deployment requirements. If you don't want to allow free/busy sharing between your on-premises and Exchange Online organization users in the hybrid deployment, you can manually disable free/busy sharing by using the Shell and the Set-HybridConfiguration cmdlet after the Manage Hybrid Configuration wizard has completed.

The hybrid deployment features shown in the following table have a dependency on federation trusts and organization relationships.

Messaging area	Feature
E-mail client	• Message tracking • MailTips • Multi-mailbox search
Transport	• Mailbox moves • Secure intra-organization message

	delivery
Compliance	• Exchange Online Archiving

1.14.10.6 Understanding Transport Options in Exchange 2010 Hybrid Deployments

Understanding Transport Options in Exchange 2010 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-01-25*

In hybrid deployments, you can have mailboxes that reside in your on-premises organization and also in an Exchange Online organization. A critical component of making these two separate organizations appear as one combined organization to users and messages exchanged between them is hybrid transport. With hybrid transport, messages sent between recipients in either organization are authenticated, transferred using Transport Layer Security (TLS), and appear as "internal" to Exchange components such as transport rules, journaling, and anti-spam policies. Hybrid transport is automatically configured by the Manage Hybrid Configuration wizard in Service Pack 3 (SP3) for Exchange 2010.

For hybrid transport configuration to work with the Manage Hybrid Configuration wizard, the on-premises SMTP endpoint that accepts connections from Exchange Online Protection (EOP), which handles transport for the Exchange Online organization, must be an Exchange 2010 SP3 Hub Transport or Edge Transport server. Hybrid transport makes use of new features provided in Exchange 2010 SP3 to secure messages and make them appear as "internal."

Important:

There can be no other SMTP hosts, services, or appliances between the on-premises Exchange 2010 SP3 Hub Transport or Edge Transport server and EOP. Information added to messages that enables hybrid transport features is removed when they pass through a non-Exchange 2010 SP3 server or SMTP host. This includes earlier versions of Exchange.
Hub Transport and Edge Transport servers must run Exchange 2010 SP3 to use the Manage Hybrid Deployment wizard for hybrid deployment configuration.

Inbound messages sent to recipients in both organizations from external Internet senders follow a common inbound route. Outbound messages sent from the organizations to external Internet recipients can either follow a common outbound route or can be sent via independent routes.

You'll need to choose how to route inbound and outbound mail when you configure your hybrid deployment. The route taken by inbound and outbound messages sent to and from recipients in the on-premises and Exchange Online organizations depends on the following:

- Do you want to route inbound Internet mail for both your on-premises and Exchange Online mailboxes through Microsoft Office 365 and EOP or through your on-premises organization?
  You can choose to route inbound Internet mail for both organizations through your on-premises organization or through EOP and the Exchange Online organization. The route that inbound messages for both organizations take depends on whether you enable centralized mail transport in your hybrid deployment.

- Do you want to route outbound mail to external recipients from your Exchange Online organization through your on-premises organization (centralized mail transport), or do you want to route it directly to the Internet?
  Known as centralized mail transport, you can route all mail from mailboxes in the Exchange Online organization through the on-premises organization before they're delivered to the Internet. This approach is helpful in compliance scenarios where all mail to and from the Internet must be processed by on-premises servers. Alternately, you can configure Exchange Online to deliver messages for external recipients directly to the Internet.

  Note:
  Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- Do you want to deploy an Edge Transport server in your on-premises organization?
  If you don't want to expose your domain-joined internal hybrid Hub Transport servers directly to the Internet, you can deploy Edge Transport servers in your perimeter network. For more information about adding an Edge Transport server to your hybrid deployment: see: Understanding Edge Transport Servers in Exchange 2010 Hybrid Deployments

Regardless of how you route messages to and from the Internet, all messages sent between the on-premises and Exchange Online organizations are sent using secure transport. For more information, see "Trusted Communication" later in this topic.

To learn more about how these options affect message routing in your organization, see Understanding Transport Routing in Exchange 2010 Hybrid Deployments.

Exchange Online Protection in Hybrid Deployments

EOP is an online service provided by Microsoft that's used by many companies to protect their on-premises organizations from viruses, spam, phishing scams, and policy violations. In Office 365, EOP is used to protect Exchange Online organizations from the same threats. When you sign up for Office 365, an EOP company is automatically created that's tied to your Exchange Online organization.

An EOP company contains several of the mail transport settings that can be configured for your Exchange Online organization. You can specify which SMTP domains must come from specific IP addresses, require a TLS and a Secure Sockets Layer (SSL) certificate, can bypass anti-spam filtering or compliance policies, and more. EOP is the front door to your Exchange Online organization. All messages, regardless of their origin, must pass through EOP before they reach mailboxes in your Exchange Online organization. And, all messages sent from your Exchange Online organization must go through EOP before they reach the Internet.

When you configure a hybrid deployment with the Manage Hybrid Configuration wizard, all transport settings are automatically configured in your on-premises organization and in the EOP company set up for your Exchange Online organization. The Manage Hybrid Configuration wizard configures all inbound and outbound connectors and other settings in this EOP company to secure messages sent between the on-premises and Exchange Online organizations and route messages to the right destination. If you want to configure custom transport settings for your Exchange Online organization, you'll configure them in this EOP company also.

Trusted Communication

To help protect recipients in both the on-premises and Exchange Online organizations, and to help ensure that messages sent between the organizations aren't intercepted and read, transport between the on-premises organization and EOP is configured to use forced TLS. TLS transport uses Secure Sockets Layer (SSL) certificates provided by a trusted third-party Certificate Authority (CA). Messages between EOP and the Exchange Online organization also use TLS.

When using forced TLS transport, the sending and receiving servers examine the certificate configured on the other server. The subject name, or one of the subject alternative names (SANs), configured on the certificates must match the FQDN that an administrator has explicitly specified on the other server. For example, if EOP is configured to accept and secure messages sent from the hybrid.contoso.com FQDN, the sending on-premises hybrid server must have an SSL certificate with hybrid.contoso.com in either the subject name or SAN. If this requirement isn't met, the connection is refused.

Note:

The FQDN used doesn't need to match the e-mail domain name of the recipients. The only requirement is that the FQDN in the certificate subject name or SAN must match the FQDN that the receiving or sending servers are configured to accept.

In addition to using TLS, messages between the organizations are treated as "internal". This approach allows messages to bypass anti-spam settings and other services.

Learn more about SSL certificates and domain security at: Understanding Certificate Requirements for Hybrid Deployments, Understanding TLS Certificates

1.14.10.7 Understanding Transport Routing in Exchange 2010 Hybrid Deployments

Understanding Transport Routing in Exchange 2010 Hybrid Deployments

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2013-02-01*

This topic discusses your routing options for inbound messages from the Internet and outbound messages to the Internet.

Note:

The examples in this topic don't include the addition of Edge Transport servers into the hybrid deployment. The routes messages take between the on-premises organization, the Exchange Online organization, and the Internet don't change with the addition of an Edge Transport server. The routing only changes within the on-premises organization. For more information about adding Edge Transport servers to a hybrid deployment, see Understanding Edge Transport Servers in Exchange 2010 Hybrid Deployments.

Inbound Messages from the Internet

As part of planning and configuring your hybrid deployment, you need to decide whether you want all messages from Internet senders to be routed through your on-premises organization or through the Exchange Online organization. All messages from Internet senders will initially be delivered to the organization you select and then routed according to where the recipient's mailbox is located. Whether you choose to have messages routed through your on-premises organization or the Exchange Online organization depends on various factors, including whether you want to apply compliance policies to all messages sent to both organizations, how many mailboxes are in each organization, and

so on.

The path messages sent to recipients in your on-premises and Exchange Online organizations take depends on how you decide to configure your MX record in your hybrid deployment. The Manage Hybrid Configuration wizard doesn't configure the routing for inbound Internet messages for either the on-premises or Exchange Online organizations. You must manually configure your MX record if you want to change how your inbound Internet mail is delivered.

- If you keep your MX record pointed to your on-premises organization: All messages sent to any recipient in either organization will be routed through your on-premises organization first. A message addressed to a recipient that's located in Exchange Online will be routed first through your on-premises organization and then delivered to the recipient in Exchange Online. This route can be helpful for organizations where you have compliance policies that require messages sent to and from an organization be examined by a journaling solution. This route is also recommended if you have more recipients in your on-premises organization than in your Exchange Online organization.
- If you decide to change your MX record to point to the Microsoft Exchange Online Protection (EOP) service in Office 365: All messages sent to any recipient in either organization will be routed through the Exchange Online organization first. A message addressed to a recipient that's located in your on-premises organization will be routed first through your Exchange Online organization and then delivered to the recipient in your on-premises organization. This route is recommended if you have more recipients in your Exchange Online organization than in your on-premises organization.

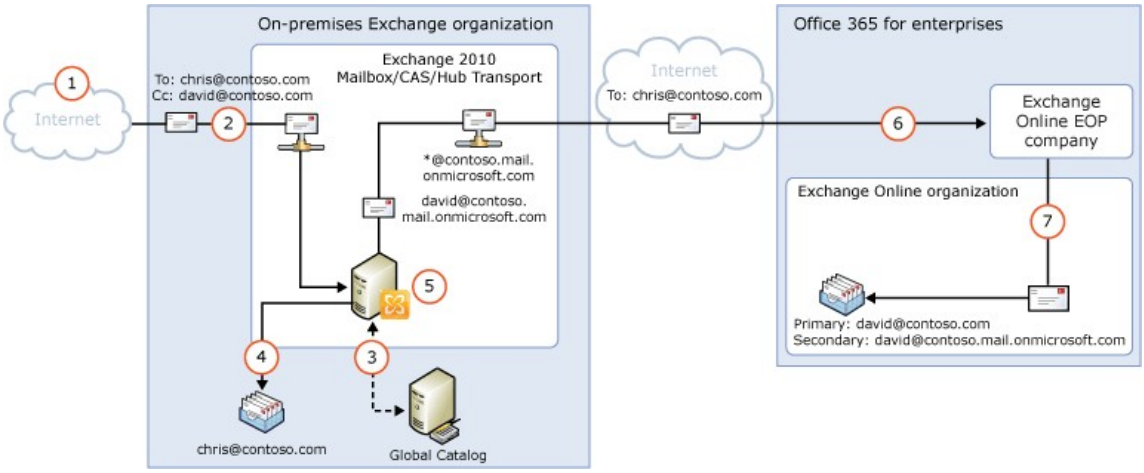
Read the section below that matches how you plan to route messages sent from Internet recipients to your on-premises and Exchange Online recipients.

Route Incoming Internet Messages Through Your On-Premises Organization

The following steps and diagram illustrate the inbound Internet message path that will occur in your hybrid deployment if you decide to keep your MX record pointed to your on-premises organization.

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2010 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to the on-premises organization, the message is delivered to an Exchange 2010 Mailbox server.
3. The Exchange 2010 Mailbox server performs a lookup for each recipient using an on-premises global catalog server. Through the global catalog lookup, it determines that Chris's mailbox is located on the Exchange 2010 Mailbox server while David's mailbox is located in the Exchange Online organization and has a hybrid routing address of david@contoso.mail.onmicrosoft.com.
4. The Exchange 2010 Mailbox server splits the message into two copies. One copy of the message is delivered to Chris's mailbox.
5. The second copy of the message is sent through the routing group connector that's configured between the hybrid servers and the Exchange 2010 server.
6. A hybrid Hub Transport server sends the message to EOP, which receives messages sent to the Exchange Online organization, using a Send connector configured to use TLS.
7. EOP sends the message to the Exchange Online organization where the message is scanned for viruses and delivered to David's mailbox.

Route mail through the on-premises organization for both on-premises and Exchange Online organizations



Route Incoming Internet Messages Through the Exchange Online Organization

The following steps and diagrams illustrate the inbound message path that occurs in your hybrid deployment if you decide to point your MX record to the EOP service in the Office 365 organization. The message path differs depending on whether you choose to enable centralized mail transport.

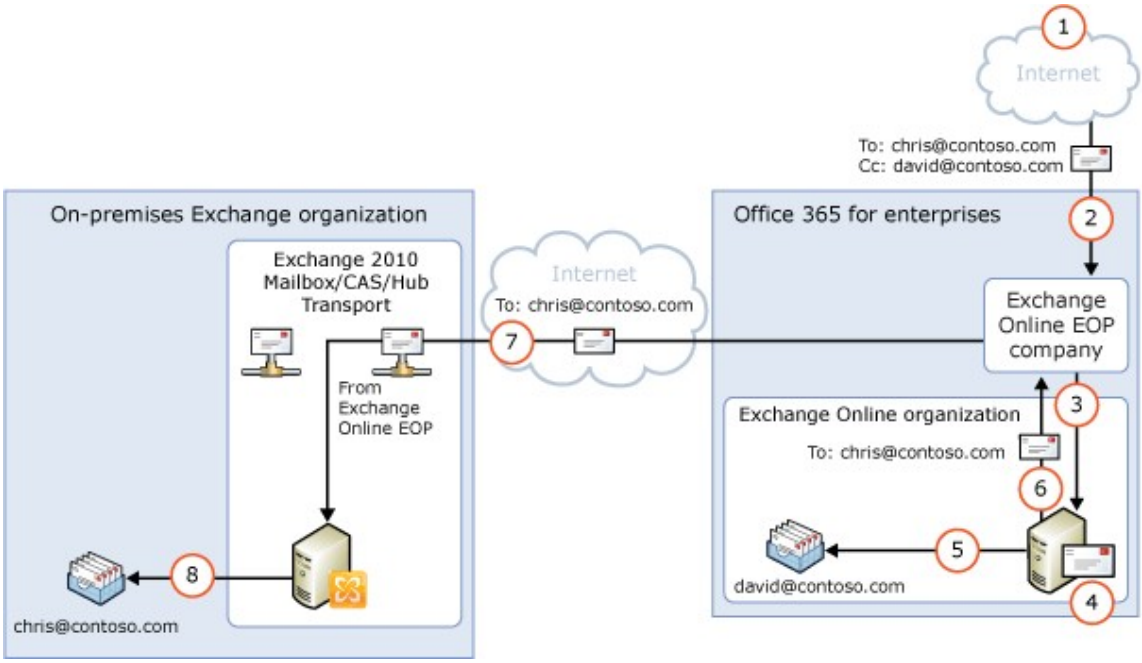
Important:

You may need to purchase EOP licenses for each on-premises mailbox that receives messages that are first delivered to EOP and then routed through the Exchange Online organization. Contact your Microsoft reseller for more information.

When centralized mail transport is *disabled* (default configuration), incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2010 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to EOP, the message is delivered to EOP.
3. EOP routes the messages for both recipients to Exchange Online.
4. Exchange Online scans the messages for viruses and performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. Exchange Online splits the message into two copies. One copy of the message is delivered to David's mailbox.
6. The second copy is sent from Exchange Online back to EOP.
7. EOP sends the message to the hybrid Exchange 2010 Hub Transport servers in the on-premises organization.
8. A hybrid Hub Transport server sends the message through the routing group connector that’s configured between the hybrid servers and the Exchange 2010 Mailbox server delivers the message to Chris's mailbox.

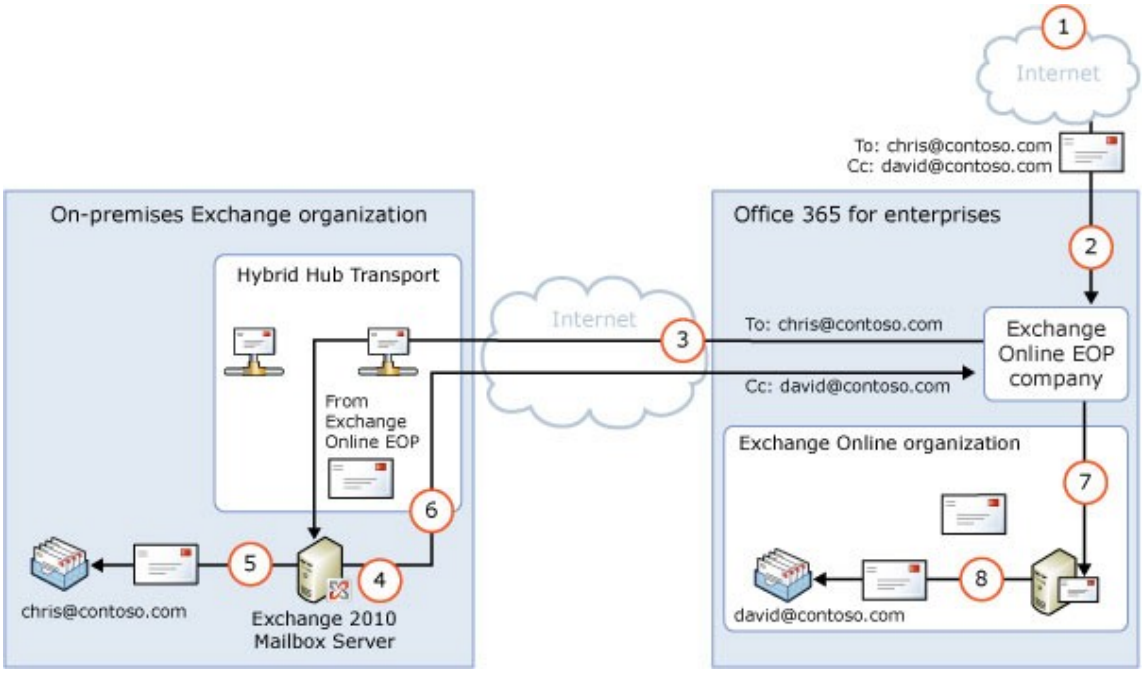
Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport disabled (default configuration)



When centralized mail transport is *enabled*, incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2010 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to EOP, the message is delivered to EOP and scanned for viruses.
3. Since centralized mail transport is enabled, EOP routes the messages for both recipients to the on-premises hybrid Exchange 2010 Hub Transport server.
4. The hybrid Hub Transport server performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. The hybrid Hub Transport server splits the message into two copies. One copy of the message is delivered to Chris’s mailbox in the on-premises Exchange 2010 server.
6. The second copy is sent from the hybrid Hub Transport server back to EOP.
7. EOP sends the message to Exchange Online.
8. Exchange delivers the message to David's mailbox.

Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport enabled



Outbound Messages to the Internet

In addition to choosing how inbound messages addressed to recipients to your organizations are routed, you can also choose how outbound messages sent from Exchange Online recipients are routed. When you run the Hybrid Configuration wizard, you can select one of two options:

- **Enable centralized mail transport** Selecting this option routes outbound messages sent from the Exchange Online organization through your on-premises organization. Except for messages sent to other recipients in the same Exchange Online organization, all messages sent from recipients in the Exchange Online organization are sent through the on-premises organization. This enables you to apply compliance rules to these messages and any other processes or requirements that must be applied to all of your recipients, regardless of whether they're located in the Exchange Online organization or the on-premises organization.

  Note:
  Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- **Don’t enable centralized mail transport** Selected by default in the Manage Hybrid Configuration wizard, this option routes outbound messages sent from the Exchange Online organization directly to the Internet. Use this option if you don't need to apply any on-premises compliance policies or other processing rules to messages that are sent from recipients in the Exchange Online organization.

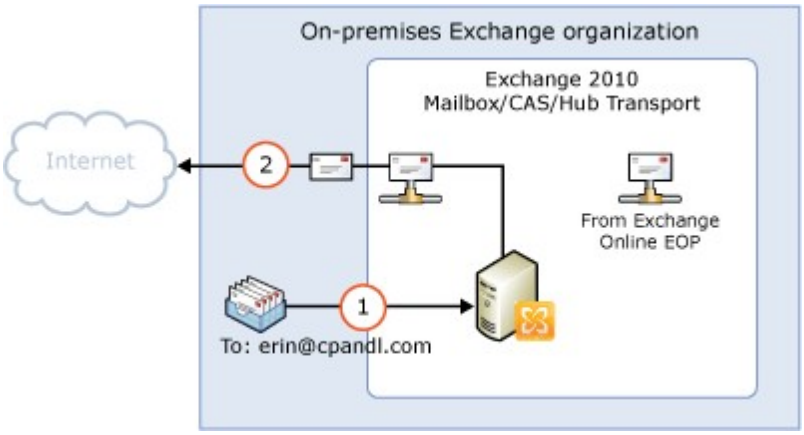
Messages sent from on-premises recipients are always sent to directly to Internet recipients using DNS regardless of which of the above choices you select in the Manage Hybrid Configuration wizard.

The following steps and diagram illustrate the outbound message path for messages sent from on-premises recipients.

1. Chris, who has a mailbox on the on-premises Exchange 2007 Mailbox server, sends a message to an external Internet recipient, erin@cpandl.com.

2. The Exchange 2010 server looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

Messages from on-premises senders to Internet recipients



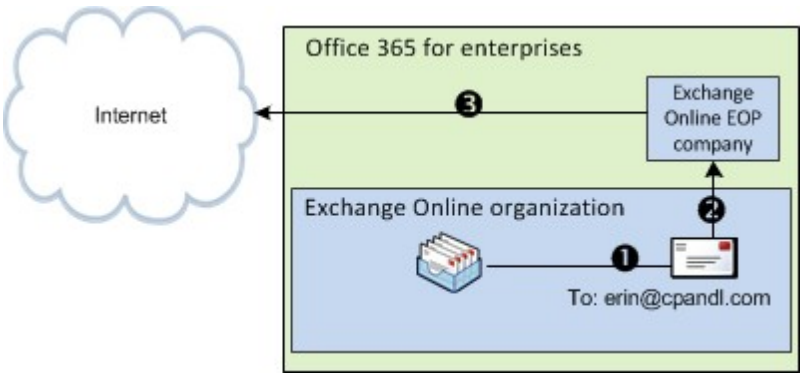
Read the section below that matches how you plan to route messages sent from recipients in the Exchange Online organization to Internet recipients.

Deliver Internet-Bound Messages from Exchange Online using DNS (Centralized Mail Transport Disabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when **Enable centralized mail transport** is not selected in the Manage Hybrid Configuration wizard, which is the default configuration.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to the Exchange Online EOP company.
3. EOP looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

Mail from Exchange Online senders routed directly to the Internet with centralized mail transport disabled (default configuration)

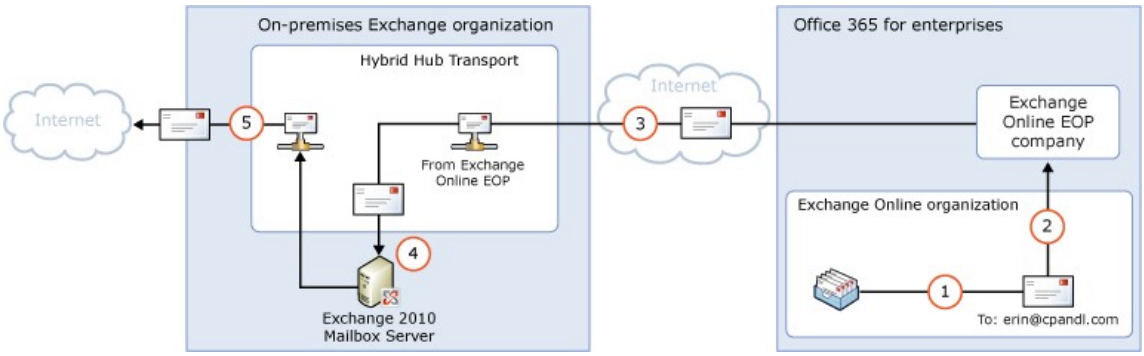


Route Internet-Bound Messages from Exchange Online Through Your On-Premises Organization (Centralized Mail Transport Enabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when you select **Enable centralized mail transport** in the Manage Hybrid Configuration wizard.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to EOP.
3. EOP is configured to send all Internet-bound messages to an on-premises server, so the message is routed to a hybrid Hub Transport server. The message is sent using TLS.
4. An hybrid Hub Transport server performs compliance and any other processes configured by the administrator on David's message.
5. The hybrid Hub Transport server looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

Mail from Exchange Online senders routed through on-premises organization with centralized mail transport enabled



1.14.10.8 Understanding IRM in Exchange 2010 Hybrid Deployments

Understanding IRM in Exchange 2010 Hybrid Deployments

Exchange Server 2010 > Hybrid Deployments > Hybrid Deployments with Exchange 2010 SP3 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-18*

Information Rights Management (IRM) helps you to protect against leakage of sensitive information by providing persistent online and offline protection of e-mail messages and attachments. Both Exchange 2010, in your on-premises organization, and Exchange Online, in Office 365 for enterprises, support IRM. However, there are differences between the two implementations, and you must configure IRM in the Exchange Online organization before users in that organization can use it.

IRM uses Active Directory Rights Management Services (AD RMS), which is a component of Windows Server 2008 R2. AD RMS allows users to create rights-protected content, such as e-mail messages and attachments, and then control how that content is used, and to whom it's distributed. Users can specify templates that determine how content can be used. For example, a user may specify that an e-mail message can't be forwarded to other recipients or that information in the message can't be copied.

Learn more about IRM in Exchange 2010 at: Understanding Information Rights Management

Learn more about AD RMS at: Active Directory Rights Management Services Overview

Learn more about configuring IRM at: Configure IRM in Exchange 2010 Hybrid Deployments

IRM in Hybrid Deployments

Exchange uses AD RMS servers in the Active Directory forest in which the Exchange server is installed. For your on-premises Exchange 2010 servers, the on-premises AD RMS server is used. For your Exchange Online organization, AD RMS servers that are maintained within the Microsoft Office 365 datacenters are used. The AD RMS configuration that each Exchange organization uses is independent of any other AD RMS deployment.

AD RMS configuration, and therefore IRM configuration, isn't automatically replicated between your on-premises Exchange organization and the Exchange Online organization. Any AD RMS templates that you've defined aren't automatically copied to the Exchange Online organization. If you want the same AD RMS templates to be available in the Exchange Online organization, you must manually export the templates from your on-premises organization and apply them to the cloud-based organization. See the IRM Configuration in Hybrid Deployments section later in this topic.

User Experience

The IRM configuration that's applied to a user depends on the client the user uses and the location of the user's mailbox. The following table shows the AD RMS server a user will use.

Active AD RMS server

Client	On-premises mailbox	Cloud-based mailbox
Outlook 2007 or Outlook 2010	On-premises AD RMS	On-premises AD RMS
Outlook Web App	On-premises AD RMS	Exchange Online AD RMS
ActiveSync device	On-premises AD RMS	Exchange Online AD RMS

It's possible that, depending on the AD RMS configuration you configure in your on-premises and Exchange Online organizations, a user who uses Outlook 2007 and Outlook Web App may see different AD RMS templates. For this reason, we strongly recommend that you apply the same templates to both your on-premises and Exchange Online organizations.

There should be no difference in the IRM experience for Outlook client users, regardless of whether their mailbox is located in the on-premises or Exchange Online organization.

An Outlook Web App user whose mailbox is located on an Exchange 2010 server can only open rights-protected messages after installing the Rights Management for Internet Explorer add-in. They can't reply to or create new rights-protected messages.

An Outlook Web App user whose mailbox is located in Exchange Online can open rights-protected messages without any additional software and can reply to, and create, new rights-protected messages.

Server Functionality

On-premises Exchange 2010 servers use the AD RMS pre-licensing agent to decrypt rights-protected messages so that users don't need to supply credentials when they open those messages. The on-premises Exchange 2010 server contacts the on-premises AD RMS server to check usage policies and rights, and to request authorization to decrypt the message.

The Exchange Online organization provides several additional IRM-related features that make use of Exchange Online AD RMS. These features, such as journal report decryption, make the content of right-protected messages available to Exchange services for

additional processing. For example, the decrypted contents of a journaled message can be saved, along with the original rights-protected message, to allow for easier discovery. Additionally, IRM templates can automatically be applied to messages using either Outlook protection rules or transport rules to ensure that messages adhere to organization policies regarding information protection.

IRM Configuration in Hybrid Deployments

IRM in Exchange relies on AD RMS being deployed in the Active Directory forest in which the Exchange server resides. AD RMS configuration isn't automatically synchronized between the on-premises and Exchange Online organizations. You must manually export the AD RMS configuration, known as a trusted publishing domain (TPD), from your on-premises AD RMS server, and import that configuration into the Exchange Online organization. The TPD contains the AD RMS configuration, including templates, which the Exchange Online organization needs to use IRM.

Learn more at: AD RMS Trusted Publishing Domain Considerations

In addition to applying your on-premises AD RMS configuration to the Exchange Online organization, you must ensure that your AD RMS servers can be contacted by Outlook and ActiveSync clients outside of your on-premises network. You must do this if you want these clients to access rights-protected messages outside of your on-premises network.

After you've configured your on-premises network and exported the TPD data, you need to configure the Exchange Online organization by importing the TPD data and enabling IRM.

Note:

Any time you modify your on-premises AD RMS configuration, you must manually apply the new configuration in the Exchange Online organization. To do so, export the TPD data from your on-premises AD RMS server and import it into the Exchange Online organization.

Learn more at: Configure IRM in Exchange 2010 Hybrid Deployments

1.14.10.8.1 Configure IRM in Exchange 2010 Hybrid Deployments

Configure IRM in Exchange 2010 Hybrid Deployments

Hybrid Deployments > Hybrid Deployments with Exchange 2010 SP3 > Understanding IRM in Exchange 2010 Hybrid Deployments >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

If you use Information Rights Management (IRM) in your on-premises Exchange organization and you want your Exchange Online users to also use IRM, you need to do the following:

1. Configure your on-premises Active Directory Rights Management Services (AD RMS) server.
2. Enable IRM in your Exchange Online organization.
3. Distribute the imported AD RMS templates to users in the Exchange Online organization.

Learn more at: Understanding IRM in Exchange 2010 Hybrid Deployments

How do I configure on-premises AD RMS servers?

To configure IRM in a hybrid deployment, you need to use Windows PowerShell to access your on-premises AD RMS server. Learn more at: Using Windows PowerShell to Administer AD RMS

Do the following to export trusted publishing domain (TPD) data from your on-premises AD RMS server and then configure access to the AD RMS server for external clients.

1. Export TPD data from your on-premises organization. Learn more at: Exporting a Trusted Publishing Domain
2. Configure access to AD RMS servers from external clients. Learn more at: Adding an Extranet Cluster URL

How do I enable IRM in the Exchange Online organization?

After you export the TPD data from your on-premises AD RMS servers, you need to import that data into the Exchange Online organization and then enable IRM.

1. In the Exchange Online organization, import the TPD data.

```
Import-RMSTrustedPublishingDomain -FileData $( [Byte[]] (Get-Content -
```

2. Enable IRM in the Exchange Online organization.

```
Set-IRMConfiguration -InternalLicensingEnabled $True
```

How do I distribute AD RMS templates in the Exchange Online organization?

After you've enabled IRM in the Exchange Online organization, you must distribute the imported AD RMS templates. The following Exchange Online users and features use AD RMS templates:

- Outlook Web App users
- Exchange ActiveSync users
- Transport rules
- Journal report decryption
- Outlook protection rules

1. In the Exchange Online organization, retrieve a list of AD RMS templates.

```
Get-RMSTemplate -Type All
```

2. Distribute the AD RMS templates to users and features in the Exchange Online organization.

```
Set-RMSTemplate <template name> -Type Distributed
```

Note:
You can't modify the "Do Not Forward" AD RMS template.

3. Repeat step 2 for each AD RMS template you want to distribute.

How do I know this worked?

Outlook Web App users should be able to apply AD RMS templates to new messages. Outlook Web App and Exchange ActiveSync users should be able to read messages that have AD RMS templates applied to them. In addition, all the AD RMS templates that were imported from your on-premises organization should be listed when you run the **Get-**

RMSTemplate cmdlet.

Run the following command in the Exchange Online organization.

```
Get-RMSTemplate
```

Learn more at: Understanding Information Rights Management in Outlook Web App

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

1.15 Performance and Scalability

Performance and Scalability

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

Understanding performance and scalability is critical to designing and maintaining a high performance messaging infrastructure with Microsoft Exchange Server 2010. The topics in this section will help you understand the considerations that you should evaluate when designing, deploying, and maintaining your Exchange 2010 infrastructure.

Understanding Exchange Performance

Learn about all the variables that affect your system's performance, including user profile, architecture, and hardware.

Tools for Performance and Scalability Evaluation

Learn about using the Microsoft Exchange Jetstress and the Microsoft Exchange Load Generator tools to manage user load on your system.

Performance and Scalability Counters and Thresholds

Learn about performance and scalability counters that you can use to monitor your Exchange organization.

1.15.1 Understanding Exchange Performance

Understanding Exchange Performance

Exchange Server 2010 > Performance and Scalability >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-05-02*

Tuning a system for optimum performance is an iterative process. You must take the time to understand all the variables that affect your system, including user profile, architecture, and hardware. With this knowledge, you can establish baseline metrics for your systems and make adjustments to improve system performance.

Generally, the maximum level performance for a server is determined by the component that has the lowest performance—the bottleneck in the system. The key to improving

performance is being able to identify bottlenecks, determine their cause, and take the appropriate corrective action.

As you plan your Microsoft Exchange Server 2010 deployment, you can use the topics in this section to help design and optimize your environment for high performance:

- Understanding Processor Configurations and Exchange Performance
- Understanding Memory Configurations and Exchange Performance
- Understanding Server Role Ratios and Exchange Performance
- Understanding Multiple Server Role Configurations in Capacity Planning
- Understanding Client Access and Hub Transport Combined Role Configurations in Capacity Planning
- Calculate Megahertz Per User and IOPS Per User

The concept of performance is closely related to the concept of scalability. When you have a solid understanding of the factors influencing the performance of system components, you can deploy components in a way that scales to support periods of high demand.

This topic provides information about:

- Measuring performance
- Hardware performance

Measuring Performance

Several tools for measuring performance are available for use with Exchange 2010, including Jetstress and Load Generator (LoadGen). The Windows Server 2008 operating system also includes some general performance tools including Windows Performance Monitor.

In addition to these tools, you should analyze your current user loads to establish a minimum server requirements baseline. Understanding how your users use the system is one of your biggest challenges. After you determine your hardware requirements, you should conduct a pilot test to make sure performance levels are acceptable.

For more information, see Tools for Performance and Scalability Evaluation.

Hardware Performance

When selecting hardware for your Exchange servers you must consider many factors. The hardware that you select for your Exchange deployment has the greatest effect on performance. Two of the most critical resources to evaluate are processor and memory. Because of the large number of variables that affect performance, it's difficult to predict the effects of high server utilization on the performance of any particular hardware component. The following definitions apply to the terms minimum, maximum, and recommended:

Minimum This is the minimum processor and memory configuration suitable for specific Exchange 2010 server roles (also defined in system requirements). Minimum hardware requirements must be met to receive Microsoft Customer Service and Support.

Maximum This is the maximum recommended processor and memory configuration for specific Exchange 2010 server roles. Maximum is defined as the upper bound of viable processor and memory configurations for Exchange 2010 based on price and performance. Maximum is a guideline and not a support criterion. It doesn't take into account the resource requirements of third-party applications. The recommended maximum may change over time based on price changes and technology advancements.

Recommended This is the recommended processor and memory configuration for specific

Exchange 2010 server roles. Recommended can be defined as the best configuration based on price and performance. The recommended configuration also provides a balance between processor and memory capacity. The goal is to match the memory configuration to the processor configuration so the system will effectively utilize the processors without becoming bottlenecked on memory or vice versa.

Processor Performance

Exchange 2010 benefits significantly when running on multi-core processors. The performance benefit for Exchange from multi-core technology depends upon the specific processor utilized. Multi-core processors are an attractive option for Exchange 2010 servers based on price and performance. It's important to consult with your server hardware vendor about multi-core benefits for Exchange, specific to a given hardware architecture.

The processor usage on a server should maintain a load of about 60 percent during peak working hours. This percentage level allows room for periods of extreme load. If the processor usage is consistently greater than 75 percent, processor performance is considered a bottleneck.

There are several factors by which the CPU in a server affects performance. These include:

- The processor clock speed, measured in megahertz (MHz) or gigahertz (GHz)
- The number of processors
- The type of processor

For performance, selecting the fastest processor yields the best results. However, budget and cost dictate most companies' choices.

Exchange can fully use multiple processors, and using servers with more processors improves performance. However, the relationship between the number of processors, number of processor cores, and performance is complex. The optimum number of processors and cores is partly determined by the Exchange role deployed on the server.

For more information about how different processors perform, see Understanding Processor Configurations and Exchange Performance.

Memory Performance

After the required number of processor cores has been estimated for a specific server role, baseline memory recommendations can be applied. Exchange 2010 on the 64-bit editions of the Windows Server 2008 operating system can efficiently utilize upwards of 64 GB of memory (Mailbox server role).

With effective planning and an understanding of the basic processor and memory requirements for specific Exchange 2010 server roles, a balanced and cost-effective topology can be attained.

For more information about how different memory configurations perform, see Understanding Memory Configurations and Exchange Performance.

Network Performance

Much of the network interface subsystem is tuned automatically. Server-based network adapters are capable of detecting the type and level of traffic passing through the network interface, and they self-tune to reflect this information. We recommend that you have operational practices in place to ensure that the latest device drivers are maintained on the server.

For Mailbox servers, gigabit Ethernet (1,000 megabits per second (Mbps) or 1 gigabit per second (Gbps)) is recommended.

Multiple switched fast Ethernet networks of gigabit Ethernet connections are recommended.

Performance-related issues may arise because your hardware, firmware, or software drivers aren't designed to work in your configuration. For more information, see the Windows Hardware Development Web site.

Storage Performance

As storage requirements increase and companies consolidate servers, you must balance cost, availability, and performance when you design a storage system. Take time to invest in good storage design before you implement it. Unlike processors and memory, which you can scale while the network is active, storage redesign requires network downtime to implement. Tuning your Exchange storage becomes a critical component in the overall performance of your Exchange environment.

There are a few guidelines that can be followed for selecting a storage configuration that provides good performance and a strong platform for Exchange 2010. Capacity and performance are often at odds with each other when it comes to selecting a storage solution, and both must be considered before making a purchase. Generally, the decision involves analysis of the following factors:

- Making sure there will be enough space to store all of the data. Determining your capacity needs is a relatively straightforward process.
- Making sure the solution provides acceptable disk latency and a responsive user experience. This is determined by measuring or predicting transactional input/output (I/O) delivered by the solution.
- Making sure that non-transactional I/O has both enough time to complete and enough disk throughput to meet your service level agreements (SLAs).

The goal is to find a balance of these factors so that you can design the actual hardware solution for your servers.

For more information about choosing a storage solution for Exchange 2010, see Mailbox Server Storage Design.

1.15.1.1 Understanding Processor Configurations and Exchange Performance

Understanding Processor Configurations and Exchange Performance

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-02-10*

Three of the most critical factors to consider when selecting hardware for use by Microsoft Exchange Server 2010 are choice of processor, amount of memory, and selection of storage. This topic provides guidelines for processor configurations that provide good performance and a strong platform for Exchange.

For detailed guidance and recommended configurations for memory, see Understanding Memory Configurations and Exchange Performance. For more information about selecting storage, see Understanding Storage Configuration.

Contents

Selecting the Appropriate Processor

For production environments, you must choose a processor that works with the 64-bit edition of the Windows Server operating system.

The release to manufacturing (RTM) version of Exchange 2010 is only supported in production environments when the x64 version of Exchange 2010 is installed on a computer with x64-compatible processors running 64-bit editions of Windows Server 2008 or Windows Server 2008 R2.

You can select processors from Intel that support Intel Extended Memory 64 Technology or processors from AMD that support AMD64. For more information about these processor options, see the Intel 64 Architecture Web site or the AMD Opteron Processor Family Web site at http://www.amd.com/us-en/Processors/ProductInformation/0,,30_118_8825,00.htm.

Exchange 2010 is designed to run only on x64-capable processors such as those listed previously, and it doesn't run on Itanium-based systems.

Regardless of which processor you choose, the server product must have the Designed for Windows logo to be supported. For more information, see Windows Logo Program: Overview. To ensure support, you must select a server listed in the Windows Server Catalog. If your server isn't listed, you should verify with the hardware vendor that testing is in progress.

Return to top

Hyperthreading

Hyperthreading causes capacity planning and monitoring challenges, and as a result, the expected gain in CPU overhead is likely not justified. Hyperthreading should be disabled by default for production Exchange servers and only enabled if absolutely necessary as a temporary measure to increase CPU capacity until additional hardware can be obtained.

Return to top

Recommended Processor Configurations

You can use the following table to assist you in purchasing server hardware for Exchange 2010. This table provides minimum requirements and recommended maximum configurations for Exchange 2010 based on the following definitions:

- **Minimum** This is the minimum processor and memory configuration suitable for specific server roles. The minimum hardware requirements must be met to receive support from Microsoft Customer Service and Support.
- **Recommended maximum populated processor sockets** This is the recommended maximum number of motherboard processor sockets that should be used for the roles listed, based on price and expected performance. The recommended maximum configuration is a guideline and may change over time based on price changes and technology advancements. It isn't a support

criterion.

- **Example recommended maximum processor cores (assuming 6 core processors)** This is the example maximum recommended processor and memory configuration for specific server roles. Maximum is defined as the upper bound of viable memory configurations based on price and performance. The recommended maximum configuration is a guideline. It isn't a support criterion, and it doesn't take into account the resource requirements of third-party applications that might access or be installed on the server. The recommended maximum configuration may change over time based on price changes and technology advancements.

Note:
The following guidance assumes an average concurrency profile. Concurrency is defined as the percentage of the total number of users on a server that are connected and using the server at a specific peak period of time. For a fully utilized server, concurrency is generally in the 75 to 80 percent range.

Processor configurations for Exchange 2010 server roles

Exchange 2010 server role	Minimum	Recommended maximum populated processor sockets	Example recommended maximum processor cores (assuming 6 core processors)
Edge Transport	1 x processor core	2	12 x processor cores
Hub Transport	1 x processor core	2	12 x processor cores
Client Access	2 x processor core	2	12 x processor cores
Unified Messaging **Note:** Recommendations based on Unified Messaging being deployed with the default configuration that includes Voice Mail Preview enabled.	2 x processor core	2	12 x processor cores
Mailbox	2 x processor core	2	12 x processor cores
Client Access/Hub Transport combined (Client Access and Hub Transport roles running on the same physical server)	2 x processor core	2	12 x processor cores
Multiple (Client Access, Hub Transport, and Mailbox server roles running on the same physical server)	2 x processor cores	4	24 x processor cores

Important:
Some server virtualization platforms may not support the maximum number of processors identified in the preceding table. If you're planning to deploy Exchange server roles on a virtualization platform, check the documentation for that platform to determine the maximum number of supported virtual processors.

Note:
Ratings available at the Standard Performance Evaluation Corporation Web site may be used to rationalize unlike processor and server configurations.

Hub Transport Server Role

We recommend a configuration for the Hub Transport server role of 8 x processor cores in organizations where Hub Transport servers are deployed with several Mailbox servers and thousands of mailboxes. Servers with larger processor cores can be efficiently used when the Hub Transport server is configured to use antivirus and anti-spam tools. Processor utilization is based on several factors such as message rate, average message size, number of enabled transport agents, antivirus configuration, and third-party applications.

Client Access Server Role

In Exchange 2010 architecture, most of the client-specific functions have been moved from the Mailbox server to the Client Access server. In Exchange 2010, messages are converted on the Client Access server when they're accessed by a non-MAPI client (for example, POP3 and IMAP4 clients). In addition, rendering for Microsoft Office Outlook Web App is performed on the Client Access server, as opposed to the Microsoft Exchange Information Store service in previous versions of Exchange.

These architectural changes allow the Client Access server to offload significant processing from the Mailbox server and to effectively utilize 8 x processor cores. Servers with 2 x processor cores can be utilized for Client Access servers in organizations where there aren't enough mailboxes or insufficient non-MAPI client traffic to warrant using 4 x processor core servers.

Unified Messaging Server Role

We recommend a configuration for the Unified Messaging server role of 8 x processor cores. Multiple cores are used on the Unified Messaging server for several architectural functions such as .wav to Microsoft Windows Media Audio (WMA) conversions for voice mail messages. Servers with 2 x processor cores can be used for Unified Messaging servers in organizations where there aren't enough mailboxes or insufficient Unified Messaging server activity to warrant using 4 x processor core servers.

Mailbox Server Role

We recommend a configuration for the Mailbox server role based predominantly on mailbox count and user profile. A 4 x processor core server provides a good balance between price and performance, and it should be able to host several thousand mailboxes. Sizing for the Mailbox server requires an understanding of the average client user profile. This profile can be collected using transport performance counters that indicate overall message throughput within an Exchange system. You can also use third-party tools.

For more information about processor requirements for specific user profiles (based on message throughput), see Mailbox Server Processor Capacity Planning.

Multiple Role Server

As a general guideline, a multiple role server should be sized to use half of the available processor cores for the Mailbox server role and the other half for the Client Access and Hub Transport server roles. The maximum recommended processor core configuration is listed at 24 x processor cores for the multiple server roles configuration to indirectly provide guidance on the maximum number of users that should be hosted on a multiple role server. Although this configuration can use more than 24 x processor cores, we don't recommend it. For more information, see Understanding Multiple Server Role Configurations in Capacity Planning. For more information about the combined Hub Transport and Client Access server roles, see Understanding Client Access and Hub Transport Combined Role Configurations in Capacity Planning.

Return to top

Virtual Deployments

The CPU overhead associated with running a guest operating system in a virtual machine was found in testing to range from 9 percent through 12 percent. For example, a guest operating system running on a virtual machine typically had available 88 percent to 91 percent of the CPU resources available to an equivalent operating system running on physical hardware. We recommend reducing the user capacity of Mailbox servers by 10 percent to account for hypervisor processor overhead.

Return to top

1.15.1.2 Understanding Memory Configurations and Exchange Performance

Understanding Memory Configurations and Exchange Performance

Exchange Server 2010 > Performance and Scalability > Understanding Exchange Performance >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-04-23*

This topic provides guidelines for memory configurations that provide good performance and a strong platform for Microsoft Exchange Server 2010. For detailed guidance and recommended configurations for processors, see Understanding Processor Configurations and Exchange Performance.

When selecting hardware for Exchange 2010, we recommend that you consider the server maximum memory configuration. Different server architectures have different memory limits. We recommend that you check the following technical specifications of the server to determine the most cost-efficient maximum memory configuration for your servers:

- **Memory speed** Some server architectures require slower memory modules to scale to the maximum supported amount of memory in a specific server. For example, maximum server memory could be limited to 32 GB with PC3 10666 (DDR3 1333) or 128 GB using PC2 6400 (DDR2 800). You should check with the manufacturer to ensure that the memory configuration target for Exchange 2010 is compatible in terms of speed.
- **Memory module size** Consider the largest memory module size that the server will support. Generally, the larger the memory module, the more expensive. For example, two 2 GB DDR SDRAM memory modules generally cost much less than one 4GB DDR SDRAM memory module and two 4 GB DDR SDRAM memory modules generally cost much less than one 8GB DDR SDRAM memory module. Make sure the maximum memory module size allows you to meet your target memory requirements for Exchange 2010.
- **Total number of memory slots** Consider how many memory modules that a specific server will support. The total number of slots multiplied by the maximum memory module size provides the maximum memory configuration for the server. Keep in mind that memory modules must sometimes be installed in pairs.

Be aware that some servers experience a performance improvement when more memory slots are filled, while others experience a reduction in performance. Check with your hardware vendor to understand this effect on your server architecture.

Recommended Memory Configurations

After the number of processor cores estimated to be required per server role is understood, baseline memory recommendations can be applied. The following table illustrates the minimum supported and recommended memory configurations for Exchange 2010 server roles.

The following describes the minimum requirements and recommended maximum configurations:

Minimum Supported This is the minimum memory configuration suitable for Exchange 2010 servers. The minimum hardware requirements must be met to receive support from Microsoft Customer Service and Support.

Recommended Maximum This is the recommended memory configuration for specific server roles. Recommended maximum is defined as the upper limit of viable processor and memory configurations based on price and performance. The recommended maximum configuration is a guideline. It isn't a support criterion, and it doesn't take into account the resource requirements of third-party applications that might access or be installed on the server. The recommended maximum configuration may change over time based on price changes and technology advancements.

The following table shows the minimum supported and recommended maximum memory configurations for Exchange 2010.

Memory configurations for Exchange 2010 servers based on installed server roles

Exchange 2010 server role	Minimum supported	Recommended maximum
Edge Transport	4 GB	1 GB per core (4 GB minimum)
Hub Transport	4 GB	1 GB per core (4 GB minimum)
Client Access	4 GB	2 GB per core (8 GB minimum)
Unified Messaging	4 GB	2 GB per core (4 GB minimum)
Mailbox	4 GB	4 GB base plus additional memory based on the user profile and database cache size. For more information about how to determine the total required memory, see Understanding the Mailbox Database Cache.
Client Access/Hub Transport combined role (Client Access and Hub Transport server roles running on the same physical server)	4 GB	2 GB per core (8 GB minimum)
Multiple roles (combinations of Hub Transport, Client Access, and Mailbox server roles)	8 GB	4 GB plus 3-30 MB additional memory per mailbox: The total required memory is based on the user profile and database cache size. For

		more information about how to determine the total required memory, see Understanding the Mailbox Database Cache.

Edge Transport and Hub Transport Server Roles

The Edge Transport and Hub Transport server roles don't require substantial quantities of memory to perform well in optimal conditions. Generally, 1 GB of RAM per processor core (4 GB minimum total) is sufficient to handle all but the most demanding loads. Most deployments will be optimally configured with the recommended memory configuration of 1 GB per processor core (4 GB minimum total).

Client Access Server Role

In general, memory utilization on Client Access servers has a linear relationship with the number of client connections and the transaction rate. Based on the current recommendations of 2 GB per core processor and memory configurations, a Client Access server will be balanced in terms of memory and processor utilization, and it will become processor-bound at approximately the same time it becomes memory- bound.

These recommendations are based on the Exchange 2010 feature, RPC Client Access. This feature requires a larger memory and processor configuration to manage the increased loads placed on the Client Access server role.

Mailbox Server Role

The memory configuration process for the Mailbox server role is more complex than the other roles because the optimal memory configuration depends upon the server roles installed, the mailbox count, the client profile (similar to estimating processor core requirements), and the number of active databases.

Memory sizing for the Mailbox server role is critical to reducing disk input/output (I/O) on the server. The more memory you add to the Mailbox server, the less disk I/O will be generated by Exchange. There is, however, a point of diminishing returns at which adding memory to the server may not be justifiable based on price and performance. The recommendations discussed in "Recommended Memory Configurations" earlier in this topic consider this point of diminishing returns and are based on current memory prices and performance metrics.

For more information about how to perform appropriate memory sizing for the Mailbox server role, see the following topics:

- Mailbox Server Storage Design
- Understanding the Mailbox Database Cache

Multiple Server Roles

When determining memory requirements for multiple role server configurations, you need to consider the requirements of Hub Transport, Client Access, and Mailbox server roles. To assist you, we have provided the calculated memory requirements in the preceding table. For additional information, see the following:

- "Memory Recommendations for Multiple Role Servers" in Understanding Multiple Server Role Configurations in Capacity Planning
- Understanding Client Access and Hub Transport Combined Role Configurations in Capacity Planning

1.15.1.3 Understanding Server Role Ratios and Exchange Performance

Understanding Server Role Ratios and Exchange Performance

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-01-26*

After you've determined your optimal processor, memory, and disk configurations, you should determine how many server roles of each type are required for your deployment. Every environment is different, so consider these recommendations as starting points that can be tailored to your environment.

Contents

Server Role Ratios

The following table shows recommended server role ratios that are based on the processor core guidance in the topic Understanding Processor Configurations and Exchange Performance. Also, the Mailbox server role is the basis for the processor core ratios. Hub Transport and Client Access server roles relate to the Mailbox server role with regard to the recommendation.

Note:
You can also use the ratings available at Standard Performance Evaluation Corporation to rationalize different processor and server configurations.

Recommended processor core ratio based on server role configuration

Server role configuration	Recommended processor core ratio
Mailbox:Hub Transport	7:1 (no antivirus scanning on Hub Transport server) 5:1 (with antivirus scanning on Hub Transport server)
Mailbox:Client Access	4:3
Mailbox:Client Access and Hub Transport combined role	1:1

Important:
The recommended Mailbox to Client Access server role ratios are based on the use of the Exchange 2010 feature, RPC Client Access. This feature requires a larger memory and processor configuration to manage the increased loads placed on the Client Access server role. The RPC Client Access feature is enabled by default. For more information, see Understanding RPC Client Access.

When considering these recommendations, be aware of the following:

- The preceding ratios are a general rule (not definitive), and they may not be valid for every topology. A general rule means that the ratios aren't a requirement for support.
- Ratios can change dramatically based on user profiles. A user that creates a larger than expected load against the Mailbox server role rather than the Hub Transport server role will increase the Mailbox:Hub Transport ratio, and vice versa.
- These recommendations are derived from the internal deployment of Mailbox servers at Microsoft, which is based on approximately 750 heavy users per processor core.
- These ratios assume that Mailbox servers are at greater than 60 percent processor utilization during peak periods, with corresponding processor utilization on Hub Transport or Client Access servers.
- For these recommendations, the processors used on Mailbox, Hub Transport, and Client Access server roles were the same type and speed.
- A minimum of two Hub Transport and two Client Access servers should be deployed for redundancy and to ensure uninterrupted service in case of planned or unplanned server downtime.
- The Hub Transport server role ratio that includes antivirus scanning was obtained using Microsoft Forefront Security for Exchange Server with five active scanning engines.
- The Client Access server role ratio includes using Secure Sockets Layer (SSL) for all access protocols.

It's not possible to provide a ratio for the Unified Messaging server role because its utilization isn't directly tied to the Mailbox server role. For more information about Unified Messaging server capacity planning, see Understanding Unified Messaging Availability.

Return to top

Edge Transport Server Ratio

To determine how many Edge Transport servers are required, you must measure or estimate the following metrics during peak periods:

- Connections per second
- Messages per second
- Average message size

Sizing is based on the number of connections and messages processed, with average message size being a secondary factor. Because every SMTP connection doesn't become an SMTP message, and because every accepted message won't survive antivirus and anti-spam scanning, it's difficult to provide a simple sizing methodology based on message rate. Edge Transport server utilization depends on several factors that are unique to each organization.

Note:
A minimum of two Edge Transport servers should be deployed for redundancy and to ensure uninterrupted service in case of planned or unplanned server downtime.

The following table provides performance data values for key metrics from internal deployment at Microsoft. You can use the metrics and their values to help you understand the performance characteristics of an Edge Transport server.

Performance metrics from internal deployment of Edge Transport servers at Microsoft

Performance metric	Value
SMTP Connections/Sec	55

% Connections Accepted	80 %
SMTP Messages IMF Scanned/Sec	3.7
% SMTP Messages passed IMF Scanning	80 %
SMTP Messages A/V Scanned/Sec	3
Avg. Message Size	70 KB
CPU Utilization	20 %**

** System included a 2-socket, dual-core AMD Opteron 275 2.2 gigahertz (GHz) processor

A significant percentage of the server processing is associated with the overhead of analyzing connections and scanning accepted messages. For this reason, it's not possible to provide a sizing metric based solely on the number of messages sent and received per second because antivirus and anti-spam operations are significant processor utilization functions of the Edge Transport server role.

Return to top

Active Directory Server and Mailbox Server Ratios

The recommended number of Active Directory directory servers in each site containing Exchange 2010 Mailbox servers or users depends on the number of processor cores in each computer running the Exchange 2010 Mailbox server role and the hardware platform on which Active Directory is running. Specifically, consider the following scenarios:

- If Active Directory is running on the x86 platform (32-bit), the recommended ratio of Active Directory directory server processor cores to Exchange 2010 Mailbox server processor cores is 1:4.
- If Active Directory is running on the x64 platform (64-bit), the recommended ratio of Active Directory directory server processor cores to Exchange 2010 Mailbox server processor cores is 1:8. To achieve the 1:8 ratio, you must have enough memory installed on the directory server to cache the entire Active Directory database in memory. To check the size of your Active Directory database, examine the NTDS.DIT file on a global catalog server. By default, this file is located in %WINDIR%\NTDS.

In the preceding ratios, it's important to note that this is a ratio of processor *cores* and not processors. Thus, a dual-core processor counts as 2 when calculating the ratio. The ratio difference between 32-bit and 64-bit is due to the larger amount of memory that a 64-bit operating system can support as compared to a 32-bit operating system.

For Exchange 2010, we recommend that you deploy one 32-bit global catalog server processor core for every four Exchange 2010 Mailbox server processor cores, or one 64-bit global catalog server processor core for every eight Exchange 2010 Mailbox server processor cores. Although other server roles will influence the number of global catalog processor cores required, the Mailbox servers that are deployed influences the deployment of each of the other roles, so basing the number of global catalog processor cores on Mailbox server processor cores will suffice.

For additional guidance about Active Directory directory server sizing and ratios, see Planning Active Directory.

Return to top

1.15.1.4 Understanding Multiple Server Role Configurations in Capacity Planning

Understanding Multiple Server Role Configurations in Capacity Planning

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-14*

Several trends in server hardware apply to the Microsoft Exchange Server 2010 timeframe. One trend is a significant increase in processor performance and an increasing number of processor cores supported on a physical processor. This means that deploying a single Exchange server role on a standard commodity server with multi-core processors might leave a large portion of available CPU underutilized. Some customers expect server virtualization to more effectively utilize server CPU resources. Other customers want to combine Exchange server roles on the same physical server. Both are valid solutions.

Another trend is the availability of server models with multi-core processors and 10 to 16 internal disks. If you consider the number of mailboxes that can be supported by the input/output transactions per second (IOPS) provided by 10 to 16 disks, the Mailbox server role by itself generally won't utilize more than half of the available CPU resources. Adding the Client Access server role and the Hub Transport server role to this server will more effectively utilize the capacity of the server.

You can use the information in this topic as guidance for when to deploy multiple-role server configurations and how to correctly plan for multiple-role server configurations. An example illustrates the server sizing process for multiple-role servers.

Contents

Why Multiple-Role Configurations are Recommended

First, and foremost, the hardware you can procure today has processors that are extremely fast, yielding 5,000-6,000 megacycles when compared to our baseline processor configuration. That configuration consists of 2 x 4 core Intel Xeon x5470 3.33-GHz processors. (You can read more about our baseline processor configuration in the section "Example of Capacity Planning for a Mailbox Server" in Mailbox Server Processor Capacity Planning.) If you were to replace the processor architecture in your environment with processors on the market today, while keeping all other environmental factors the same, you would see a significant decrease in processor utilization.

To effectively lower the total cost of ownership on the servers you purchase, you should ensure efficient utilization of the system, which means the system must achieve and sustain near-80 percent CPU utilization during the worst failure mode at peak load. Here are four ways you can efficiently utilize the processors available today:

- Increase the workload, by deploying more active mailboxes per server.
- Introduce a virtualization layer, and deploy the mailbox role as a guest machine, along with additional guest machines.
- Deploy additional Exchange server roles onto the system.
- Use a combination of the above methodologies to find the optimal configuration that utilizes the hardware as efficiently as possible.

Deploying Exchange 2010 with a multiple-role architecture provides several benefits:

- The multiple-role architecture becomes a building block-based architecture. With the multiple-role architecture, all servers in the Exchange environment (excluding Unified Messaging and Edge Transport) are exactly the same—the same hardware, the same configuration, and so forth. This uniformity simplifies ordering the hardware, as well as performing maintenance and management of the servers.
  - From a cost perspective, the overall goal is to ensure that the architecture is balanced from both a CPU perspective and from a disk perspective. Deploying server roles on separate machines can result in long-term cost disadvantages as you may purchase more CPU, disk, and memory resources than you will actually use. For example, consider a server that hosts only the Client Access server role. Many servers enable you to add a given number of disks in a very economical fashion—when you are deploying that number of disks and, more importantly utilizing them, the cost is essentially zero. But if you deploy a server role that uses far less than the given number of disks, you're paying for a disk controller that is either under-utilized or not utilized at all.
- In many cases, using a multiple-role architecture enables you to have fewer physical Exchange servers in the environment. Fewer physical servers mean lower costs for a variety of reasons:
  - Operational expenditures are almost always higher than the capital expenditures. It costs more to manage a server over its lifetime than it does to purchase it.
  - You purchase fewer Exchange server licenses. A multiple-role server only requires a license for one Exchange server and one operating system, while breaking out the roles requires multiple Exchange server licenses and possibly multiple operating system licenses. For more information, see About Licensing: Licensing for Virtual Environments.
  - Deploying fewer servers has a trickle-down effect across the rest of the infrastructure. For example, deploying fewer physical servers may reduce the total rack and floor space required for the Exchange infrastructure, which in turn reduces power and cooling costs.
- A multi-role architecture ultimately distributes the load across a greater number of servers than deploying single-role servers because all Mailbox servers also become Hub Transport servers and Client Access servers. This architecture provides two benefits:
  - From a scalability perspective, you're distributing the load across a greater number of physical machines. During a failure event, the increased load on the remaining servers only increases incrementally, which ensures the other functions the server is performing aren't adversely affected.
  - From a resiliency perspective, the solution can survive a greater number of Hub Transport and Client Access role (or service) failures and still provide service.

For these reasons, the deployment strategy we recommend for Exchange 2010 is a multiple-role server configuration for most scenarios.

When Multiple-Role Configurations are Recommended

Multiple-role configurations are recommended for most scenarios for the following reasons:

- **Simple unit of scale** Organizations that anticipate regular growth in the number of mailboxes should consider deploying multiple-role servers. Because each multiple-role server represents a building block, this model allows the easy addition of building blocks to support the need for increased capacity.
- **Large-scale deployments that want to leverage modern processors** Based on scalability testing performed prior to the release-to-manufacturing (RTM) version of Exchange 2010, multiple-role servers can effectively utilize hex core (or more) processors in a single server. This capability allows large organizations to reduce the number of servers by combining the Mailbox, Hub Transport, and Client Access server roles instead of deploying these roles separately on servers with fewer processor cores. This approach leverages the building block model described earlier to provide a platform for large-scale deployments while reducing the overall number of servers required. Scalability of the multiple-role configuration on larger core count systems should be validated with lab testing prior to production deployment.
- **Server deployments with internal storage** Many servers available today have two physical multi-core processors and 10 to 16 internal disks. Several improvements in Exchange 2010 reduce I/O requirements, making these servers a cost-effective solution. Depending on user profile and disk type, these servers generally support up to 4,000 mailboxes. We recommend adding the Client Access and Hub Transport server roles to these servers to utilize the additional CPU and make these servers self-contained building blocks.
- **Risk mitigation scenarios where the number of mailboxes hosted on a Mailbox server is limited** Multiple-role servers are a solution for deployments where risk management policies limit the number of mailboxes that can be deployed on a Mailbox server. For example, say an organization with 10,000 mailboxes has a policy that a single server outage can't affect more than 25 percent of the mailboxes in the environment. This requirement limits the number of mailboxes per Mailbox server to 2,500. The additional capacity on that server could be utilized by adding the Client Access and Hub Transport server roles to the server.
- **Small organizations and branch office deployments** Except as noted below when Windows Network Load Balancing is used, a multiple-role deployment is a recommended solution for deployments where the primary goals are to minimize the number of physical servers, operating system instances, and Exchange servers to manage. Running the Client Access, Hub Transport, and Mailbox server roles on the same physical server provides the necessary role redundancy with a minimum requirement of two or three physical servers.

Return to top

When Multiple-Role Configurations Aren't Recommended

Multiple-role configurations aren't recommended for the following scenarios:

- **Small organizations, or branch office deployments, that want to use Windows Network Load Balancing (NLB)** Multiple-role servers may not work well for small deployments where two or three multiple-role servers are being deployed as members of a database availability group (DAG). For more

information about DAGs, see Managing Database Availability Groups. The clustering component added to Mailbox servers that are members of a DAG prevents NLB from being installed on the server. For more information about load balancing recommendations, see Understanding Load Balancing in Exchange 2010. However, there's still a requirement to load balance inbound traffic to the Client Access servers. In this case, there are two main options:

- Purchase a hardware load balancing appliance. Although there are some entry-level NLB appliances, this option can be costly, especially for smaller environments.
- Virtualize the Exchange server roles. In some environments, a limited number of servers results in having to deploy domain controllers, file and print servers, and other applications on the same physical hardware as the Exchange 2010 servers. We recommend that you implement the physical servers as host servers and isolate applications inside a virtual environment. With this isolation, you can run NLB for Client Access servers running on virtual machines.

- **Virtualization** The maximum number of active mailboxes that can be hosted by a virtual machine may be reduced based on the combination of message profile and running in a multi-role configuration. If you have light messaging users, co-locating server roles in a virtual machine may make sense. However, if you have heavy messaging users, you may be limited for resources in a virtual machine, and thus you may need to either reduce the number of mailboxes per Mailbox virtual machine or split out the roles into separate virtual machines. In these cases, it may be more efficient to deploy a single Exchange server role in each virtual machine, or to deploy one combined Client Access and Hub Transport virtual machine for every Mailbox server virtual machine.

Note:
You can’t install an Exchange server role on the hypervisor host server. Only management software (for example, antivirus software, backup software, or virtual machine management software) can be deployed on host servers. No other server-based applications should be installed on the host server (for example, Exchange, Microsoft SQL Server, or Active Directory). The host servers should be dedicated to running guest virtual machines.

For more information, see Understanding Client Access and Hub Transport Combined Role Configurations in Capacity Planning.

Return to top

Hardware Recommendations for Multiple-Role Servers

As a general guideline, a multiple-role server should be sized to use half of the available processor cores for the Mailbox server role and the remaining half for the Client Access and Hub Transport server roles. Microsoft doesn't specify a maximum number of recommended processor cores for multiple-role servers. Instead, a maximum number of populated processor sockets are provided. This refers to the number of processor sockets on the motherboard where multi-core processors are connected. For more information, see Understanding Processor Configurations and Exchange Performance.

In addition to sizing the processor architecture, the memory must also be sized correctly for deploying a multiple-role configuration. For more information, see Understanding Memory Configurations and Exchange Performance.

Deploying a Multiple-Role Server in a DAG

When you're deploying single-role Mailbox servers in a DAG, consider capacity planning for single and multiple server failures in relationship to Mailbox server load. If you have four Mailbox servers in a DAG, size the Mailbox servers at 50 percent capacity so that they can accommodate double the number of active users, in the event of simultaneous failure of two Mailbox servers. Because the Hub Transport and Client Access servers are on different physical servers, the load on those servers isn't impacted much by the loss of one or two Mailbox servers.

When you're deploying multiple-role servers in a DAG, think about capacity planning for Client Access, Hub Transport, and Mailbox server load. If you have four multiple-role servers in a DAG, make sure there is sufficient capacity to accommodate a potential doubling of Hub Transport and Client Access server load. Because the multiple-role configuration aligns with the recommended processor core ratios for server roles, if you correctly size the maximum active databases for the Mailbox server role, Hub Transport and Client Access servers should meet the performance objectives for this scenario.

Return to top

Example of Sizing for an Exchange 2010 Multiple-Role Scenario

The following example illustrates the server sizing process for multiple-role servers. The example has the following design assumptions:

- **Total mailbox count** 24,000
- **Mailbox profile** 100 messages per day (for example, 20 sent and 80 received)
- **Database cache per mailbox** 6 MB (based on a 100 message per day profile)
- **Availability requirements** Mailbox resiliency within a single site; protection against simultaneous failure of three database copies and two servers
- **Database requirements** 120 databases in the DAG, 200 mailboxes per database
- **Server platform** 2 x 6 core 2.26 gigahertz (GHz) processor-based (X5650) server (12 cores)

The following process applies:

1. **Calculate server count** A four-node DAG is required to protect against the simultaneous failure of two servers. However, the customer has decided to deploy six servers to control the maximum number of active mailboxes during a double server failure event. Therefore, the design begins with six Mailbox servers within the DAG.
2. **Calculate maximum active mailboxes per server based on the activation model** Assuming the active databases are equally distributed across the nodes, each server ideally hosts 4,000 active mailboxes (24,000 ÷ 6). To calculate the active mailbox count after a double-node failure (based on this example), the mailbox count is divided by the remaining four nodes, which equals 6,000 active mailboxes per node (24,000 ÷ 4).
   In this example, the *MaximumActiveDatabases* parameter on the **Set-MailboxServer** cmdlet is configured for 30 to ensure that no more than 40 percent of the databases become active on a single server.
3. **Calculate active mailbox CPU requirements** Multiply the maximum number of active mailboxes on a server by the megacycles per active mailbox (6,000 × 2 megacycles = 12,000 megacycles), based on the **Estimated IOPS per mailbox based on message activity and mailbox database cache** table in Understanding the Mailbox Database Cache. Multiply this value by 10 percent

for each additional database copy.
In this example, there's one active copy and three passive copies for every database, so the 12,000 megacycles is increased by 30 percent (12,000 × 1.3 = 15,600 megacycles). For more information, see "Database Cache Metrics" in Understanding the Mailbox Database Cache.

4. **Calculate passive mailbox CPU requirements** Multiply the number of passive mailboxes (when a server is hosting the maximum number of active mailboxes) by the megacycles per passive mailbox (10,000 × 0.3 megacycles = 3,000 megacycles), based on the **Estimated IOPS per mailbox based on message activity and mailbox database cache** table in Understanding the Mailbox Database Cache. For more information, see "Database Cache Metrics" in Understanding the Mailbox Database Cache.
5. **Add active and passive CPU requirements to get total CPU requirement** In this example, 15,600 active mailbox megacycles + 3,000 passive mailbox megacycles = 18,600 megacycles total CPU requirement.
6. **Apply Mailbox CPU requirement to hardware platform** This example uses a 2 x 6 core 2.26-GHz processor-based (x5650) server. Based on the guidance in Mailbox Server Processor Capacity Planning, this equates to 60,083 megacycles. Divide the required megacycles by the available megacycles based on the server platform to estimate the CPU utilization at peak period after a double-node failure (18,600 ÷ 60,083 = 31 percent predicted CPU utilization).
   We recommend that the Mailbox server role portion of multiple-role configurations be designed to not exceed 40 percent utilization during peak periods (for example, simultaneous failure of two nodes). This design allows sufficient space to accommodate CPU utilization of Client Access and Hub Transport server roles while maintaining total server CPU utilization at less than 80 percent during peak periods (for example, simultaneous failure of two nodes).
7. **Calculate active mailbox memory requirements** Multiply the number of active mailboxes by the required database cache per mailbox. In this example, with a double server failure, the remaining servers will host 6,000 active mailboxes (6,000 × 6 MB) ÷ 1,024 = 35.1 GB. The database cache requirements are based on the mailbox profile. For more information, see "Database Cache Metrics" in Understanding the Mailbox Database Cache.
8. **Apply total memory requirements to hardware platform** The total memory required is based on the database cache requirements and the server design (dedicated or multi-role). For more information, see the **Default mailbox database cache sizes** table in Understanding the Mailbox Database Cache. The total memory requirement for the multi-role server in this example is 52.2 GB ((4 GB + 35.1 GB) ÷ 0.75). Because 52.2 GB isn't a standard memory configuration, round up to 64 GB or the closest memory configuration that your server supports.

Return to top

1.15.1.5 Understanding Client Access and Hub Transport Combined Role Configurations in Capacity Planning

Understanding Client Access and Hub Transport Combined Role Configurations in Capacity Planning

Exchange Server 2010 > Performance and Scalability > Understanding Exchange Performance >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-21*

A common trend in server hardware is a significant increase in processor performance and an increasing number of processor cores supported on a physical processor. This means that deploying a single Exchange server role on a standard commodity server with two physical processors may leave a portion of available CPU underutilized. Some customers expect server virtualization to more effectively use server CPU resources. Other customers want to combine Exchange server roles on the same physical server. Both can be valid solutions if implemented according to deployment recommendations and best practices.

You can use the information in this topic to help determine when you should deploy the Client Access server role and the Hub Transport server role on the same physical server, and how to properly plan for the combined role configuration. For information about deploying the Client Access, Hub Transport, and Mailbox server roles on the same physical server, see Understanding Multiple Server Role Configurations in Capacity Planning.

Contents

When Client Access and Hub Transport Combined Role Configurations Are Recommended

We recommend that you deploy the Client Access and Hub Transport server roles on the same physical server if you're considering the following:

- **Server consolidation** For deployments where the primary goals are to minimize the number of physical servers, operating system instances, and Exchange servers to manage, a Client Access and Hub Transport combined role deployment is a recommended solution. Running the Client Access and Hub Transport server roles on the same physical server provides the necessary role redundancy with a minimum requirement of two physical servers.
- **Virtualization** For deployments where virtualization host servers have processor counts divisible by 8 (8, 16, 24, 32, or 48), deploying Client Access and Hub Transport combined role servers in a 1:1 processor core ratio with single role Mailbox servers ensures a well-balanced virtual machine placement regardless of host server size.

Return to top

Processor Recommendations for Client

Access and Hub Transport Combined-Role Servers

The maximum recommended processor core configuration is 12 processor cores for the Client Access and Hub Transport combined role servers. Although the Client Access and Hub Transport combined role configuration can be deployed on servers with more than 12 processor cores, we don't recommend it.

The following describes the minimum requirements and recommended maximum configurations:

- **Minimum** This is the minimum processor and memory configuration suitable for the Client Access and Hub Transport combined role server. The minimum hardware requirements must be met to receive support from Microsoft Customer Service and Support.
- **Recommended maximum** This is the maximum recommended processor and memory configuration for the Client Access and Hub Transport combined role server. Recommended maximum is defined as the upper limit of viable processor and memory configurations based on price and performance. The recommended maximum configuration is a guideline. It isn't a support criterion, and it doesn't include the resource requirements of third-party applications that might access or be installed on the server. The recommended maximum configuration may change over time based on price changes and technology advancements.

The following table shows the minimum and recommended maximum processor cores for Microsoft Exchange Server 2010 combined role servers.

Processor configurations for Exchange 2010 Client Access and Hub Transport combined role servers

Exchange 2010 server role	Minimum	Recommended maximum
Client Access and Hub Transport combined role servers	2 x processor cores	12 x processor cores

Important:

Some server virtualization platforms may not support the maximum number of processors identified in the table above. If you're planning to deploy Exchange server roles on a virtualization platform, please check the documentation for that platform to determine the maximum number of supported virtual processors.

Return to top

Client Access and Hub Transport Combined Role Server Configuration Alignment with Recommended Processor Core Ratios

The following table outlines the recommended number of processor cores deployed for the Client Access and Hub Transport server roles relative to the number of processor cores deployed for the Mailbox server role. The standard core ratios don't align well to the number of processor cores available on systems today. Unless you have a large organization with many Client Access, Hub Transport, and Mailbox servers, your

deployment probably won't match the desired processor core ratios.

Client Access and Hub Transport combined role server configurations can solve this problem and should result in more optimal hardware utilization. For example, if you have a server with four processor cores, the Client Access server role uses approximately three cores, and the Hub Transport server role uses approximately one core. If you deploy this in combination with four core Mailbox servers, the result is a 4:1 Mailbox to Hub Transport server role core ratio and a 4:3 Mailbox to Client Access server role core ratio. This closely aligns with the recommended processor core ratio guidance.

The following table shows the recommended server role ratios based on processor core for combined role servers.

Processor configurations for Exchange 2010 Client Access and Hub Transport combined role servers

Server role ratio	Recommended processor core ratio
Mailbox:Hub Transport	7:1 (with no antivirus application scanning on the Hub Transport server) 5:1 (with an antivirus application scanning on the Hub Transport server)
Mailbox:Client Access	4:3
Mailbox:Client Access and Hub Transport combined role server	1:1

Return to top

Memory Recommendations for Client Access and Hub Transport Combined Role Servers

The following table illustrates the minimum and recommended maximum memory configurations for Exchange 2010 combined role server configurations.

Memory configuration for Exchange 2010 combined role servers

Exchange 2010 server role	Minimum	Recommended maximum
Client Access and Hub Transport combined role servers	4 GB	2 GB per core

Return to top

Determining Client Access and Hub Transport Combined Role Server Hardware Requirements

To determine the hardware requirements for the Client Access and Hub Transport combined role server, you first need to determine the hardware requirements for the Mailbox server role. For more information, see Mailbox Server Processor Capacity

Planning.

Use the number of processor cores that will be deployed for the Mailbox server role and deploy an equal number of processor cores for the Client Access and Hub Transport combined role server. For example, for every Mailbox server with eight processor cores, deploy a Client Access and Hub Transport combined role server with eight processor cores. Then apply memory configuration guidelines to the processor core count. For example, if your Client Access and Hub Transport combined role server has eight processor cores, you will need 2 GB per core or 16 GB of memory per server.

Return to top

Client Access and Hub Transport Combined Role Servers and Virtualization

If you plan to virtualize Exchange, using Client Access and Hub Transport combined role servers can make the planning process easier. The recommended sizing for virtual machines is summarized in the following table.

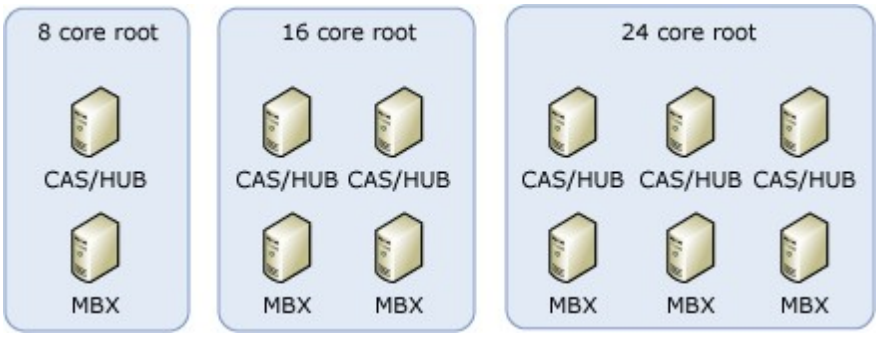
Recommended sizing for virtual machines for Exchange 2010 Client Access and Hub Transport combined role servers

Virtual machine role	Recommended number of virtual processors	Recommended memory
Client Access and Hub Transport combined role servers	4 x processor core	8 GB
Mailbox server role	4 x processor core	4 GB plus 3-30 megabytes (MBs) per mailbox. This variable is based on the user profile. For details, see "Recommended Memory Configurations" in Understanding Memory Configurations and Exchange Performance.

Note:
Not all server virtualization platforms support the same number of maximum virtual processors. If you plan to deploy Exchange server roles on a virtualization platform, check the documentation for that platform to determine the maximum number of supported virtual processors.

We recommend that you deploy these virtual machines in a 1:1 ratio (for example, deploy one Client Access and Hub Transport combined role virtual machine for every Mailbox server role virtual machine).

If you're using virtualization servers dedicated to hosting Exchange virtual machines and the processor core count is divisible by 8 (8, 16, 24, 32, or 48), placement of virtual machines is straightforward. For example, if your virtualization root server has eight processor cores, deploy one Client Access and Hub Transport combined role virtual machine and one Mailbox server role virtual machine. If your virtualization root server has 16 processor cores, deploy two of each. If your root server has 24 cores, deploy 3 of each, as shown in the following figure.



With this design, you can maintain Exchange role redundancy across root servers and balance Exchange workloads for effective utilization of root server resources. The following table provides a summary of recommended sizing guidance for root servers hosting Client Access and Hub Transport combined role virtual machines.

Recommended sizing for virtual machines for Exchange 2010 Client Access and Hub Transport combined role servers

Root server processor cores (root servers with 12 x processor cores don't fit this model)	Root server memory requirements	Recommended memory configuration	Number of Client Access and Hub Transport combined role virtual machines	Number of Mailbox server role virtual machines
8	26 - 34 GB	32 GB	1	1
16	53 - 69 GB	64 GB	2	2
24	76 - 100 GB	96 GB	3	3
32	131 - 143 GB	160 GB	4	4
48	152 - 200 GB	192 GB	6	6

Note:
Root server memory recommendations are based on root operating system requirements, plus virtual machine requirements. Mailbox virtual machine requirements are dependent on mailbox profiles. For more information, see "Recommended Memory Configurations" in Understanding Memory Configurations and Exchange Performance.

Note:
Costs should be considered when purchasing memory. You may have to reduce the number of active mailboxes hosted on each Mailbox server virtual machine to align root server memory requirements with the purchased memory configuration.

Return to top

1.15.1.6 Calculate Megahertz Per User and IOPS Per User

Calculate Megahertz Per User and IOPS Per User

Exchange Server 2010 > Performance and Scalability > Understanding Exchange Performance >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010*

Topic Last Modified: *2012-07-23*

Knowing how to estimate the resource consumption of an Exchange user helps you with hardware and capacity planning. You can use the procedures in this topic to determine the megacycles and input/output per second (IOPS) per user for Microsoft Exchange Server 2010. For more information related to your hardware and capacity planning, see the following topics:

- Understanding Processor Configurations and Exchange Performance
- Understanding Multiple Server Role Configurations in Capacity Planning
- Understanding Client Access and Hub Transport Combined Role Configurations in Capacity Planning

You'll need to understand the following terms to perform the procedures discussed in this topic:

- **Megahertz/user** This term refers to the megacycles per second per user, which is the raw processor usage required per user measured during the peak (two-hour) period on a production server.
- **IOPS/Total number of active mailboxes** This term refers to the input/output (I/O) per second per active mailbox, which is the raw database disk usage (IOPS) required per user measured during the peak period on a production server. This metric doesn't include either transaction log I/O operations or I/O to passive database copies. It also excludes I/O to content indexing files.

Prerequisites

If the active mailboxes in a company have diverse usage requirements, you may want to measure usage profiles separately for different groups of users. For example, sales engineers may have a different usage profile than the marketing group. However, be aware that separate measurements are helpful only if the groups of users have significantly different requirements.

To accurately measure the megacycles and IOPS of the different types of users, you need to:

- Isolate the user groups on distinct databases and Mailbox servers.
- Associate those Mailbox servers with distinct Hub Transport and Client Access servers.
- Create unique namespaces for each profile.

You can then use the values of the following counters to determine the relative weight of the users:

- MSExchangeIS Mailbox\Messages Delivered/sec
- MSExchangeIS Mailbox\Messages Sent/sec

For an example, consider the following calculation. If the database with 100 sales engineers receives 0.5 messages per second and sends 0.3 messages per second, while the database with 50 marketing employees receives 0.1 messages per second and sends 0.1 messages per second, the resulting value of 2.0 indicates that one sales engineer generates twice the megacycles and IOPS on all roles as one marketing employee.

$$\frac{\text{cost of Sales Engineer}}{\text{cost of Marketer}} = \frac{\frac{0.5\ \text{messages/sec.} + 0.3\ \text{messages/sec.}}{\text{100 engineers}}}{\frac{0.5\ \text{messages/sec.} + 0.1\ \text{messages/sec.}}{\text{50 marketers}}} = 2.0$$

Calculate total megacycles per user for

the Client Access, Hub Transport, and Mailbox server roles without mailbox resiliency

You can use the example in this section to help you calculate megacycles for your server roles.

The total megacycles consumed per second is the product of the (percent total CPU) × (number of cores) × (speed of each core in megahertz (MHz)).

To calculate the MHz per mailbox, perform the following steps:

1. Select a production server with a typical user load.
2. Use Performance Monitor (Perfmon.exe) to monitor the Processor\% Processor Time_Total counter over the peak hours of server activity.
3. Calculate the average CPU usage (percent) from the data you obtain in step 2.
4. Calculate your current MHz per user as described in the following formula:

   MHz per mailbox = ((average CPU usage) × (number of processors × number of cores per processor) × (speed of processors in MHz)) ÷ (number of mailboxes)

For example, let's assume the following values for a Mailbox server:

- Average CPU usage = 30 percent of total CPU during the user peak period
- Number of processors = 2
- Number of cores per processor = 4
- Speed of processors in megacycles = 3,000 MHz
- Number of active mailboxes = 6,000

Given these values, and using the formula described earlier in step 4 of this section, we find that the CPU cost per mailbox is:

30% × (2 processors × 4 cores) × (3,000 MHz) ÷ 6,000

= 1.2 megacycles per mailbox

Calculate the total megahertz per user for the Mailbox server role with mailbox resiliency

If mailbox resiliency is enabled, you should identify the costs of supporting the database copies. For example, estimate that a passive user's mailbox consumes 15 percent less megahertz than an active user's mailbox, and additionally that each passive copy hosted elsewhere adds 10 percent to the user's CPU footprint on the active server.

Use the following equation to calculate megahertz consumed with mailbox resiliency enabled:

Megahertz consumed = (active users) × (megacycles per user) + (0.1) × (active users) × (number of passive copies) × (megacycles per user) + (0.15) × (passive users) × (megacycles per user)

Combine the preceding equation with the following:

Megahertz consumed = %_Total CPU × (number of cores) × (speed of a core)

The following figure shows the solution for the preceding equations.

$$\frac{\text{Megacycles}}{\text{user}} = \frac{\%(\square_{\text{Total}}\text{CPU}) * (\text{number of cores}) * \left(\frac{\text{MHzMHz}}{\text{core}}\right)}{((\text{Active Users}) * (1+(0.1*\text{passive copies}))) + (0.15*\text{Passive Users})}$$

$$\frac{\text{Megacycles}}{\text{user}} = \frac{(30\%) * \left(2 \text{ proc x } 4\frac{\text{cores}}{\text{proc}}\right) * \left(3000\frac{\text{MHzMHz}}{\text{core}}\right)}{((3000)3000*(1+(0.1*2))) + (0.15*2000)} = 1.8\ \frac{\text{Megacycles}}{\text{user}}$$

For example, assume the following values for the Mailbox server:

- Average CPU usage = 30 percent of total CPU during the user peak period
- Number of processors = 2
- Number of cores per processor = 4
- Speed of processors in megacycles = 3,000 MHz
- Number of active mailboxes = 3,000
- Number of passive mailboxes = 2,000
- Number of database copies = 2

Given these values, the CPU cost per user is 1.8, as shown in the preceding figure.

Therefore, to calculate megacycles per mailbox for a Mailbox server with mailbox resiliency, perform the following steps:

1. Select a production server with a typical user load.
2. Use System Monitor to monitor the Processor\% Processor Time_Total counter over the peak two hours of server activity.
3. Calculate the average CPU usage (percent) from the data you obtain in step 2.
4. Calculate your current MHz per user as described in the following formula: MHz per mailbox = ((average CPU usage) × (number of processors × number of cores per processor) × (speed of processors in megacycles)) ÷ [(number of active mailboxes)(1 + 0.1) × (number of database copies) + (0.15) × (number of passive mailboxes)]

Calculate the mailbox disk IOPS per user

Random database reads and writes are a concern when considering mailbox disk IOPS per mailbox. However, sequential log writes are lower cost and rarely a problem. To find the number of IOPS on an active database, add the values of the following MSExchange database counters at the peak load period:

- Instances\I/O Database Reads/sec (Information Store\database)
- Instances \I/O Database Writes/sec (Information Store\database)

To measure IOPS per mailbox, perform the following steps:

1. Select a production server with a typical user load.
2. Use System Monitor to monitor the following counters over the peak two hours of server activity:
   - MSExchange Database Instances\I/O Database Reads/sec (Information Store\database)
   - MSExchange Database Instances\I/O Database Writes/sec (Information Store\database)
3. Calculate current mailbox disk IOPS per mailbox as described in the following formula:

   Mailbox disk IOPS per mailbox = (MSExchange Database Instances\I/O Database Reads/sec (Information Store\database)) + MSExchange Database

Instances\I/O Database Writes/sec (Information Store\database) ÷ (number of mailboxes on that database)

For example, assume the following values for a database:

- MSExchange Database Instances\I/O Database Reads/sec (Information Store \database) = 7
- MSExchange Database Instances\I/O Database Writes/sec (Information Store \database) = 8
- Number of mailboxes = 250

Given these values, the following determines the IOPS per mailbox:

(7 + 8) ÷ 250 = 0.06 IOPS per user

For more information, see the values recommended for planning a topology in Mailbox Server Processor Capacity Planning.

Estimates of Mailbox Database Cache, IOPS, and CPU Usage

The following table provides data estimates that you can use to determine the megacycles and IOPS per user for your Exchange 2010 system.

In the table, the megacycles estimate is based on the measurement of Intel Xeon x5470 3.33 gigahertz (GHz) processors (2 × 4 core arrangement). A 3.33 GHz processor core provides 3300 megacycles of performance throughput. You can consider other processor configurations by comparing this measured platform to server platforms tested by the Standard Performance Evaluation Corporation (SPEC) at SPEC CPU2006.

Note:

You must increase the megacycles per active mailbox by 10 percent for each additional database copy after the one active copy.

Per mailbox database cache, IOPS, and CPU estimates based on message activity

Messages sent or received per mailbox per day	Database cache per mailbox in megabytes (MB)	Single database copy (stand-alone) with estimated IOPS per mailbox	Multiple database copies (mailbox resiliency) with estimated IOPS per mailbox	Megacycles for active mailbox or stand-alone mailbox	Megacycles for passive mailbox
50	3	0.06	0.05	1	0.15
100	6	0.12	0.1	2	0.3
150	9	0.18	0.15	3	0.45
200	12	0.24	0.2	4	0.6
250	15	0.3	0.25	5	0.75
300	18	0.36	0.3	6	0.9

350	21	0.42	0.35	7	1.05
400	24	0.48	0.4	8	1.2
450	27	0.54	0.45	9	1.35
500	30	0.6	0.5	10	1.5

1.15.2 Tools for Performance and Scalability Evaluation

Tools for Performance and Scalability Evaluation

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-21*

When evaluating the scalability and performance of Exchange in a lab environment, you can use tools provided by Microsoft to generate a simulated Exchange workload on your system and analyze the effect of that workload.

To determine how many Exchange 2010 servers are required to manage user load, use the following capacity planning tools:

- Microsoft Exchange Jetstress
- Microsoft Exchange Load Generator

Important:

Microsoft Exchange Jetstress should be used on systems prior to placing production data on the server. Jetstress should not be used on systems containing production data. Exchange Load Generator is intended for use in test environments, not in production environments.

Exchange Server Jetstress 2010

The Jetstress tool is designed to simulate Exchange I/O at the database level by interacting directly with the database technology of the Extensible Storage Engine (ESE), also known as Jet, that Exchange is built on. Jetstress can be configured to test the maximum I/O throughput available to your disk subsystem within the required performance constraints of Exchange, or it can accept a desired profile of user count and I/Os per second per user and validate that the disk subsystem is capable of maintaining an acceptable level of performance with such a profile. Jetstress testing can be used to validate storage reliability and performance prior to the deployment of Exchange servers. You should run Jetstress if you are concerned about your storage subsystem performance or if you need to determine a system's I/O capacity.

The documentation for Jetstress describes how to configure and execute an I/O validation or evaluation on your server hardware. You can download Jetstress from Microsoft Exchange Server Jetstress 2010 (64 bit) and Microsoft Exchange Server Jetstress 2010 (32 bit).

For more information, see Microsoft Exchange Server Jetstress 2010.

Exchange Server Load Generator 2010

The Load Generator (LoadGen) tool is designed to produce a simulated client workload

against a test Exchange deployment. This workload can be used to evaluate how Exchange performs, and can also be used to analyze the effect of various configuration changes on Exchange behavior and performance while the system is under load. The documentation for LoadGen describes how to configure and execute a load test against an Exchange server. LoadGen is capable of simulating Microsoft Office Outlook 2003 (online and cached), Outlook 2007 (online and cached), POP3, IMAP4, SMTP, ActiveSync, and Outlook Web App client activity. It can be used to generate a single-protocol workload, or these client protocols can be combined in some form to generate a multi-protocol workload.

Use the output from these tests in the following ways:

- Validate deployments
- Calculate the client computer response time for the server configuration under client load
- Estimate the number of users per server
- Identify bottlenecks on the server

You can download LoadGen at Exchange Load Generator 2010 (64 bit) and Exchange Load Generator 2010 (32 bit).

When to Use Performance and Scalability Tools

Jetstress and LoadGen are typically used as part of the pre-deployment process, either to provide data for hardware sizing requirements prior to hardware purchasing, or to analyze the stability and performance of a system prior to placing it into production.

Whenever possible, you should run a Jetstress test prior to placing a mailbox server into production. Jetstress testing is straightforward and can be accomplished with little additional work beyond the hardware setup and operating system configuration that would already be necessary prior to the installation of Exchange.

LoadGen testing is much more involved and should be considered and planned carefully. Set a realistic goal for the information to be obtained as a result of the test, and always remember that LoadGen doesn't provide a 100 percent accurate simulation of all client activity. Therefore, any measurements generated by Loadgen testing should be used as a part of your decision-making process and should not be the only data points used to make a final decision for server sizing or configuration changes.

Important:

Test tools like LoadGen are not designed to be run in a production environment and should never be run against a live production system or in an environment that has any connection to a live production system. Additionally, you should use extreme caution when running LoadGen against a test environment that contains copies of actual data, as it may be possible for LoadGen to act on messages in your test environment in such a way that outgoing mail leaves your test environment and ends up in a production mailbox (depending on the message routing configuration of your test environment).

Evaluating Test Results

Both Jetstress and LoadGen produce a test report at the conclusion of any test activity. The test report contains a high-level pass/fail metric that you can use to determine if the other reported values will be usable for server sizing or pre-deployment validation. Both tools also provide various performance metrics. In addition to the values provided in the test reports, you should read the tool documentation for additional suggestions about server performance counters that should be monitored during the test to evaluate system health and performance.

1.15.3 Performance and Scalability Counters and Thresholds

Performance and Scalability Counters and Thresholds

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-09-01*

The topics in this section describe the performance and scalability counters you can use to monitor Microsoft Exchange Server 2010 server roles. You can use Performance Monitor to automatically collect performance data from local or remote Exchange 2010 servers. You can define start and stop times for automatic log generation, manage multiple logging sessions from a single console window, and set an alert on a computer that enables a message to be sent or a log to be started when your criteria are met. The Windows Server 2008 operating system defines the performance data collected with regard to objects, counters, and instances. By using the performance tool and performance logs and alerts, you can select performance objects, counters, and instances to collect, and then present data about the performance of system components or installed software. For more information about performance monitoring, see the Performance Monitoring Getting Started Guide.

This section contains the following topics:

Common Counters

Virtualization Counters

Client Access Server Counters

Mailbox Server Counters

Transport Server Counters

Unified Messaging Counters

You can also use the Microsoft Operations Framework (MOF) to help with managing and maintaining your organization. MOF is a collection of best practices, principles, and models that give you technical guidance about the management of IT projects such as daily Exchange operations. The MOF Technology Library provides guidance and best practices to help IT pros better understand how to use MOF with Microsoft technologies. The first component of the library is a new series of reliability workbooks. These resources provide the knowledge, specific tasks, and schedules needed to keep technologies running smoothly so IT can deliver the services an organization expects. For more information about MOF, see the MOF Technology Library. From there, you can download workbooks related to many aspects of Microsoft Exchange.

1.15.3.1 Common Counters

Common Counters

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic provides information about counters common to all server roles in Microsoft Exchange Server 2010. You can use Performance Monitor (perfmon.exe) to monitor these counters. For more information, see Performance Monitor Getting Started Guide. For information about other counters relevant to Exchange 2010, see Performance and Scalability Counters and Thresholds.

Processor and Process Counters

The following table provides information about processor and process counters.

Counter	Description	Threshold	Troubleshooting
Processor(_Total)\% Processor Time	Shows the percentage of time that the processor is executing application or operating system processes. This is when the processor isn't idle.	Should be less than 75% on average.	
Processor(_Total)\% User Time	Shows the percentage of processor time spent in user mode. User mode is a restricted processing mode designed for applications, environment subsystems, and integral subsystems.	Should remain below 75%.	
Processor(_Total)\% Privileged Time	Shows the percentage of processor time spent in privileged mode. Privileged mode is a processing mode designed for operating system components and hardware-manipulating drivers. It allows direct access to hardware and all memory.	Should remain below 75%.	If total processor time is high, use this counter to determine which process is causing high CPU.
Process(*)\% Processor Time	Shows the percentage of elapsed processor time that all process threads used to execute instructions. An instruction is the basic unit of execution in a computer. A thread is the object that executes instructions,		If total processor time is high, use this counter to determine which process is causing high CPU.

	and a process is the object created when a program is run. Code executed to handle some hardware interruptions and trap conditions are included in this count.		
System\Processor Queue Length (all instances)	Indicates the number of threads each processor is servicing. Processor Queue Length can be used to identify if processor contention or high CPU utilization is caused by the processor capacity being insufficient to handle the workloads assigned to it. Processor Queue Length shows the number of threads that are delayed in the Processor Ready Queue and are waiting to be scheduled for execution. The value listed is the last observed value at the time the measurement was taken.	Shouldn't be greater than 5 per processor.	On a computer with a single processor, observations where the queue length is greater than 5 are a warning that there is frequently more work available than the processor can handle readily. When this number is greater than 10, it's a strong indicator that the processor is at capacity, particularly when coupled with high CPU utilization. On systems with multiprocessors, divide the queue length by the number of physical processors. A multiprocessor system configured using hard processor affinity (processes are assigned to specific CPU cores), which have large values for the queue length, can indicate that the configuration is unbalanced. Although Processor Queue Length typically isn't used for capacity planning, it can be used to identify if systems within the environment are capable of running the loads or if additional processors or faster processors should be purchased

			for future servers.

Memory Counters

The following table shows common memory counters.

Counter	Description	Threshold	Troubleshooting
Memory\Available Mbytes	Shows the amount of physical memory, in megabytes (MB), immediately available for allocation to a process or for system use. It's equal to the sum of memory assigned to the standby (cached), free, and zero page lists. For a full explanation of the memory manager, refer to Microsoft Developer Network (MSDN) or "System Performance and Troubleshooting Guide" in the Windows Server 2003 Resource Kit.	Should remain above 100 MB at all times.	
Memory\Pool Nonpaged bytes	Consists of system virtual addresses guaranteed to be resident in physical memory at all times and can thus be accessed from any address space without incurring paging input/output (I/O). Like paged pool, nonpaged pool is created during system initialization and is used by kernel-mode components to allocate system memory.	Not applicable.	
Memory\Pool Paged bytes	Shows the portion of shared system memory that can be paged to the disk paging file. Paged pool is created during system initialization and is used by kernel-	Not applicable.	Monitor for increases in pool paged bytes indicating a possible memory leak.

	mode components to allocate system memory.		
Memory\Cache Bytes	Shows the current size, in bytes, of the file system cache. By default, the cache uses up to 50% of available physical memory. The counter value is the sum of Memory\System Cache Resident Bytes, Memory \System Driver Resident Bytes, Memory\System Code Resident Bytes, and Memory\Pool Paged Resident Bytes.	Not applicable.	Should remain steady after applications cache their memory usage. Check for large dips in this counter, which could be attributed to working set trimming and excessive paging. Used by the content index catalog and continuous replication log copying.
Memory\Committed Bytes	Shows the amount of committed virtual memory, in bytes. Committed memory is the physical memory that has space reserved on the disk paging files. There can be one or more paging files on each physical drive. This counter displays the last observed value only; it isn't an average.	Not applicable.	Determines the amount of committed bytes in use.
Memory\%Committed Bytes in Use	Shows the ratio of Memory\Committed Bytes to the Memory \Commit Limit. Committed memory is the physical memory in use for which space has been reserved in the paging file should it need to be written to disk. The commit limit is determined by the size of the paging file. If the paging file is enlarged, the commit limit increases, and the ratio is reduced. This counter displays the current percentage value only; it isn't an	Not applicable.	If this value is high (more than 90%), you may begin to see commit failures. This is a clear indication that the system is under memory pressure.

	average.		

Memory Paging Counters

The following table shows common memory paging counters.

Counter	Description	Threshold	Troubleshooting
Memory->Transition Pages Repurposed/sec	Indicates system cache pressure.	Should be less than 100 on average. Spikes should be less than 1,000.	
Memory\Page Reads/sec	Indicates data must be read from the disk instead of memory. Indicates there isn't enough memory and paging is beginning. A value of more than 30 per second means the server is no longer keeping up with the load.	Should be less than 100 on average.	
Memory\Pages/Sec	Shows the rate at which pages are read from or written to disk to resolve hard page faults. This counter is a primary indicator of the kinds of faults that cause system-wide delays. It's the sum of Memory\Pages Input/sec and Memory\Pages Output/sec. It's counted in numbers of pages, so it can be compared to other counts of pages, such as Memory\Page Faults/sec, without conversion. It includes pages retrieved to satisfy faults in the file system cache (usually requested by applications) and non-cached mapped memory files.	Should be below 1,000 on average.	The values returned by this counter may be more than you expect. These values may not be related to either paging file activity or cache activity. Instead, these values may be caused by an application that is sequentially reading a memory-mapped file. Use Memory\Pages Input/sec and Memory\Pages Output/sec to determine page file I/O.
Memory\Pages Input/sec	Shows the rate at which pages are read from disk to resolve hard page faults. Hard page faults	Should be below 1,000 on average.	

	occur when a process refers to a page in virtual memory that isn't in its working set or elsewhere in physical memory, and must be retrieved from disk. When a page is faulted, the system tries to read multiple contiguous pages into memory to maximize the benefit of the read operation. Compare the value of Memory\Pages Input/sec to the value of Memory\Page Reads/sec to determine the average number of pages read into memory during each read operation.		
Memory\Pages Output/sec	Shows the rate at which pages are written to disk to free space in physical memory. Pages are written back to disk only if they are changed in physical memory, so they are likely to hold data, and not code. A high rate of pages output might indicate a memory shortage. Microsoft Windows writes more pages back to disk to free up space when physical memory is in short supply. This counter shows the number of pages, and can be compared to other counts of pages, without conversion.	Should be below 1,000 on average.	

Memory Consumption Counters

The following table shows common process memory consumption counters.

Counter	Description	Threshold	Troubleshooting
Process(*)\Private Bytes	Shows the current number of bytes this	Not applicable.	This counter can be used for determining any memory leaks

	process has allocated that can't be shared with other processes.		against processes. For the information store process, compare this counter value with database cache size to determine if there is a memory leak in the information store process. An increase in information store private bytes, together with the same increase in database cache, equals correct behavior (no memory leak).
Process(*)\Virtual Bytes	Represents (in bytes) how much virtual address space the process is currently consuming.	Not applicable.	Used to determine if processes are consuming a large amount of virtual memory.

Process Working Set Counter

The following table shows a common process working set counter.

Counter	Description	Threshold	Troubleshooting
Process(_Total) \Working Set	Shows the current size, in bytes, of the working set of this process. The working set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the working set of a process event if they aren't in use. When free memory falls below a threshold, pages are trimmed from working sets. If they are needed, they will be soft-faulted back to the working set before leaving main memory.	Not applicable.	Large increases or decreases in working sets cause paging. Ensure that the paging file is set to the recommended value of RAM+10. If working sets are being trimmed, add Process(*)\Working Set to determine what processes are affected. This counter could indicate either system-wide or process-wide issues. Cross-reference this counter with Memory \System Cache Resident Bytes to determine if system-wide working set trimming is occurring.

Process Handle Counter

The following table shows a common process handle counter.

Counter	Description	Threshold	Troubleshooting
Process(*)\Handle Count	Shows the total number of handles currently open by this process. This number is the sum of the handles currently open by each thread in this process.	Not applicable.	An increase in handle counts for a particular process may be the symptom of a faulty process with handle leaks, which is causing performance issues on the server. This isn't necessarily a problem, but is something to monitor over time to determine if a handle leak is occurring.

.NET Framework Counters

The following table shows Microsoft .NET Framework counters.

Counter	Description	Threshold	Troubleshooting
.NET CLR Memory(*)\ % Time in GC	Shows when garbage collection has occurred. When the counter exceeds the threshold, it indicates that CPU is cleaning up and isn't being used efficiently for load. Adding memory to the server would improve this situation.	Should be below 10% on average.	If this counter increases to a high value, there might be some objects that are surviving Gen 1 garbage collections and being promoted to Gen 2. Gen 2 collections require a full global catalog for clean up. Add other .NET Framework memory counters to determine if this is the case.
.NET CLR Exceptions (*)\# of Excepts Thrown / sec	Displays the number of exceptions thrown per second. These include both .NET Framework exceptions and unmanaged exceptions that get converted into .NET Framework exceptions. For example, the null pointer reference exception in unmanaged code would get thrown	Should be less than 5% of total requests per second (RPS) (Web Server(_Total) \Connection Attempts/sec * .05).	Exceptions should only occur in rare situations and not in the normal control flow of the program. This counter was designed as an indicator of potential performance problems due to a large (>100 sec) rate of exceptions thrown. This counter isn't an average over time. It displays the difference between

	again in managed code as a .NET Framework System.NullReference Exception. This counter includes both handled and unhandled exceptions.		the values observed in the last two samples divided by the duration of the sample interval.
.NET CLR Memory(*) \# Bytes in all Heaps	Shows the sum of four other counters: Gen 0 Heap Size, Gen 1 Heap Size, Gen 2 Heap Size, and Large Object Heap Size. This counter indicates the current memory allocated in bytes on the GC Heaps.	Not applicable.	These regions of memory are of type MEM_COMMIT. The value of this counter is always less than the value of Process \Private Bytes, which counts all MEM_COMMIT regions for the process. Private bytes minus # bytes in all heaps is the number of bytes committed by unmanaged objects. Used to monitor possible memory leaks or excessive memory usage of managed or unmanaged objects.

Network Counters

The following table shows common network counters.

Counter	Description	Threshold	Troubleshooting
Network Interface(*) \Bytes Total/sec	Indicates the rate at which the network adapter is processing data bytes. This counter includes all application and file data, in addition to protocol information such as packet headers.	For a 100-megabytes per second (MBps) network adapter, should be below 6–7 MBps. For a 1000-megabits per second (Mbps) network adapter, should be below 60–70 Mbps.	
Network Interface(*) \Packets Outbound Errors	Indicates the number of outbound packets that couldn't be transmitted because of errors.	Should be 0 at all times.	
TCPv4\Connections Established	Shows the number of TCP connections for	Not applicable.	Determines current user load.

	which the current state is either ESTABLISHED or CLOSE-WAIT. The number of TCP connections that can be established is constrained by the size of the nonpaged pool. When the nonpaged pool is depleted, no new connections can be established.		
TCPv6\Connection Failures	Shows the number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT. The number of TCP connections that can be established is constrained by the size of the nonpaged pool. When the nonpaged pool is depleted, no new connections can be established.	Not applicable.	Determines current user load.
TCPv4\Connections Reset	Shows the number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.	An increasing number of resets or a consistently increasing rate of resets can indicate a bandwidth shortage.	Some browsers send TCP reset (RST) packets, so be cautious when using this counter to determine reset rate.
TCPv6\Connections Reset	Shows the number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.	An increasing number of resets or a consistently increasing rate of resets can indicate a bandwidth shortage.	Some browsers send TCP reset (RST) packets, so be cautious when using this counter to determine reset rate.

Exchange Domain Controllers Connectivity Counters

The following table shows Exchange domain controllers connectivity counters.

Counter	Description	Threshold	Troubleshooting
MSExchange ADAccess Caches(*) \LDAP Searches/Sec	Shows the number of LDAP search requests issued per second.	Not applicable.	Used to determine current LDAP search rate.
MSExchange ADAccess Domain Controllers(*)\LDAP Read Time	Shows the time in milliseconds (ms) to send an LDAP read request to the specified domain controller and receive a response.	Should be below 50 ms on average. Spikes (maximum values) shouldn't be higher than 100 ms.	
MSExchange ADAccess Domain Controllers(*)\LDAP Search Time	Shows the time (in ms) to send an LDAP search request and receive a response.	Should be below 50 ms on average. Spikes (maximum values) shouldn't be higher than 100 ms.	
MSExchange ADAccess Processes (*)\LDAP Read Time	Shows the time (in ms) to send an LDAP read request to the specified domain controller and receive a response.	Should be below 50 ms on average. Spikes (maximum values) shouldn't be higher than 100 ms.	
MSExchange ADAccess Processes (*)\LDAP Search Time	Shows the time (in ms) to send an LDAP search request and receive a response.	Should be below 50 ms on average. Spikes (maximum values) shouldn't be higher than 100 ms.	
MSExchange ADAccess Domain Controllers(*)\LDAP Searches timed out per minute	Shows the number of LDAP searches that returned LDAP_Timeout during the last minute.	Should be below 10 at all times for all roles. Higher values may indicate issues with Active Directory resources.	
MSExchange ADAccess Domain Controllers(*)\Long running LDAP operations/Min	Shows the number of LDAP operations on this domain controller that took longer than the specified threshold per minute. (Default threshold is 15 seconds.)	Should be less than 50 at all times.	Higher values may indicate issues with Active Directory resources.

1.15.3.2 Virtualization Counters

Virtualization Counters

Exchange Server 2010 > Performance and Scalability > Performance and Scalability Counters and Thresholds >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic provides information about virtualization counters in Microsoft Exchange Server 2010. You can use Performance Monitor (perfmon.exe) to monitor these counters. For more information, see Performance Monitor Getting Started Guide. For information about other counters relevant to Exchange 2010, see Performance and Scalability Counters and Thresholds.

Hyper-V Counters

The following table shows Microsoft Hyper-V counters.

Counter	Description	Threshold	Troubleshooting
Hyper-V Virtual Machine Health Summary\Health OK	Shows that the host server is running as expected.	Should be 1 at all times.	
Hyper-V Virtual Machine Health Summary\Health Critical	Shows the percentage of processor time spent in guest code. This is used to measure the total processor utilization for all virtual machines (VMs) running on the host server. This value is equal to the sum of the Hyper-V Hypervisor Root Virtual Processor\% Guest Run Time and Hyper-V Hypervisor Virtual Processor\% Guest Run Time counters.	Should remain below 65%.	If you see a value of 1, the server is in a critical state, and you should investigate further to determine the exact issue.

Hyper-V Processor Counters

The following table shows Hyper-V processor counters.

Counter	Description	Threshold	Troubleshooting
Hyper-V Hypervisor Logical Processor\% Guest Run Time	Shows the percentage of processor time spent in guest code. This is used to measure the total processor utilization for all VMs running on the host server. This value is equal to the sum of the Hyper-V Hypervisor Root Virtual Processor\% Guest Run Time and Hyper-V Hypervisor Virtual Processor\% Guest Run Time	Should remain below 65%.	There is one logical processor that carries more load than the rest and that is LP0. This logical processor is where all interrupts in the system are directed. If there is too much load, this logical processor may reach 100%, which likely means input/ output (I/O) is a bottleneck in the system. There are some technologies in Windows Server 2008

	counters.		R2 that help reduce the load for networking. These technologies include Virtual Machine Queue (VMQ), VM Chimney, and RSS. There is no RSS support in guest VMs.
Hyper-V Hypervisor Logical Processor\% Hypervisor Run Time	Shows the percentage of processor time spent in hypervisor code. This is used to measure the total processor utilization of the hypervisor for the entire system.	Should remain below 5%.	
Hyper-V Hypervisor Logical Processor\% Idle Run Time	Shows the percentage of processor time spent in an idle state. This is used to measure the idle processor for the entire system.	Should remain above 30%.	
Hyper-V Hypervisor Logical Processor\% Total Run Time	Shows the percentage of processor time spent in guest and hypervisor code. This is used to measure the total processor utilization for hypervisor and all VMs running on the host server.	Should remain below 70%.	
Hyper-V Hypervisor Virtual Processor\% Guest Run Time	Shows the percentage of virtual processor time spent in guest code for a specific VM.	Should remain below 65%.	
Hyper-V Hypervisor Virtual Processor\% Hypervisor Run Time	Shows the percentage of processor time spent in hypervisor code for a specific VM.	Should remain below 5%.	
Hyper-V Hypervisor Virtual Processor\% Idle Run Time	Shows the percentage of processor time spent in an idle state for a specific VM.	Should remain above 30%.	
Hyper-V Hypervisor Virtual Processor\%	Shows the percentage of	Should remain below 70%.	

Total Run Time	processor time spent in guest and hypervisor code for a specific VM.		
Hyper-V Hypervisor Root Virtual Processor \% Guest Run Time	Shows the percentage of time used by the virtual processor in guest code. This is used to determine the processor utilization of the virtualization stack on the host server.	Should remain below 5%.	
Hyper-V Hypervisor Virtual Processor\% Hypervisor Run Time	Shows the percentage of time used by the virtual processor in hypervisor code. This is used to determine the processor unitization by the hypervisor used by the host (and isn't specific to any VMs).	Should remain below 5%.	

Hyper-V Memory Counters

The following table shows common Hyper-V memory counters.

Counter	Description	Threshold	Troubleshooting
Memory\Available MBytes	Available megabytes (MB) is the amount of physical memory, in megabytes, immediately available for allocation to a process or for system use. This shows how much memory is remaining for guests. There is a reserve of 256 MB, 512 MB, or 2,048 bytes that the root will always leave outside of guest memory. The exact amount varies depending on the Hyper-V release. If a VM won't start, it may be because there are too few available bytes to satisfy the reserve.	Should be greater than 2 MB.	

Memory\Pages/sec	Pages/sec is the rate at which pages are read from or written to disk, to resolve hard page faults. This is a measure of memory pressure because it tracks hard faults. Hard faults are page faults that require disk access. Usually, the number spikes when there are too few available bytes available on the system, and processes are competing with each other for physical RAM.	Not applicable.	
Hyper-V VM Vid Partition\Physical Pages Allocated	Shows the total number of guest pages and Virtual Infrastructure Driver (VID) pages needed to manage the VM.	Not applicable.	
Hyper-V VM Vid Partition\Remote Pages Allocated	On non-uniform memory access (NUMA)-based systems, this shows whether a VM is spanning multiple nodes.	Not applicable.	You want to avoid this whenever possible. You can require a VM to start from a particular node by using the API described in Looking for that last ounce of performance? Then try affinitizing your VM to a NUMA node. Another way is to stop and restart the VM. If possible, Hyper-V will allocate all memory on a single NUMA node. **Note** The content of each blog and its URL are subject to change without notice. The content within each blog is provided "AS IS" with no warranties, and confers no rights. Use of included script samples or code is subject to the terms specified in the

			Microsoft Terms of Use.
Hyper-V Hypervisor [ROOT] Partition\1G GPA Pages	Shows the number of 1G pages present in the Guest Physical Address (GPA) space of the partition. This indicates whether a VM is using large pages, which improves overall VM performance.	Not applicable.	Large pages are only used on systems that have vTLB hardware support. T learn more about vTLB, see Why does my desktop box slowdown when I install Hyper-V. **Note** The content of each blog and its URL are subject to change without notice. The content within each blog is provided "AS IS" with no warranties, and confers no rights. Use of included script samples or code is subject to the terms specified in the Microsoft Terms of Use.
Hyper-V Hypervisor [ROOT] Partition\2M GPA Pages	Shows the number of 2M pages present in the GPA space of the partition. This indicates whether a VM is using large pages, which improves overall VM performance.	Not applicable.	Large pages are only used on systems that have vTLB hardware support. To learn more about vTLB, see Why does my desktop box slowdown when I install Hyper-V. **Note** The content of each blog and its URL are subject to change without notice. The content within each blog is provided "AS IS" with no warranties, and confers no rights. Use of included script samples or code is subject to the terms specified in the Microsoft Terms of Use.
Hyper-V Hypervisor [ROOT] Partition \Deposited Pages	Shows the number of pages deposited into the partition. This indicates how much	Not applicable.	

	memory the hypervisor is using for managing the VM.		

Hyper-V Network Counters

The following table shows common Hyper-V network counters.

Counter	Description	Threshold	Troubleshooting
Network Interface(*) \Bytes Total/sec	Indicates the rate at which the network adapter is processing data bytes. This counter includes all application and file data, in addition to protocol information such as packet headers.	For a 100-megabytes per second (MBps) network adapter, should be below 6–7 MBps. For a 1000-megabits per second (Mbps) network adapter, should be below 60–70 Mbps.	
Network Interface(*) \Packets Outbound Errors	Indicates the number of outbound packets that couldn't be transmitted because of errors.	Should be 0 at all times.	
TCPv4\Connection Failures	Shows the number of times TCP connections have made a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.	An increasing number of failures, or a consistently increasing rate of failures, can indicate a bandwidth shortage.	
TCPv6\Connection Failures	Shows the number of times TCP connections have made a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.	An increasing number of failures, or a consistently increasing rate of failures, can indicate a bandwidth shortage.	

TCPv4\Connections Reset	Shows the number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.	An increasing number of resets, or a consistently increasing rate of resets, can indicate a bandwidth shortage.	Some browsers send TCP reset (RST) packets, so be cautious when using this counter to determine reset rate.
TCPv6\Connections Reset	Shows the number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.	An increasing number of resets, or a consistently increasing rate of resets, can indicate a bandwidth shortage.	Some browsers send TCP reset (RST) packets, so be cautious when using this counter to determine reset rate.
Hyper-V Virtual Switch \Bytes/sec	This counter represents the total number of bytes that have traversed the network adapter.	Not applicable.	
Hyper-V Virtual Switch \Packets/sec	This counter represents the total number of bytes received per second by the network adapter.	Not applicable.	
Hyper-V Virtual Network Adapter \Bytes/sec	This counter represents the total number of bytes per second traversing the virtual switch.	For a 100-MBps network adapter, should be below 6–7 MBps. For a 1000-Mbps network adapter, should be below 60–70 Mbps.	
Hyper-V Virtual Network Adapter \Packets/sec	This counter represents the total number of packets per second traversing the virtual switch.	Not applicable.	

1.15.3.3 Client Access Server Counters

Client Access Server Counters

Exchange Server 2010 > Performance and Scalability > Performance and Scalability Counters and Thresholds >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic provides information about counters relevant to the Client Access server role in Microsoft Exchange Server 2010. You can use Performance Monitor (perfmon.exe) to monitor these counters. For more information, see Performance Monitor Getting Started Guide. For information about other counters relevant to Exchange 2010, see Performance and Scalability Counters and Thresholds.

Outlook Web App Counter

The following table shows a Microsoft Office Outlook Web App counter.

Counter	Description	Threshold
MSExchange OWA\Average Search Time	Shows the average time that elapsed while waiting for a search to complete.	Should be less than 5,000 milliseconds (ms) at all times.

ASP.NET Counters

The following table shows ASP.NET counters.

Counter	Description	Threshold	Troubleshooting
ASP.NET\Application Restarts	Shows the number of times the application has been restarted during the Web server's lifetime.	Should be 0 at all times.	
ASP.NET\Worker Process Restarts	Shows the number of times a worker process has restarted on the computer.	Should be 0 at all times.	
ASP.NET\Request Wait Time	Shows the number of ms the most recent request was waiting in the queue.	Should be 0 at all times.	Values greater than 0 should be investigated.
ASP.NET Applications (*)\Requests In Application Queue	Shows the number of requests in the application request queue.	Should be 0 at all times.	Values greater than 0 should be investigated.

Availability Service Counter

The following table shows an availability service counter.

Counter	Description	Threshold
MSExchange Availability Service\Average Time to Process a Free Busy Request	Shows the average time to process a free/busy request in seconds. One request may contain multiple mailboxes. Free/busy responses don't have meeting suggestions.	Should always be less than 5.

ActiveSync Service Counters

The following table shows ActiveSync service counters.

Counter	Description	Threshold
MSExchange ActiveSync\Ping Commands Pending	Shows the number of ping commands currently pending on the server.	Ping Commands Pending and Sync Commands Pending are the number of hanging requests, which should be almost equal to the number of Direct Push and hanging sync users.
MSExchange ActiveSync\Sync Commands Pending	Shows the number of sync commands currently pending on the server.	Ping Commands Pending and Sync Commands Pending are the number of hanging requests, which should be almost equal to the number of Direct Push and hanging sync users.
MSExchange ActiveSync \Current Requests	Shows the number of HTTP requests waiting to be assigned to a thread.	Average of 50–100.

RPC/HTTP Proxy Counters (Windows Server 2008 Only)

The following table shows Windows Server 2008 RPC/HTTP proxy counters.

Counter	Description	Threshold
RPC/HTTP Proxy\Number of Failed Back-End Connection attempts per Second	Shows the rate at which the RPC proxy attempts are occurring but failing to establish a connection to a back-end server.	Should be 0 at all times.
RPC/HTTP Proxy\Current Number of Incoming RPC over HTTP Connections	Shows the current number of front-end HTTP connections. Determines current user load.	Not applicable.
RPC/HTTP Proxy\Current Number of Unique Users	Shows the number of unique users currently connected to a back-end server via RPC/HTTP. Determines current user load.	Not applicable.
RPC/HTTP Proxy\RPC/HTTP Requests per Second	Shows the rate of RPC/HTTP requests sent to the back-end servers. Determines current Microsoft Outlook Anywhere load.	Not applicable.

RPC Client Access Counters

The following table shows RPC Client Access counters.

Counter	Description	Threshold
MSExchange RpcClientAccess \RPC Averaged Latency	Shows the latency, in ms, averaged for the past 1,024 packets.	Should be below 250 ms.
MSExchange RpcClientAccess \RPC Operations/sec	Shows the rate at which RPC operations occur, per second.	
MSExchange RpcClientAccess \RPC Requests	Shows the number of client requests currently being processed by the RPC Client Access service.	Shouldn't be over 40.

Address Book Service Counters

The following table shows Exchange 2010 address book service counters.

Counter	Description	Threshold
MSExchangeAB\NSPI RPC Browse Requests Average Latency	Shows the average time, in ms, that Name Service Provider Interface (NSPI) browse requests took to complete during the sampling period.	Should be below 1,000 ms.
MSExchangeAB\NSPI RPC Requests Average Latency	Shows the average time, in ms, that NSPI requests took to complete during the sampling period.	Should be below 1,000 ms.
MSExchangeAB\Referral RPC Requests Average Latency	Shows the average time, in ms, that referral requests took to complete during the sampling period.	Should be below 1,000 ms.

Control Panel Counters

The following table shows Exchange 2010 Control Panel counters.

Counter	Description	Threshold
MSExchange Control Panel \Outbound Proxy Requests - Average Response Time	Shows the average time (in ms) that requests sent to a secondary Client Access server took to complete during the sampling period.	The average should be under 6,000 ms.
MSExchange Control Panel \Requests - Average Response Time	Shows the average time (in ms) the Exchange Control Panel took to respond to a request during the sampling period.	The average should be under 6,000 ms.

Client Access Server OAB Download

Counters

The following table shows Client Access server offline address book (OAB) download counters.

Counter	Description	Threshold	Troubleshooting
MSExchangeFDS:OAB (*)\Download Task Queued	Shows the number of OAB download tasks queued since the File Distribution service started.	Should be 0 at all times.	Values greater than 0 indicate a failure to copy OAB data files from Mailbox servers.
MSExchangeFDS:OAB (*)\Download Tasks Completed	Shows the number of OAB download tasks completed since the File Distribution service started. The default value is every 480 minutes or 8 hours.	Should be less than or equal to 3 per day.	Values greater than 3 per day indicate the schedule for the Client Access server to download updated OAB files isn't a default schedule.

Client Activity Counters

The following table shows client activity counters.

Counter	Description	Threshold
MSExchangeIS\RPC Client Backoff/sec	Indicates the rate at which client backoffs are occurring. Higher values may indicate that the server may be incurring a higher load resulting in an increase in overall averaged RPC latencies, causing client throttling to occur. This can also occur when certain client user actions are being performed. Depending on what the client is doing and the rate at which RPC operations are occurring, it may be normal to see backoffs occurring.	Not applicable.

Client Access Server Counters

The following table shows some common Client Access server counters for determining load on your servers.

Counter	Description	Threshold
MSExchange ActiveSync \Requests/sec	Shows the number of HTTP requests received from the client via ASP.NET per second. Determines the current Exchange ActiveSync request rate.	Not applicable.

MSExchange ActiveSync\Ping Commands Pending	Shows the number of ping commands currently pending in the queue.	Not applicable.
MSExchange ActiveSync \Requests/sec	Shows the number of HTTP requests received from the client via ASP.NET per second. Used only to determine current user load.	Not applicable.
MSExchange ActiveSync\Sync Commands/sec	Shows the number of sync commands processed per second. Clients use this command to synchronize items within a folder.	Not applicable.
MSExchange Availability Service\Availability Requests (sec)	Shows the number of requests serviced per second. The request can be only for free/ busy information or include suggestions. One request may contain multiple mailboxes. Determines the rate at which Availability service requests are occurring.	Not applicable.
MSExchange OWA\Current Unique Users	Shows the number of unique users currently logged on to Outlook Web App. This value monitors the number of unique active user sessions, so that users are only removed from this counter after they log off or their session times out. Determines current user load.	Not applicable.
MSExchange OWA\Requests/ sec	Shows the number of requests handled by Outlook Web App per second. Determines current user load.	Not applicable.
MSExchangeAutodiscover \Requests/sec	Shows the number of Autodiscover service requests processed each second. Determines current user load.	Not applicable.
MSExchangeWS\Requests/ sec	Shows the number of requests processed each second. Determines current user load.	Not applicable.
Web Service(_Total)\Current Connections	Shows the current number of connections established with the Web service. Determines	Not applicable.

	current user load.	
WebService(_Total) \Connection Attempts/sec	Shows the rate that connections to the Web service are being attempted. Determines current user load.	Not applicable.
Web Service(_Total)\ISAPI Extension Requests/sec	Shows the rate that Internet Server API (ISAPI) extension requests are received by the Web service. Determines current user load. Outlook Anywhere clients make use of this ISAPI extension for RPC over HTTP requests on servers running Windows Server 2003. For Windows Server 2008 counters, see "RPC/HTTP Proxy Counters (Windows Server 2008 Only)" earlier in this topic.	Not applicable.
Web Service(_Total)\Other Request Methods/sec	Shows the rate HTTP requests are made that don't use the OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, MOVE, COPY, MKCOL, PROPFIND, PROPPATCH, SEARCH, LOCK, or UNLOCK methods. Determines current user load.	Not applicable.

Exchange Control Panel Load Counters

The following table shows Exchange 2010 Control Panel load counters.

Counter	Description	Threshold
MSExchange Control Panel \ASP.Net Request Failures/ sec	Shows the number of failures per second detected by ASP.NET in the Exchange Control Panel.	Not applicable.
MSExchange Control Panel \Explicit Sign-On Inbound Proxy Requests/sec	Shows the number of explicit sign-on requests received from a primary Client Access server per second.	Not applicable.
MSExchange Control Panel \Explicit Sign-On Inbound Proxy Sessions/sec	Shows the number of explicit sign-on inbound proxy sessions loaded per second in the Exchange Control Panel.	Not applicable.
MSExchange Control Panel \Explicit Sign-On Outbound Proxy Requests/sec	Shows the number of explicit sign-on requests sent to a secondary Client Access server per second.	Not applicable.

MSExchange Control Panel \Explicit Sign-On Outbound Session Requests/sec	Shows the number of explicit sign-on outbound proxy sessions loaded per second in the Exchange Control Panel.	Not applicable.
MSExchange Control Panel \Explicit Sign-On Standard RBAC Requests/sec	Shows the number of requests received per second by an explicit sign-on standard RBAC session.	Not applicable.
MSExchange Control Panel \Explicit Sign-On Standard RBAC Sessions/sec	Shows the number of explicit sign-on standard RBAC sessions loaded per second in the Exchange Control Panel.	Not applicable.
MSExchange Control Panel \Inbound Proxy Requests/sec	Shows the number of requests received from a primary Client Access server per second.	Not applicable.
MSExchange Control Panel \Inbound Proxy Sessions/sec	Shows the number of inbound proxy sessions loaded per second in the Exchange Control Panel.	Not applicable.
MSExchange Control Panel \Outbound Proxy Requests - Average Response Time	Shows the average time (in ms) that requests sent to a secondary Client Access server took to complete during the sampling period.	Should be under 6,000 ms.
MSExchange Control Panel \Outbound Proxy Requests/ sec	Shows the number of requests sent to a secondary Client Access server per second.	Not applicable.
MSExchange Control Panel \Outbound Proxy Sessions/ sec	Shows the number of outbound proxy sessions loaded per second in the Exchange Control Panel.	Not applicable.
MSExchange Control Panel \PowerShell Runspaces - Activations/sec	Shows the number of Windows PowerShell runspaces activated per second in the Exchange Control Panel.	Not applicable.
MSExchange Control Panel \PowerShell Runspaces - Average Active Time	Shows the average time (in seconds) that a Windows PowerShell runspace stays active while executing cmdlets in the Exchange Control Panel during the sampling period.	Not applicable.
MSExchange Control Panel \PowerShell Runspaces/sec	Shows the number of Windows PowerShell runspaces created per second in the Exchange	

	Control Panel.	
MSExchange Control Panel \RBAC Sessions/sec	Shows the number of RBAC sessions loaded per second in the Exchange Control Panel.	Not applicable.
MSExchange Control Panel \Requests - Activations/sec	Shows the number of requests activated per second in the Exchange Control Panel.	Not applicable.
MSExchange Control Panel \Requests - Average Response Time	Shows the average time (in ms) the Exchange Control Panel took to respond to a request during the sampling period.	Should be under 6,000 ms.

Availability Service Load Counter

The following table shows an availability service load counter.

Counter	Description	Threshold
MSExchange Availability Service\Availability Requests (sec)	Shows the number of requests serviced per second. The request can be only for free/busy information or include suggestions. One request may contain multiple mailboxes. Determines the rate at which Availability service requests are occurring.	Not applicable.

RPC Client Access Load Counters

The following table shows RPC Client Access load counters.

Counter	Description	Threshold
MSExchange RpcClientAccess \Active User Count	Shows the number of unique users that have shown some activity in the last 2 minutes.	Not applicable.
MSExchange RpcClientAccess \Connection Count	Shows the total number of client connections maintained.	Not applicable.
MSExchange RpcClientAccess \RPC Operations/sec	Shows the rate at which RPC operations occur, per second.	Not applicable.
MSExchange RpcClientAccess \User Count	Shows the number of users connected to the service.	Not applicable.

Exchange Address Book Load Counters

The following table shows Exchange Address Book load counters.

Counter	Description	Threshold
MSExchangeAB\NSPI Connections Current	Shows the number of NSPI clients currently connected to the server.	Not applicable.
MSExchangeAB\NSPI Connections/sec	Shows the number of NSPI client connections established to the server each second.	Not applicable.
MSExchangeAB\NSPI RPC Requests/sec	Shows the rate at which NSPI requests occur each second.	Not applicable.
MSExchangeAB\Referral RPC Requests/sec	Shows the rate at which referral requests occur each second.	Not applicable.

1.15.3.4 Mailbox Server Counters

Mailbox Server Counters

Exchange Server 2010 > Performance and Scalability > Performance and Scalability Counters and Thresholds >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic describes performance and scalability counters relevant to the Mailbox server role in Microsoft Exchange Server 2010. You can use Performance Monitor (perfmon.exe) to monitor these counters. For more information, see Performance Monitor Getting Started Guide. For information about other counters relevant to Exchange 2010, see Performance and Scalability Counters and Thresholds.

Active Database Copy I/O Latency Requirements Counters

The following table shows active database copy input/output (I/O) latency requirements counters. When these values are exceeded, the client experience degrades. For example, users may experience slow system performance and message delivery delays.

Counter	Description	Threshold	Troubleshooting
MSExchange Database\I/O Database Reads (Attached) Average Latency	Indicates the average time, in milliseconds (ms), to read from the database file.	The average value should be below 20 ms. Spikes (maximum values) shouldn't be higher than 100 ms.	
MSExchange Database\I/O Database Writes (Attached) Average Latency	Indicates the average time, in ms, to write to the database file. This counter isn't a	In general, this latency should be less than the MSExchange Database\I/O Database Reads	

	good indicator for client latency because database writes are asynchronous.	(Attached) Average Latency when battery-backed write caching is utilized.	
Database\Database Page Fault Stalls/sec	Indicates the rate of page faults that can't be serviced because there are no pages available for allocation from the database cache.	This counter should be 0 on production servers.	If this counter is above 0, it's an indication that the MSExchange Database\I/O Database Writes (Attached) Average Latency is too high.

Active Log I/O Latency Requirements Counters

The following table shows active log I/O latency requirements counters. When these values are exceeded, the client experience degrades. For example, users may experience slow system performance and message delivery delays.

Counter	Description	Threshold	Troubleshooting
MSExchange Database\IO Log Writes Average Latency	Indicates the average time, in ms, to write a log buffer to the active log file.	This counter should be 10 on production servers.	If this counter is greater than 10, it's an indication that the MSExchange Database\I/O Database Writes (Attached) Average Latency is too high.
Database\Log Record Stalls/sec	Indicates the number of log records that can't be added to the log buffers per second because the log buffers are full.	The average value should be below 10 per second. Spikes (maximum values) shouldn't be higher than 100 per second.	
Database\Log Threads Waiting	Indicates the number of threads waiting to complete an update of the database by writing their data to the log.	The average value should be less than 10 threads waiting.	

Passive Database Copy I/O Latency Requirements Counters

The following table shows passive database copy I/O latency requirements counters. When these values are exceeded, the database copy may lag by not replaying logs to the passive database copy fast enough. Log replication performance may also be affected.

Counter	Description	Threshold	Troubleshooting
MSExchange Database\I/O Database Reads (Recovery) Average Latency	Indicates the average time, in ms, to read from the database file.	The average value should be below 200 ms. Spikes (maximum values) shouldn't be higher than 1,000 ms.	
MSExchange Database\I/O Database Writes (Recovery) Average Latency	Indicates the average time, in ms, to write to the database file.	In general, this latency should be less than the MSExchange Database\I/O Database Reads (Recovery) Average Latency when battery-backed write caching is utilized.	
Database\Database Page Fault Stalls/sec	Indicates the rate of page faults that can't be serviced because there are no pages available for allocation from the database cache.	This counter should be 0 on production servers.	If this counter is greater than 0, it's an indication that the MSExchange Database\I/O Database Writes (Attached) Average Latency is too high.

Replay Log I/O Latency Requirements Counter

The following table shows a replay log I/O latency requirements counter. When these values are exceeded, the database copy may lag by not replaying logs to the passive database copy fast enough. Log replication performance may also be affected.

Counter	Description	Threshold
MSExchange Database\IO Log Read Average Latency	Indicates the average time, in ms, to read data from a log file. Specific to log replay and database recovery operations.	The average value should be below 200 ms. Spikes (maximum values) shouldn't be higher than 1,000 ms.

Information Store RPC Processing Counters

The following table shows information store RPC processing counters.

Counter	Description	Threshold	Troubleshooting
MSExchangeIS\RPC Requests	Indicates the overall RPC requests currently executing within the information store process.	Should be below 70 at all times.	

MSExchangeIS\RPC Averaged Latency	Indicates the RPC latency, in ms, averaged for all operations in the last 1,024 packets. For information about how clients are affected when overall server RPC averaged latencies increase, see Understanding Client Throttling Policies.	Shouldn't be higher than 100 ms on average.	To determine if certain protocols are causing overall RPC latencies, monitor MSExchangeIS Client (*)\RPC Average Latency to separate latencies based on client protocol.
MSExchangeIS Mailbox\RPC Averaged Latency	Indicates the RPC latency, in ms, averaged for all operations in the last 1,024 packets.	Shouldn't be higher than 100 ms on average.	
MSExchangeIS Client (*)\RPC Average Latency	Shows a server RPC latency, in ms, averaged for the past 1,024 packets for a particular client protocol.	Should be less than 50 ms on average for each client.	Wide disparities between different client types, such as IMAP4, Microsoft Outlook Anywhere, or other clients (MAPI), can help direct troubleshooting to appropriate subcomponents.

RPC Client Throttling Counters

The following table shows RPC client throttling counters.

Counter	Description	Threshold	Troubleshooting
MSExchangeIS Client (*)\RPC Average Latency	RPC Average Latency is a server RPC latency, in ms, averaged for the past 1,024 packets.	Should be less than 50 ms on average for each client.	Wide disparities between different client types, such as IMAP4, Microsoft Outlook Anywhere, or other clients (MAPI), can help direct troubleshooting to appropriate subcomponents.
MSExchangeIS\Client: RPCs Failed:Server Too Busy/sec	Shows the client-reported rate of failed RPCs (since the store was started) due to the server too busy ROC error.	Should be 0 at all times.	Higher values may indicate RPC threads are exhausted or client throttling is occurring for clients running versions of Outlook earlier than Office Outlook 2007.
MSExchangeIS\Client:	The client-reported a	Should be 0 at all	

RPCs Failed:Server Too Busy	number of failed RPCs (since the store was started) due to the server too busy ROC error.	times.	

Message Queuing Counters

The following table shows message queuing counters.

Counter	Description	Threshold	Troubleshooting
MSExchangeIS Mailbox(_Total) \Messages Queued for Submission	Shows the current number of submitted messages not yet processed by the transport layer.	Should be below 50 at all times. Shouldn't be sustained for more than 15 minutes.	This may indicate connectivity issues to the transport server.
MSExchangeIS Public (_Total)\Messages Queued for Submission	Shows the current number of submitted messages not yet processed by the transport layer.	Should be less than 20 at all times.	

Database Counters

The following table shows database counters.

Counter	Description	Threshold	Troubleshooting
MSExchange Database ==> Instances(*)\Log Generation Checkpoint Depth	Represents the amount of work in the log file count that needs to be redone or undone to the database files if the process fails.	Should be below 500 at all times for the Mailbox server role. A healthy server should indicate between 20 and 30 for each database instance.	If checkpoint depth increases continually for a sustained period, this indicates either a long-running transaction, (which will impact the version store), or a bottleneck involving the database disks.
MSExchange Database(Information Store)\Database Page Fault Stalls/sec	Shows the rate that database file page requests require of the database cache manager to allocate a new page from the database cache.	If this value is nonzero, this indicates that the database isn't able to flush dirty pages to the database file fast enough to make pages free for new page allocations.	
MSExchange Database(Information Store)\Log Record Stalls/sec	Shows the number of log records that can't be added to the log buffers per second because the log buffers are full. If this counter is nonzero for a long period of time,	The average value should be below 10 per second. Spikes (maximum values) shouldn't be higher than 100 per second.	If I/O log write latencies are high, check for RAID5 or synchronize replication on log devices. You can also use the MSExchange Database Instances

	the log buffer size may be a bottleneck.		(Information store/ <Database Name>) \log record stalls/sec counter to determine which database(s) may be having issues. This will assist you in determining which drive(s) to focus on. This counter is an extended Exchange counter in Performance Monitor.
MSExchange Database(Information Store)\Log Threads Waiting	Shows the number of threads waiting for their data to be written to the log to complete an update of the database. If this number is too high, the log may be a bottleneck.	Should be less than 10 on average.	Regular spikes concurrent with log record stall spikes indicate that the transaction log disks are a bottleneck. If the value for log threads waiting is more than the spindles available for the logs, there is a bottleneck on the log disks.
MSExchange Database(Information Store)\Version buckets allocated	Shows the total number of version buckets allocated.	Should be less than 12,000 at all times.	The maximum default version is 16,384. If version buckets reach 70% of maximum, the server is at risk of running out of the version store.
MSExchange Database Instances (*)\I/O Database Reads Average Latency	Shows the average length of time, in ms, per database read operation.	Should be 20 ms on average. Should show 50 ms spikes.	
MSExchange Database Instances (*)\I/O Database Writes Average Latency	Shows the average length of time, in ms, per database write operation.	Should be 50 ms on average.	Spikes of up to 100 ms are acceptable if not accompanied by database page fault stalls.
MSExchange Database(Information Store)\Database Cache Size (MB)	Shows the amount of system memory, in megabytes (MB), used by the database cache manager to hold commonly used information from the database files to prevent file operations.	Maximum value is RAM-2GB (RAM-3GB for servers with sync replication enabled). This and Database Cache Hit % are useful counters for gauging whether a server's performance problems might be resolved by adding more physical	Use this counter along with store private bytes to determine if there are store memory leaks. If the database cache size seems too small for optimal performance and there is little available memory on the system (check the

		memory.	value of Memory/ Available Bytes), adding more memory to the system may increase performance. If there is ample memory on the system and the database cache size isn't growing beyond a certain point, the database cache size may be capped at an artificially low limit. Increasing this limit may increase performance.
MSExchange Database(Information Store)\Database Cache % Hit	Shows the percentage of database file page requests fulfilled by the database cache without causing a file operation. If this percentage is too low, the database cache size may be too small.	Should be over 90% for companies with majority online mode clients. Should be over 99% for companies with majority cached mode clients.	If the hit ratio is less than these numbers, the database cache may be insufficient.
MSExchange Database\Log Bytes Write/sec	Shows the rate of bytes written to the log.	Should be less than 10,000,000 at all times.	With each log file being 1,000,000 bytes in size, 10,000,000 bytes/sec would yield 10 logs per second. This may indicate a large message being sent or a looping message.

Client-Related Search Counters

The following table shows client-related search counters.

Counter	Description	Threshold	Troubleshooting
MSExchangeIS Mailbox(*)\Slow Findrow Rate	Shows the rate at which the slower FindRow needs to be used in the mailbox store.	Should be no more than 10 for any specific mailbox store.	Higher values indicate applications are crawling or searching mailboxes, which is affecting server performance. These include desktop search engines, customer relationship management (CRM), or other third-party applications.

MSExchangeIS Mailbox(*)\Search Task Rate	Shows the number of search tasks created per second.	Should be less than 10 at all times.	
MSExchangeIS\Slow QP Threads	Shows the number of query processor threads currently running queries that aren't optimized.	Should be less than 10 at all times.	
MSExchangeIS\Slow Search Threads	Shows the number of search threads currently running queries that aren't optimized.	Should be less than 10 at all times.	

Content Indexing Counters

The following table shows content indexing counters.

Counter	Description	Threshold	Troubleshooting
Process (Microsoft.Exchange.Search.ExSearch)\% Processor time	Shows the amount of processor time currently being consumed by the Exchange Search service.	Should be less than 1% of overall CPU typically and not sustained above 5%. Should be less than 10% of what the store process is during steady state.	
Process(msftefd*)\% Processor Time	Shows the amount of processor time being consumed to update content indexing within the store process.	Full crawls increase overall processing time, but should never exceed overall store CPU capacity.	Check throttling counters to determine if throttling is occurring due to server performance bottlenecks.
MSExchange Search Indices(*)\Recent Average Latency of RPCs Used to Obtain Content	Shows the average latency, in ms, of the most recent RPCs to the Information Store service. These RPCs are used to get content for the filter daemon for the specified database.	Should coincide with the latencies that Outlook clients are experiencing.	
MSExchange Search Indices(*)\ Average Document Indexing Time	Shows the average, in ms, of how long it takes to index documents.	Should be less than 30 seconds at all time.	
MSExchange Search Indices(*)\Full Crawl Mode Status	This counter is used to determine if a full crawl is occurring for any specified database.	Indicates whether this .mdb file is going through a full crawl (value=1) or not (value=0).	If CPU resources are high, it's possible content indexing is occurring for a database or set of databases.

Mailbox Assistant Counters

The following table shows mailbox assistant counters.

Counter	Description	Threshold
Process (MSExchangeMailboxAssistants)\%Processor Time	Shows the amount of processor time being consumed by mailbox assistants.	Should be less than 5% of overall CPU capacity.
MSExchange Assistants(*) \Events in queue	Shows the number of events in the in-memory queue waiting to be processed by the assistants.	Should be a low value at all times. High values may indicate a performance bottleneck.
MSExchange Assistants(*) \Average Event Processing Time in Seconds	Shows the average processing time of the events chosen.	Should be less than 2 at all times.

Resource Booking Counters

The following table shows resource booking counters.

Counter	Description	Threshold
MSExchange Resource Booking\Average ResourceBooking Processing Time	Shows the average time to process an event in the Resource Booking Attendant.	Should be a low value at all times. High values may indicate a performance bottleneck.
MSExchange Resource Booking\Requests Failed	Shows the total number of failures that occurred while the Resource Booking Attendant was processing events.	Should be 0 at all times.

Calendar Attendant Counters

The following table shows Calendar Attendant counters.

Counter	Description	Threshold
MSExchange Calendar Attendant\Average Calendar Attendant Processing time	Shows the average time to process an event in the Calendar Attendant.	Should be a low value at all times. High values may indicate a performance bottleneck.
MSExchange Calendar Attendant\Requests Failed	Shows the total number of failures that occurred while the Calendar Attendant was processing events.	Should be 0 at all times.

Store Client Request Counters

The following table shows store client request counters.

Counter	Description	Threshold

MSExchange Store Interface (_Total)\RPC Latency average (msec)	Shows the average latency, in ms, of RPC requests. The average is calculated over all RPCs since exrpc32 was loaded.	Should be less than 100 ms at all times.
MSExchange Store Interface (*)\ROP Requests outstanding	Shows the total number of outstanding remote operations requests. Used for determining current load.	
MSExchange Store Interface (_Total)\RPC Requests outstanding	Shows the current number of outstanding RPC requests.	Should be 0 at all times.
MSExchange Store Interface (*)\RPC Requests Outstanding	Shows the total number of outstanding RPC requests. Used for determining current load.	
MSExchange Store Interface (*)\RPC Requests Sent/sec	Shows the current rate of initiated RPC requests per second. Used for determining current load.	Not applicable.
MSExchange Store Interface (*)\RPC Slow Requests latency average (msec)	Shows the average latency, in ms, of slow requests. Used for determining the average latencies of RPC slow requests.	
MSExchange Store Interface (*)\RPC Requests failed (%)	Shows the percentage of failed requests in the total number of RPC requests. Failed means the sum of failed with error code plus failed with exception.	Should be less than 1 at all times.
MSExchange Store Interface (*)\RPC Slow Requests (%)	Shows the percentage of slow RPC requests among all RPC requests. A slow RPC request is one that has taken more than 500 ms.	Should be less than 1 at all times.
MSExchangeMailSubmission (*)\Successful Submissions Per Second	Determines current mail submission rate.	Not applicable.
MSExchangeMailSubmission (*)\Hub Servers In Retry	Shows the number of Hub Transport servers in retry mode.	Should be 0 at all times.
MSExchangeMailSubmission (*)\Failed Submissions Per Second	Shows the number of failed submissions per second.	Should be 0 at all times.
MSExchangeMailSubmission (*)\Temporary Submission Failures/sec	Shows the number of temporary submission failures per second.	Should be 0 at all times.
MSExchange Replication(*)	Shows the number of	Should be less than 1 at all

\CopyQueueLength	transaction log files waiting to be copied to the passive copy log file folder. A copy isn't considered complete until it has been checked for corruption.	times for continuous replication.
MSExchange Replication(*) \ReplayQueueLength	Shows the number of transaction log files waiting to be replayed into the passive copy.	Indicates the current replay queue length. Higher values cause longer store mount times when a handoff, failover, or activation is performed.
MSExchange Replica Seeder (*)\Seeding Finished %	Shows the finished percentage of seeding. Its value is from 0 through 100% . Used to determine if seeding is occurring for a particular database, which is possibly affecting overall server performance or current network bandwidth.	Not applicable.
MSExchangeIS\RPC Operations/sec	Indicates the current number of RPC operations occurring per second.	Should closely correspond to historical baselines. Values much higher than expected indicate that the workload has changed, while values much lower than expected indicate a bottleneck preventing client requests from reaching the server.

Client Activity Counters

The following table shows client activity counters.

Counter	Description	Threshold
MSExchangeIS\RPC Client Backoff/sec	Indicates the rate at which client backoffs are occurring. Higher values may indicate that the server may be incurring a higher load resulting in an increase in overall averaged RPC latencies, causing client throttling to occur. This can also occur when certain client user actions are being performed. Depending on what the client is doing and the rate at which RPC operations are occurring, it may be normal to see backoffs occurring.	Not applicable.
MSExchangeIS\Client: RPCs	Shows the client-reported	Should be 0 at all times.

Failed:Server Too Busy/sec	rate of failed RPCs (since the store was started) due to the server too busy ROC error.	Higher values may indicate RPC threads are exhausted or client throttling is occurring for clients running versions of Outlook earlier than Outlook 2007.
MSExchangeIS\Client: RPCs Failed:Server Too Busy	The client-reported number of failed RPCs (since the store was started) due to the server too busy ROC error.	Should be 0 at all times.

Information Store Counters

The following table shows information store counters for determining user load.

Counter	Description	Threshold
MSExchangeIS Client(*)\RPC Operations/sec	Shows what client protocol is performing an excessive amount of RPC Operations/sec. High IMAP4, POP3, or Outlook Anywhere latency can indicate problems with Client Access servers rather than Mailbox servers. This is especially true when other clients (which includes MAPI) latency is lower in comparison. In some instances, high IMAP latencies could indicate a bottleneck on the Mailbox server in addition to the latencies that the Client Access server is experiencing.	Not applicable.
MSExchangeIS Client (*)\RPC Average Latency	RPC Average Latency is a server RPC latency, in ms, averaged for the past 1,024 packets.	Should be less than 50 ms on average.
MSExchangeIS Client(*)\JET Log Records/sec	Shows the rate that database log records are generated while processing requests for the client. Used to determine current load.	Not applicable.
MSExchangeIS Client(*)\JET Pages Read/sec	Shows the rate that database pages are read from disk while processing requests for the client. Used to determine current load.	Not applicable.
MSExchangeIS Client(*) \Directory Access: LDAP Reads/sec	Shows the current rate that LDAP reads occur while processing requests for the client. Used to determine the	Not applicable.

	current LDAP read rate per protocol.	
MSExchangeIS Client(*) \Directory Access: LDAP Searches/sec	Shows the current rate that LDAP searches occur while processing requests for the client. Used to determine the current LDAP search rate per protocol.	Not applicable.
MSExchangeIS Mailbox (_Total)\Messages Delivered/sec	Shows the rate that messages are delivered to all recipients. Indicates current message delivery rate to the store.	Not applicable.
MSExchangeIS Mailbox (_Total)\Messages Sent/sec	Shows the rate that messages are sent to transport. Used to determine current messages sent to transport.	Not applicable.
MSExchangeIS Mailbox (_Total)\Messages Submitted/sec	Shows the rate that messages are submitted by clients. Used to determine current rate that messages are being submitted by clients.	Not applicable.
MSExchangeIS\User Count	Shows the number of users connected to the information store. Used to determine current user load.	Not applicable.
MSExchangeIS Public(_Total) \Replication Receive Queue Size	Shows the number of replication messages waiting to be processed.	Should be less than 100 at all times. This value should return to a minimum value between replication intervals.

Mailbox Assistant Counters

The following table shows mailbox assistant counters.

Counter	Description	Threshold
MSExchange Assistants(*) \Mailboxes Processed/sec	Shows the rate of mailboxes processed by time-based assistants per second. Determines current load statistics for this counter.	Not applicable.
MSExchange Assistants(*) \Events Polled/sec	Shows the number of events polled per second. Determines current load statistics for this counter.	Not applicable.

1.15.3.5 Transport Server Counters

Transport Server Counters

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2012-07-23*

This topic provides information about counters relevant to the Hub Transport and Edge Transport server roles in Microsoft Exchange Server 2010. You can use Performance Monitor (perfmon.exe) to monitor these counters. For more information, see Performance Monitor Getting Started Guide. For information about other counters relevant to Exchange 2010, see Performance and Scalability Counters and Thresholds.

Transport Disk Counters

The following table shows transport disk counters.

Counter	Description	Threshold
Logical/Physical Disk(*)\Avg. Disk sec/Read	Shows the average time, in seconds, of a read of data from the disk.	Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) shouldn't be higher than 50 ms.
Logical/Physical Disk(*)\Avg. Disk sec/Write	Shows the average time, in seconds, of a write of data to the disk.	Should be less than 20 ms on average. Spikes (maximum values) shouldn't be higher than 50 ms.

Transport Queue Length Counters

The following table shows transport queue length counters.

Counter	Description	Threshold
\MSExchangeTransport Queues(_total)\Aggregate Delivery Queue Length (All Queues)	Shows the number of messages queued for delivery in all queues.	Should be less than 3,000 and not more than 5,000.
\MSExchangeTransport Queues(_total)\Active Remote Delivery Queue Length	Shows the number of messages in the active remote delivery queues.	Should be less than 250 at all times.
\MSExchangeTransport Queues(_total)\Active Mailbox Delivery Queue Length	Shows the number of messages in the active mailbox queues.	Should be less than 250 at all times.
\MSExchangeTransport Queues(_total)\Submission Queue Length	Shows the number of messages in the submission queue.	Shouldn't exceed 100. If sustained high values are occurring, investigate Active Directory and Mailbox servers for bottlenecks or performance-related issues.

\MSExchangeTransport Queues(_total)\Active Non-Smtp Delivery Queue Length	Shows the number of messages in the drop directory used by a Foreign connector.	Should be less than 250 at all times.
\MSExchangeTransport Queues(_total)\Retry Mailbox Delivery Queue Length	Shows the number of messages in a retry state attempting to deliver a message to a remote mailbox.	Should be less than 100 at all times.
\MSExchangeTransport Queues(_total)\Retry Non-Smtp Delivery Queue Length	Shows the number of messages in a retry state in the non-SMTP gateway delivery queues.	Shouldn't exceed 100.
\MSExchangeTransport Queues(_total)\Retry Remote Delivery Queue Length	Shows the number of messages in a retry state in the remote delivery queues.	Shouldn't exceed 100. We recommend that you check the next hop to determine the causes for queuing.
\MSExchangeTransport Queues(_total)\Unreachable Queue Length	Shows the number of messages in the Unreachable queue.	Shouldn't exceed 100.
\MSExchangeTransport Queues(_total)\Largest Delivery Queue Length	Shows the number of messages in the largest delivery queues.	Should be less than 200 for the Edge Transport and Hub Transport server roles.
\MSExchangeTransport Queues(_total)\Poison Queue Length	Shows the number of messages in the poison message queue.	Should be 0 at all times.

Transport Dumpster Counters

The following table shows transport dumpster counters.

Counter	Description	Threshold
\MSExchangeTransport Dumpster\Dumpster Size	Shows the total size (in bytes) of mail items currently in the transport dumpster on this server.	Not applicable.
\MSExchangeTransport Dumpster\Dumpster Inserts/sec	Shows the rate at which items are inserted into the transport dumpster on this server. Determines the current rate of transport dumpster inserts.	Not applicable.
\MSExchangeTransport Dumpster\Dumpster Item Count	Shows the total number of mail items currently in the transport dumpster on this server. Shows the current number of items being held in the transport dumpster.	Not applicable.
\MSExchangeTransport Dumpster\Dumpster Deletes/sec	Shows the rate at which items are deleted from the transport dumpster on this	Not applicable.

	server. Determines the current rate of transport dumpster deletions.	

Transport Database Counters

The following table shows transport database counters.

Counter	Description	Threshold
MSExchange Database ==> Instances(edgetransport/ Transport Mail Database)\I/O Log Writes/sec	Shows the rate of log file write operations completed. Determines the current load. Compare values to historical baselines.	Not applicable.
MSExchange Database ==> Instances(edgetransport/ Transport Mail Database)\I/O Log Reads/sec	Shows the rate of log file read operations completed. Determines the current load. Compare values to historical baselines.	Not applicable.
MSExchange Database ==> Instances(edgetransport/ Transport Mail Database)\Log Generation Checkpoint Depth	Represents the amount of work (in count of log files) that needs to be redone or undone to the database files if the process fails.	Not applicable.
MSExchange Database ==> Instances(edgetransport/ Transport Mail Database) \Version buckets allocated	Total number of version buckets allocated. Shows the default backpressure values as listed in the edgetransport.exe.config file.	Should be less than 200 at all times.
MSExchange Database ==> Instances(edgetransport/ Transport Mail Database)\I/O Database Reads/sec	Shows the rate of database read operations completed. Determines the current load. Compare values to historical baselines.	Not applicable.
MSExchange Database ==> Instances(edgetransport/ Transport Mail Database)\I/O Database Writes/sec	Shows the rate of database write operations completed. Determines the current load. Compare values to historical baselines.	Not applicable.
MSExchange Database ==> Instances(edgetransport/ Transport Mail Database)\Log Record Stalls/sec	Shows the number of log records that can't be added to the log buffers per second because they are full. If this counter is nonzero most of the time, the log buffer size may be a bottleneck.	Should be less than 10 per second on average. Spikes (maximum values) shouldn't be greater than 100 per second.
MSExchange Database ==> Instances(edgetransport/ Transport Mail Database)\Log Threads Waiting	Shows the number of threads waiting for their data to be written to the log to complete an update of the database. If this number is too high, the log may be a	Should be less than 10 threads waiting on average.

	bottleneck.	

Extensibility Agent Counters

The following table shows extensibility agent counters.

Counter	Description	Threshold
MSExchange Extensibility Agents(*)\Average Agent Processing Time (sec)	Shows the average agent processing time in seconds per event.	Should be less than 20 at all times. Sustained higher latencies may indicate a hung agent.
MSExchange Extensibility Agents(*)\Total Agent Invocations	Shows the total number of invocations since the last restart. Shows the current invocation rate.	Not applicable.

Transport Load Assessment Counters

The following table shows transport load assessment counters.

Counter	Description	Threshold
\MSExchangeTransport Queues(_total)\Messages Submitted Per Second	Shows the number of messages queued in the Submission queue per second. Determines current load. Compare values to historical baselines.	Not applicable.
\MSExchangeTransport Queues(_total)\Messages Completed Delivery Per Second	Shows the number of messages delivered per second. Determines current load. Compare values to historical baselines.	Not applicable.
\MSExchange Store Driver (_total)\Inbound: LocalDeliveryCallsPerSecond	Shows the number of local delivery attempts per second. Determines current load. Compare values to historical baselines.	Not applicable.
\MSExchange Store Driver (_total)\Outbound: Submitted Mail Items Per Second	Shows the number of mail items per second being submitted. Determines current load. Compare values to historical baselines.	Not applicable.
\MSExchangeTransport SmtpReceive(_total)\Average bytes/message	Shows the average number of message bytes per inbound message received. Determines sizes of messages being received for an SMTP receive connector.	Not applicable.
\MSExchangeTransport SmtpReceive(_total) \Messages Received/sec	Shows the number of messages received by the SMTP server each second. Determines current load.	Not applicable.

	Compare values to historical baselines.	
\MSExchangeTransport SmtpSend(_total)\Messages Sent/sec	Shows the number of messages sent by the SMTP send connector each second. Determines current load. Compare values to historical baselines.	Not applicable.
\MSExchange Store Driver (_total)\ Inbound: MessageDeliveryAttemptsPer Second	Shows the number of attempts for delivering transport mail items per second. Determines current load. Compare values to historical baselines.	Not applicable.
MSExchange Store Driver (_total)\Inbound: Recipients Delivered Per Second	Shows the number of inbound recipients delivered per second. Determines current load. Compare values to historical baselines.	Not applicable.
MSExchangeTransport Queues(_total)\Messages Queued for Delivery Per Second	Shows the number of messages queued for delivery per second. Determines current load. Compare values to historical baselines.	Not applicable.
MSExchangeTransport Queues(_total)\Messages Completed Delivery Per Second	Shows the number of messages delivered per second. Determines current load. Compare values to historical baselines.	Not applicable.

1.15.3.6 Unified Messaging Counters

Unified Messaging Counters

Exchange Server 2010 > Performance and Scalability > Performance and Scalability Counters and Thresholds >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-09-15*

Performance and Scalability Counters for Unified Messaging

General Performance Counters for Unified Messaging

Call Answering Performance Counters for Unified Messaging

Subscriber Access Performance Counters for Unified Messaging

Auto Attendant Performance Counters for Unified Messaging

System Availability Counters for Unified Messaging

Performance Monitoring Counters for Unified Messaging

Fax Answering Performance Counters for Unified Messaging

1.15.3.6.1 Performance and Scalability Counters for Unified Messaging

Performance and Scalability Counters for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-11-16*

The following table provides information about performance counters that are used by the Unified Messaging (UM) server role in Microsoft Exchange Server 2010. You can use Performance Monitor (perfmon.exe) to monitor these counters.

For more information, see Performance Monitor Getting Started Guide. For information about other counters relevant to Exchange 2010, see Performance and Scalability Counters and Thresholds.

Object	Counter	Description	Threshold	Troubleshooting
MSExchangeUMA vailability	% of Failed Mailbox Connection Attempts Over the Last Hour	Shows the percentage of mailbox connection attempts that failed in the last hour.	Should be less than 5%.	
MSExchangeUMA vailability	% of Inbound Calls Rejected by the UM Service Over the Last Hour	Shows the percentage of inbound calls that were rejected by the Microsoft Exchange Unified Messaging service over the last hour.	Should be less than 5%.	
MSExchangeUMA vailability	% of Inbound Calls Rejected by the UM Worker Process Over the Last Hour	Shows the percentage of inbound calls that were rejected by the UM worker process over the last hour.	Should be less than 5%.	
MSExchangeUMA vailability	% of Messages Successfully Processed Over the Last Hour	Shows the percentage of messages that were successfully	Should be greater or equal to 95%	

		processed by the Microsoft Exchange Unified Messaging service over the last hour.		
MSExchangeUMAvailability	% of Partner Voice Message Transcription Failures Over the Last Hour	Shows the percentage of voice messages for which transcription failed in the last hour.	Should be less than 5%.	
MSExchangeUMAvailability	Directory Access Failures	Shows the number of times that attempts to access Active Directory failed.	Should be 0 at all times.	
MSExchangeUMAvailability	Calls Disconnected on Irrecoverable Internal Error	Shows the number of calls disconnected after an internal system error occurred.	Should be 0 at all times.	
MSExchangeUMPerformance	Operations over Six Seconds	Shows the number of all UM operations that took more than six seconds to complete. This is the time during which a caller was waiting for UM to respond.	Should be 0 at all times.	
MSExchangeUMCallAnswer	Calls Disconnected by Callers During UM Audio Hourglass	Shows the number of calls during which the caller disconnected while Unified Messaging was playing the audio hourglass tones.	Should be 0 at all times.	A nonzero value suggests excessive latency between a Unified Messaging server and targeted domain controller.
MSExchangeUMAvailability	Total Inbound Calls Rejected by the UM Service	Shows the total number of inbound calls that were rejected by the Microsoft Exchange Unified Messaging Service since the service was started.	Should be 0 at all times.	

MSExchangeUMAvailability	Total Inbound Calls Rejected by the UM Worker Process	Shows the total number of inbound calls that were rejected by the UM Worker process since the service was started.	Should be 0 at all times.	

1.15.3.6.2 General Performance Counters for Unified Messaging

General Performance Counters for Unified Messaging

Performance and Scalability > Performance and Scalability Counters and Thresholds > Unified Messaging Counters >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-08*

There are many performance counters that can be used to maintain and troubleshoot a Microsoft Exchange Server 2010 Unified Messaging (UM) server. Unified Messaging performance counters measure quantities of information or data for Unified Messaging based on the number, size, duration, and rate of data that's being requested or received.

General Performance Counters

The following table provides a list of the general performance counters that can be used to monitor Exchange 2010 Unified Messaging.

General performance counters for Unified Messaging

Performance counter	Performance object	Description
% Successful Caller ID Resolutions	MSExchangeUMGeneral	% Successful Caller ID Resolutions is the percentage of caller IDs that were resolved successfully.
% Successful Extension Caller ID Resolutions	MSExchangeUMGeneral	% Successful Extension Caller ID Resolutions is the percentage of successful attempts to resolve caller IDs that contained no "@" or "+" signs and were of the same length as the dial plan's extension. This counter is used only for TelExtn dial plans.
Average Call Duration	MSExchangeUMGeneral	Average Call Duration is the average duration, in seconds, of calls since the service was started.
Average MWI Latency	MSExchangeUMGeneral	Average MWI Latency is the average time, in milliseconds,

		from the moment a voice mail event occurs and Unified Messaging receives confirmation from the IP gateway that the message was delivered. This average is calculated over the last 50 messages.
Average Recent Call Duration	MSExchangeUMGeneral	Average Recent Call Duration is the average duration, in seconds, of the last 50 calls.
Call Duration Exceeded	MSExchangeUMGeneral	Call Duration Exceeded is the number of calls that were disconnected because they exceeded the UM maximum call length. This number includes all types of calls, including fax calls.
Caller ID Resolutions Attempted	MSExchangeUMGeneral	Caller ID Resolutions Attempted is the number of caller ID resolutions that were attempted.
Caller ID Resolutions Succeeded	MSExchangeUMGeneral	Caller ID Resolutions Succeeded is the number of caller IDs that were resolved successfully.
Calls Disconnected by User Failure	MSExchangeUMGeneral	Calls Disconnected by User Failure is the total number of calls disconnected after too many user entry failures.
Current Auto Attendant Calls	MSExchangeUMGeneral	Current Auto Attendant Calls is the number of auto attendant calls that are currently connected to the UM server.
Current Calls	MSExchangeUMGeneral	Current Calls is the number of calls that are currently connected to the UM server.
Current Fax Calls	MSExchangeUMGeneral	Current Fax Calls is the number of fax calls that are currently connected to the UM server. Voice calls become fax calls after a fax tone is detected.
Current Play on Phone Calls	MSExchangeUMGeneral	Current Play on Phone Calls is the number of outbound calls initiated to play back messages.
Current Prompt Editing Calls	MSExchangeUMGeneral	Current Prompt Editing Calls is the number of logged on users who are editing custom

		prompts.
Current Subscriber Access Calls	MSExchangeUMGeneral	Current Subscriber Access Calls is the number of logged on subscribers who are currently connected to the UM server.
Current Unauthenticated Pilot Number Calls	MSExchangeUMGeneral	Current Unauthenticated Pilot Number Calls is the number of voice calls to the pilot number that have not yet been authenticated.
Current Voice Mail Calls	MSExchangeUMGeneral	Current Voice Mail Calls is the number of voice mail calls that are currently connected to the Unified Messaging server.
Delayed Calls	MSExchangeUMGeneral	Delayed Calls is the number of calls that experienced one or more delays longer than 2 seconds.
Extension Caller ID Resolutions Attempted	MSExchangeUMGeneral	Extension Caller ID Resolutions Attempted is the number of attempts to resolve caller IDs that contained no "@" or "+" signs and were of the same length as the dial plan's extension. This counter is used only for TelExtn dial plans.
Extension Caller ID Resolutions Succeeded	MSExchangeUMGeneral	Extension Caller ID Resolutions Succeeded is the number of successful attempts to resolve caller IDs that contained no "@" or "+" signs and were of the same length as the dial plan's extension. This counter is used only for TelExtn dial plans.
OCS User Event Notifications	MSExchangeUMGeneral	OCS User Event Notifications is the total number of OCS user event notifications that occurred since the service was started.
Total Calls	MSExchangeUMGeneral	Total Calls is the number of calls answered or placed since the service was started. Transfers are not included.
Total Calls per Second	MSExchangeUMGeneral	Total Calls per Second is the number of new calls that

		have arrived in the last second.
Total Play on Phone Calls	MSExchangeUMGeneral	Total Play on Phone Calls is the total number of Play on Phone calls that have been initiated since the service was started.
User Response Latency	MSExchangeUMGeneral	User Response Latency is the average response time, in milliseconds, for the system to respond to a user request. This average is calculated over the last 25 calls. This counter is limited to calls that require significant processing.

1.15.3.6.3 Call Answering Performance Counters for Unified Messaging

Call Answering Performance Counters for Unified Messaging

Performance and Scalability > Performance and Scalability Counters and Thresholds > Unified Messaging Counters >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-08*

There are many performance counters that can be used to maintain and troubleshoot a Microsoft Exchange Server 2010 Unified Messaging (UM) server. Unified Messaging performance counters are used to measure quantities of information or data for Unified Messaging and are based on the number, size, duration, and rate of data that's being requested or received.

Call Answering Performance Counters

The following table provides a list of the call answering performance counters that can be used to monitor Unified Messaging.

Unified Messaging call answering performance counters

Performance counter	Performance object	Description
Average Greeting Size	MSExchangeUMCallAnswering	Average Greeting Size is the average size, in seconds, of recorded greetings that have been retrieved by the Unified Messaging server.
Average Recent Voice Message Size	MSExchangeUMCallAnswering	Average Recent Voice Message Size is the average size, in seconds, of the last 50 voice messages that have been left for subscribers.

Average Time Taken for Call Answering Rule Evaluations	MSExchangeUMCallAnswering	Average Time Taken for Call Answering Rule Evaluations is the average time it takes to determine if one or more call answering rules apply to a call answering call.
Average Voice Message Size	MSExchangeUMCallAnswering	Average Voice Message Size is the average size, in seconds, of voice messages left for subscribers.
Call Answering Calls	MSExchangeUMCallAnswering	Call Answering Calls is the number of diverted calls that were answered on behalf of subscribers.
Call Answering Escapes	MSExchangeUMCallAnswering	Call Answering Escapes is the number of times a caller pressed the * key to connect to another user instead of leaving a message.
Call Answering Missed Calls	MSExchangeUMCallAnswering	Call Answering Missed Calls is the number of times a diverted call was dropped without a message being left.
Call Answering Protected Voice Messages	MSExchangeUMCallAnswering	Call Answering Protected Voice Messages is the total number of protected voice messages that were submitted because calls were answered on behalf of subscribers.
Call Answering Voice Message Protection Failures	MSExchangeUMCallAnswering	Call Answering Voice Message Protection Failures is the total number of voice messages, submitted because calls were answered on behalf of the subscribers, for which the attempt to apply protection failed.
Call Answering Voice Messages	MSExchangeUMCallAnswering	Call Answering Voice Messages is the total number of voice messages that were submitted for delivery because the calls were answered on behalf of subscribers.
Calls Disconnected by Callers During UM Audio Hourglass	MSExchangeUMCallAnswering	Calls Disconnected by Callers During UM Audio Hourglass is the number of calls during which the caller disconnected while Unified Messaging was playing the audio hourglass tones.

Calls Disconnected by UM on Irrecoverable External Error	MSExchangeUMCallAnswering	Calls Disconnected by UM on Irrecoverable External Error is the number of calls that have been disconnected after an irrecoverable external error occurred.
Calls Without Personal Greetings	MSExchangeUMCallAnswering	Calls Without Personal Greetings is the number of diverted calls received for subscribers that did not have recorded greeting messages.
Diverted Extension Not Provisioned	MSExchangeUMCallAnswering	Diverted Extension Not Provisioned is the number of calls received for which the diverted extension supplied with the call is not a UM subscriber extension.
Fetch Greeting Timed Out	MSExchangeUMCallAnswering	Fetch Greeting Timed Out is the number of diverted calls for which the subscriber's personal greeting could not be retrieved within the time allowed.
Total Calls to Subscribers with One or More Call Answering Rules Configured	MSExchangeUMCallAnswering	Total Calls to Subscribers with One or More Call Answering Rules Configured evaluates calls to determine whether any call answering rules should be applied.
Total Number of Call Answering Rules Calls	MSExchangeUMCallAnswering	Total Number of Call Answering Rules Calls is the total number of calls that fulfill the conditions of at least one call answering rule. The rule is subsequently invoked to handle the call.
Total Number of Timed-out Call Answering Rule Evaluations	MSExchangeUMCallAnswering	Total Number of Timed-out Call Answering Rule Evaluations is the total number of calls for which call answering rules weren't applied because the system timed out. As a result, the calls were answered using the Exchange 2007 UM voice mail behavior.

Return to top

Subscriber Access Performance Counters for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-08*

There are many performance counters that can be used to maintain and troubleshoot a Microsoft Exchange Server 2010 Unified Messaging (UM) server. Unified Messaging performance counters are used to measure quantities of information or data for Unified Messaging based on the number, size, duration, and rate of data that's being requested or received.

Subscriber Access Performance Counters

The following table provides a list of the subscriber access performance counters that can be used to monitor Unified Messaging.

Unified Messaging subscriber access performance counters

Performance counter	Performance object	Description
Average Recent Sent Voice Message Size	MSExchangeUMSubscriberAccess	Average Recent Sent Voice Message Size is the average size, in seconds, of the last 50 voice messages that were sent.
Average Recent Subscriber Call Duration	MSExchangeUMSubscriberAccess	Average Recent Subscriber Call Duration is the average length of time, in seconds, that subscribers spent logged on to the system for the last 50 subscriber calls.
Average Sent Voice Message Size	MSExchangeUMSubscriberAccess	Average Sent Voice Message Size is the average size, in seconds, of voice messages that are sent. This size doesn't include any attachment data.
Average Subscriber Call Duration	MSExchangeUMSubscriberAccess	Average Subscriber Call Duration is the average duration, in seconds, that subscribers spent logged on to the system. This timer starts when logon completes.
Calendar Accessed	MSExchangeUMSubscriberAccess	Calendar Accessed is the number of times subscribers accessed their calendars using the telephone user interface.
Calendar Items Details Requested	MSExchangeUMSubscriberAccess	Calendar Items Details Requested is the number of times a subscriber requested

		additional details for a calendar item.
Calendar Items Heard	MSExchangeUMSubscriberAccess	Calendar Items Heard is the number of Calendar items that have been heard by authenticated subscribers.
Calendar Late Attendance	MSExchangeUMSubscriberAccess	Calendar Late Attendance is the number of messages that have been sent to inform the organizer of a meeting that the subscriber will be late.
Called Meeting Organizer	MSExchangeUMSubscriberAccess	Called Meeting Organizer is the number of times subscribers called the meeting organizer.
Calls Disconnected by Callers During UM Audio Hourglass	MSExchangeUMSubscriberAccess	Calls Disconnected by Callers During UM Audio Hourglass is the number of calls in which the caller disconnected while UM was playing the audio hourglass tones.
Calls Disconnected by UM on Irrecoverable External Error	MSExchangeUMSubscriberAccess	Calls Disconnected by UM on Irrecoverable External Error is the total number of calls that have been disconnected after an irrecoverable external error occurred.
Contact Items Heard	MSExchangeUMSubscriberAccess	Contact Items Heard is the number of times authenticated subscribers listened to directory details.
Contacts Accessed	MSExchangeUMSubscriberAccess	Contacts Accessed is the number of times subscribers accessed the Main Menu Contacts option by using the telephone user interface.
Directory Accessed	MSExchangeUMSubscriberAccess	Directory Accessed is the number of times subscribers accessed the Main Menu Directory option by using the telephone user interface.
Directory Accessed by Dial by Name	MSExchangeUMSubscriberAccess	Directory Accessed by Dial by Name is the number of directory access operations where the subscriber used the Dial by Name feature.
Directory Accessed by Extension	MSExchangeUMSubscriberAccess	Directory Accessed by Extension is the number of directory access operations in which the user supplied the extension number.

Directory Accessed by Spoken Name	MSExchangeUMSubscriberAccess	Directory Accessed by Spoken Name is the number of directory access operations in which the subscriber spoke a recipient name.
Directory Accessed Successfully by Dial by Name	MSExchangeUMSubscriberAccess	Directory Accessed Successfully by Dial by Name is the number of Dial by Name directory access operations that completed successfully on behalf of users.
Directory Accessed Successfully by Spoken Name	MSExchangeUMSubscriberAccess	Directory Accessed Successfully by Spoken Name is the number of speech recognition directory access operations that completed successfully on behalf of subscribers.
Email Message Queue Accessed	MSExchangeUMSubscriberAccess	Email Message Queue Accessed is the number of times subscribers accessed their e-mail message queue by using the telephone user interface.
Email Messages Deleted	MSExchangeUMSubscriberAccess	Email Messages Deleted is the number of e-mail messages that were deleted by authenticated subscribers.
Email Messages Heard	MSExchangeUMSubscriberAccess	Email Messages Heard is the number of e-mail messages that were heard by authenticated subscribers.
Forward Messages Sent	MSExchangeUMSubscriberAccess	Forward Messages Sent is the number of messages that have been forwarded by authenticated subscribers.
Launched Calls	MSExchangeUMSubscriberAccess	Launched Calls is the number of subscriber calls that resulted in an outbound call being placed.
Meetings Accepted	MSExchangeUMSubscriberAccess	Meetings Accepted is the number of Meeting Accepted messages sent by subscribers.
Meetings Declined	MSExchangeUMSubscriberAccess	Meetings Declined is the number of Meeting Declined messages sent by subscribers.
Protected Voice Messages	MSExchangeUMSubscriberAcc	Protected Voice Messages

Heard	ess	Heard is the number of protected voice messages played (all, or in part) to subscribers.
Protected Voice Messages Sent	MSExchangeUMSubscriberAccess	Protected Voice Messages Sent is the number of protected voice messages sent by authenticated UM subscribers.
Replied to Organizer	MSExchangeUMSubscriberAccess	Replied to Organizer is the number of times subscribers sent reply messages to meeting organizers.
Reply Messages Sent	MSExchangeUMSubscriberAccess	Reply Messages Sent is the number of replies sent by authenticated subscribers.
Subscriber Authentication Failures	MSExchangeUMSubscriberAccess	Subscriber Authentication Failures is the number of authentication failures that have occurred since the service was started. This number is incremented once for every failed authentication. It is possible that a single phone call could generate several authentication failures.
Subscriber Logon Failures	MSExchangeUMSubscriberAccess	Subscriber Logon Failures is the number of logon failures since the service was started. This number is incremented at most once per phone call.
Subscriber Logons	MSExchangeUMSubscriberAccess	Subscriber Logons is the number of successful authentications by UM subscribers since the service was started.
Voice Message Decryption Failures	MSExchangeUMSubscriberAccess	Voice Message Decryption Failures is the total number of times that an attempt to decrypt a protected voice message failed.
Voice Message Protection Failures	MSExchangeUMSubscriberAccess	Voice Message Protection Failures is the total number of interpersonal voice messages for which an attempt to apply protection failed.
Voice Message Queue Accessed	MSExchangeUMSubscriberAccess	Voice Message Queue Accessed is the number of times subscribers accessed

		their voice message queues by using the telephone user interface.
Voice Messages Deleted	MSExchangeUMSubscriberAccess	Voice Messages Deleted is the number of voice messages that were deleted by authenticated subscribers.
Voice Messages Heard	MSExchangeUMSubscriberAccess	Voice Messages Heard is the number of voice messages played to subscribers. This count is incremented as soon as playback starts. The subscriber does not need to listen to the entire message.
Voice Messages Sent	MSExchangeUMSubscriberAccess	Voice Messages Sent is the number of voice messages that have been sent by authenticated UM subscribers.

1.15.3.6.5 Auto Attendant Performance Counters for Unified Messaging

Auto Attendant Performance Counters for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-08*

There are many performance counters that can be used to maintain and troubleshoot a Microsoft Exchange Server 2010 Unified Messaging (UM) server.

Unified Messaging performance counters are used to measure quantities of information or data for Unified Messaging based on the number, size, duration, and rate of data that's being requested or received. The **MSExchangeUMAutoAttendant** performance object can contain multiple instances. The number of instances for the performance object depends on the number of UM auto attendants that are created in the Exchange organization.

UM Auto Attendant Performance Counters

The following table provides a list of the auto attendant performance counters that can be used to monitor Exchange 2010 Unified Messaging.

Auto attendant performance counters for Unified Messaging

Performance counter	Performance object	Description
% Successful Calls	MSExchangeUMAutoAttendant	% Successful Calls calculates the success rate of the auto attendant.
Ambiguous Name Transfers	MSExchangeUMAutoAttenda	Ambiguous Name Transfers is

	nt	the number of times that callers were transferred to the operator because the name that they spelled or spoke was too common in the search results.
Average Call Time	MSExchangeUMAutoAttendant	Average Call Time is the average length of time that callers interacted with the auto attendant.
Average Recent Call Time	MSExchangeUMAutoAttendant	Average Recent Call Time is the average length of time, in seconds, of the last 50 auto attendant calls.
Business Hours Calls	MSExchangeUMAutoAttendant	Business Hours Calls is the number of calls processed by this auto attendant during business hours.
Calls Disconnected by UM on Irrecoverable External Error	MSExchangeUMAutoAttendant	Calls Disconnected by UM on Irrecoverable External Error is the total number of calls that were disconnected after an irrecoverable external error occurred.
Calls with DTMF fallback	MSExchangeUMAutoAttendant	Calls with DTMF fallback is the number of calls to this auto attendant during which a caller has been passed to the DTMF fallback auto attendant. This only happens for speech-enabled auto attendants.
Calls with Sent Message	MSExchangeUMAutoAttendant	Calls with Sent Message is the number of calls to this auto attendant in which a caller has sent a voice message.
Calls with Speech Input	MSExchangeUMAutoAttendant	Calls with Speech Input is the total number of calls during which the caller is determined to have spoken at least once.
Calls with Spoken Name	MSExchangeUMAutoAttendant	Calls with Spoken Name is the number of calls to this auto attendant during which a caller has spoken a name at least once.
Custom Menu Options	MSExchangeUMAutoAttendant	Custom Menu Options is the number of times that callers have selected custom menu options.
Directory Accessed	MSExchangeUMAutoAttendant	Directory Accessed is the number of directory access operations performed by this

		auto attendant.
Directory Accessed by Dial by Name	MSExchangeUMAutoAttendant	Directory Accessed by Dial by Name is the number of directory access operations in which the subscriber used the Dial by Name feature.
Directory Accessed by Extension	MSExchangeUMAutoAttendant	Directory Accessed by Extension is the number of directory access operations in which the user supplied the extension number.
Directory Accessed by Spoken Name	MSExchangeUMAutoAttendant	Directory Accessed by Spoken Name is the number of directory access operations in which the subscriber spoke a recipient name.
Directory Accessed Successfully by Dial by Name	MSExchangeUMAutoAttendant	Directory Accessed Successfully by Dial by Name is the number of successful directory access operations in which the caller used the Dial by Name feature.
Directory Accessed Successfully by Spoken Name	MSExchangeUMAutoAttendant	Directory Accessed Successfully by Spoken Name is the number of successful directory access operations in which the caller spoke a recipient name.
Disallowed Transfers	MSExchangeUMAutoAttendant	Disallowed Transfers is the number of times a caller was transferred to the operator because the user they identified was configured to accept calls only from users who are logged on.
Disconnected Without Input	MSExchangeUMAutoAttendant	Disconnected Without Input is the number of calls that were dropped without input being offered in response to the auto attendant prompts.
Menu Option 1 Used	MSExchangeUMAutoAttendant	Menu Option 1 Used is the number of times that a caller has chosen option 1 from the custom menu. **Note:** This value is always zero if no menu or option is defined.
Menu Option 2 Used	MSExchangeUMAutoAttendant	Menu Option 2 Used is the number of times that a caller has chosen option 2 from the custom menu. **Note:**

		This value is always zero if no menu or option is defined.
Menu Option 3 Used	MSExchangeUMAutoAttendant	Menu Option 3 Used is the number of times that a caller has chosen option 3 from the custom menu. **Note:** This value is always zero if no menu or option is defined.
Menu Option 4 Used	MSExchangeUMAutoAttendant	Menu Option 4 Used is the number of times that a caller has chosen option 4 from the custom menu. **Note:** This value is always zero if no menu or option is defined.
Menu Option 5 Used	MSExchangeUMAutoAttendant	Menu Option 5 Used is the number of times that a caller has chosen option 5 from the custom menu. **Note:** This value is always zero if no menu or option is defined.
Menu Option 6 Used	MSExchangeUMAutoAttendant	Menu Option 6 Used is the number of times that a caller has chosen option 6 from the custom menu. **Note:** This value is always zero if no menu or option is defined.
Menu Option 7 Used	MSExchangeUMAutoAttendant	Menu Option 7 Used is the number of times that a caller has chosen option 7 from the custom menu. **Note:** This value is always zero if no menu or option is defined.
Menu Option 8 Used	MSExchangeUMAutoAttendant	Menu Option 8 Used is the number of times that a caller has chosen option 8 from the custom menu. **Note:** This value is always zero if no menu or option is defined.
Menu Option 9 Used	MSExchangeUMAutoAttendant	Menu Option 9 Used is the number of times that a caller has chosen option 9 from the custom menu. **Note:** This value is always zero if no menu or option is defined.

Menu Option Timed Out	MSExchangeUMAutoAttendant	Menu Option Timed Out is the number of times that the system has timed out while waiting for a caller to select an option from the custom menu. **Note:** This value is always zero if no menu is defined.
Operator Transfers	MSExchangeUMAutoAttendant	Operator Transfers is the number of calls that have been transferred to the operator.
Operator Transfers Requested by User	MSExchangeUMAutoAttendant	Operator Transfers Requested by User is the number of times that a caller to this auto attendant has asked to be transferred to an operator.
Operator Transfers Requested by User from Opening Menu	MSExchangeUMAutoAttendant	Operator Transfers Requested by User from Opening Menu is the number of times that a caller to this auto attendant has asked to be transferred to an operator while at the opening menu.
Out of Hours Calls	MSExchangeUMAutoAttendant	Out of Hours Calls is the number of calls processed by this auto attendant outside of business hours.
Sent to Auto Attendant	MSExchangeUMAutoAttendant	Sent to Auto Attendant is the number of times that a caller to this auto attendant has used the custom menu to go to an auto attendant.
Total Calls	MSExchangeUMAutoAttendant	Total Calls is the number of calls that have been processed by this auto attendant.
Transferred Count	MSExchangeUMAutoAttendant	Transferred Count is the number of calls that were transferred by this auto attendant. This number does not include calls that were transferred by the operator.

Return to top

System Availability Counters for Unified Messaging

Performance and Scalability > Performance and Scalability Counters and Thresholds > Unified Messaging Counters >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-04-28*

There are many performance counters that can be used to maintain and troubleshoot a computer that's running Microsoft Exchange Server 2010.

Unified Messaging performance counters are used to measure quantities of information or data for Unified Messaging based on the number, size, duration, and rate of data that's being requested or received.

UM System Availability Performance Counters

The following table provides a list of the system availability performance counters that can be used to monitor Unified Messaging.

System availability performance counters for Unified Messaging

Performance counter	Performance object	Description
% of Failed Mailbox Connection Attempts Over the Last One Hour	MSExchangeAvailability	% of Failed Mailbox Connection Attempts Over the Last One Hour is the percentage of mailbox connection attempts that failed in the last hour.
% of Inbound Calls Rejected by the UM Service over the Last Hour	MSExchangeAvailability	% of Inbound Calls Rejected by the UM Service Over the Last Hour is the percentage of incoming calls that were rejected by the Microsoft Exchange Unified Messaging service in the last hour.
% of Inbound Calls Rejected by the UM Worker Process Over the Last Hour	MSExchangeAvailability	% of Inbound Calls Rejected by the UM Worker Process Over the Last Hour is the percentage of incoming calls that were rejected by the UM Worker process in the last hour.
% of Messages Successfully Processed Over the Last Hour	MSExchangeAvailability	% of Messages Successfully Processed Over the Last Hour is the percentage of messages that were successfully processed by the Microsoft Exchange Unified Messaging service in the last hour.

% of Partner Voice Message Transcription Failures Over the Last Hour	MSExchange Availability	% of Partner Voice Message Transcription Failures Over the Last Hour is the percentage of partner voice message transcription failures in the last hour.
Call Answer Queued Messages	MSExchangeAvailability	Call Answer Queued Messages is the number of messages created and not yet submitted for delivery.
Calls Disconnected by UM on Irrecoverable External Error	MSExchangeAvailability	Calls Disconnected by UM on Irrecoverable External Error is the number of calls disconnected after an irrecoverable external error occurred.
Calls Disconnected by UM on Irrecoverable External Error/ sec	MSExchangeAvailability	Calls Disconnected by UM on Irrecoverable External Error/ sec is the number of calls disconnected after an irrecoverable external error occurred in the last second.
Calls Disconnected on Irrecoverable Internal Error	MSExchangeAvailability	Calls Disconnected on Irrecoverable Internal Error is the number of calls that were disconnected after an internal system error occurred.
Directory Access Failures	MSExchangeAvailability	Directory Access Failures is the number of times that attempts to access Active Directory failed.
Failed Mailbox Connection Attempts %	MSExchangeAvailability	Failed Mailbox Connection Attempts % is the percentage of failed attempts to connect to the Mailbox server.
Incomplete Signaling Information	MSExchangeAvailability	Incomplete Signaling Information is the number of calls for which the signaling information was missing or incomplete.
Maximum Calls Allowed	MSExchangeAvailability	Maximum Calls Allowed is the length of time, in seconds, that the server concurrently processed the maximum number of calls allowed.
Name TTSed	MSExchangeAvailability	Name TTSed is the number of times the system used Text-to-Speech (TTS) to create an audio version of the display name of a subscriber.

Queued OCS User Event Notifications	MSExchangeAvailability	Queued OCS User Event Notifications is the number of notifications that have been created and not yet submitted for delivery.
Spoken Name Accessed	MSExchangeAvailability	Spoken Name Accessed is the number of times the system retrieved the recorded name of a user.
Total Worker Process Call Count	MSExchangeAvailability	Total Worker Process Call Count is the number of calls handled by this UM worker process.
Worker Process Recycled	MSExchangeAvailability	Worker Process Recycled is the number of times a new UM worker process has been started.

1.15.3.6.7 Performance Monitoring Counters for Unified Messaging

Performance Monitoring Counters for Unified Messaging

Performance and Scalability > Performance and Scalability Counters and Thresholds > Unified Messaging Counters >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-24*

There are many performance counters that can be used to maintain and troubleshoot a Microsoft Exchange Server 2010 Unified Messaging (UM) server. Unified Messaging performance counters are used to measure quantities of information or data for Unified Messaging based on the number, size, duration, and rate of data that's being requested or received.

UM Performance Monitoring Counters

The following table provides a list of the Unified Messaging performance monitoring counters that can be used to monitor Unified Messaging.

Unified Messaging performance monitoring counters

Performance counter	Performance object	Description
Operations Between Five and Six Seconds	MSExchangeUMPerformance	Operations Between Five and Six Seconds is the number of all UM operations that took between 5 and 6 seconds to complete. This is the time during which a caller was waiting for UM to respond.
Operations Between Four and Five Seconds	MSExchangeUMPerformance	Operations Between Four and Five Seconds is the number of all UM operations

		that took between 4 and 5 seconds to complete. This is the time during which a caller was waiting for UM to respond.
Operations Between Three and Four Seconds	MSExchangeUMPerformance	Operations Between Three and Four Seconds is the number of all UM operations that took between 3 and 4 seconds to complete. This is the time during which a caller was waiting for UM to respond.
Operations Between Two and Three Seconds	MSExchangeUMPerformance	Operations Between Two and Three Seconds is the number of all UM operations that took between 2 and 3 seconds to complete. This is the time during which a caller was waiting for UM to respond.
Operations over Six Seconds	MSExchangeUMPerformance	Operations over Six Seconds is the number of all UM operations that took more than 6 seconds to complete. This is the time during which a caller was waiting for Unified Messaging to respond.
Operations under Two Seconds	MSExchangeUMPerformance	Operations under Two Seconds is the number of all UM operations that took less than 2 seconds to complete. This is the time during which a caller was waiting for Unified Messaging to respond.

1.15.3.6.8 Fax Answering Performance Counters for Unified Messaging

Fax Answering Performance Counters for Unified Messaging

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-12-07*

There are many performance counters that can be used to maintain and troubleshoot a Microsoft Exchange Server 2010 Unified Messaging server. Unified Messaging performance counters are used to measure quantities of information or data for Unified Messaging based on the number, size, duration, and rate of data that is being requested or received.

Fax Answering Performance Counters

The following table provides a list of the fax answering performance counters that can be used to monitor Unified Messaging.

Unified Messaging fax answering performance counters

Performance counter	Performance object	Description
Percentage of Successful Valid Fax Calls	MSExchangeUMFax	Percentage of Successful Valid Fax Calls is the percentage of successful valid fax call requests.
Total Invalid Fax Calls	MSExchangeUMFax	Total Invalid Fax Calls is the total number of fax call requests to extensions that resolved to mailboxes that are not enabled for fax.
Total Successful Valid Fax Calls	MSExchangeUMFax	Total Successful Valid Fax Calls is the total number of valid fax call requests to extensions that resolved to mailboxes that are enabled for fax and were successfully transferred to a fax partner.
Total Valid Fax Calls	MSExchangeUMFax	Total Valid Fax Calls is the total number of valid fax call requests to extensions that resolved to mailboxes that are enabled for fax and were successfully transferred to the fax partner.

1.16 About Exchange Documentation

About Exchange Documentation

Exchange Server 2010 >

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2011-11-28*

This is a collection of conceptual and procedural topics organized by subject or by technologies used by Microsoft Exchange Server 2010 Service Pack 2 (SP2). You can access each topic directly from the table of contents in the left pane, from a link in another Help topic, from the results of a search, or from your own custom list of favorite topics.

For more detail about Exchange 2010 SP2 documentation, see the following topics:

- Accessibility for People with Disabilities
- Third-Party Copyright Notices

Where to Find Exchange 2010

Documentation

The Exchange Server 2010 TechCenter is your primary gateway to in-depth technical information about Exchange 2010. Through the TechCenter, which is located on the Microsoft TechNet site, you can access the Exchange 2010 Library and the Exchange Team Blog.

Exchange 2010 Library

The Exchange 2010 Library contains the most up-to-date Help documentation. This documentation is reviewed and approved by the Exchange product team and will evolve over time as Exchange 2010 gains exposure and new information, issues, and troubleshooting information becomes available.

The topics in the library also act as the in-product Help, which is accessible via the Exchange Management Console.

When you install Microsoft Exchange Server 2010 for the first time, the advanced security settings in Internet Explorer may block you from the TechNet site, which is where Exchange Server Help documentation is located. If that happens, use the following procedure to add Microsoft TechNet to your list of trusted Web sites.

1. Open Internet Explorer. Copy the following URL into the Internet Explorer address field: http://technet.microsoft.com/en-us/library/bb124558(EXCHG.141).aspx
   A pop-up box appears saying that the content is being blocked.
2. Click **Add**. The **Trusted sites** dialog box appears.
3. In **Add this website to the zone** box, make sure that the URL in step 1 is displayed.
4. Click **Add**, and then click **Close**.

Note:
Another dialog box may appear asking you to add another Microsoft site. In this case, repeat the process.

Offline Copy of the Help File

Looking for an offline version of this Exchange 2010 SP2 Help content? Download the Help file from the Microsoft Download Center.

Note:
Haven't upgraded to Exchange 2010 SP2? You can also download the Help file for previous versions of Exchange.

- Exchange 2010 SP1 Help
- Exchange 2010 RTM Help

Exchange Team Blog

The Exchange Team Blog contains technical articles written by the Exchange Team, as well as product announcements and updates. Through the use of feedback and comments, the blog is an excellent way to interact with the Exchange Team.

Additional Resources

Looking for more than just documentation? Check out these other Exchange 2010 resources:

- Exchange 2010 Learning Resources Use this page to take self-paced training for Exchange 2010, review learning plans and course descriptions for certifications, and order administrative guides.

- Exchange Server Downloads Use this page to download service packs, add-ins, tools, and trial software to help you optimize your Exchange 2010 organization.
- Exchange 2010 Forum The forum provides a place to discuss Exchange 2010 with customers and Exchange Team members.
- Exchange Support Use this page to locate support resources for Exchange 2010. You can search the Microsoft Knowledge Base, TechNet forums, or you can contact Microsoft Support for additional help.

Note:
Looking for Exchange 2010 developer documentation? Check out the Exchange Server Developer Center.

1.16.1 Accessibility for People with Disabilities

Accessibility for People with Disabilities

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2010-07-28*

Microsoft is committed to making its products and services easier for everyone to use. The following sections provide information about the features, products, and services that help make Microsoft Exchange 2010 more accessible for people with disabilities.

Accessibility Features of Exchange 2010

The following features in Exchange 2010 help make it more accessible for people with disabilities:

- Keyboard shortcuts
- Outlook Voice Access
- The light version of Outlook Web App

In addition, some accessibility features and utilities of Windows may benefit Exchange users with disabilities. Microsoft Management Console (MMC) keyboard shortcuts provide accessibility options when using the Exchange Management Console. Windows PowerShell size and color changes provide accessibility options when using the Exchange Management Shell. For more information about using keyboard shortcuts in MMC, see Accessibility for MMC. For more information about Windows PowerShell accessibility options, see Customizing the Windows PowerShell Console.

Note:
The information in this section applies only to users who license Microsoft products in the United States. If you obtained this product outside of the United States, you can use the subsidiary information card that came with your software package or visit Microsoft Accessibility for a list of telephone numbers and addresses for Microsoft support services. You can contact your subsidiary to find out whether the type of products and services described in this section are available in your area. Information about accessibility is available in other languages, including Japanese and French.

Keyboard Shortcuts

By using keyboard shortcuts in the Exchange Management Console, you can quickly accomplish the following common tasks.

To do this	Use this keyboard shortcut
Switch cursor between the console tree,	TAB

elements in the result pane, the divider between the result pane and the work pane, elements in the work pane, and the action pane	
Switch between **File**, **Action**, **View**, and **Help** menus	ALT + underlined letter of the menu
Select actions in the action pane and on the **Action** menu	ALT + A
Switch between elements on each page of a wizard	TAB

Outlook Voice Access

Outlook Voice Access provides blind and low-vision users another way to access their e-mail and calendar. Outlook Voice Access allows Unified Messaging-enabled users to retrieve e-mail messages from their Exchange 2010 mailbox by using an analog, digital, or mobile telephone. They can then interact with their mailbox by using touchtone or voice commands. They can read e-mail, listen to voice messages, interact with their Microsoft Office Outlook calendar, access their personal contacts, and manage personal options, for example, configuring their Outlook Voice Access PIN or recording their voice mail recordings. For more information about using Outlook Voice Access, see Outlook Voice Access Quick Start Guide.

Light Version of Outlook Web App

The light version of Outlook Web App is optimized for accessibility, such as for users who are blind or have low vision. The light version provides fewer features and is faster for some operations. Users may prefer the light version if they're on a slow connection or using a computer with unusually strict browser security settings. The light version can be used with almost any browser and has the same features across all browsers.

Accessibility Features of Exchange 2010 Help

Exchange 2010 Help includes features that make it accessible to a wider range of users, including those who have limited dexterity, low vision, or other disabilities. In addition, Exchange 2010 Help is available on the Web at the Exchange Server 2010 Library.

Keyboard Shortcuts for Using the Help Window

By using the following keyboard shortcuts in Help, you can quickly accomplish many common tasks.

To do this	Use this keyboard shortcut or function key
Display the Help window.	F1
Switch the cursor between the Help topic pane and the navigation pane (tabs such as **Contents**, **Search**, and **Index**).	F6
Change between tabs (for example, **Contents**, **Search**, and **Index**) while in the navigation pane.	ALT + underlined letter of the tab
Select the next hidden text or hyperlink.	TAB
Select the previous hidden text or hyperlink.	SHIFT+TAB

Perform the action for the selected Show All, Hide All, hidden text, or hyperlink.	ENTER
Display the **Options** menu to access any Help toolbar command.	ALT+O
Hide or show the pane containing the **Contents**, **Search**, and **Index** tabs.	ALT+O, and then press T
Display the previously viewed topic.	ALT+O, and then press B
Display the next topic in a previously displayed sequence of topics.	ALT+O, and then press F
Return to the specified home page.	ALT+O, and then press H
Stop the Help window from opening a Help topic (useful if you want to stop a Web page from downloading).	ALT+O, and then press S
Open the **Internet Options** dialog box for Microsoft Internet Explorer, where you can change accessibility settings.	ALT+O, and then press O
Refresh the topic (useful if you have linked to a Web page).	ALT+O, and then press R
Print all topics in a book or a selected topic only.	ALT+O, and then press P
Close the Help window.	ALT+F4

Alternate Text for Figures

Every figure in Exchange 2010 Help, including screenshots, diagrams, flow charts, and other figures, has associated alternate text. Users who have difficulty viewing figures can pause the cursor on the figure to read the alternate text. The alternate text describes what is illustrated in the figure.

Accessibility Products and Services from Microsoft

The following sections provide information about the features, products, and services that make Microsoft Windows more accessible for people with disabilities.

Note:

The information in this section may apply only to users who license Microsoft products in the United States. If you obtained this product outside of the United States, you can use the subsidiary information card that came with your software package or visit Microsoft Accessibility for a list of Microsoft support service telephone numbers and addresses. You can contact your subsidiary to find out whether the type of products and services described in this section are available in your area. Information about accessibility is available in other languages, including Japanese and French.

Accessibility Features of Windows

The Windows operating system has many built-in accessibility features that are useful for individuals who have difficulty typing or using a mouse, are blind or have low vision, or who are deaf or hard-of-hearing. The features are installed during Setup. For more information about these features, see Help in Windows and Microsoft Accessibility.

- **Free Step-by-Step Tutorials** Microsoft offers a series of step-by-step tutorials that provide detailed procedures for adjusting the accessibility

options and settings on your computer. This information is presented in a side-by-side format so that you can learn how to use the mouse, the keyboard, or a combination of both.
To find step-by-step tutorials for Microsoft products, see Microsoft Accessibility.

- **Assistive Technology Products for Windows** A wide variety of assistive technology products are available to make computers easier to use for people with disabilities. You can search a catalog of assistive technology products that run on Windows at Microsoft Accessibility.
  If you use assistive technology, be sure to contact your assistive technology vendor before you upgrade your software or hardware to check for possible compatibility issues.

Documentation in Alternative Formats

If you have difficulty reading or handling printed materials, you can obtain the documentation for many Microsoft products in more accessible formats. You can obtain an index of accessible product documentation at Microsoft Accessibility.

In addition, you can obtain additional Microsoft publications from Recording for the Blind & Dyslexic, Inc (RFB&D). RFB&D distributes these documents to registered, eligible members of their distribution service. For information about the availability of Microsoft product documentation and books from Microsoft Press, contact RFB&D.

Recording for the Blind & Dyslexic, Inc.

20 Roszel Road

Princeton, NJ 08540

Telephone number from within the United States: (800) 221-4792

Web site: Recording for the Blind & Dyslexic

Customer Service for People with Hearing Impairments

If you're deaf or hard-of-hearing, complete access to Microsoft product and customer services is available through a text telephone (TTY/TDD) service:

- For customer service, contact Microsoft Sales Information Center at (800) 892-5234 between 6:30 A.M. and 5:30 P.M. Pacific Time, Monday through Friday, excluding holidays.
- For technical assistance in the United States, contact Microsoft Product Support Services at (800) 892-5234 between 6:00 A.M. and 6:00 P.M. Pacific Time, Monday through Friday, excluding holidays. In Canada, dial (905) 568-9641 between 8:00 A.M. and 8:00 P.M. Eastern Time, Monday through Friday, excluding holidays.

Microsoft Support Services are subject to the prices, terms, and conditions in place at the time the service is used. For more information, see Microsoft Support.

For More Information

For more information about how accessible technology for computers helps to improve the lives of people with disabilities, see Microsoft Accessibility.

1.16.2 Third-Party Copyright Notices

Third-Party Copyright Notices

Applies to: *Exchange Server 2010 SP3, Exchange Server 2010 SP2*

Topic Last Modified: *2009-11-20*

The following components are licensed to Microsoft in object code form by Stellent Chicago Sales, Inc.:

Components – Version 8.0

Outside In ® HTML Export Version 8.0

Platforms Supported – Version 8.0:

Windows Intel (32 bit binaries)

Windows® 2000/XP/Server 2003

Windows Itanium (64 bit binaries)

Windows.NET ® Server 2003 Enterprise Edition for Itanium

Windows AMD (64 bit binaries)

Windows Server 2003, Enterprise Edition for AMD Opteron

Back Cover